А.М. Голиков

КОДИРОВАНИЕ И ШИФРОВАНИЕ ИНФОРМАЦИИ В СИСТЕМАХ СВЯЗИ

Методические указания по курсовой работе

по дисциплине «Кодирование и шифрование информации
в системах связи» для студентов
специальности 210601.65 - "Радиоэлектронные системы и комплексы"
специализация - 210601-2.65 - "Радиоэлектронные системы передачи"

2016

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ

Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования

ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИСТЕТ СИСТЕМ УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ

УТВЕРЖДАЮ

Заведующий кафедрой РТС

_____С.В. Мелихов

КОДИРОВАНИЕ И ШИФРОВАНИЕ ИНФОРМАЦИИ В СИСТЕМАХ СВЯЗИ

Методические указания по курсовой работе

по дисциплине «Кодирование и шифрование информации в системах связи» для студентов специальности 210601.65 - "Радиоэлектронные системы и комплексы" специализация - 210601-2.65 - "Радиоэлектронные системы передачи"

Разработчик

Доцент каф. РТС, к.т.н., ст.н.с.

_____ __А.М. Голиков

2016

Рекомендовано к изданию кафедрой радиотехнических систем Томского государственного университета систем управления и радиоэлектроники

Голиков А.М. Кодирование и шифрование информации в системах связи. Методические указания по курсовой работе студентов специальности 210601.65 Радиоэлектронные системы и комплексы - Томск: Том. гос. ун-т систем управления и радиоэлектроники, 2016. - 123 с.

Приводятся указания по курсовой работе студентов по дисциплине «Кодирование и шифрование информации в системах связи» для студентов специальности 210601.65 Радиоэлектронные системы и комплексы. Предложены как типовые задания на курсовую работу по кодированию и шифрованию, так и индивидуальны курсовые работы повышенной сложности

СОДЕРЖАНИЕ

1. Цели и задачи дисциплины

Дисциплина "Кодирование и шифрование информации в системах связи" (КиШИвСС) относится к числу дисциплин по выбору С3+В1.2 рабочего учебного плана для подготовки инженеров по специальности 210601.65-Радиоэлектронные системы и комплексы (специализация 210601-2.65-Радиоэлектронные системы передачи информации). Целью преподавания дисциплины является изучение основных закономерностей передачи информации в цифровых телекоммуникационных системах.

Основной задачей дисциплины является формирование у студентов *компетенций*, позволяющих самостоятельно проводить математический анализ физических процессов в аналоговых и цифровых устройствах формирования, преобразования и обработки сигналов, оценивать реальные и предельные возможности пропускной способности и помехоустойчивости телекоммуникационных систем и сетей.

В курсе КиШИвСС принят единый методологический подход к анализу и синтезу современных телекоммуникационных систем и устройств на основе вероятностных моделей сообщений, сигналов, помех и каналов в системах связи. Предусмотренные программой курса КиШИвСС знания являются не только базой для последующего изучения специальных дисциплин, но имеют также самостоятельное значение для формирования инженеров по специальности 210601.65-Радиоэлектронные системы и комплексы.

1. Место дисциплины в структуре ООП

Дисциплина КиШИвСС относится к числу специальных дисциплин по выбору С3+В1.2 рабочего учебного плана подготовки инженеров.

Теоретической базой курса КиШИвСС *являются основные сведения из дисциплин естественнонаучного и профессионального циклов подготовки инженеров: Теория вероятности и статистика в радиоэлектронике, Информационные технологии, Цифровая обработка сигналов, Основы теории радиосистем передачи информации*

Минимальным требованием к «входным» знаниям, необходимым для успешного усвоении данной дисциплины, является удовлетворительное усвоение программ по указанных выше курсам.

Изучаемая дисциплина является предшествующей при изучении специальных и профилирующих дисциплин: Системы радиосвязи, Транспортные и мультисервисные системы и сети связи, Компьютерное проектирование и моделирование систем связи, а также может быть использована при подготовке выпускной квалификационной работы.

2. Требования к результатам освоения дисциплины:

Изучение рассматриваемой дисциплины направлено на формирование у студентов следующих **компетенций:**

способностью к самостоятельному обучению новым методам исследования, к изменению научного и научно-производственного профиля своей профессиональной деятельности (ОК-2);

способностью использовать результаты освоения фундаментальных и прикладных дисциплин магистерской программы (ПК-1);

способностью понимать основные проблемы в своей предметной области, выбирать методы и средства их решения (ПК-3);

способностью использовать результаты освоения фундаментальных и прикладных дисциплин магистерской программы (ПК-5);

готовностью оформлять, представлять и докладывать результаты выполненной работы (ПК-6).

В результате изучения дисциплины студент должен:

знать

- физические и математические модели процессов и явлений, лежащих в основе принципов действия радиотехнических устройств и систем;
- основные закономерности исторического процесса в науке и технике, этапы исторического

развития радиотехники, место и значение радиотехники в современном мире;

- методологические основы и принципы современной науки; **уметь**
- формулировать и решать задачи, грамотно использовать математический аппарат и численные методы для анализа и синтеза радиотехнических устройств и систем;
- готовить методологическое обоснование научных исследований и технических разработок в области радиотехники;

владеть

- математическим аппаратом для решения задач теоретической и прикладной радиотехники, методами исследования и моделирования объектов радиотехники;
- навыками методологического анализа научных исследований и их результатов.

2. ТЕМАТИКА КУРСОВОГО ПРОЕКТИРОВАНИЯ

2.1. ТИПОВЫЕ ЗАДАНИЯ НА КУРСОВЫЕ РАБОТЫ ПО КОДИРОВАНИЮ В СИСТЕМАХ СВЯЗИ

2.1.1. Оптимизация методов помехоустойчивого кодирования для телекоммуникационных связи (ТКС)

Помехоустойчивое кодирование является эффективным способом оптимизации ТКС. На практике инженеру проектировщику ТКС приходится решать задачи оптимизации на основе численных расчетов и соответствующего сравнения методов помехоустойчивого кодирования и выбора конкретных методов и соответствующим им кодов. Решение именно такой задачи положено в основу КР [1].

Исходные данные заданы в таблице вариантов 2:

1. Цифровая информация передается двоичным кодом. Виды передаваемой цифровой информации:

ДК - данные компьютерного обмела;

ЦТЛФ - цифровая телефония;

ЦТВ - сообщения цифрового ТВ;

ЦЗВ - сообщения цифрового звукового вещания.

2. Канал святи - канал с постоянными параметрами и аддитивным белым гауссовым шумом.

3. Отношение с/ш на входе демодулятора $h_б = E_б / N_0$.

4. Методы модуляции: ФМ-2, ФМ-4.

5. Прием - когерентный.

6. Производительность источника $R_{ист}(бит/с)$.

7. Полоса пропускания канала $F_K(кГц)$.

8. Вероятность ошибки бита в сообщениях, отдаваемых получателю, не более *p.*

9. Допустимая сложность декодера СК (показатель сложности решетки кода) - не более *W.*

Необходимо:

1. Выбрать и обосновать выбор корректирующего кода для проектируемой ТКС, обеспечивающего требуемую вероятность ошибки бита p в сообщениях, отдаваемых получателю, при условии выполнения следующих ограничений:

1.1. *Полоса частот* кодированного сигнала не должна превышать полосу пропускания канала F_K.

1.2. При использовании сверточных кодов *показатель сложности* решетки кода должен быть не более величины *W*.

2. Разработать и дать подробное описание *структурной и функциональных схем кодера и декодера* выбранного кода и обосновать их параметры.

3. Проанализировать показатели энергетической и частотной эффективности телекоммуникационной системы и сравнить их с предельными значениями эффективности.

4. Сделать *заключение* по выполненной работе.

Содержание пояснительной записки работы:

1. Задание и исходные данные.

2. Описание структурной схемы проектируемой телекоммуникационной системы с указанием мест включения кодера помехоустойчивого кода, модулятора, демодулятора и декодера с подробными пояснениями выполняемых ими функций.

3. Классификация корретирующих кодов по структуре. Сравнительный анализ преимуществ и недостатков помехоустойчивых блоковых и сверточных кодов. Обоснование применения в проекте сверточных кодов.

4. Классификация и сравнительный анализ алгоритмов декодирования сверточных кодов. Обоснование выбора алгоритма Витерби для декодирования СК.

5. Расчет ширины спектра цифрового сигнала с заданным видом модуляции.

6. Расчет ширины спектра кодированного цифрового сигнала с заданным видом модуляции в зависимости от скорости кода.

7. Определение допустимой скорости кода $R^*_{КОД}$ из условия *непревышения* полосой частот кодированного сигнала полосы пропускания канала.

8. Определение перечня кодов со скоростями, превышающими допустимую скорость $R^*_{КОД}$, которые могут быть использованы для решения поставленной задачи.

9. Выбор СК из этого перечня, обеспечивающего заданную вероятность ошибки бита и удовлетворяющего требованию ограничения по сложности декодера.

10. Проверочный расчет зависимости вероятности ошибки на выходе декодера выбранного СК.

11. Разработка и описание структурных и функциональных схем кодера и декодера выбранного СК.

12. Заключение с подведением итогов выполненной работы.

13. Список использованных источников.

Методические указания к выполнению КР

Расчет ширины спектра сигнала ФМ-2 (ФМ-4) следует производить по рекомендациям материалов [1]. Применение корректирующих кодов со скоростью $R^*_{КОД}$ приводит к расширению спектра кодированного сигнала в ($K_F = 1/R_{КОД}$) раз. С другой стороны, корректирующая способность кода возрастает с уменьшением скорости кода (т.е. с увеличением избыточности). Поэтому *задача оптимизации* параметров корректирующего кода состоит в выборе кода со скоростью, при которой ширина спектра кодированного сигнала *не превышает заданную полосу пропускания канала.* Если требуемая полоса пропускания канала для передачи ФМ сигнала с информационной скоростью $R_{ИСТ}$ равна $F_{(ФМ)}$, а скорость кода выбрана равной $R_{КОД}$, то полоса пропускания канала, необходимая для передачи кодированного ФМ сигнала, будет равна

$$F_{К(ФМ-СК)} = \frac{F_{(ФМ)}}{R_{КОД}}.$$

Тогда из условия непревышения этой полосой частот сигнала полосы пропускания канала ($F_{К(ФМ-СК)} < F_К$) получаем простое *условие для выбора скорости кода*

$$R^*_{КОД} > R_{КОД} = \frac{F_{(ФМ)}}{F_К}. \qquad (1)$$

Сказанное иллюстрируется рисунком 1. Ширина спектра кодированного ФМ сигнала пропорциональна коэффициенту расширения полосы. По мере снижения скорости кода (возрастания K_F) полоса расширяется и достигает значения полосы пропускания канала. На этом же рисунке показана зависимость АЭВК от K_F (что равноценно скорости кода). Пересечение кривой полосы с граничным заданным значением $F^*_К$ определяет допустимое значение коэффициента расширения полосы пропускания канала $K_р = 1/R_{КОД}$ и, соответственно, скорость кода $R^*_{КОД}$. Первым этапом выбора корректирующего кода.является выбор класса кодов (класс блоковых либо непрерывных (сверточных) кодов). Используя материалы [1], рекомендуется *аргументированно обосновать выбор класса сверточных кодов* для применения в своей работе. Среди алгоритмов декодирования СК по широте практического применения *лидирующее место* занимает алгоритм Витерби. Рекомендуется в работе применить именно алгоритм Витерби. В разделе проекта с обоснованием применения этого алгоритма следует привести сведения о сложности реализации алгоритма. Среди кодов, отобранных по критерию скорости в соответствии с формулой (1), могут оказаться коды с

различной длиной кодового ограничения (и, соответственно, с различной сложностью декодера). Помехоустойчивость декодирования СК характеризуется величиной ЭВК. В таблицах кодов не приводятся значения ЭВК при определенном уровне вероятности ошибки декодирования. В то же время, величина асимптотического энергетического выигрыша (АЭВК) является верхней оценкой ЭВК. Поэтому при отборе кодов рекомендуется использовать величины АЭВК, значения которых имеются в таблицах приложения А. Среди отобранных кодов-кандидатов следует применить код, *обеспечивающий максимальный АЭВК и удовлетворяющий требованиям по скорости и сложности декодера.* Окончательные данные о вероятности ошибки на выходе декодера следует получить на основе расчетов зависимости вероятности ошибки декодирования от отношения сигнал/шум для выбранного кода. В случае невыполнения требований задания рекомендуется *применить код с большей величиной АЭВК.*

Пример расчетов и процедуры оптимизации кода

Исходные данные:

1. Вид передаваемой цифровой информации - ЦТЛФ.

3. Отношение с/ш $h_б$ = 4 дБ.

4. Метод модуляции: ФМ-4.

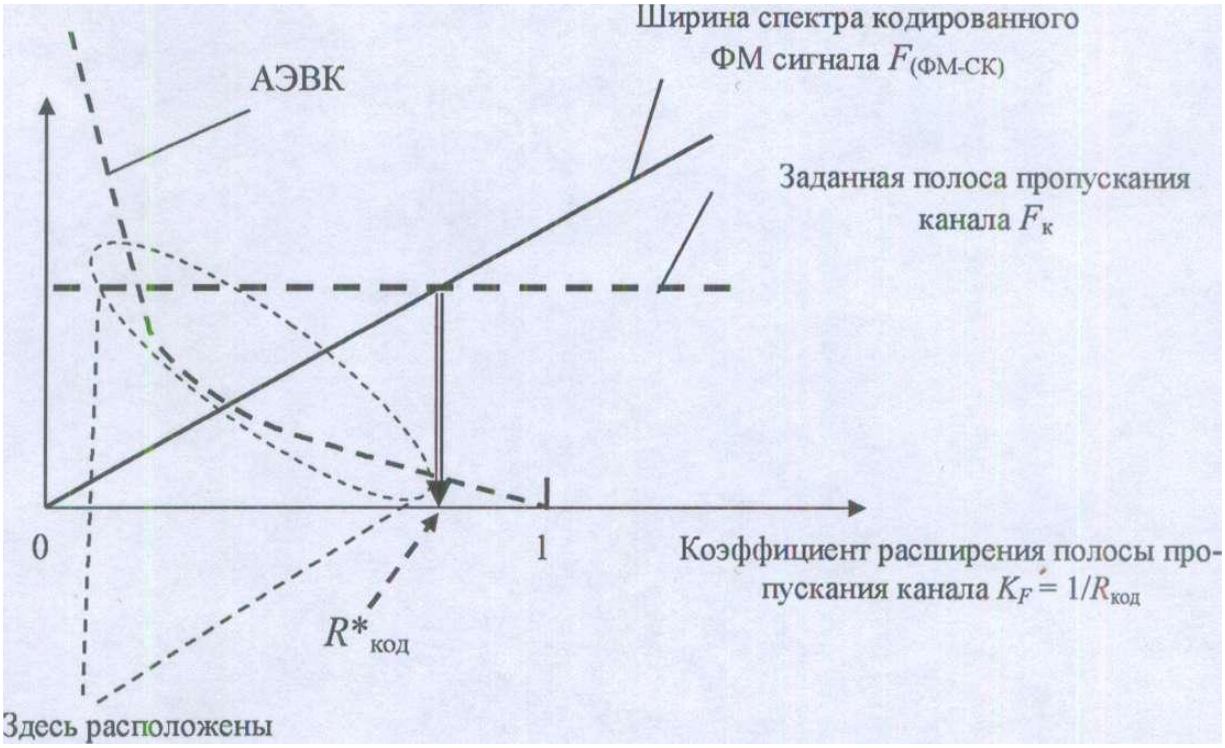
5. Прием-когерентный.

6. Производительность источника $R_{ИСТ}$ = 64 кбит/с

7. Ширина полосы частот канала F_K = 100 кГц.

8. Допустимая вероятность ошибки бита $p = 10^{-5}$.

9. Допустимая сложность решетки кода W = 150.



коды-кандидаты на выбор

Рис. 1. К процедуре оптимизации кода

1. Расчет полосы пропускания канала связи, необходимой для передачи цифровой информации с заданной скоростью методом ФМ-4, производим по формуле $F_{(ФМ-4)} = [R_{ИСТ}(1-\alpha)]/2,$ где α - коэффициент ската спектра. Задаваясь значением α = 0,4, получаем $F_{(ФМ-4)} = [R_{ИСТ}(1-\alpha)]/2$ = [64(1 + 0,4)]/2 = 44,8 кГц.

2. В соответствии с формулой (5.1) определяем предельное значение скорости С К

$$R^*_{КОД} > \frac{F_{ФМ-СК}}{F_К} = \frac{44,8}{100} = 0,448.$$

3. По таблицам СК отбираем коды, удовлетворяющие требованию по скорости. Данные об этих кодах сведены в таб. 1.

Таблица 1. Характеристики СК для выбора кода

Скорость кода $R_{КОД}$	Порождающие многочлены	ДКО v	Сложность решетки W	АЭВК дБ
1/4	463,535,733,745	8	512	8,29
1/3	557,663,711	8	512	7,78
1/2	53,75	5	64	6,02
1/2	61,73	5	64	6,02
1/2	71,73	5	64	6,02
1/2	133,171	6	128	6,99
1/2	247,371	7	256	6,99

Из таблицы видно, что для выполнения поставленной задачи могут быть использованы СК со скоростями $R_{КОД} = 1/2,$ которые обеспечивают достаточно большой АЭВК. На аснове данных таблицы выбираем для проекта код с порождающими многочленами (133, 171), который при скорости $R_{КОД} = 0{,}5$ обеспечивает АЭВК = 6,99 дБ. Данные расчета вероятности ошибки приведены в [1].

Видно, что применение выбраного кода обеспечивает выполнение задания: при отношении сигнал/шум $h_б^2 =$ 4 дБ вероятность ошибки декодирования менее $3 \cdot 10^{-5}$ Сравнение с кривыми помехоустойчивости некодированной ФМ [1] показывает, что при вероятности ошибки $p = 10^{-5}$ этот код обеспечивает ЭВК 5,3 дБ.

Таблица 2. Исходные данные для выполнения КР

Номер варианта для выполнения СР должен соответствовать номеру фамилии студента в журнале академической группы							
Номер варианта	Вид перед, информ.	Отношение С/Ш на входе $h_б^2, дБ$	Метод модул.	Производит. источника $R_{ИСТ}$, кбит/с	Полоса пропуск, канала $F_{К,}$ кГц	Вер. ошибки бита p	Сложи. декодера W
1	ДК	4,0	ФМ-4	64	80	10^{-6}	150

2	ЦТЛФ	5,0	ФМ-4	16	25	10^{-4}	160
3	ЦЗВ	6,0	ФМ-2	256	800	10^{-5}	170
4	ДК	6,5	ФМ-2	64	200	10^{-6}	180
5	ЦТЛФ	4,0	ФМ-4	16	25	10^{-4}	250
6	ЦЗВ	7,0	ФМ-4	128	200	10^{-5}	350
7	НТВ	5,0	ФМ-2	2400	7000	10^{-8}	560
8	ДК	6,0	ФМ-4	32	50	10^{-6}	200
9	ЦТЛФ	5,0	ФМ-2	24	70	10^{-4}	300
10	ЦЗВ	4,5	ФМ-4	256	400	10^{-5}	250
11	ЦТВ	5,5	ФМ-2	3000	1200	10^{-8}	550
12	ДК	4,0	ФМ-4	48	70	10^{-6}	150
13	ЦТЛФ	5,0	ФМ-4	32	50	10^{-4}	250
14	ЦЗВ	7,0	ФМ-2	256	800	10^{-5}	300
15	ЦТВ	4,0	ФМ-4	4500	1300	10^{-9}	550
16	ДК	7,0	ФМ-4	56	90	10^{-6}	150
17	ЦТЛФ	5,0	ФМ-2	24	70	10^{-4}	160
18	ЦЗВ	4,5	ФМ-4	256	400	10^{-5}	200
19	ЦТВ	5,5	ФМ-4	5000	1400	10^{-9}	550
20	ДК	6,0	ФМ-2	64	200	10^{-6}	150
21	ЦТЛФ	7,5	ФМ-4	256	400	10^{-4}	250
23	ЦЗВ	6,5	ФМ-4	16	50	10^{-5}	150
24	ДК	6,0	ФМ-4	64	150	10^{-6}	150
25	ЦГЛФ	4,5	ФМ-2	16	25	10^{-6}	200
26	ЦТВ	5,0	ФМ-2	6000	16000	10^{-9}	550
27	ЦЗВ	6,0	ФМ-4	384	600	10^{-5}	250
28	ДК	4,5	ФМ-4	64	100	10^{-6}	150
29	ЦГЛФ	5,0	ФМ-2	16	50	10^{-4}	250
30	ЦТВ	5,5	ФМ-2	5500	32000	10^{-9}	560
31	ЦГЛФ	4,5	ФМ-4	64	200	10^{-5}	150
32	ДК	5,0	ФМ-4	64	300	10^{-5}	250

Примеры расчетов для разных вариантов

Вариант №7

Таблица 5.3. Параметры проектируемой ТКС

Номер варианта для выполнения индивидуальной работы должен соответствовать номеру фамилии студента в журнале академической группы							
Номер варианта	Вид перед. Информации	Отношение С/Ш $h_б^2$, дБ	Метод модуляции	Произв. источника $R_{ист}$, кбит/с	Пропускная способность канала $F_к$, кГц	Вер. Ошибки бита	Сложн. декодера
7	ЦТВ	5.0	ФМ-2	2400	7000	10^{-8}	560

Структурная схема проектируемой телекоммуникационной системы

В общем виде обобщенная структурная схема проектируемой ТКС может быть сформирована в виде, представленном на рисунке 1.

В передатчике кодер вносит в информационное сообщение избыточность в виде проверочных символов. Закодированные символы поступают на модулятор, который преобразует их в аналоговый сигнал.

В приемнике демодулятор преобразует принятый сигнал в последовательность чисел, представляющих оценку переданных данных – метрики. Метрики поступают в декодер, который исправляет возникающие при передаче ошибки, используя внесенную кодером избыточность [1].

Классификация корректирующих кодов

Обнаружение ошибок в технике связи — действие, направленное на контроль целостности данных при записи/воспроизведении информации или при её передаче по линиям связи. Исправление ошибок (коррекция ошибок) — процедура восстановления информации после чтения её из устройства хранения или канала связи.

Для обнаружения ошибок используют коды обнаружения ошибок, для исправления — корректирующие коды(коды, исправляющие ошибки, коды с коррекцией ошибок, помехоустойчивые коды).

В общем виде классификация корректирующих кодов может быть представлена в следующем виде:

1. Блочные коды:

1.1 Линейные коды общего вида;

1.1.2 Коды Хемминга;

1.2 Линейные циклические коды:

1.2.1 Коды CRC;

1.2.2 Коды БЧХ;

1.2.3 Коды коррекции ошибок Рида — Соломона;

2. Сверточные коды;

3. Каскадные коды.

Стоит отметить, что блочные коды, как правило, хорошо справляются с редкими, но большими пачками ошибок, их эффективность при частых, но небольших ошибках (например, в канале с АБГШ), менее высока.

Вместе с этим, сверточные коды эффективно работают в канале с белым шумом, но плохо справляются с пакетами ошибок. Более того, если декодер ошибается, на его выходе всегда возникает пакет ошибок.

Так как в начальных условиях поставленной задачи не были сформулированы требования к методам кодирования, выбор остановился на сверточных кодах. Однако, при проектировании телекоммуникационных систем необходимо четко формировать критерии оптимальности разрабатываемой системы.

Классификация методов декодирования сверточных кодов

Классификация методов декодирования сверточных кодов имеет следующий вид:

1. Алгебраические методы декодирования;
2. Вероятностные методы декодирования:

2.1 Алгоритм последовательного декодирования;

2.2 Алгоритм Витерби.

Алгоритм Витерби характеризуется постоянством вычислительной работы, однако сложность декодера Витерби растет, как при переборных алгоритмов, по экспоненциальному закону от длины кодового ограничения сверточного кода.

Так как в данной работе в целях оптимизации проектируемой системы будут использоваться короткие сверточные коды, сложность декодера будет мала, что позволяет использовать алгоритм декодирования Витерби.

Расчет и оптимазация параметров телекоммуникацонной системы

Расчет ширины спектра цифрового сигнала с заданным видом модуляции:

$$F_{ФМ-2} = \frac{R_{ист} \cdot (1+\alpha)}{2} = \frac{2400 \cdot 10^3 \cdot (1+0.4)}{2} = 1.68 МГц .$$

Расчет ширины спектра кодированного цифрового сигнала с заданным видом модуляции в зависимости от скорости кода:

$$R_{код*} = \frac{F_{ФМ-2}}{F_к} = \frac{1680 \cdot 10^3}{7000 \cdot 10^3} = 0.24.$$

Следовательно скорость кода должна быть не менее 0.24. Полученный результат позволяет сформировать список подходящих сверточных кодов в виде представленном в таблице 3.

Татлица 4. Перечень подходящих сверточных кодов

Скорость кода $R_{код}$	Порождающие многочлены	ДКО v	Сложность решетки W	АЭВК, дБ
1/4	463,535,733,745	8	512	8,29
1/3	557,663,711	8	512	7,78
1/2	53,75	5	64	6,02
1/2	61,73	5	64	6,02
1/2	71,73	5	64	6,02
1/2	133,171	6	128	6,99
1/2	247,371	7	256	6,99

В силу того, критерием оптимальности проектируемой ТКС является простота используемого кодера/декодера, был выбран код /133,171/ с длиной кодового ограничения 7, который при скорости кода 0.5 обеспечивает АЭВК = 6.99 дБ.

Изложенное позволяет рассчитать ширину спектра кодированного цифрового сигнала:

$$F_{ФМ-2+СК} = \frac{F_{ФМ-2}}{R_{код}} = \frac{1680 \cdot 10^3}{0.5} = 3.36 МГц$$

Рисунок 6.2 позволяет сделать вывод о том, что применение выбранного кода обеспечивает выполнение поставленной задачи, так как при отношении С/Ш = 5 дБ вероятность ошибки декодирования меньше 10^{-5}.

Сравнение с кривыми помехоустойчивости некодированной ФМ показывает, что при вероятности ошибки 10^{-8} этот код обеспечивает значение ЭВК более 10 дБ.

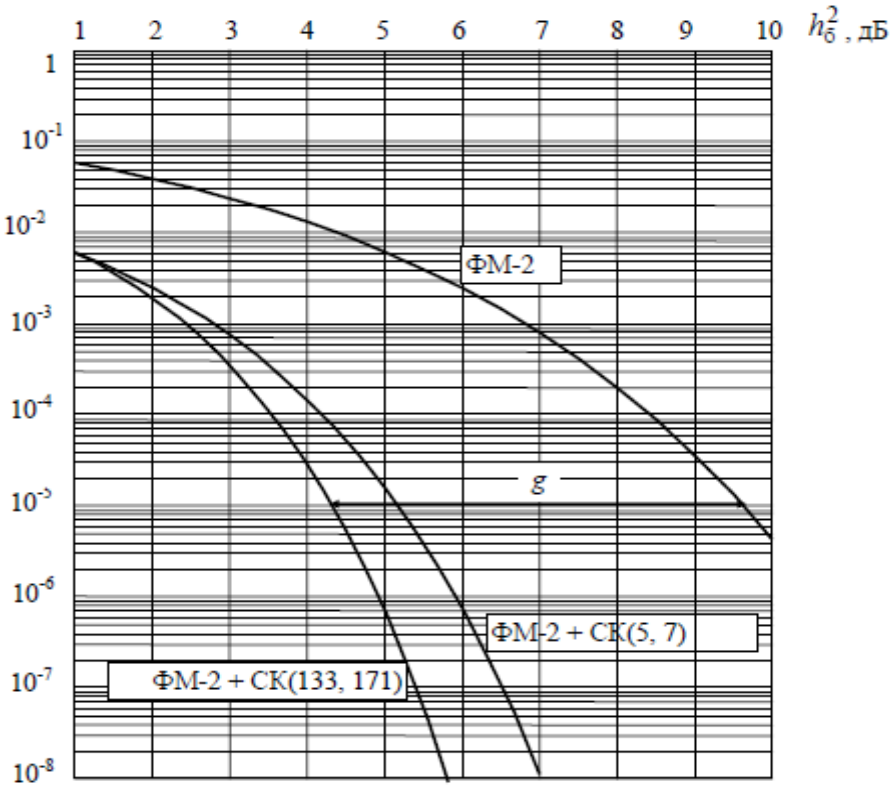


Рис. 2. Помехоустойчивость декодирования сверточных кодов

Проверочный расчет вероятности ошибки на выходе декодера:

$$Q = 0.65 \cdot \exp(-0.44 \cdot (z + 0.75)^2) = 0.65 \cdot$$

$$\cdot \exp(-0.44 \cdot (5.01 + 0.75)^2) = 2.972 \cdot 10^{-7}$$

$$p_o = w_{df} \cdot Q \cdot (\sqrt{2 \cdot d_f \cdot R_{код} \cdot h_б}) = 36 \cdot 2.972 \cdot 10^{-7} \cdot (\sqrt{2 \cdot 10 \cdot 0.5 \cdot 5}) = 7.565 \cdot 10^{-5}$$

Расчет показал, что реальное значение вероятности ошибки кодера меньше теоретического значения, следовательно, условия задачи были выполнены.

Разработка кодера и декодера сверточного кода 133,171

В предыдущем разделе был описан выбор сверточного кодера /133,171/. Функциональная и структура схема кодера/декодера может быть представлена в следующем виде:

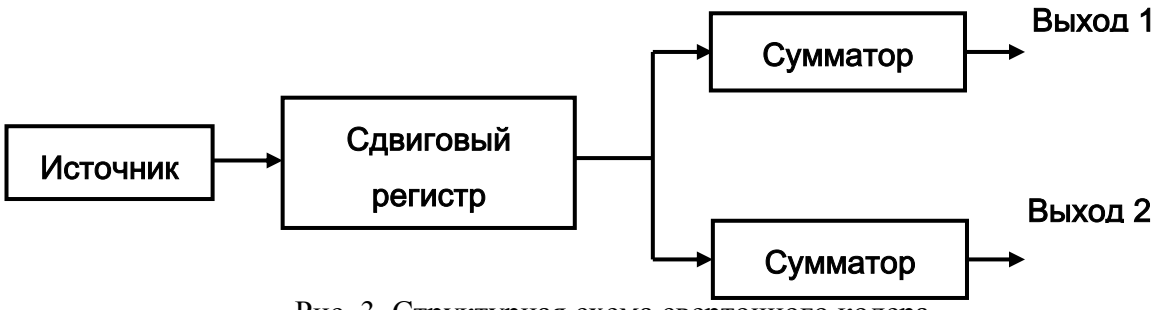


Рис. 3. Структурная схема сверточного кодера

$133_8 \rightarrow 1011011_2$

$171_8 \rightarrow 1111001_2$

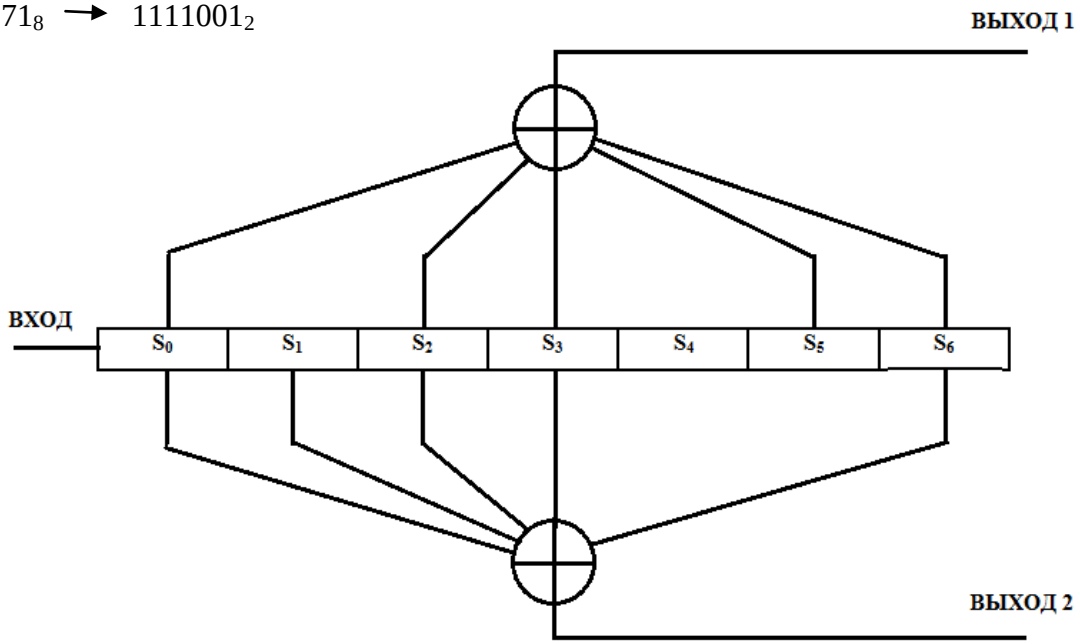


Рис. 4. Функциональная схема сверточного кодера 133,171

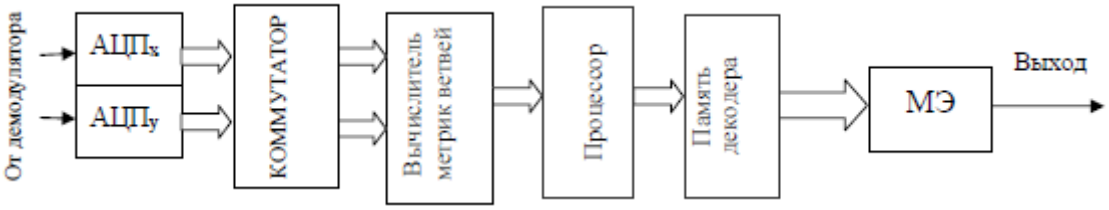


Рис. 5. Структурная схема декодера Витерби

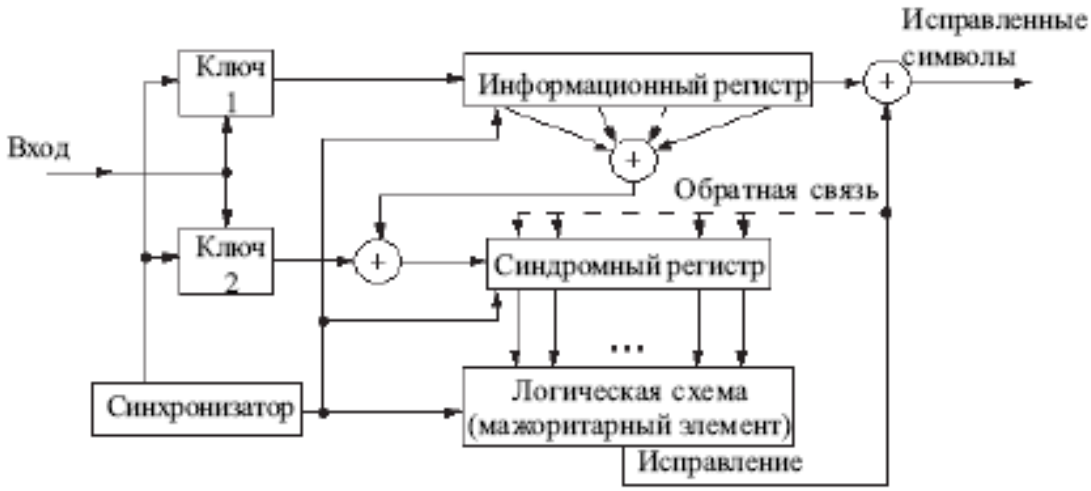


Рис. 6. Функциональная схема декодера Витерби

В результате выполнения данной индивидуальной работы было сделано следующее:

1. Спроектирована телекоммуникационная система с использованием сверточного кодера;

2. Рассчитаны и оптимизированы параметры сверточного кода используемого в ТКС в целях повышения ее эффективности и помехоустойчивости;

3. Предложены структурные и функциональные схемы кодера и кодера, используемых в разработанной ТКС.

Варианты № 16, 3, 8

Для решения поставленной задачи предложены общие параметры проектируемой ТКС, которые представленные в таблице 5.

Таблица 5. Параметры проектируемой ТКС

Номер варианта	Вид перед. инф-ии	Отношение С/Ш $h_б^2$, дБ	Метод модуляции	Произв. источника $R_{ист}$, кбит/с	Пропускная способность канала $F_к$, кГц	Вер. ошибки бита p	Сложн. декодера W
16	ДК	7,0	ФМ-4	56	90	10^{-6}	150
3	ЦЗВ	6,0	ФМ-2	256	800	10^{-5}	170
8	ДК	6,0	ФМ-4	32	50	10^{-6}	200

Структурная схема проектируемой телекоммуникационной системы

Структурная схема проектируемой телекоммуникационной системы представлена в [1].

Источник сообщения генерирует бинарную последовательность с определенной скоростью $R_{ист}$. Курсивом отмечены блоки, которые кодируют и декодируют информацию с применением помехоустойчивых кодов (вводится избыточность при кодировании, например код Хемминга, БЧХ, сверточный код). Что касается источника, то он кодируется и декодируется с помощью таких алгоритмов как, Хаффмана, Шеннона-Фано или Лемпела-Зива. В данных алгоритмах не вводится избыточность. Помимо кодирования система связи содержит в себе квадратурную модуляцию/демодуляцию. Где на выходе модулятора мы получаем сначала комплексные числа (квадратурные и синфазные составляющие), которые в свою очередь садятся на несущие, сдвинутые на 90 градусов и в конечном итоге суммируются. Демодуляция представляет собой обратный процесс. Варианты работы содержит в себе модуляцию ФМ-2 или BPSK, которая имеет только два синфазных значения постоянной амплитуды и фазы 0 и 180 градусов и ФМ-4 или QPSK, которая имеет четыре значения постоянной амплитуды и фазы. И, конечно же, любая система передачи не обходится без воздействия на нее шумов, в канале беспроводной сети (канал связи).

4 Классификация корректирующих кодов

Обнаружение ошибок в технике связи — действие, направленное на контроль целостности данных при записи/воспроизведении информации или при её передаче по линиям связи. Исправление ошибок (коррекция ошибок) — процедура восстановления информации после чтения её из устройства хранения или канала связи.

Для обнаружения ошибок используют коды обнаружения ошибок, для исправления — корректирующие коды(коды, исправляющие ошибки, коды с коррекцией ошибок, помехоустойчивые коды).

Преимущества и недостатки блоковых кодов:

Блоковые коды, как правило, хорошо справляются с редкими, но большими пачками ошибок, их эффективность при частых, но небольших ошибках (например, в канале с АБГШ), менее высока.

Преимущества и недостатки свёрточных кодов:

Свёрточные коды эффективно работают в канале с белым шумом, но плохо справляются с пакетами ошибок. Более того, если декодер ошибается, на его выходе всегда возникает пакет ошибок. Выбор в индивидуальной работе сверточных кодов обосновывается тем, что свёрточное кодирование - очень простая операция. Кодирование свёрточным кодом производится с помощью регистра сдвига, отводы от которого суммируются по модулю два. Таких сумм может быть две (чаще всего) или больше.

Классификация корректирующих кодов по структуре представлена на рисунке в.

Классификация методов декодирования сверточных кодов

Классификация методов декодирования сверточных кодов имеет следующий вид:

3. Алгебраические методы декодирования;
4. Вероятностные методы декодирования:
   - 4.1 Алгоритм последовательного декодирования;
   - 4.2 Алгоритм Витерби.

Задача декодирования сверточного кода заключается в выборе пути (в этом и состоит отличие декодирования сверточных кодов) вдоль решетки наиболее похожего на принятую последовательность. Каждый путь вдоль решетчатой диаграммы складывается из ветвей соединяющих узлы. Каждой ветви решетки соответствует кодовое слово из двух бит. Каждую ветвь на каждом периоде можно пометить расстоянием Хемминга между полученным кодовым словом и кодовым словом, соответствующим ветви. Складывая расстояния Хемминга ветвей, составляющих путь, получим метрику соответствующего пути. Данная метрика будет характеризовать степень подобия каждого пути принятой последовательности. Чем меньше метрика, тем более похожи путь и принятая последовательность. Таким образом,

результатом декодирования будет информационная последовательность, соответствующая пути с минимальной метрикой. Если в одно и тоже состояние входят два пути выбирается тот, который имеет лучшую метрику. Такой путь называется выжившим. Отбор выживших путей проводится для каждого состояния. Это не иначе как алгоритм декодирования Витерби и он наиболее эффективный.

Расчет ширины спектра цифрового сигнала с заданным видом модуляции

Вариант	Расчеты
16	$F_{ФМ4} = \frac{R_{ист}*(1+\alpha)}{2} = \frac{56*(1+0,4)}{2} = 39,2$ кГц
3	$F_{ФМ4} = \frac{R_{ист}*(1+\alpha)}{2} = \frac{256*(1+0,4)}{2} = 179,2$ кГц
8	$F_{ФМ4} = \frac{R_{ист}*(1+\alpha)}{2} = \frac{32*(1+0,4)}{2} = 22,4$ кГц

Определение допустимой скорости кода из условия непревышения полосой частот кодированного сигнала полосы пропускания канала

Вариант	Расчеты
16	$R_{код*} = \frac{F_{ФМ4}}{F_K} = 0.436$
3	$R_{код*} = \frac{F_{ФМ4}}{F_K} = 0.224$
8	$R_{код*} = \frac{F_{ФМ4}}{F_K} = 0,448$

Определение кода

Полученный результат позволяет сформировать список подходящих сверточных кодов в виде, представленном в таблице 6.

Таблица 6. Характеристики СК для выбора кода

Скорость кода $R_{код}$	Порождающие многочлены	ДКО v	Сложность решетки W	АЭВК, дБ
1/4	463,535,733,745	8	512	8,29
1/3	557,663,711	8	512	7,78
1/2	53,75	5	64	6,02
1/2	61,73	5	64	6,02
1/2	71,73	5	64	6,02
1/2	133,171	6	128	6,99
1/2	247,371	7	256	6,99

Вариант	Условия
16	СК со скоростями 1/2 и сложностью решетки W не более 150
3	Все СК со сложностью решетки W не более 170
8	СК со скоростями ½ и сложностью решетки W не более 200

Произведен выбор СК из перечня, обеспечивающего заданную вероятность ошибки бита и удовлетворяющего требованию ограничения по сложности декодера.

Вариант	Выбранный СК
16	Код с порождающими многочленами (133, 171), который при скорости 1/2 обеспечивает АЭВК = 6,99 дБ
3	Код с порождающими многочленами (133, 171), который при скорости 1/2 обеспечивает АЭВК = 6,99 дБ
8	Код с порождающими многочленами (133, 171), который при скорости 1/2 обеспечивает АЭВК = 6,99 дБ

Расчет ширины спектра кодированного цифрового сигнала с заданным видом модуляции в зависимости от скорости кода

Вариант	Расчеты
16	$F_{ФМ4+СК} = \frac{F_{FM4}}{R_{код}} = \frac{39,2}{0,5} = 78,4$ кГц
3	$F_{FM2+СК} = \frac{F_{FM2}}{R_{код}} = \frac{179,2}{0,5} = 358,4$ кГц
8	$F_{ФМ4+СК} = \frac{F_{FM4}}{R_{код}} = \frac{22,4}{0,5} = 44,8$ кГц

Рисунок 7 позволяет сделать вывод о том, что применение выбранного кода обеспечивает выполнение поставленной задачи, так как

Вариант	Отношение С/Ш $h_б^2$, дБ	Вероятность ошибки декодирования меньше
16	7,0	10^{-6}
3	6,0	10^{-5}
8	6,0	10^{-6}

Сравнение с кривыми помехоустойчивости некодированной ФМ показывает, что

Вариант	Вероятность ошибки	АЭВК, дБ
16	10^{-6}	более 10
3	10^{-5}	9,4
8	10^{-6}	более 10

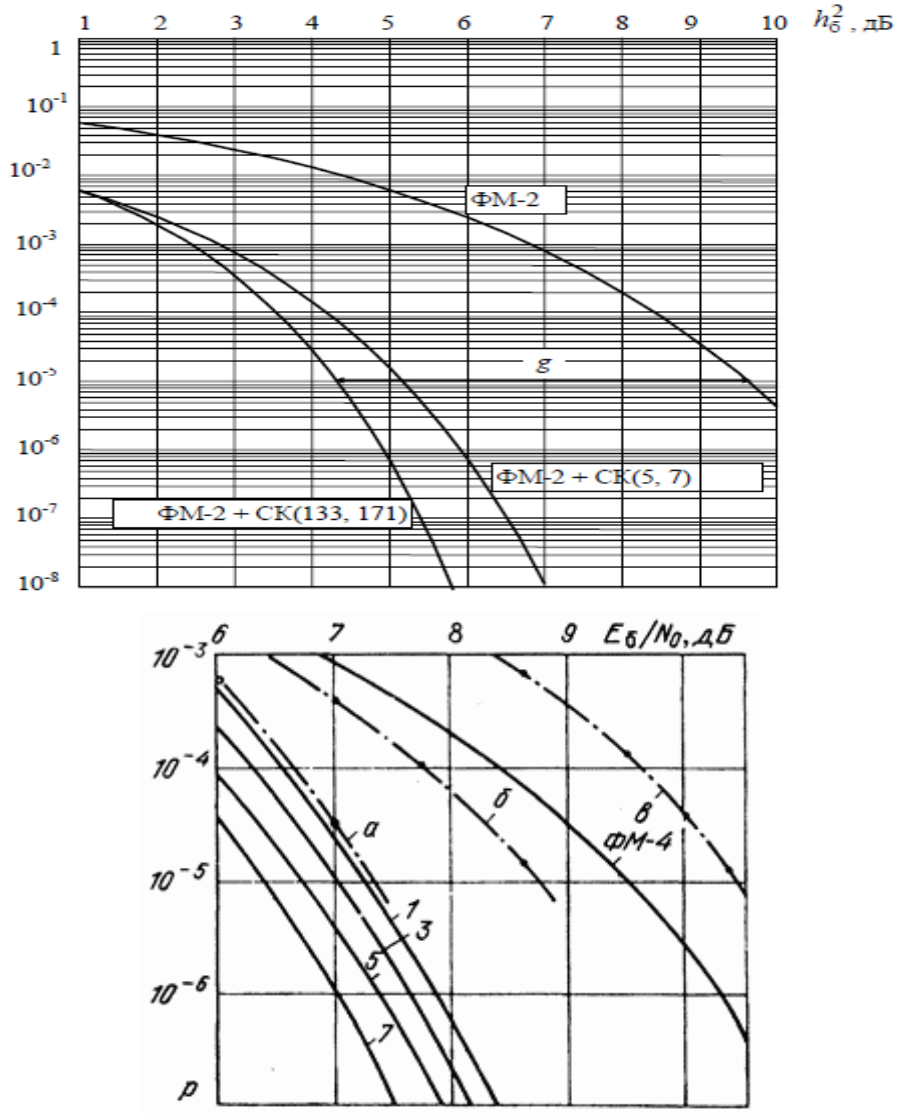


Рис. 8. Помехоустойчивость декодирования сверточных кодов

Проверочный расчет зависимости вероятности ошибки на выходе декодера

В результате получим (примерно для заданной вероятности ошибки бита):

Вариант	Расчеты
16	$Q = \frac{1}{x * \sqrt{2\pi}} * \exp\left(-\frac{x^2}{2}\right) = \frac{1}{5{,}01 * \sqrt{2\pi}} * \exp\left(-\frac{5{,}01^2}{2}\right) = 4{,}45 * 10^{-5}$ $p_d = w_{df} \cdot Q \cdot \sqrt{2 \cdot d_f \cdot R_{kod} \cdot h_b} = 36 \cdot 4.45 \cdot 10^{-5} \cdot \sqrt{2 \cdot 10 \cdot 0.5 \cdot 7} = 4.2 \cdot 10^{-3}$

3	$Q = \frac{1}{x * \sqrt{2\pi}} * \exp\left(-\frac{x^2}{2}\right) = \frac{1}{4 * \sqrt{2\pi}} * \exp\left(-\frac{4^2}{2}\right) = 3{,}3 * 10^{-5}$ $p_d = w_{df} \cdot Q \cdot \sqrt{2 \cdot d_f \cdot R_{kod} \cdot h_b} = 36 \cdot 3.3 \cdot 10^{-5} \cdot \sqrt{2 \cdot 10 \cdot 0.5 \cdot 6} = 9.2 \cdot 10^{-3}$
8	$Q = \frac{1}{x * \sqrt{2\pi}} * \exp\left(-\frac{x^2}{2}\right) = \frac{1}{5{,}01 * \sqrt{2\pi}} * \exp\left(-\frac{5{,}01^2}{2}\right) = 4{,}45 * 10^{-5}$ $p_d = w_{df} \cdot Q \cdot \sqrt{2 \cdot d_f \cdot R_{kod} \cdot h_b} = 36 \cdot 4.45 \cdot 10^{-5} \cdot \sqrt{2 \cdot 10 \cdot 0.5 \cdot 6} = 4.2 \cdot 10^{-3}$

Расчет показал, что реальное значение вероятности ошибки кодера меньше теоретического значения, следовательно, условия задачи были выполнены.

Разработка кодера и декодера СК 133, 171

В предыдущем разделе был описан выбор сверточного кодера (133,171).

$133_8 = 1011011_2; 171_8 = 1111001_2$

Функциональная и структура схема кодера/декодера может быть представлена в следующем виде:

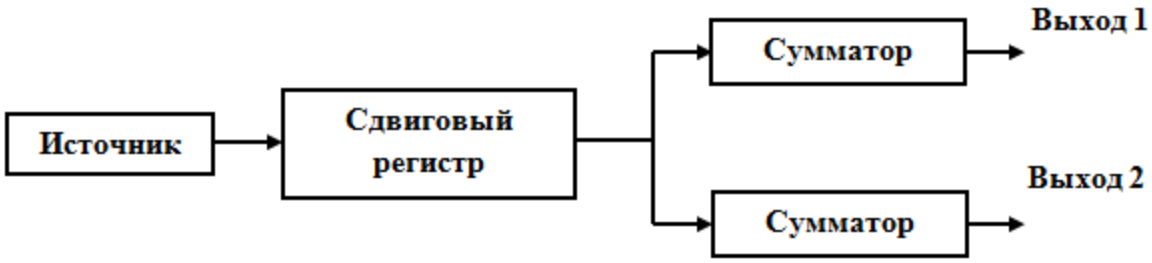


Рис. 9. Структурная схема сверточного кодера

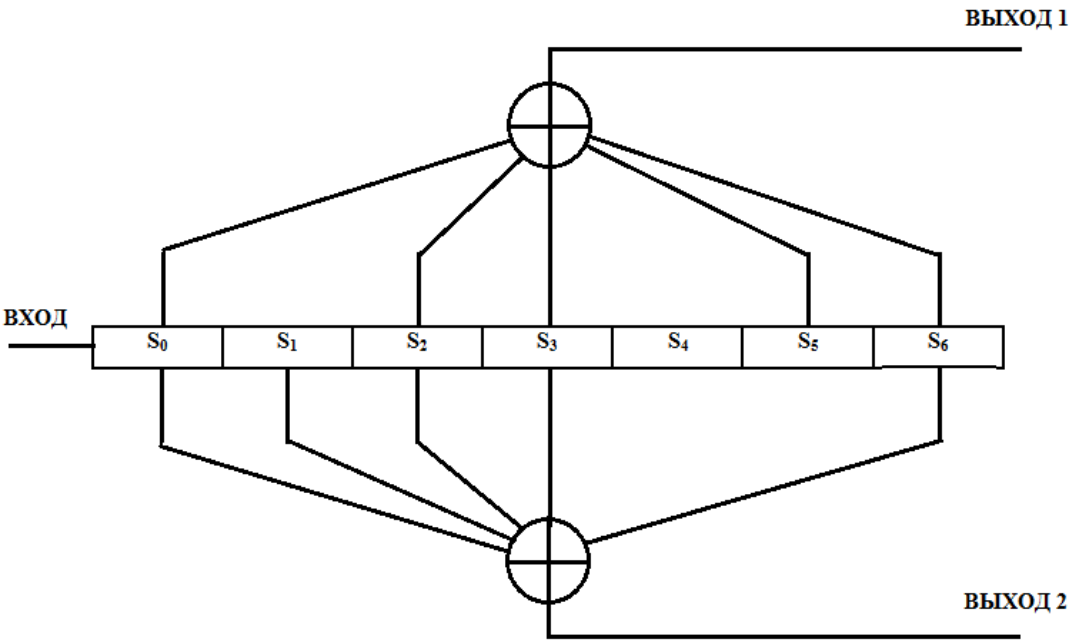


Рис. 10. Функциональная схема сверточного кодера 133,171

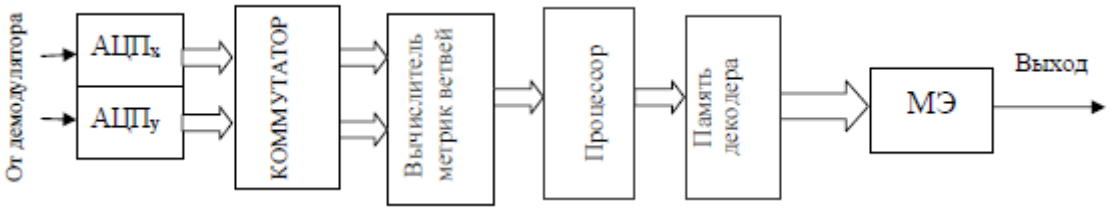


Рис. 5.11. Структурная схема декодера Витерби

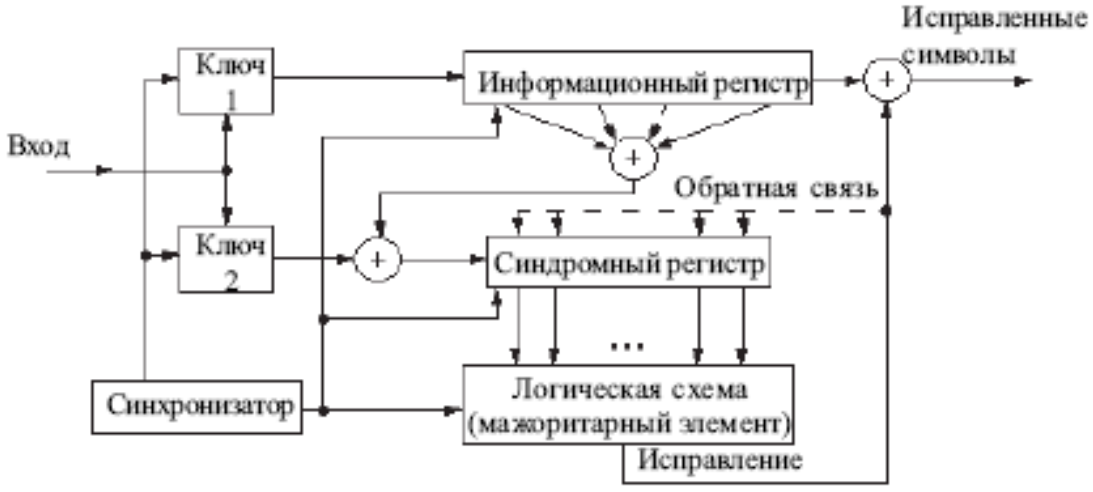


Рис. 5.12. Функциональная схема декодера Витерби

кодера со скоростью 1/2.

В результате выполнения данного индивидуального задания было выполнено следующее:

- Спроектирована телекоммуникационная система с использованием сверточного кодера;

- Рассчитаны и оптимизированы параметры сверточного кода используемого в ТКС в целях повышения ее эффективности и помехоустойчивости при различных начальных заданных условиях (ширина спектра, скорость кода, битовая вероятность ошибки в зависимости от заданного значения отношения сигнал/шум);
- Предложены структурные и функциональные схемы кодера и кодера, используемых в разработанной ТКС.

Варианты № 4, 5, 14

Исходные данные

Вариант № 4:

- Передаваемая информация: данные компьютера;
- Отношение сигнал/шум: $h_б^2 = 6{,}5$ дБ;
- Метод модуляции: ФМ-2;
- Производительность источника: $R_{ист} = 64$ кбит/с;
- Прием: когерентный;
- Полоса пропускания канала: $F_k = 200$ *кГц*;
- Битовая вероятность ошибки (BER): $p = 10^{-6}$;
- Сложность декодера не более (показатель сложности решетки кода): $W = 180$;

Вариант № 5:

- Передаваемая информация: сообщения цифрового ТВ;
- Отношение сигнал/шум: $h_б^2 = 4$ дБ;
- Метод модуляции: ФМ-4;
- Производительность источника: $R_{ист} = 16$ кбит/с;
- Прием: когерентный;
- Полоса пропускания канала: $F_k = 25$ *кГц*;
- Битовая вероятность ошибки (BER): $p = 10^{-4}$;
- Сложность декодера не более (показатель сложности решетки кода): $W = 250$;

Вариант № 14:

- Передаваемая информация: сообщения цифрового звукового вещания;
- Отношение сигнал/шум: $h_б^2 = 7$ дБ;
- Метод модуляции: ФМ-2;
- Производительность источника: $R_{ист} = 256$ кбит/с;
- Прием: когерентный;
- Полоса пропускания канала: $F_k = 400$ *кГц*;

- Битовая вероятность ошибки (BER): $p = 10^{-5}$;
- Сложность декодера не более (показатель сложности решетки кода): $W = 300$;

Описание структурной схемы проектируемой ТКС. Указание мест включения кодера/декодера, модулятора/демодулятора с описанием их функций

Ни одна ТКС не обходится без системы связи, представленной на рисунке 13.

Рис. 13. Обобщенная модель

Любая система передачи цифровой информации имеет в своем составе блоки, изображенные на рисунке 13.

Источник сообщения генерирует бинарную последовательность с определенной скоростью $R_{ист}$. Курсивом отмечены блоки, которые кодируют и декодируют информацию с применением помехоустойчивых кодов (вводится избыточность при кодировании, например код Хемминга, БЧХ, сверточный код). Что касается источника, то он кодируется и декодируется с помощью таких алгоритмов как, Хаффмана, Шеннона-Фано или Лемпела-Зива. В данных алгоритмах не вводится избыточность. Помимо кодирования система связи содержит в себе квадратурную модуляцию/демодуляцию. Где на выходе модулятора мы получаем сначала комплексные числа (квадратурные и синфазные составляющие), которые в свою очередь садятся на несущие, сдвинутые на 90 градусов и в конечном итоге суммируются. Демодуляция представляет собой обратный процесс. Варианты работы содержит в себе модуляцию ФМ-2 или BPSK, которая имеет только два синфазных значения постоянной амплитуды и фазы 0 и 180 градусов и ФМ-4 или QPSK, которая имеет четыре значения постоянной амплитуды и фазы.

И, конечно же, любая система передачи не обходится без воздействия на нее шумов, в канале беспроводной сети (канал связи).

Классификация корректирующих кодов по структуре. Сравнительный анализ преимуществ и недостатков помехоустойчивых блоковых и сверточных кодов. Обоснование применения в проекте сверточных кодов

Классификация корректирующих кодов по структуре представлена на рисунке 14.

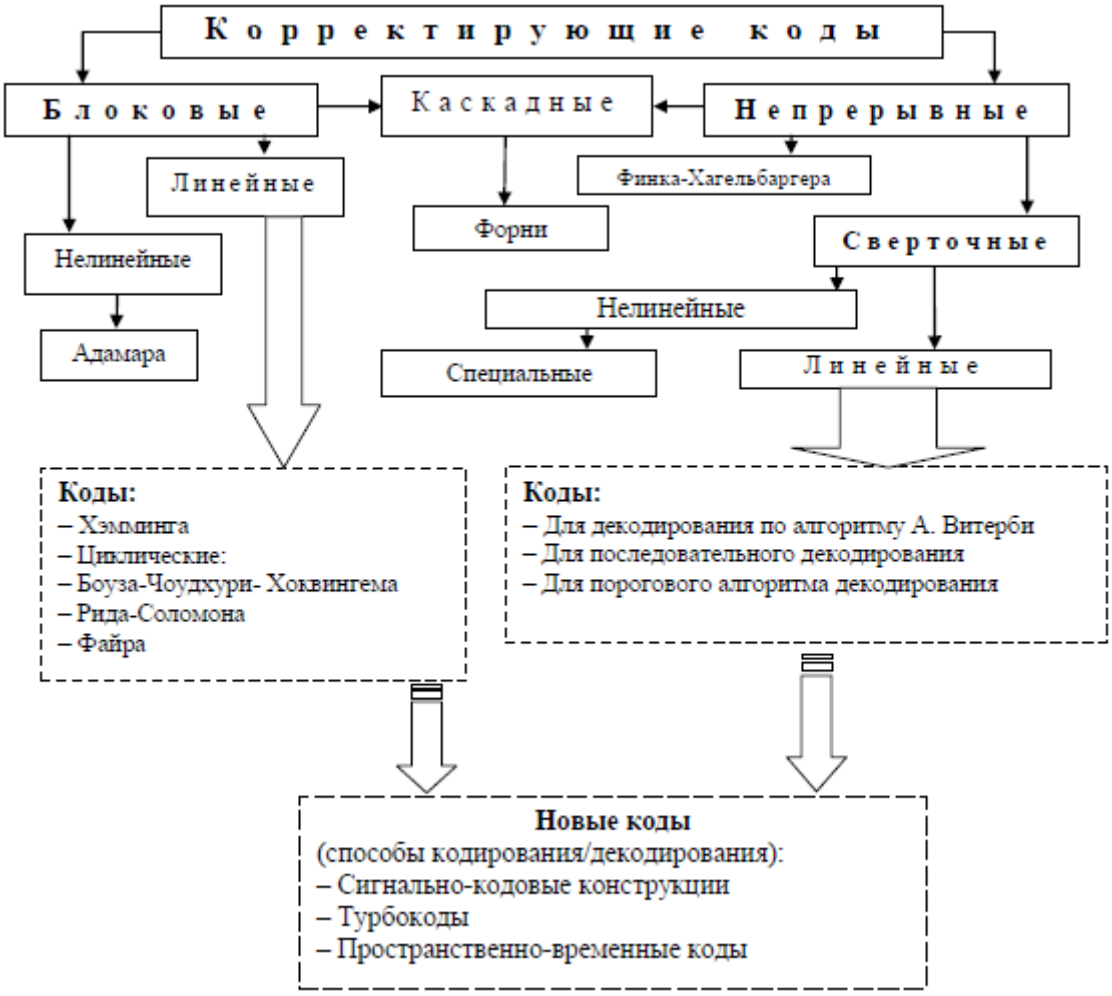


Рис. 14. Классификация корректирующих кодов

Преимущества и недостатки блоковых кодов:

Блоковые коды, как правило, хорошо справляются с редкими, но большими пачками ошибок, их эффективность при частых, но небольших ошибках (например, в канале с АБГШ), менее высока.

Преимущества и недостатки свёрточных кодов:

Свёрточные коды эффективно работают в канале с белым шумом, но плохо справляются с пакетами ошибок. Более того, если декодер ошибается, на его выходе всегда возникает пакет ошибок.

Выбор в индивидуальной работе сверточных кодов обосновывается тем, что свёрточное кодирование - очень простая операция. Кодирование свёрточным кодом производится с

помощью регистра сдвига, отводы от которого суммируются по модулю два. Таких сумм может быть две (чаще всего) или больше.

Классификация и сравнительный анализ алгоритмов декодирования сверточных кодов. Обоснование выбора алгоритма Витерби для декодирования сверточных кодов.

Существует несколько методов:

1) *Алгебраические методы декодирования* основаны на использовании алгебраических свойств кодовых последовательностей. В ряде случае эти методы приводят к простым реализациям кодека. Такие алгоритмы являются неоптимальными, так как используемые алгебраические процедуры декодирования предназначены для исправления конкретных (и не всех) конфигураций ошибок в канале. Данные методы отождествляют с поэлементным приёмом последовательностей, который для кодов с избыточностью, как известно, даёт худшие результаты, чем «приём в целом». Оперируют с конечным алфавитом входных данных, для получения которых на выходе непрерывного канала необходимо выполнить квантование.

А) Наиболее простым из алгебраических алгоритмов является *алгоритм порогового декодирования* сверточных кодов. Этот алгоритм далек от оптимального и поэтому редко используется, в первую очередь, в системах с высокой скоростью передачи информации.

2) *Вероятностные методы декодирования* значительно ближе к оптимальному «приёму в целом», так как в этом случае декодер оперирует с величинами, пропорциональными апостериорным вероятностям, оценивает и сравнивает вероятности различных гипотез и на этой основе выносит решения о передаваемых символах.

А) *Алгоритм последовательного декодирования* обеспечивает произвольно малую вероятность ошибки при ненулевой скорости передачи сообщений по каналу. При последовательном декодировании производится поиск пути на кодовой решетке, соответствующего переданной информационной последовательности. Последовательное декодирование используется для декодирования длинных сверточных кодов.

Б) *Алгоритм Витерби* реализует поиск максимально правдоподобного пути на кодовой решетке с отбрасыванием части наименее правдоподобных вариантов путей на каждом шаге декодирования. Он характеризуется постоянством во времени затрат ресурсов процессора, однако сложность декодера Витерби растет, как при всех переборных алгоритмах, по экспоненциальному закону от длины кодового ограничения сверточного кода. Поэтому алгоритм Витерби используется для декодирования коротких сверточных кодов.

Расчет ширины спектра цифрового сигнала с заданным видом модуляции

На основании исходных данных произведём вычисления:

Вариант 4:

$$F_{FM4} = 2 * (m_{FM4} + 1) * F_K = 2 * \left(\frac{\Delta f}{F_K} + 1\right) * F_K = 2 * \left(\frac{200}{200} + 1\right) * 200 = 800 \text{ кГц};$$

Вариант 5:

$$F_{FM2} = 2 * (m_{FM2} + 1) * F_K = 2 * \left(\frac{\Delta f}{F_K} + 1\right) * F_K = 2 * \left(\frac{25}{25} + 1\right) * 25 = 100 \text{ кГц};$$

Вариант 14:

$$F_{FM4} = 2 * (m_{FM4} + 1) * F_K = 2 * \left(\frac{\Delta f}{F_K} + 1\right) * F_K = 2 * \left(\frac{800}{800} + 1\right) * 800 = 3200 \text{ кГц};$$

Расчёт ширины спектра кодированного цифрового сигнала с заданным видом модуляции в зависимости от скорости кода

Вариант 4:

$$F_{ФM4} = \frac{1}{R_{код}} * 2 * (m_{FM4} + 1) * F_K = \frac{1}{R_{код}} * 2 * \left(\frac{\Delta f}{F_K} + 1\right) * F_K = \frac{1}{0{,}224} * 2 * \left(\frac{200}{200} + 1\right) * 200 = 3571 \text{ кГц};$$

Вариант 5:

$$F_{FM2} = \frac{1}{R_{код}} * 2 * (m_{FM2} + 1) * F_K = \frac{1}{R_{код}} * 2 * \left(\frac{\Delta f}{F_K} + 1\right) * F_K = \frac{1}{0{,}448} * 2 * \left(\frac{25}{25} + 1\right) * 25 = 223 \text{ кГц};$$

Вариант 14:

$$F_{ФM4} = \frac{1}{R_{код}} * 2 * (m_{FM4} + 1) * F_K = \frac{1}{R_{код}} * 2 * \left(\frac{\Delta f}{F_K} + 1\right) * F_K = \frac{1}{0{,}448} * 2 * \left(\frac{800}{800} + 1\right) * 800 = 7142 \text{ кГц};$$

Определение допустимой скорости кода из условия непревышения полосой частот кодированного сигнала полосы пропускания канала

Вариант 4:

$$F_{ФM4} = \frac{R_{ист} * (1+\alpha)}{2} = 44{,}8 \text{ кГц};$$

$$R_{код} = \frac{F_{ФM4}}{F_K} = 0.224;$$

Вариант 5:

$$F_{ФM4} = \frac{R_{ист} * (1+\alpha)}{2} = 11{,}2 \text{ кГц};$$

$$R_{код} = \frac{F_{ФM4}}{F_K} = 0.448\ ;$$

Вариант 14:

$$F_{ФМ4} = \frac{R_{ист}*(1+\alpha)}{2} = 197.2 \text{ кГц};$$

$$R_{код} = \frac{F_{ФМ4}}{F_K} = 0.224 ;$$

Определение перечня кодов со скоростями, превышающими допустимую скорость, которые могут быть использованы для решения поставленной задачи

Таблица 7. Характеристики СК для выбора кода

Скорость кода $R_{код}$	Порождающие многочлены	ДКО ν	Сложность решетки W	АЭВК, дБ
1/4	463,535,733,745	8	512	8,29
1/3	557,663,711	8	512	7,78
1/2	53,75	5	64	6,02
1/2	61,73	5	64	6,02
1/2	71,73	5	64	6,02
1/2	133,171	6	128	6,99
1/2	247,371	7	256	6,99

На основании таблицы 7 определим следующие коды:

Вариант 4:

Все коды.

Вариант 5:

Коды со скоростью выше 0,448.

Вариант 14:

Все коды.

Выбор СК из этого перечня, обеспечивающего заданную вероятность ошибки бита и удовлетворяющего требованию ограничения по сложности декодера

Вариант 4:

Коды с порождающими многочленами (463,535,733,745) АЭВК = 8,29 дБ, (557, 663, 711) АЭВК = 7,78 дБ, (247, 371) АЭВК = 6,99 дБ.

Вариант 5:

Код с порождающими многочленами (247, 371) АЭВК = 6,99 дБ.

Вариант 14:

Коды с порождающими многочленами (463,535,733,745) АЭВК = 8,29 дБ, (557, 663, 711) АЭВК = 7,78 дБ.

Проверочный расчет зависимости вероятности ошибки на выходе декодера

$$BER = Q * \sqrt{2 * h_б^2}$$

$$Q = \frac{1}{x * \sqrt{2\pi}} * \exp\left(-\frac{x^2}{2}\right)$$

В результате получим (примерно для заданной вероятности ошибки бита):

Вариант 4:

$$Q = \frac{1}{5 * \sqrt{2\pi}} * \exp\left(-\frac{5^2}{2}\right) = 0{,}3 * 10^{-6}$$

$$BER = Q * \sqrt{2 * 6{,}5} = 2{,}75 * 10^{-6}$$

Вариант 5:

$$Q = \frac{1}{3 * \sqrt{2\pi}} * \exp\left(-\frac{3^2}{2}\right) = 3{,}3 * 10^{-5}$$

$$BER = Q * \sqrt{2 * 4} = 186 * 10^{-6}$$

Вариант 14:

$$Q = \frac{1}{4{,}5 * \sqrt{2\pi}} * \exp\left(-\frac{4{,}5^2}{2}\right) = 3{,}5 * 10^{-6}$$

$$BER = Q * \sqrt{2 * 7} = 34{,}6 * 10^{-6}$$

Разработка и описание структурных и функциональных схем кодера и декодера выбранного СК

Вариант 4

Кодер выглядит следующим образом:

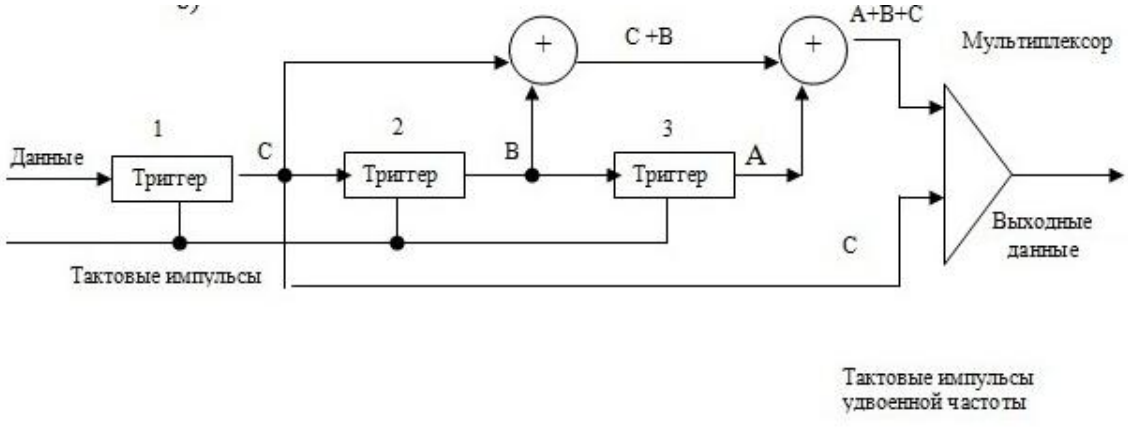


Рис. 15. Структурная схема кодера

Свёрточный кодер состоит из регистра сдвига, блока сумматора по модулю 2, входы соединены с некоторыми выходами регистра сдвига. Таким образом, на каждом такте в регистр сдвига последовательно поступает блок из k исходных информационных символов. В

том же такте на выходе преобразователя формируется кодовая последовательность длиной n последовательных символов. С помощью мультиплексора они передаются в канал.

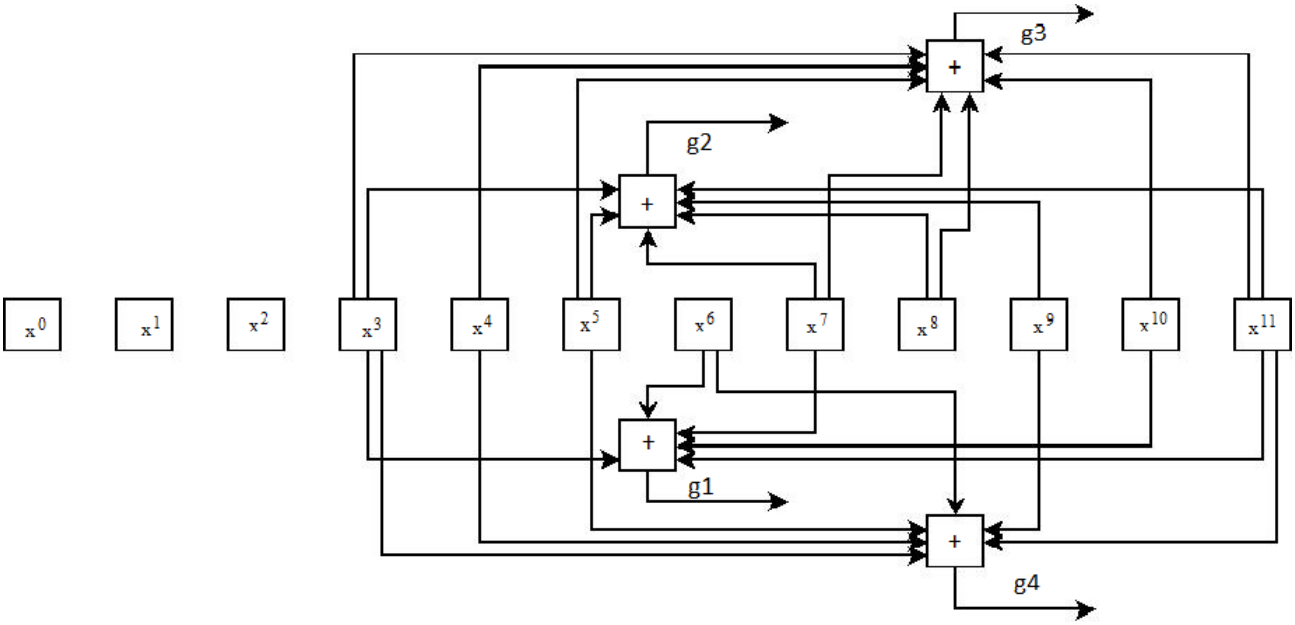


Рис. 16. Функциональная схема кодера с порождающими многочленами (463,535,733,745)

Вариант 5

Кодер выглядит следующим образом:

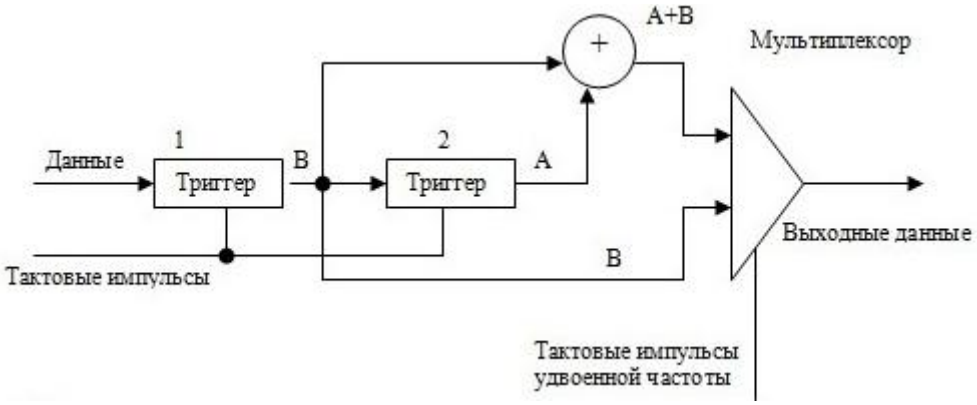


Рис. 17. Структурная схема кодера

Свёрточный кодер состоит из регистра сдвига, блока сумматора по модулю 2, входы соединены с некоторыми выходами регистра сдвига. Таким образом, на каждом такте в регистр сдвига последовательно поступает блок из k исходных информационных символов. В том же такте на выходе преобразователя формируется кодовая последовательность длиной n последовательных символов. С помощью мультиплексора они передаются в канал.

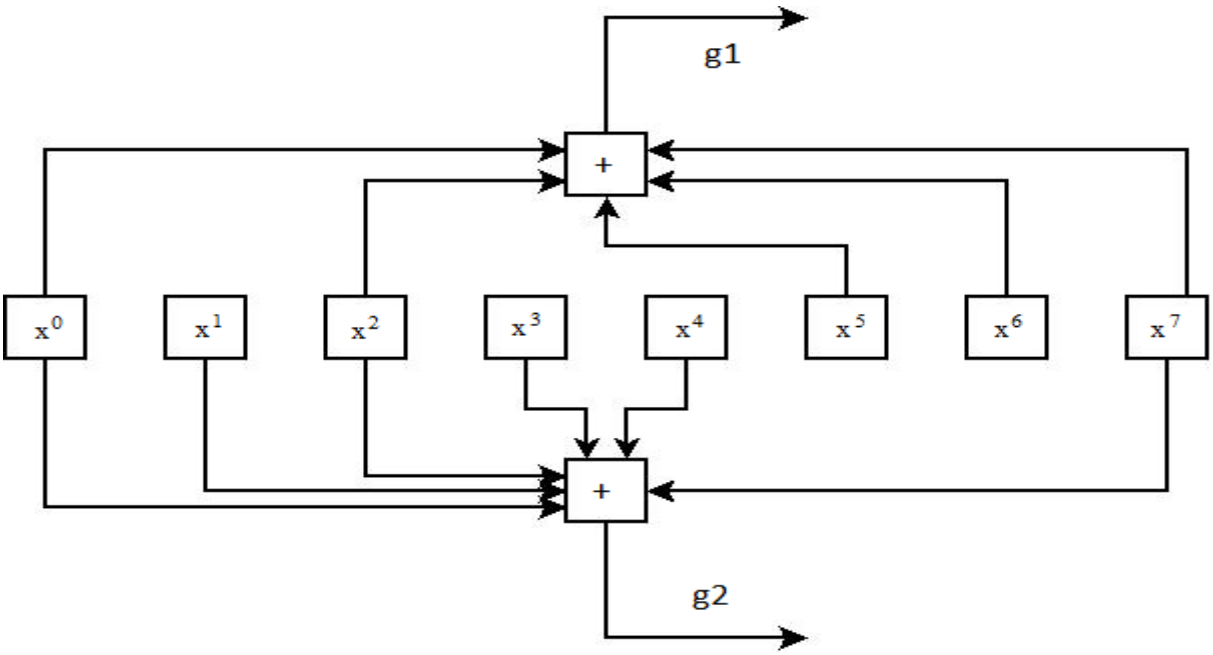


Рис. 18. Функциональная схема кодера с порождающими полиномами (247, 371)

Вариант 14

Кодер выглядит следующим образом:

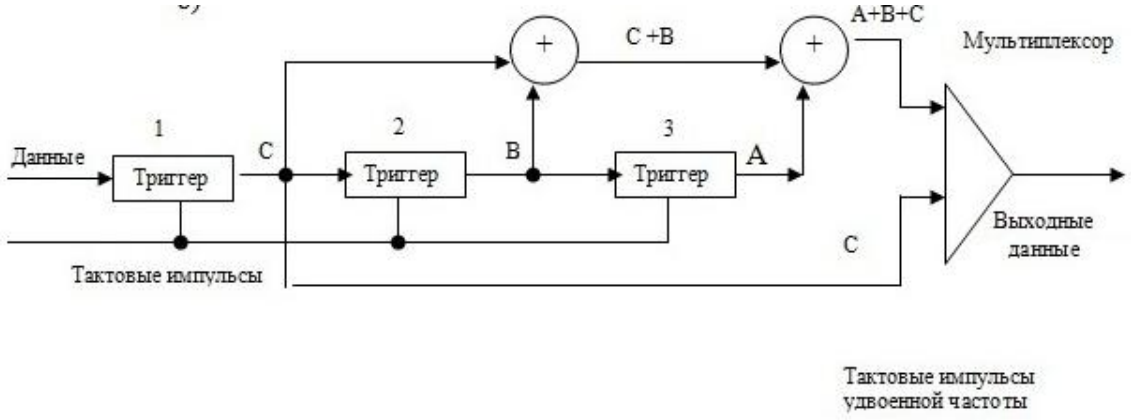


Рис. 19. Структурная схема кодера

Свёрточный кодер состоит из регистра сдвига, блока сумматора по модулю 2, входы соединены с некоторыми выходами регистра сдвига. Таким образом, на каждом такте в регистр сдвига последовательно поступает блок из k исходных информационных символов. В том же такте на выходе преобразователя формируется кодовая последовательность длиной n последовательных символов. С помощью мультиплексора они передаются в канал.

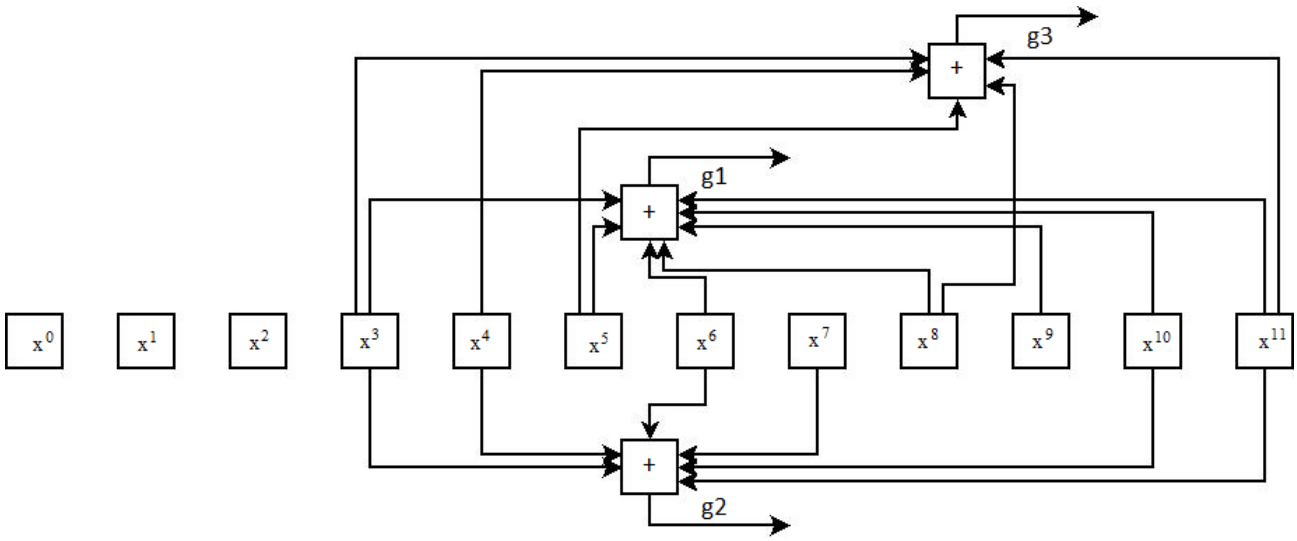


Рис. 20. Функциональная схема кодера с порождающими полиномами (557, 663, 711)

Общая структурная схема декодера:

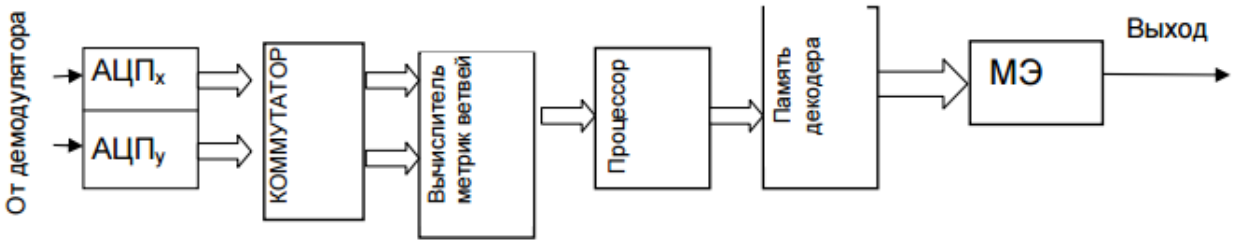


Рис. 21. Структурная схема декодера сверточного кода.

Декодер состоит из АЦП в каналах X и Y, вычислителя метрик ветвей, процессора, в котором производятся операции сложения, сравнения и выбора, устройства памяти путей, которые выжили, и мажоритарного элемента МЭ, в котором выбирается путь с наибольшей метрикой. Оптимальное значение шага квантования зависит от отношения сигнал/шум на входе АЦП.

В данном индивидуальном задании были исследованы внутренние составляющие телекоммуникационной системы (ТКС) при различных начальных заданных условий, а именно были посчитаны: ширина спектра, скорость кода, битовая вероятность ошибки в зависимости от заданного значения отношения сигнал/шум.

А также было исследовано:

1. Работа кодера/декодера ТКС;
2. Модулятора/демодулятора ТКС;
3. Классификация корректирующих кодов;
4. Преимущества и недостатки корректирующих кодов;
5. Алгоритмы кодирования и декодирования сверточных кодов.

2.2. ТИПОВЫЕ ЗАДАНИЯ НА КУРСОВЫЕ РАБОТЫ ПО ШИФРОВАНИЮ В СИСТЕМАХ СВЯЗИ

2.2.1. Задания на курсовую работу по классическим шифрам

Задания на криптоанализ классических шифров

Шифр столбцовой перестановки

При решении заданий на криптоанализ шифров перестановки необходимо восстановить начальный порядок следования букв текста. Для этого используется анализ совместимости символов, в чем может помочь таблица сочетаемости.

Таблица 8. Сочетаемость букв русского языка

Г	С	Слева		Справа	Г	С
3	97	л, д, к, т, в, р, н	**А**	л, н, с, т, р, в, к, м	12	88
80	20	я, е, у, и, а, о	**Б**	о, ы, е, а, р, у	81	19
68	32	я, т, а, е, и, о	**В**	о, а, и, ы, с, н, л, р	60	40
78	22	р, у, а, и, е, о	**Г**	о, а, р, л, и, в	69	31
72	28	р, я, у, а, и, е, о	**Д**	е, а, и, о, н, у, р, в	68	32
19	81	м, и, л, д, т, р, н	**Е**	н, т, р, с, л, в, м, и	12	88
83	17	р, е, и, а, у, о	**Ж**	е, и, д, а, н	71	29
89	11	о, е, а, и	**З**	а, н, в, о, м, д	51	49
27	73	р, т, м, и, о, л, н	**И**	с, н, в, и, е, м, к, з	25	75
55	45	ь, в, е, о, а, и, с	**К**	о, а, и, р, у, т, л, е	73	27
77	23	г, в, ы, и, е, о, а	**Л**	и, е, о, а, ь, я, ю, у	75	25
80	20	я, ы, а, и, е, о	**М**	и, е, о, у, а, н, п, ы	73	27

55	45	д, ь, н, о, а, и, е	**Н**	о, а, и, е, ы, н, у	80	20
11	89	р, п, к, в, т, н	**О**	в, с, т, р, и, д, н, м	15	85
65	35	в, с, у, а, и, е, о	**П**	о, р, е, а, у, и, л	68	32
55	45	и, к, т, а, п, о, е	**Р**	а, е, о, и, у, я ,ы, н	80	20
69	31	с, т, в, а, е, и, о	**С**	т, к, о, я, е, ь, с, н	32	68
57	43	ч, у, и, а, е, о, с	**Т**	о, а, е, и, ь, в, р, с	63	37
15	85	п, т, к, д, н, м, р	**У**	т, п, с, д, н, ю, ж	16	84
70	30	н, а, е, о, и	**Ф**	и, е, о, а, е, о, а	81	19
90	10	у, е, о, а, ы, и	**Х**	о, и, с, н, в, п, р	43	57
69	31	е, ю, н, а, и	**Ц**	и, е, а, ы	93	7
82	18	е, а, у, и, о	**Ч**	е, и, т, н	66	34
67	33	ь, у, ы, е, о, а, и, в	**Ш**	е, и, н, а, о, л	68	32
84	16	е, б, а, я, ю	**Щ**	е, и, а	97	3
0	100	м, р, т, с, б, в, н	**Ы**	л, х, е, м, и, в, с, н	56	44
0	100	н, с, т, л	**Ь**	н, к, в, п, с, е, о, и	24	76
14	86	с, ы, м, л, д, т, р, н	**Э**	н, т, р, с, к	0	100
58	42	ь, о, а, и, л, у	**Ю**	д, т, щ, ц, н, п	11	89
43	57	о, н, р, л, а, и, с	**Я**	в, с, т, п, д, к, м, л	16	84

Таблица 9. Сочетаемость букв английского языка

Г	С	Слева		Справа	Г	С
19	81	l,c,d,m,n,s,w,t,r,e,h	**A**	n,t,s,r,l,d,c,m	6	94
55	45	y,b,n,t,u,d,o,s,a,e	**B**	e,l,u,o,a,y,b,r	70	30
61	39	u,o,s,n,a,i,l,e	**C**	h,o,e,a,i,t,r,l,k	59	41
52	48	r,i,l,a,n,e	**D**	e,i,t,a,o,u	54	46
8	92	c,b,e,m,v,d,s,l,n,t,r,h	**E**	r,d,s,n,a,t,m,e,c,o	21	79
69	31	s,n,f,d,a,i,e,o	**F**	t,o,e,i,a,r,f,u	52	48
36	64	o,d,u,r,i,e,a,n	**G**	e.h.o.r.a.t.f.w.i.s	42	58
7	93	g,e,w,s,c,t	**H**	e,a,i,o	90	10
13	87	f,m,w,e,n,l,d,s,r,h,t	**I**	n,t,s,o,c,r,e,m,a,l	17	83
28	72	y,w,t,s,n,e,c,b,a,c	**J**	u,o,a,e,m,w	88	12
53	47	y,u,i,n,a,r,o,c	**К**	e,i,n,a,t,s	68	32
52	48	m,p,t,i,b,u,o,e,l,a	**L**	e,i,y,o,a,d,u	65	35
69	31	s,d,m,r,i,a,o,e	**M**	e,a,o,i,p,m	71	29
89	11	u,e,o,a,i	**N**	d,t,g,e,a,s,o,i,c	32	68
21	79	o,d,l,p,h,n,e,c,f,s,i,r,t	**O**	n,f,r,u,t,m,l,s,w,o	18	82
47	53	r,l,t,n,i,p,m,a,o,u,e,s	**P**	o,e,a,r,l,u,p,t,i,s	59	41
20	80	o,n,l,e,d,r,s	**Q**	u	100	0
70	30	p,i,u,t,a,o,e	**R**	e,o,a,t,i,s,y	61	39
48	52	d,t,o,u,r,n,s,i,a,e	**S**	t,e,o,i,s,a,h,p,u	41	59
43	57	u,o,d,t,f,e,i,n,s.a	**T**	h,i,o,e,a,t,r	38	62
35	65	p,f,t,l,b,d,s,o	**И**	n,s,t,r,l,p,b,c	8	92
88	12	r,u,o,a,i,e	**V**	e,i,o,a	99	1
48	52	g,d,y,n,s,t,o,e	**W**	a,h,i,e,o,n	80	20
95	5	u,n,i,e	**X**	p,t,i,a,u,c,k,o	38	62
24	76	b,n,a,t,e,r,l	**Y**	a,o,s,t,w,h,i,e,d,m	38	62
88	12	o,n,a,i	**Z**	e,i,w	86	14

При анализе сочетаемости букв друг с другом следует иметь в виду зависимость появления букв в открытом тексте от значительного числа предшествующих букв. Для анализа этих закономерностей используют понятие условной вероятности.

Систематически вопрос о зависимости букв алфавита в открытом тексте от предыдущих букв исследовался известным русским математиком А.А.Марковым (1856 — 1922). Он доказал, что появления букв в открытом тексте нельзя считать независимыми друг от друга. В связи с этим А. А. Марковым отмечена еще одна устойчивая закономерность открытых текстов, связанная с чередованием гласных и согласных букв. Им были подсчитаны частоты встречаемости биграмм вида гласная-гласная (*г,г*), гласная-согласная (*г,с*), согласная-гласная (*с,г*), согласная-согласная (*с,с*) в русском тексте длиной в 10^5 знаков. Результаты подсчета отражены в следующей таблице:

Таблица 10. Чередование гласных и согласных

	Г	С	Всего
Г	6588	38310	44898
С	38296	16806	55102

Пример решения:

Дан шифр-текст: СВПООЗЛУЙЬСТЬ_ЕДПСОКОКАЙЗО

Текст содержит 25 символов, что позволяет записать его в квадратную матрицу 5x5. Известно, что шифрование производилось по столбцам, следовательно, расшифрование следует проводить, меняя порядок столбцов.

С	В	П	О	О
З	Л	У	Й	Ь
С	Т	Ь	_	Е
Д	П	С	О	К
К	А	Й	З	О

Необходимо произвести анализ совместимости символов (Таблица сочетаемости букв русского и английского алфавита, а также таблицы частот биграмм представлена выше). В первом и третьем столбце сочетание СП является крайне маловероятным для русского языка, следовательно, такая последовательность столбцов быть не может. Рассмотрим другие запрещенные и маловероятные сочетания букв: ВП (2,3 столбцы), ПС (3,1 столбцы), ПВ (3,2 столбцы). Перебрав их все, получаем наиболее вероятные сочетания биграмм по столбцам:

В	О	С	П	О
Л	Ь	З	У	Й

Т	Е	С	Ь	_
П	О	Д	С	К
А	З	К	О	Й

Получаем осмысленный текст: ВОСПОЛЬЗУЙТЕСЬ_ПОДСКАЗКОЙ

Задание: Расшифровать фразу, зашифрованную столбцовой перестановкой.

1. ОКЕСНВРП_ЫРЕАДЕЫН_В_РСИКО
2. ДСЛИЕЗТЕА_Ь_ЛЬЮВМИ_ _АОЧХК
3. НМВИАИ_НЕВЕ_СМСТУОРДИАНКМ
4. ЕДСЗЬНДЕ_МУБД_УЭ_КРЗЕМНАЫ
5. СОНРЧОУО_ХДТ_ИЕИ_ВЗКАТРРИ
6. _ОНКА_БНЫЕЦВЛЕ_К_ТГОАНЕИР
7. НЗМАЕЕАА_Г_НОТВОССОТЬЯАЛС
8. РППОЕААДТВЛ_ЕББЛНЫЕ_ПА_ВР
9. ОПЗДЕП_ИХРДОТ_И_ВРИТЧ_САА
10. ВКЫОСИРЙУ_ОЬВНЕ_СОАПНИОТС
11. ПКТИРАОЛНАОИЧ_З_ЕСЬНЕЛНЖО
12. ИПКСОЕ_ТСМНАЧИ_ОЕН_ГДЕЛА_
13. АМВИННЬТЛЕАНЕ_ЙОВ_ОПХАРТО
14. АРЫКЗЫ_КЙТНЛ_ААЫ_ОЛБКЫТРТ
15. _ПАРИИВИАРЗ_БРА_ИСТЬЛТОЕК
16. П_ЛНАЭУВКАА_ЦИИВР_ОКЧЕДРО
17. ЖВНОАН_АТЗОЬСН_ЫО_ФВИИКИЗ
18. ОТВГОСЕЬЬТАДВ_С_ЬЗАТТЕЫАЧ
19. ЯАМРИТ_ДЖЕХ_СВЕД_ТСУВЕТНО
20. УЬБДТ_ОЕГТВ_ОЫКЭА_ВКАИУЦИ
21. ЛТБЕЧЛЖЫЕ_ _ОАПТЖРДУ_ЛМНОА
22. ИТПРКРФАГО_АВЯИА_ЯНЖУАКАН
23. ПКЕЕРРПО_ЙУСТ_ИТПСУТЛЯЕИН
24. ИЬЖЗНСД_ТДН_ЕТ_НУВЕУРЫГОЫ
25. ЕОУРВА_НЬРИАДИЦЕПИ_РНШВЫЕ

Шифр двойной перестановки

Пример решения:

Дан шифр-текст: ЫОЕЧТТОУ_СНСОРЧТРНАИДЬН_Е

Текст содержит 25 символов, что позволяет записать его в квадратную матрицу 5х5. известно, что шифрование производилось сначала по столбцам, а затем по строкам, следовательно, расшифрование следует проводить тем же способом.

Ы	О	Е	Ч	Т
Т	О	У	_	С
Н	С	О	Р	Ч
Т	Р	Н	А	И
Д	Ь	Н	_	Е

Производим анализ совместимости символов. Если в примере столбцовой перестановки можно было легко подобрать нужную комбинацию путем перебора, то здесь лучше воспользоваться таблицей частот букв русского языка (см. приложение). Для оптимизации скорости выполнения задания можно проверить все комбинации букв только в первой строке. Получаем ОЕ-15, ОЧ-12, ЕТ-33, ТЕ-31, ЧО-х, ЕО-7, ЧЫ-х, ОЫ-х, ТЫ-11, ТЧ-1, ЧЕ-23 (где х-запрещенная комбинация).

Из полученных результатов можно предположить следующую комбинацию замены столбцов **2 4 3 5 1:**

О	Ч	Е	Т	Ы
О	_	У	С	Т
С	Р	О	Ч	Н
Р	А	Н	И	Т
Ь	_	Н	Е	Д

Теперь необходимо переставить строки в нужном порядке. **3 2 4 5 1:**

С	Р	О	Ч	Н
О	_	У	С	Т

Р	А	Н	И	Т
Ь	_	Н	Е	Д
О	Ч	Е	Т	Ы

Получаем осмысленный текст: СРОЧНО_УСТРАНИТЬ_НЕДОЧЕТЫ

Задание: Расшифровать фразу, зашифрованную двойной перестановкой (сначала были переставлены столбцы, затем строки)

1. СЯСЕ_ _ЛУНЫИАККННОГЯДУЧАТН
2. МСЕЫ_ЛЫВЕНТОСАНТУЕИ_РЛПОБ
3. АМНРИД_УЕБСЫ_ЕЙРСООКОТНВ_
4. ОПЧУЛС_БООНЕВ_ОЖАЕОНЕЩЕИН
5. ЕШИАНИРЛППГЕЧАВРВ_СЕЫНА_ЛО
6. АРАВНРСВЕЕОАВ_ЗАНЯА_КМРЕИ
7. А_ЛТАВЙООЛСО_ТВ_ШЕЕНЕСТ_Ь
8. ФИ_ЗИММУЫНУУБК_Е_ДЬШЫИВЧУ
9. ВР_ЕСДЕИ_ТПХРОИ_ЗБУАДНУА_
10. ЦТААЙПЕЕ_ТБГУРРСВЬЕ_ОРЗВВ
11. АВАРНСЧАА_НЕДВЕДЕРПЕОЙ_ИС
12. ДОПК_СОПАЛЕЧНЛ_ГИНЙОИЖЕ_Т
13. ЛУАЗИЯНСА_ДТДЕАИ_ШРФЕОНГ_
14. С_ОЯНВ_СЬСЛААВРЧЕАРТОГДЕС
15. ЗШАФИПРАЛОЕНЖ_ОЬН_ДАРВОНА
16. КЭЕ_ТДУМБ_ЬСЗЕДНЕЗМАОР_ТУ
17. _ЕАЛЯРАНВЯАЧДА_ЕРПЕСАНВ_Ч
18. _И_ЕНТРЗИ_ОКЕВНОДЛЕША_ИМП
19. РОБДОЕВПС_МСХЬА_ _ИВПСНИОТ
20. ЕСДНОГТЕАНН_НЕОВМР_ЕУНПТЕ
21. _ЙЕСТОВО_НИИНЛАЕТИЖДСОПВ_
22. НДИАЕОЫЛППНЕ_ _НВЕАНГТ_ИЗЛА
23. П_БИРДЛЬНЕВ_ОП_ОПЗДЕВЫГЕА
24. МДООИТЕЬ_СМТ_НАДТЕСУБЕХНО
25. АИНАЛЖНОЛЕШФ_ЗИ_УАРОЬСНЕ_

Шифр простой замены

Криптоанализ шифра простой замены основан на использовании статистических закономерностей языка. Так, например, известно, что в русском языке частоты букв распределены следующим образом:

Таблица 9. Частоты букв русского языка
(в 32-буквенном алфавите со знаком пробела)

- 0,175	О 0,090	Е,Ё 0,072	А 0,062
И 0,062	Т 0,053	Н 0,053	С 0,045
Р 0,040	В 0,038	Л 0,035	К 0,028
М 0,026	Д 0,025	П 0,023	У 0,021
Я 0,018	Ы 0,016	З 0,016	Ь,Ъ 0,014
Б 0,014	Г 0,013	Ч 0,012	Й 0,010
Х 0,009	Ж 0,007	Ю 0,006	Ш 0,006
Ц 0,004	Щ 0,003	Э 0,003	Ф 0,002

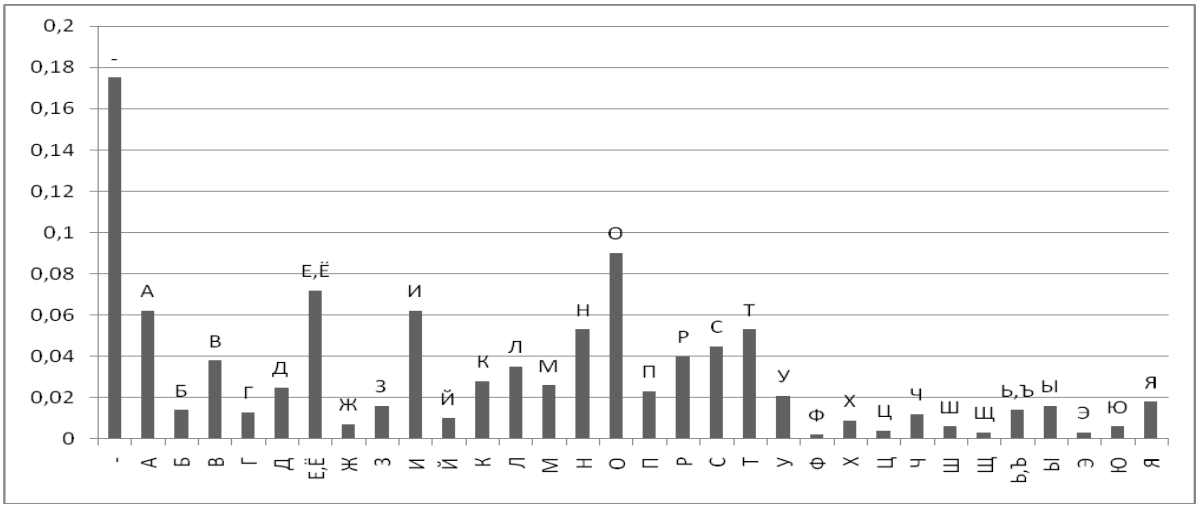


Рис. 22. Диаграмма частот букв русского языка

Для получения более точных сведений об открытых текстах можно строить и анализировать таблицы k-грамм при k>2, однако для учебных целей вполне достаточно ограничиться биграммами. Неравновероятность k -грамм (и даже слов) тесно связана с характерной особенностью открытого текста – наличием в нем большого числа повторений отдельных фрагментов текста: корней, окончаний, суффиксов, слов и фраз. Так, для русского языка такими привычными фрагментами являются наиболее частые биграммы и триграммы:

	А	Б	В	Г	Д	Е	Ж	З	И	И	К	Л	М	Н	О	П
А	2	12	35	8	14	7	6	15	7	7	19	27	19	45	3	11
Б	5					9	1		6			6		2	21	
В	35	1	5	3	3	32		2	17		7	10	3	9	58	6
Г	7				3	3			5		1	5		1	50	
Д	25		3	1	1	29	1	1	13		1	5	1	13	22	3
Е	2	9	18	11	27	7	5	10	6	15	13	35	24	63	7	16
Ж	5	1			6	12			5					6		
З	35	1	7	1	5	3			4		2	1	2	9	9	1
И	4	6	22	5	10	21	2	23	19	11	19	21	20	32	8	13
И	1	1	4	1	3		1	2	4		5	1	2	7	9	7
К	24	1	4	1		4	1	1	26		1	4	1	2	66	2
Л	25	1	1	1	1	33	2	1	36		1	2	1	8	30	2
М	18	2	4	1	1	21	1	2	23		3	1	3	7	19	5
Н	54	1	2	3	3	34			58		3		1	24	67	2
О	1	28	84	32	47	15	7	18	12	29	19	41	38	30	9	18
П	7					15			4			9		1	46	

СТ, НО, ЕН, ТО, НА, ОВ, НИ, РА, ВО, КО,

СТО, ЕНО, НОВ, ТОВ, ОВО, ОВА

Полезной является информация о сочетаемости букв, то есть о предпочтительных связях букв друг с другом, которую легко извлечь из таблиц частот биграмм.

Имеется в виду таблица, в которой слева и справа от каждой буквы расположены наиболее предпочтительные "соседи" (в порядке убывания частоты соответствующих биграмм). В таких таблицах обычно указывается также доля гласных и согласных букв (в процентах), предшествующих (или следующих за) данной букве.

Пример криптоанализа шифра замены

Известно, что зашифровано стихотворение Р. Киплинга в переводе С.Я. Маршака. Шифрование заключалось в замене каждой буквы на двузначное число. Отдельные слова разделены несколькими пробелами, знаки препинания сохранены. Таблица частот букв русского языка приведена выше.

29 15 10 17 29 22 25 31 15 33 35 41 43 45 35 57 45 25 17 59 15 10 25 41 25 69, 59 78 29 82 25 78 25 17 15 10 88 90 78 25 62 25 22 10 57 73 79 35 67 78 90 88 29 45 35 29, 54 57 90 31 90 73 22 88 15 88 29 15 17 69 41 25 15, 70 17 90 57 43 59 15 78 15 62 22 25 17 57 25 69 88 15 82 17 25 88 29 45 35…

Подсчитаем частоты шифрообразований:

Обозначение	9	5	0	7	2	5	1	3	5	1	3	45	7
Количество		0				2						4	

Обозначение	9	9	8	2	8	0	2	3	9	7	4	70
Количество												1

Из таблица частот букв русского языка видно, что чаще всего встречается буква О, на втором месте Е. В нашем шифр-тексте чаще всего встречается обозначение 25 (12 раз), на втором месте идет обозначение 15 (10 раз), остальные обозначения им существенно уступают. Поэтому можем выдвинуть гипотезу: 25=О, 15=Е. Однако, текст у нас не очень большой, поэтому закономерности русского языка проявляются в нем не обязательно в строгом соответствии с таблицей частот букв русского языка. Поэтому возможен и вариант: 25=Е, 15=О. Но тогда последнее слово в третьей строке имеет окончание ЕО, что возможно, но все же более вероятный вариант ОЕ. Итак, будем работать с текстом, считая, что 25=О, 15=Е.

Теперь нам поможет знак препинания: «29, …». Крайне маловероятно, чтобы запятая стояла после согласной. Итак, 29 – гласная, причем вероятнее всего 29=И или 29=А, т.к. гласные Я, Ю, Э, У встречаются в осмысленных текстах на русском языке намного реже, чем И и А, что не противоречит таблице частот шифр-текста.

В последней строке: 88 15, но 15=Е, следовательно, 88 – согласная, причем наиболее вероятные значения – это Н и Т. Итак, 25=О, 15=Е, 29=А $\begin{pmatrix} А \\ И \end{pmatrix}$, 88=$\begin{pmatrix} Н \\ Т \end{pmatrix}$. Теперь третье слово в третьей строке имеет 4 варианта:

- 29=И, 88=Н: 22 Н Е Н И Е
- 29=И, 88=Т: 22 Т Е Т И Е
- 29=А, 88=Н: 22 Н Е Н А Е
- 29=А, 88=Т: 22 Т Е Т А Е

Из рассмотренных вариантов лишь один является осмысленным, и он позволяет найти значение 22. Имеем: 22=М и третье слово в третье строке М Н Е Н И Е.

Теперь рассмотрим второе слово в первой строке. Е 10 17 И, причем 10 и 17 – согласные, и это не М и не Н. Наиболее вероятное слово Е С Л И, т.е. 10=С, 17=Л. Конечно, если мы, продолжая работать с текстом, вдруг получим «нечитаемое» слово, то придется вернуться к этому этапу и рассмотреть другие варианты. Однако, это маловероятно, поскольку вряд ли в стихотворении были слова наподобие Е Р Т И, Е В Л И и т.п.

Далее, первое слово второй строки: 59 78 И, причем 59 и 78 – согласные, и это не С, не Л, не М и не Н. Так что это слово П Р И, т.е. 59=П, 78=Р. Тогда шестое слово первой строки 45 О Л П Е, что дает значение 45=Т и тогда при 57=В получаем фрагмент «…В Т О Л П Е…». Также второе слово последней строки П Е Р Е 62 дает нам значение 62=Д.

Далее рассмотрим начало второй строки: «П Р И 82 О Р О Л Е С Н 90 Р О Д О М …». Из него следует, что 82=К и 90=А.

Зная, что 82=К, посмотрим на самое последнее слово К Л О Н И Т 35, откуда станет ясно, что 35=Ь.

Перед последней атакой выпишем текст, заменяя известные обозначения буквами.

И Е С Л И М О 31 Е 33 Ь 41 43 Т Ь В Т О Л П Е С О 41 О 69,
П Р И К О Р О Л Е С Н А Р О Д О М С В 73 79 Ь 67 Р А Н И Т Ь
И, 54 В А 31 А 73 М Н Е Н И Е Л 69 41 О Е,
70 Л А В 43 П Е Р Е Д М О Л В О 69 Н Е К Л О Н И Т Ь…

Из последней строки: 69=Ю, тогда слова Л Ю 41 О Е и С О 41 О Ю определяют 41: 41=Б. Теперь из четвертого слова первой строки Б 43 Т Ь получаем, что 43=Ы. А первое слово из последней строки 70 Л А В Ы – это Г Л А В Ы. Слово в первой строке М О 31 Е 33 Ь угадывается из контекста: М О Ж Е Ш Ь, т.е. 31=Ж, 33=Ш. Теперь второе слово в третьей строке запишется как 54 В А Ж А 73, откуда, с учетом контекста: 54=У, 73=Я. После этого окончание второй строки имеет вид «… С В Я 79 Ь 67 Р А Н И Т Ь». Легко определяются буквы 79=З, 67=Х.

Ответ: И Е С Л И М О Ж Е Ш Ь Б Ы Т Ь В Т О Л П Е С О Б О Ю,
П Р И К О Р О Л Е С Н А Р О Д О М С В Я З Ь Х Р А Н И Т Ь
И, У В А Ж А Я М Н Е Н И Е Л Ю Б О Е,
Г Л А В Ы П Е Р Е Д М О Л В О Ю Н Е К Л О Н И Т Ь…

Задания: Расшифровать текст. Каждой букве алфавита соответствует двузначное число.

1.

58 62 32 39 99 31 29 58 72 62 99 58 13 54 15 56 31 63 39 72 84 15 13 56 77 15 82 56 56 56 58 54 29 77 56 – 39 99 56 31 56 7732 12 15 54 31 48 7663 15 52 13 39 72 39 5416 72 39 32 72 62 58 58 15,37 62 7752 39 13 39 72 39 32 3931 62 54 39 77 84 39 21 31 3916 72 62 99 58 13 15 54 56 13 4616 39 58 13 95 16 15 13 62 12 46 31 39 6272 15 77 54 56 13 56 6284 31 39 32 56 7658 63 62 7233 62 12 39 54 62 33 62 58 52 39 9199 62 29 13 62 12 46 31 39 58 13 56.56 31 63 39 72 84 15 82 56 39 31 31 48 6213 62 76 31 39 12 39 32 56 5616 72 39 33 31 3954 39 53 12 565437 56 77 31 62 58,39 37 72 15 77 39 54 15 31 56 62,16 72 39 56 77 54 39 99 58 13 54 39,39 13 52 72 48 5433 62 12 39 54 62 52 9531 62 37 48 54 15 12 48 6254 39 77 84 39 21 31 39 58 13 5616 3958 52 39 72 39 58 13 5616 39 12 95 33 62 31 56 295639 37 72 15 37 39 13 52 6256 31 63 39 72 84 15 82 56 56,1513 15 52 21 6216 3915 54 13 39 84 15 13 56 77 15 82 56 5616 72 39 56 77 54 39 99 58 13 54 62 31 31 48 76,95 16 72 15 54 12 62 31 33 62 58 52 56 765656 31 48 76 16 72 39 82 62 58 58 39 54.

2.

3925 20 34 82 6366 46 35 20 25 828639 51 74 35 51 66 20 4437 25 27 51 35 44 20 90 37 51 25 25 51 6391 20 11 37 46 4825 20 37 61 51 14 82 8266 82 35 29 82 91 25 5174 51 24 78 51 24 59 46 86 51 44 74 20 25 37 37,37 44 82 31 11 37 82 51 46 25 51 34 82 25 37 828637 25 27 51 35 44 20 90 37 51 25 25 48 4446 82 78 25 51 14 51 18 37 59 44,51 74 82 35 20 90 37 59 446690 82 25 25 48 44 3761 10 44 20 18 20 44 37,8661 20 25 86 51 39 66 86 51 44 1066 82 86 46 51 35 10 3766 51 46 51 39 51 6366

39 59 91 37.56 46 51 86 20 66 20 82 46 66 5924 35 10 18 37 7851 35 18 20 25 37 91 20 90 37 63,4651,66 51 18 14 20 66 25 5135 82 91 10 14 29 46 20 46 20 4435 20 91 14 37 56 25 48 7837 66 66 14 82 24 51 39 20 25 37 63, 35 10 86 51 39 51 24 37 46 82 14 3744 25 51 18 37 7837 9125 37 7891 25 20 31 4651 61 51 66 25 51 39 25 48 7839 37 24 20 78 10 18 35 51 91,25 5125 82 10 24 82 14 59 31 4624 51 14 42 25 51 18 5139 25 37 44 20 25 37 5924 20 25 25 48 4439 51 74 35 5166 20 44,66 56 37 46 20 59,56 46 5151 61 82 66 74 82 56 82 25 37 8237 25 27 51 35 44 20 90 37 51 25 25 51 6361 82 91 51 74 20 66 25 51 66 46 3725 8237 44 82 82 4666 44 48 66 14 20,82 66 14 3751 46 66 10 46 66 46 39 10 82 4639 37 24 37 44 20 5910 18 35 51 91 20.

3.

74 29 23 27 17 99 71 254932 29 34 27 63 32 25 17 99 60 62 25 34 95 29 53 59 82 27 71 29 77 99 34 27 91 17 99 71 49 99 27 15 60 32 25 50 27 17 62 27 95 27 50 25 91 32 59 77 95 29 50 25 99 59,25 99 74 29 53 25 59 17 99 25 91 23 49 71 25 17 99 604925 34 32 25 71 95 27 82 27 32 32 2529 50 17 25 15 77 99 32 59 7762 95 25 53 95 29 23 32 25 17 99 60 34 15 35 17 27 99 27 71 25 12 2599 95 29 45 49 74 29. 62 95 27 63 34 2771 17 27 12 25,50 27 17 62 27 95 27 50 25 91 32 29 3595 29 50 25 99 29 17 29 82 49 8362 2517 27 50 2762 95 25 34 59 74 99 25 7150 27 53 25 62 29 17 32 25 17 99 4917 71 35 53 29 32 2917 32 29 15 49 23 49 27 8232 29 34 27 63 32 2595 29 50 25 99 29 77 10 27 12 2525 50 25 95 59 34 25 71 29 32 49 3549 95 27 53 27 95 71 49 95 25 71 29 32 49 27 8274 95 49 99 49 23 32 89 837425 99 74 29 53 5950 15 25 74 25 7162 49 99 29 32 49 354953 29 62 25 82 49 32 29 77 10 49 8359 17 99 95 25 91 17 99 71.34 15 3562 25 17 15 27 34 32 49 8325 62 99 49 82 29 15 60 32 2562 95 49 82 27 32 27 32 49 2734 49 17 74 25 71 89 8382 29 17 17 49 71 25 7112 25 95 35 23 27 9153 29 82 27 32 89.74 29 23 27 17 99 71 25 49 32 29 34 27 63 32 25 17 99 60 95 29 50 25 99 8934 25 17 99 49 12 29 27 99 17 3525 62 99 49 82 49 53 29 67 49 27 9162 95 25 12 95 29 82 82 32 25 12 2525 50 27 17 62 27 23 27 32 49 35.

4.

48 2318 40 94 35 62 53 94 25 53 15 3591 35 40 35, 52 23 5253 40 3594 35 40 2394 23 91 52 94 49 24 23 84 8994 23 64 55 53 15 18 53 91, 24 53 88 23 62 12 25 7694 2364 35 24 49, 35 9449 88 5348 94 23 24,41 91 3591 23 5231 49 15 53 91. 47 91 3541 49 62 84 91 62 3535 91 41 23 84 91 2531 29 24 3564 35 27 35 88 5394 2391 35,52 35 91 35 55 35 5335 9425 84 64 29 91 23 24,52 35 40 15 2348 23 62 53 55 94 49 2448 2349 40 35 242541 49 91 8994 5394 23 24 53 91 53 24 94 2315 53 62 49 12 52 49,12 53 15 12 49 6053 18 4994 23 62 84 91 55 53 41 49.53 40 3594 35 40 23,62 29 48 62 23 6284 62 35 25 1815 62 25 88 53 94 25 53 18 52 35 24 53 31 23 94 25 53 62 35 48 15 49 27 23,64 35 24 49 41 25 24 23 35 91 55 23 88 53 94 94 29 7684 25 40 94 23 243564 55 53 64 38 91 84 91 62 25 2594 2364 49 91 25 2564 35 41 91 256291 4988 5384 53 52 49 94 15 4949 15 23 55 25 24 23 84 8935 31 3541

91 35 – 91 35.52 23 52 35 76-91 3564 55 53 15 18 53 918440 24 49 27 25 1884 91 49 52 35 1835 91 24 53 91 53 246291 53 18 94 35 91 49.

5.

79 6131 96 28 35 85 5226 30 24 21 52 85 59 49 79 30 88 7949 30 52 79 59 85 26 30 24 21 59 85 42 79 88 61 28 35 86 5096 28 52 30 50,24 30 96 74 21 59 9059 30 96 30 24 85 61 8626 96 85 88 79 96 79 24 61 79 1128 52 79 78 31 85, - 21 50 30 96 85 31 21 61 59 31 85 1126 79 24 96 79 59 35 79 31 5996 30 31 52 21 50 61 79 1131 21 96 35 85 61 31 85,2126 79 78 30 50 2867 868561 30 35:35 79 24 2467 79 28 24 30 61,35 96 85 61 21 24 69 21 35 9052 30 35,61 79 96 50 21 52 90 61 86 1196 79 59 35,42 24 79 96 79 49 86 1149 30 59,49 79 52 79 59 8669 49 30 35 2159 26 30 52 79 1126 46 30 61 85 69 86,88 79 52 28 67 86 3088 52 21 42 21,96 79 49 61 86 3067 30 52 86 3042 28 67 86,42 21 88 79 96 30 52 79 3052 85 69 79,61 3085 59 26 79 96 78 30 61 61 79 3024 21 74 3061 21 50 30 31 79 5061 2149 79 42 96 21 59 35 61 86 30 26 96 86 29 85 31 85..

6.

56 27 54 54 27 56 51 32 82 16 63 49 27 63 11 30 73 35 23 54 89 70 27 63 27 493270 35 16 97 82 16 67 73 27 51 30 56 32 6370 29 63 27 49 32 73 29 5473 2748 29 13 29 82 56 82 27 9554 27 35 27 18 51 29,97 56 2770 29 63 305151 35 15 63 89 48 16.16 63 15 11 51 3082 2949 65 27 54 32 63 304929 61 2763 32 48 30-27 56 51 35 15 56 30 233227 11 70 27 35 27 18 32 56 29 63 89 82 30 23,27 82 3051 30 5111 1573 35 29 54 70 27 49 65 32 38 30 63 3073 35 32 23 56 82 16 6770 49 56 35 29 97 16.82 27 49 51 27 1351 29 54 3027 8227 73 16 49 56 32 6370 29 63 27 49 32 73 29 54 82 15 9516 73 27 353270 15 56 30 38 32 6332 92-73 27 5411 30 61 30 18 82 32 51 3049 63 27 18 29 82 82 16 67 61 30 92 29 56 16.27 8249 16 82 16 6361 30 92 29 56 1673 27 5413 15 24 51 163270 92 27 24 29 6373 2749 56 16 73 29 82 89 51 30 13.

7.

3428 68 91 1383 10 65 27 6849 10 26 65 27 68 75 26 39 785375 83 53 18 26 36 62 91.26 10 74 53 1349 10 83 10 65 5353 36 68 72 28 1028 13 18 86 10 27 53 75 3983 6857 26 18 10 91535736 53 6528 68 91 10,83 68 75 27 1334 13 24 13 18 53 36 74 5336 10 74 10 36 57 36 13,83 68 74 1091 10 91 1036 1368 26 74 18 62 34 10 27 1036 10 75 26 13 86 3968 74 36 10.83 18 10 34 28 10,26 57 2650 62 27 6883 68 65 57 86 13.26 57 2649 10 83 10 65 5334 19 13 27 53 75 395334 75 1375 68 50 68 1583 18 68 83 53 26 10 27 53.49 10 83 10 65 5310 27 74 68 72 68 27 44,83 68 28 72 68 18 13 34 80 13 72 6891 10 75 27 10,83 68 26 10,75 26 10 18 68 1568 28 13 86 28 625313 96 1327 13 74 10 18 75 26 34-91 13 36 26 68 27 1053,74 10 86 13 26 75 44,34 10 27 13 18 39 44 36 74 53.3483 18 53 65 68 86 13 15 26 13 91 36 68 26 53 96 10,5318 44 28 68 9123 26 68 2628 78 75 75 10 36 28 13 18-34 26 44

36 57 2772 68 27 68 34 573434 68 18 68 26,23 26 10 74 53 1572 18 53 47 – 75 26 13 18 34 44 26 36 53 74,86 28 57 96 53 15,74 68 72 28 1018 10 36 13 36 68 1386 53 34 68 26 36 68 1353 75 83 57 75 26 53 2628 57 65.

8.

45 34 26 34 9777 34 47 49 67 14 22 49 6747 34 49 39 77 6953 89 26 1097 10 49 10 77 45 53 31 10 14 10 47 22.17 90 56 14 34 77 67 49,49 67 75 49 1053 14 5349 26 90 47 10,77 3439 47 56 34 3156 26 67 52 34 13 10 84 22 5377 34 47 49 67 14 22 49 67 28 34 84 26 67 31,67 49 10 97 90 31 10 14 53 47 223128 70 89 49 53 9314 10 56 10 9356 47 10,5345 34 84 90 26 34 93 69 58 37 28 67 31 10 7047 84 10 14 22 77 10 7053 89 14 10,31 90 47 39 77 39 31 75 53 47 22,47 14 67 31 77 6713 10 14 67,53 9734 89 6728 67 26 69 90,31 56 26 90 47 49 53 31 10 14 1013 34 26 84 31 3453 97 26 70 69 77 39 5869 67 97 39 28 67 26 24 53 70,53 14 5356 26 67 49 10 53 77 10.97 10 84 34 2839 52 53 84 67 89 6797 31 34 26 22 49 1052 26 67 47 10 14 533156 34 45 2269 14 7047 13 53 89 10 77 53 7028 39 47 67 26 10,5353 89 26 1077 10 45 53 77 10 14 10 47 2247 77 67 31 10.

9.

81 49 86 49 1273 92 5081 50 15 5062 47 4915 56 50 51 7673 33 94 7615 94 65 81 47 76.94 76 47 49 81 47 76,15 7662 47 76 2628 16 5162 76 2628 76 51 70 58 76 2673 86 65 84 76 94,47 7615 94 65 81 47 7615 56 50 51 76.24 16 51 7062 76 49 2694 76 86 76 28 94 3362 49 47 1765 84 4915 76 92 15 49 6247 4924 86 49 51 70 96 50 51 50.56 76 31 73 5047 49 62 47 76 31 7624 76 73 65 62 50 513386 49 58 33 5115 56 50 567 065 62 47 16 62.47 65,47 50 73 7684 4943 76 56 7081 56 76-56 7673 49 51 50 56 70…1724 76 58 49 519294 76 51 51 49 73 84.76 94 50 12 50 92 58 33 15 709294 50 28 33 47 49 56 496586 49 94 56 76 86 50,1773 49 86 84 50 51 15 1765 92 49 86 49 47 47 76.86 49 94 56 76 86 76 6228 16 51 5062 76 51 76 73 50 1784 49 47 96 33 47 5028 50 51 70 12 50 94 76 92 15 94 76 31 7692 76 12 86 50 15 56 50.94 76 31 73 501792 76 58 49 51,76 47 5081 56 76-56 7615 76 15 86 49 73 76 56 76 81 49 47 47 7624 33 15 50 51 50,62 76 84 49 5647 76 92 16 2665 94 50 12.

10.

2043 40 13 15 91 31 5475 31 91 12.88 56,88 40 29 1571 3113 15 91 1249 91 15 – 91 1529 31 54 40 91 12…1715 61 69 31 44,2075 15 36 31 546275 25 15 29 84 65 31 25 56.90 4415 62 40 43 40 54 65 2088 31 17 58 65 15 62 90 2690,75 15-17 90 29 90 44 15 44 56,88 31 29 40 54 31 62 90 2649 31 54 15 17 31 621791 31 44 88 58 1315 49 62 40 13901725 15 43 15 17 15 4436 40 25 34 90 62 3188 4036 31 31.15 8862 56 25 90 5449 91 15-91 1515 49 31 88 1275 25 15 91 90 17 88 1575 40 13 88 56 69 31 31.29 40 71 3117 15 88 20 84 69 31 31.56 17 90 29 31 1744 31 88 20,75 25 15 29 84 65 31 2588 31 65 62 15 54 12 62 1544 90 88 56 9175 15 44 56 49 40 54 65 20,17 65 91 40 17 54 20 2015 91

17 90 65 36 56 8449 31 54 84 65 91 1288 4044 31 65 91 15,88 1517 65 3171 3117 43 20 5465 31 61 201725 56 62 90,43 40 91 56 36 90 5465 90 52 40 25 31 91 569043 40 52 15 17 15 25 90 54.

11.

65 27,67 40 58 34 11 4727 4227 45 82 34 11 14 4914 89 95 47.65 14 90 36 89 3434 67 36 90 36 45 67 11 36 65 65 34 89 34,11 17 82 34 67 1924 3495 40 45 17 34 45 82 36 24 65 14 7025 36 82 34 90 36 73.70 34 67 4945 67 95 40 65 40,17 34 45 95 36 24 1458 34 67 34 95 34 7334 65 1445 36 73 90 40 4517 95 36 59 47 11 40 82 14,24 40 11 65 341465 40 24 36 42 65 3417 34 24 25 49 67 4040 25 36 95 14 58 34 45 40 25 14,69 67 3411 45 3642 3645 27 11 36 95 36 65 65 40 4924 36 95 42 40 11 40,90 82 36 6534 34 65,4558 34 36 7345 34 11 36 67 45 58 14 7345 34 31 6317 34 24 24 36 95 42 14 11 40 36 6765 34 95 25 40 82 19 65 47 3624 14 17 82 34 25 40 67 14 90 36 45 58 14 3634 67 65 34 32 36 65 14 49,17 34 65 36 25 65 34 89 2765 40 82 40 42 14 11 40 36 6767 34 95 89 34 11 82 31,17 95 14 45 47 82 40 36 6765 4089 40 45 67 95 34 82 1459 40 82 36 67 65 47 3667 95 27 17 17 471434 59 25 36 65 14 11 40 36 67 45 4917 95 34 18 45 34 31 63 65 47 25 1424 36 82 36 89 40 56 14 49 25 14.4017 34 67 34 25 2763 24 36 45 1965 14 58 40 5865 3617 34 82 40 89 40 36 67 45 4965 36 82 36 89 40 82 19 65 3417 95 36 59 47 11 40 67 1945 34 11 36 67 45 58 14 2559 34 36 11 47 2517 82 34 11 56 40 25,“25 34 95 45 58 14 2524 19 49 11 34 82 40 25”.36 42 36 82 1490 67 34-45 58 40 65 24 40 8295 40 63 89 34 95 14 67 45 4917 3417 34 82 65 34 73…

12.

14 701465 3659 47 82 34,4058 40 5842 36.17 95 34 45 67 34-65 40 17 95 34 45 67 3432 36 45 67 36 95 3425 27 42 14 58 34 11,65 4011 14 24-45 67 40 65 24 40 95 67 65 47 3636 11 95 34 17 36 34 14 24 47,4563 40 17 40 24 65 34 89 36 95 25 40 65 45 58 14 25 1440 11 67 34 25 40 67 40 25 14,14 67 40 82 19 49 65 45 58 14 25 1440 58 11 40 82 40 65 89 40 25 14,32 11 36 24 45 58 14 25 1459 40 63 27 58 40 25 14,59 36 82 19 89 14 73 45 58 14 25 1425 14 65 40 25 14,18 95 40 65 56 27 63 45 58 14 25 1445 14 89 40 95 36 67 40 25 141432 11 36 73 56 40 95 45 58 14 25 1490 40 45 40 25 14.17 95 36 24 25 36 67 4745 65 40 95 49 42 36 65 14 49,11 63 49 67 47 3617 3434 67 24 36 82 19 65 34 45 67 14,25 34 42 65 3459 36 6334 45 34 59 47 7070 82 34 17 34 6717 95 14 34 59 95 36 45 67 141195 40 63 65 47 7058 34 65 56 40 7036 11 95 34 17 4758 40 5882 36 89 40 82 19 65 34,67 40 581465 4090 36 95 65 34 2595 47 65 58 36-58 40 58,45 34 59 45 67 11 36 65 65 34,1417 95 34 14 63 34 32 82 3467 95 27 24 40 25 1465 36 11 36 24 34 25 47 7025 40 63 27 95 27“14 65 67 36 65 24 40 65 67 34 11”.

13.

60 46 5746 52,28 15 57 3912 32 60 32 3246 5752 55 30 12 61 11 55 57 32 12 41,37 46 60 37 32 9152 32 11 55 12 32 75 4646 5730 32 20 15 75 46 25 99 20 52 32 52 52 4667 55 25 55 12 12 32 12 39 52 19 63“52 99 57 32 36”75 46 12 61 28 75 99(18 32 37 57 3952 99 57 32 3667 46 60 32 25 63 159991 32 57 25 46 60 46 3660 19 37 46 57 19“37 67 99 25 55 12 3930 25 15 52 46 ”67 4620 32 91 12 32).57 5537 55 91 55 4167 57 99 28 75 55.75 25 55 37 55 60 32 74,37 57 46 99 5767 25 99 20 52 55 57 39,99 20 41 45 52 19 36,11 12 99 52 52 46 75 25 19 12 19 36,37 15 67 32 25 55 29 25 46 11 99 52 55 91 99 28 32 37 75 99 36,60 19 37 46 57 52 19 36.“11 48 99 – 29 25 – 11 60 32 52 55 11 74 55 57 39”,52 46 60 32 36 18 99 3637 55 91 46 12 32 5729 12 32 75 57 25 46 52 52 46 3625 55 20 60 32 11 75 99,46 37 52 55 45 32 52 52 19 3655 67 67 55 25 55 57 15 25 46 36,78 46 25 11 4699 91 32 52 15 32 91 46 36“57 32 63 52 99 75 46 3611 60 55 11 74 55 57 3967 32 25 60 46 78 4660 32 75 55”(63 46 57 4111 4675 46 52 74 5511 60 55 11 74 55 57 46 78 4637 57 46 12 32 57 99 41,37 46 78 12 55 37 52 4663 25 46 52 46 12 46 78 99 99,46 37 57 55 12 46 37 3932 45 3267 41 57 52 55 11 74 55 57 393712 99 18 52 99 9112 32 57)…

14.

15 48 3252 326067 32 25 60 19 3625 55 2091 55 20 15 25 1567 25 99 63 46 11 99 12 466078 46 12 46 60 15,28 57 4628 99 52,46 57 60 32 28 55 60 18 99 3620 5530 32 20 46 67 55 37 52 46 37 57 3930 55 20 19,30 19 12 75 12 55 37 37 99 28 32 37 75 99 9137 15 63 46 67 15 57 28 99 75 46 91. 60 37 60 46 3260 25 32 91 4146 52 67 46 25 55 30 46 57 55 12 52 55 37 46 60 32 37 57 39,46 30 46 25 15 11 46 60 55 60 37 15 63 46 67 15 57 52 19 3267 46 11 37 57 15 67 197530 55 20 3232 91 75 46 37 57 52 19 91 9911 55 57 28 99 75 55 91 99,37 99 78 52 55 12 39 52 19 91 9925 55 75 32 57 55 91 99,67 25 9991 55 12 32 36 18 32 9167 25 99 75 46 37 52 46 60 32 52 99 997557 46 52 61 37 32 52 39 75 46 3652 99 57 9960 20 12 32 57 55 60 18 99 91 996052 32 30 32 37 5537 4637 60 99 37 57 46 91,25 55 37 37 19 67 55 4160 46 25 46 63 5525 55 20 52 46 74 60 32 57 52 19 6346 37 12 32 67 99 57 32 12 39 52 19 6399 37 75 25-9911 55 48 3267 46 12 46 37 55 91 9967 25 46 57 99 60 46 67 32 63 46 57 52 19 6391 99 52.28 57 46 75 55 37 55 32 57 37 4167 46 11 37 57 15 67 46 6060 46 11 52 19 63,28 99 5230 19 1252 3257 55 7525 32 57 99 60. 46 11 52 9957 46 12 39 75 4637 57 46 12 30 193775 46 12 61 28 75 46 369967 25 32 37 12 46 60 15 57 19 32“37 67 99 25 55 12 39 75 99”-75 46 57 46 25 19 3252 32 20 60 55 52 19 3278 46 37 57 99,6046 57 12 99 28 99 3246 5720 11 32 18 52 99 6367 55 25 57 99 20 55 52,15 91 32 12 9967 25 32 46 11 46 12 32 60 55 57 3930 19 37 57 25 469930 32 2091 55 12 32 36 18 32 78 4660 25 32 11 5511 12 4137 46 30 37 57 60 32 52 52 46 78 4646 25 78 55 52 99 20 91 55.9960 37 32.

15.

45 74 5431 10 26 38 23 74,86 74 5425 89 26 38 16 74 7475 1645 56 90 25 86 90 75 90 10 2616 74 23 56 86 75 45 16 75 7495 10 13 31 95 10 51 74 16 89 74,36 75 95 75 5936 74 95 74 91 75 31 89 90

23 74 749036 95 89 26 89 90 8313 26 75 25 86 89-75 86 86 75 47 75,45 86 7575 16 8945 74 86 90 74 95 7525 56 86 75 33,75 29 95 10 86 89 90 23 89 25 389013 95 74 16 89 748925 26 56 91,86 75 95 45 10 26 899045 10 19 75 29 74,33 10 3331 89 33 89 7475 29 74 13 38 42 16 8389 1329 95 10 13 89 26 89 89,75 86 86 75 47 75,45 86 7536 75 31 90 74 95 16 56 26 25 4286 56 36 75 4633 10 46 54 10 16,2575 31 89 16 10 33 75 90 83 5456 25 74 95 31 89 74 5416 10 36 10 31 10 90 23 89 468916 1026 74 25 16 56 5925 90 89 16 38 59,8916 1075 86 26 89 45 16 75 47 7536 10 95 16 422531 95 56 47 75 47 7533 75 16 86 89 16 74 16 86 10.109021 86 7590 95 74 54 4286 74,16 1029 10 13 74,51 89 26 899025 90 75 7456 31 75 90 75 26 38 25 86 90 89 74,25 36 10 26 8916 1045 89 25 86 74 16 38 33 89 9136 95 75 25 86 83 16 33 10 919033 75 16 31 89 17 89 75 16 89 95 75 90 10 16 16 75 4636 95 75 91 26 10 31 74,36 95 89 16 89 54 10 26 8931 56 23,51 95 10 26 8916 1013 10 90 86 95 10 3367 95 56 33 86 83,31 51 74 548929 89 67 23 86 74 33 25 839086 95 8936 10 26 38 17 1086 75 26 19 89 16 75 46-8975 33 16 1086 10 3356 59 86 16 7525 90 74 86 89 26 89 25 38,8954 56 13 83 33 1089 47 95 10 26 10,8967 56 86 29 75 26 36 75 86 74 26 74 90 89 13 75 95 56…

16 89 45 74 47 75 9021 86 75 4 613 26 75 25 86 8916 7429 83 26 7536 26 75 91 75 47 75,16 10 75 29 75 95 75 86-86 10 33 75 4616 10 25 86 95 75 4633 10 3395 10 138936 95 89 31 10 74 8629 75 74 90 75 47 7533 56 95 10 51 10…

1036 75 86 75 5436 95 89 23 74 2633 75 16 74 178936 75 25 86 75 95 75 16 16 89 5454 83 25 26 42 548929 74 13 31 74 26 38 59.54 75 95 25 33 75 46 13 54 74 4616 10 33 75 16 74 17-86 7536 75 31 10 2613 16 10 33,33 75 86 75 95 75 47 7575 16 8951 31 10 26 8945 74 86 90 74 95 7525 56 86 75 33,8921 86 7529 83 26 7525 26 75 90 16 7554 74 31 16 83 4695 74 9029 75 74 90 75 4686 95 56 29 83,21 86 7575 13 16 10 45 10 26 75,45 86 7516 10 45 10 26 10 25 3895 10 29 75 86 83,8916 89 45 74 47 7556 51 7416 7489 13 54 74 16 89 86 38,16 7475 25 86 10 16 75 90 89 86 38,16 7436 74 95 74 89 47 95 10 86 38…

16.

15 22 67 30 93 4922 94 65 94 44 49,4939 51 22 75 49 411115 22 4911 53 51 75 51 78 94,44 4927 51 22 67 44 86 51,26 49 39 51 75“78 45 94 – 62 75 – 78 11 51 44 49 78 91 49 22 72 14”,9411 67 26 93 5 144 51 90 6793 51 44 94 11 6753 75 67 41 49 45 94 11 49 93 15 3035 49 15 67 11 67 14,44 5145 78 49 11 65 94 1444 94 86 49 86 94 4115 20 75 53 75 94 26 67 11,44 5153 67 78 67 26 75 51 11 49 11 65 94 14,35 22 6751 90 6715 39 51 75 22 5853 75 51 27 72 11 49 51 2215 67 11 15 51 3944 51 53 67 78 49 93 51 86 881167 27 75 49 26 5127 51 15 53 93 67 22 44 67 90 6735 51 75 44 67 90 6753 75 94 26 75 49 86 49,44 5126 44 49 20 18 51 90 6745 49 93 67 15 22 94.

67 35 51 75 51 78 44 67 1445 51 15 2286 67 39 49 44 78 94 75 49-9439 49 26 88 751511 94 86 94 44 90 67 399415 22 75 49 65 94 93 67 1453 51 75 51 27 51 45 86 49 39 9478 11 94 44 88 93 94 15 5811 53 51 75 51 78.26 78 51 15 5841 11 49 22 49 93 6753 75 67 45 51 86 22 67 75 67 11,36 67 44

49 75 51 149486 75 67 44 65 22 51 14 44 67 111590 94 75 93 30 44 78 49 39 9493 49 39 53,44 6744 51 75 51 49 93 58 44 67 1426 49 78 49 35 51 1427 72 93 6727 7267 15 11 51 22 94 22 5811 15 2027 49 26 88.67 15 22 49 11 49 93 67 15 5844 51 39 49 93 6753 67 93 67 159453 30 22 51 4422 51 39 44 67 22 72,86 67 22 67 75 88 20 44 51 26 11 49 44 72 5190 67 15 22 9494 15 53 67 93 58 26 67 11 49 93 9439 49 15 22 51 75 15 86 94.11 15 5127 93 94 45 518615 49 39 67 93 51 22 88,27 93 94 45 51,27 93 94 45 51,67 4411 72 75 49 15 22 49 51 2244 4990 93 49 26 49 41,44 49 11 94 15 49 51 2244 49 7890 67 93 67 11 67 14,88 45 5153 75 51 86 75 49 15 44 6715 93 72 65 44 67,86 49 8635 49 15 67 11 67 1467 2215 86 88 86 9444 88 78 94 2253 67 7844 67 1544 51 26 44 49 86 67 39 88 2039 51 93 67 78 94 20,53 67 15 93 51 78 44 20 201115 11 67 51 1445 94 26 44 94…

22 94 41 67 44 58 86 6718 51 93 86 44 88 9327 51 15 65 88 39 44 72 1453 94 15 22 67 93 51 22-9439 51 93 67 78 94 3067 27 67 75 11 49 93 49 15 58,35 49 15 67 11 67 1453 67 78 93 67 39 94 93 15 301186 67 93 51 44 86 49 41,44 6788 53 49 15 22 5844 5188 15 53 51 93,9415 11 67 2049 11 22 67 39 49 22 94 35 51 15 86 88 2011 94 44 22 67 11 86 8844 5111 72 75 67 44 94 93.78 11 5122 51 44 94,27 51 15 65 88 39 44 6711 72 44 72 75 44 88 1194 26 -53 67 7836 20 26 51 93 30 45 49,53 67 78 41 11 49 22 94 93 9451 90 679488 11 67 93 67 86 93 94 44 4978 75 88 90 88 2015 22 67 75 67 44 88,1122 51 39 44 67 22 88.

17.

56 67 9218 58 39 99 27 87 67 5625 56 80 67 10 17 92 39 6225 5627 24 95 56 3195 46 27 73 56 3117 58 39 58 67 95 589256 95 40 24 40 17 92 39 626939 40 17 56 67 58-56 18 99 92 46 67 56 87,69 5669 39 3680 17 92 67 2739 40 87 56 17 58 73 40.25 56 39 73 56 10 17 92,56 43 92 80 40 10,95 56 23 80 4023 17 40 24 4025 46 92 69 14 95 67 27 739573 58 87 67 56 73 58.69 39 5869 56 95 46 27 2325 46 92 67 10 17 5638 58 73 95 92 5856 38 58 46 73 40 67 92 10.25 46 92 18 56 46 56 699225 27 17 62 73 56 6924 80 58 39 6218 14 17 5625 46 58 69 58 17 92 95 56 5887 67 56 43 58 39 73 69 56,23 17 40 24 4046 40 24 18 58 23 40 17 92 39 62.56 80 67 40 95 5618 17 40 23 56 80 40 46 1073 58 8743 58 80 69 27 8767 58 80 58 17 10 8773 46 58 67 92 46 56 69 56 9567 4087 40 95 58 73 58 9273 14 39 10 38 58 95 46 40 73 67 56 25 56 69 73 56 46 58 67 67 14 8767 40 39 73 40 69 17 58 67 92 10 8792 67 39 73 46 27 95 73 56 46 4056 67 9239 56 69 58 46 99 58 67 67 5673 56 38 67 5624 67 40 17 92,24 4038 58 8725 46 92 99 17 92.25 56 67 10 73 92 1067 5892 87 58 17 92,80 17 1038 58 23 5695 56 67 95 46 58 73 67 5625 46 58 80 67 40 24 67 40 38 58 67 1469 39 5871 73 9299 73 27 95 92-67 5656 7367 92 8271 73 56 23 56 9267 5873 46 58 18 56 69 40 17 56 39 62.

67 5825 46 56 99 17 569287 92 67 27 73 14,95 40 9556 6727 69 92 80 58 1751 58 17 6292 8267 58 17 58 23 95 56 23 569271 95 24 56 73 92 38 58 39 95 56 23 5625 27 73 58 99 58 39 73 69 92 10-73 46 9225 27 17 62 73 4025 5625 46 40 69 56 87 2718 56 46 73 27,27 39 14 25 40 67 67 14 5838 58 46 73 56 69 56 3127 31 87 56 3173 27 87 18 17 58 46 56 69,17 40 87 25 56 38 58 95,25 58 46 58 95 17 36 38 40 73 58 17 58 319295 67 56 25 56 95.73 46 9269 14 25 27 95 17 14 8271 95 46 40 67 406969

92 80 5869 58 46 73 92 95 40 17 62 67 14 8225 46 10 87 56 27 23 56 17 62 67 92 95 56 69-56 67 9239 40 87 14 58,67 92 95 40 95 56 3156 99 92 18 95 92…

18 56 80 46 56 39 73 9246 40 80 92,56 6725 56 69 73 56 46 92 1725 46 5639 58 18 1025 56 17 36 18 92 69 99 27 36 39 1051 92 73 40 73 27:“38 73 5656 80 92 6738 58 17 56 69 58 9525 56 39 73 46 56 92 17,80 46 27 23 56 3124 40 69 39 58 23 80 4046 40 24 17 56 87 40 73 6239 87 56 43 58 73”.92,25 56 82 17 56 25 40 6925 5625 17 58 38 27 39 73 46 40 99 92 17 276924 67 40 9573 56 23 56,38 73 5667 40 25 40 46 67 92 9580 56 17 43 58 6718 80 92 73 58 17 62 67 5639 73 56 10 73 6267 4099 27 82 58 46 58,80 56 39 73 40 1795 92 67 43 40 1792 2425 46 92 99 92 73 14 8267 40 8095 56 17 58 67 56 8767 56 43 58 67.

18.

67 58 26 19 88 2332 37 15 23 90 63 7146 63 26-63 2658 2463 23 3732 956763 15 32 88 58 26-6726 58 6741 16 24 90 63 52 30 2449 63 2688 26 37 23 38 23 16 6758 2390 26 41 90 63 68 24 58 58 26 7685 15 67 76 24 15 24.19 26 15 23 38 88 2663 15 32 88 58 24 2490 88 24 16 23 63 7163 23 37,46 63 26 41 5437 15 23 95 676758 2438 23 76 24 63 67 16 6768 26 68 90 24,67 58 23 46 2437 63 26 – 63 2658 24 19 16 32 85 54 4426 46 24 58 7141 54 90 63 15 2690 88 24 16 23 24 6390 26 26 63 68 24 63 90 63 68 32 11 30 67 2468 54 68 26 88 546724 30 24,46 24 19 2688 26 41 15 26 19 26,85 15 67 76 24 63 90 5237 16 24 68 24 63 23 63 71,68 15 23 95 67 58 2367 88 24 26 16 26 19 67 46 24 90 37 23 52,85 32 90 63 7188 23 95 243258 24 19 266758 2441 32 88 24 6388 26 37 23 38 23 63 24 16 71 90 63 68,58 263746 24 76 3258 23 7616 67 83 58 52 5237 16 24 68 24 63 23?63 26-63 26…49 63 26 6356 67 58 23 1685 26 38 68 26 16 52 1626 88 58 67 7676 23 73 26 7615 24 83 67 63 7158 24 90 37 26 16 71 37 2638 23 88 23 46.58 2441 54 16 2658 67 37 23 37 26 4437 15 23 95 67,90 26 68 24 15 83 24 58 58 26 4473 68 23 63 37 67 76 6763 15 24 58 67 15 26 68 23 58 58 54 76 6715 24 41 52 63 23 76 67-85 15 26 90 63 26-58 23 85 15 26 90 63 2626 37 15 24 90 63 58 54 2485 23 15 63 67 38 23 58 54,88 23 68 58 54 76-88 23 68 58 2619 15 26 38 67 68 83 67 2488 26 41 15 23 63 71 90 5268 90 2495 2488 2626 85 16 26 63 2367 76 85 24 15 67 23 16 67 38 76 23,90 67 15 24 46 7188 23 58 58 26 4441 23 38 54,90 68 26 1132 19 15 26 38 326837 26 58 29 2437 26 58 29 26 6868 54 85 26 16 58 67 16 67.58 23 19 15 52 58 32 16 6758 26 46 58 26 4485 26 15 26 44,85 26 15 24 38 23 16 6737 26 16 11 46 37 32,85 15 26 58 67 37 16 6758 2341 23 38 3285 26 8885 26 37 15 26 68 26 7676 15 23 37 23,38 23 16 26 95 67 16 679085 26 16 88 11 95 67 58 5476 67 58,85 26 90 63 15 24 16 52 16 6767 3819 15 23 58 23 63 26 76 24 63 26 6867,90 85 15 23 68 24 88 16 67 68 2615 24 83 67 68,46 63 2688 26 90 63 23 63 26 46 58 2658 23 85 23 37 26 90 63 67 16 67,38 16 26 15 23 88 58 2685 26 16 11 41 26 68 23 16 67 90 7188 24 16 26 7615 32 3790 68 26 67 736732 41 15 23 16 67 90 7168 26 90 68 26 52 90 6741 24 3876 23 16 24 44 83 24 19 2688 16 5290 24 41 5232 15 26 58 23.

19.

3492 45 25 90 30 25 7116 62 37 7155 7189 18 96 6255 85 22 71 11 6262 24 62 89 71 55 55 6285 55 16 71 92 71 24 55 62 11 62-90 30 49 30 24 55 18 7124 16 85 92 30 55 18 7152 37 85 55 24 18,49 30 92 62 22 25 3022 85 24 16 18 7392 58 89 30 67 71 25,90 58 89 55 30 2086 71 16 25 302416 45 89 85 25 62 1449 30 24 16 18-89 92 62 52 20 11 7168 16 6249 62 96 62 37 71 55 62,25 62 96 8562 5530 34 24 16 92 30 96 85 71 4692 62 52 62 14,49 30 92 3089 30 55 62 2525 62 55 24 71 92 34 62 34,49 62 22 30 16 18 9439 96 30 25 62 552462 89 71 90 90 30 92 30 37 85 34 30 45 86 85 14 8534 62 52 5816 30 89 96 71 16 25 30 14 85,24 16 30 92 18 9425 62 14 49 30 24,62 89 67 30 92 49 30 55 55 18 9439 62 55 30 92 85 258549 92 62 22 30 2052 92 71 89 71 52 71 55 19,85 90 62 89 96 85 22 30 34 67 30 203452 37 62 55 7124 16 19 45 -25 30 25 -71 11 62-16 30 1452 62 24 16 30 16 62 22 55 6262 49 18 16 55 62 11 6249 58 16 71 67 71 24 16 34 71 55 55 85 25 30,14 30 16 92 62 24 302455 71 14 30 96 18 1424 16 30 37 71 14,3462 52 85 5549 92 71 25 92 30 24 55 18 9452 71 55 1992 71 67 85 34 67 71 11 6249 62 85 24 25 30 16 1924 22 30 24 16 19 2055 3089 71 92 71 11 58.49 92 71 52 71 96 19 55 6224 25 92 62 14 55 18 7149 62 37 85 16 25 85,55 7124 49 62 24 62 89 55 18 7149 92 85 34 96 71 22 1934 55 85 14 30 55 85 7124 71 92 19 71 90 55 18 7311 92 30 89 85 16 71 96 71 94.

85 14 71 96 62 24 198562 92 58 37 85 71,3025 30 2537 71.49 92 85 96 85 22 55 18 7392 30 90 14 71 92 62 3462 73 62 16 55 85 22 85 9455 62 37,34 16 62 92 62 94,25 30 92 14 30 55 55 18 9467 34 71 94 46 30 92 24 25 85 9449 71 92 62 22 85 55 55 85 252452 34 58 14 2052 71 24 20 16 25 30 14 8549 92 85 22 85 55 52 30 96 62 34,3016 30 25 37 7149 62 16 71 92 16 18 9449 85 24 16 62 96 71 16-25 62 96 19 1689 62 96 71 7122 71 1452 34 30 52 46 30 16 85 96 71 16 55 71 11 6234 62 90 92 30 24 16 30,55 6258 73 62 37 71 55 55 18 948524 14 30 90 30 55 55 18 94-85 14 71 55 55 6216 30 25 62 7162 92 58 37 85 7114 62 37 55 6289 71 9062 24 62 89 18 7349 92 62 89 96 71 1449 92 85 62 89 92 71 24 16853449 62 92 16 62 34 18 7316 92 58 86 62 89 30 73.34 24 7149 92 62 52 58 14 30 55 62.90 52 71 67 55 85 7149 62 96 85 46 30 852489 62 96 19 67 85 1449 62 52 62 90 92 71 55 85 71 1462 16 55 62 24 20 16 24 202524 58 89 10 71 25 16 30 142430 34 16 62 14 30 16 85 22 71 24 25 85 1462 92 58 37 85 71 1455 3049 96 71 22 71,90 30 16 6255 7162 24 62 89 6255 30 34 62 92 62 22 71 55 55 18 9425 30 92 30 89 85 5585 96 8549 92 62 24 16 71 55 19 25 85 9449 85 24 16 62 96 71 163425 30 92 14 30 55 713490 52 71 67 55 85 7314 71 24 16 30 7324 22 85 16 30 45 16 24 2055 71 49 92 71 14 71 55 55 18 1430 16 92 85 89 58 16 62 1458 34 30 37 30 45 86 71 11 6224 71 89 2025 30 89 30 96 19 71 92 62,49 85 24 19 14 71 55 55 62 11 6292 30 90 92 71 67 71 55 85 2055 7116 92 71 89 58 45 1685,3462 89 86 71 14,49 62 52 62 90 92 71 55 85 9455 71 34 18 90 18 34 30 45 16,49 62 25 302485 7349 62 14 62 86 19 4555 7124 62 16 34 62 92 20 1622 71 11 62-16 62 55 71 90 30 25 62 55 55 62 11 62.

20.

16 7453 74 47 47 8531 85 66 74 29 58 55 7416 96 74 66 85 55 11 66 5896 11 12 91 74 74 50 96 11 12 91 85 49 53 58 8547 11 33 74 26 74 31 2329 47 85 2645 29 85 55 74 29,96 11 12 33 85 96 74 29,33 11 96 74 285829 74 12 96 11 47 55 11-66 85 68 28 74 29 35 53 28 5847 35 16 85 96 47 74 29 96 85 33 85 91 91 23 85,47 29 85 96 28 11 21 18 58 8591 74 29 85 91 61 28 58 3366 11 28 74 33,66 85 68 28 74 29 35 53 28 5829 96 85 33 85 9188 35 55 6166 5891 8529 55 74 96 74 4933 58 96 74 29 74 49,47 55 11 96 85 91 61 28 58 8511 29 55 74 50 35 47 23,68 96 74 33 11 31 91 23 8568 96 35 12 74 29 58 28 58-55 96 11 28 58,91 85 29 85 47 55 6174 55 28 35 31 1129 12 43 29 53 11 43 47 435891 85 29 85 31 74 33 7428 35 31 1147 16 85 53 58 29 53 11 4316 74 79 11 96 91 11 4333 11 53 58 91 11…31 74 29 74 66 61 91 7447 28 74 96 7474 9174 55 33 85 55 58 66,88 55 7447 96 85 31 5829 47 85 68 7438 55 74 68 7496 11 12 91 74 74 50 96 11 12 58 4391 8516 74 16 11 31 11 85 55 47 4391 5829 74 85 91 91 23 26,91 5816 74 66 58 45 85 49 47 28 58 2633 11 53 58 91,29 74 74 50 18 852974 28 96 85 47 55 91 74 47 55 43 26,91 11 47 28 74 66 61 28 7433 74 79 91 7447 35 31 58 55 6116 7455 74 33 35,88 55 7474 9129 58 31 85 664729 85 96 26 74 55 35 96 23,91 8591 11 50 66 21 31 11 85 55 47 4391 5833 11 66 85 49 53 58 2616 96 58 12 91 11 28 74 2988 96 85 12 29 23 88 11 49 18 58 91 23,28 11 28-55 74:33 74 50 58 66 61 91 23 2616 11 55 96 35 66 85 49,16 74 47 55 74 2991 1174 50 74 88 58 91 85,16 96 74 29 85 96 28 5831 74 28 35 33 85 91 55 74 29,12 11 47 55 11 29,50 66 74 28 16 74 47 55 74 29…91 58 88 85 68 7416 74 31 74 50 91 74 68 74.47 58 8545 85 91 91 74 8591 11 50 66 21 31 85 91 58 8591 8591 1153 35 55 28 3516 96 58 50 11 29 66 43 66 7474 16 55 58 33 58 12 33 11.

74 9116 74 47 33 74 55 96 85 6666 85 29 85 85-55 11 3374 5516 11 91 11 33 85 96 58 28 11 91 23 74 55 26 74 31 58 66 1111 47 62 11 66 61 55 58 96 74 29 11 91 91 11 4331 74 96 74 68 11,91 852916 96 58 33 85 9635 79 85,31 11 66 85 28 7491 8555 11 28 11 4374 79 58 29 66 85 91 91 11 43.5835 55 23 28 11 66 11 47 6174 91 1116 96 43 33 85 26 74 91 61 28 742955 74 55 47 11 33 23 4968 74 96 74 31 74 28,68 31 8558 2653 85 47 55 85 96 28 1131 74 66 79 91 1150 23 66 1129 23 49 55 58 91 1133 85 47 55 91 74 68 7491 85 66 85 68 11 66 11.

21.

40 77 40,29 75 5875 28 75!15 61 75 23 40 52 672929 54 52 1115 75 65 58 5415 84 40 29 54 61 67 28 75 77 7558 84 11 18 77 75 61 67 28 54 35 40,77 52 1115 75 37 11 84 11 52 54 28 11,28 4028 11 29 49 37 75 35 75 13,35 29 40 52 84 40 58 28 75 1335 54 84 15 54 65 28 75 1315 75 37 58 40 13 11 28 58 1129 75 90 29 49 72 40 11 58 37 8015 18 72 35 4029 84 11 13 11 2815 11 84 29 75 4113 54 84 75 29 75 41,5415 75 5211 1137 58 29 75 61 75 1337 61 75 82 11 28 4015 54 84 40 13 54 52 35 4054 9029 75 29 37 1118 8237 58 40 84 54 28 28 49 4680 52 11 84,35 40 35 54 13 5415 40 61 54 61 5461 11 5890 4037 58 7552 7515 75 80 29 61 11 28 54 8028 4035 75 28 29 11 41 11 84 1158 40 35 54 4629 75 5858 84 11 46 52 20 41 13 75 29 75 35-37 20 84 84 11 40 61 54 37 58 54 65 11 37 35 75

1137 75 65 11 58 40 28 54 11,11 37 61 5429 52 18 13 40 58 67 37 80,28 7513 11 37 58 28 49 46,28 40 52 7515 75 61 40 77 40 58 67,29 15 75 61 28 1118 37 58 84 40 54 29 40 11 58.54 33 7528 40 77 61 80 52 28 7515 75 35 40 90 49 29 40 11 5852 75 33 61 11 37 58 67,15 84 75 80 29 61 11 28 28 18 2054 4652 11 84 82 40 29 75 412915 11 84 29 18 2013 54 84 75 29 18 20:28 1835 40 3582 11,75 28 4075 58 15 84 40 29 54 61 4028 4011 29 84 75 15 11 41 37 35 54 4192 84 75 28 5826 11 61 49 4137 58 84 11 61 35 75 29 49 4133 40 58 40 61 67 75 285458 75 84 82 11 37 58 29 11 28 28 7515 75 84 29 40 61 4075 58 28 75 72 11 28 54 803777 11 84 13 40 28 37 35 75 4154 13 15 11 84 54 11 41,4029 52 75 33 40 29 75 3575 52 182972 11 37 58 28 40 52 26 40 58 75 1333 11 84 11 77 75 29 49 1133 40 58 40 84 11 5475 52 28 75 77 7554 9029 75 11 28 28 49 4615 75 84 58 75 2926 11 61 49 4652 29 4065 40 37 4015 40 61 54 61 5415 7558 75 4158 75 65 35 111877 75 84 54 90 75 28 58 40,77 52 1135 40 35 75 13 18 -58 7533 52 54 58 11 61 67 28 75 13 1829 75 80 35 1115 75 65 18 52 54 61 37 8077 11 84 13 40 28 37 35 54 4135 84 11 41 37 11 84…75 33 19 11 35 58 54 29 28 75 37 58 5484 40 52 5437 58 75 54 5818 58 75 65 28 54 58 67,65 58 7529 7529 58 75 84 18 2013 54 84 75 29 18 2090 52 11 72 28 54 41,15 18 37 58 675428 11 29 11 61 54 35 54 4129 75 11 28 28 75-13 75 84 37 35 75 4192 61 75 5829 13 11 37 58 113737 75 20 90 28 54 35 40 13 5415 40 58 84 18 61 54 84 75 29 40 6115 84 54 61 11 77 40 20 23 54 1129 75 52 495415 40 84 1884 40 9029 84 75 52 1133 4952 40 82 1137 58 84 11 61 80 6115 7528 40 37 58 75 80 23 54 13,4028 1115 84 54 29 54 52 11 29 72 54 13 37 8015 75 52 29 75 52 28 49 1361 75 52 35 40 1335 84 54 77 37-13 40 84 54 28 11.

22.

56 9631 57 87 3756 7584 77 87 24 96 73 68 75,56 7550 37 16 42 68 77,7720 73 3737 49 56 77 39 77 87 37,39 73 3712 84 9616 91 64 56 91 87 37.75 56 84 73 16 91 68 94 75 7531 57 87 7544 16 37 84 73 577556 96 49 77 73 96 14 87 75 12 57:96 84 87 7556 7744 37 28 37 68 37 56 56 75 68 9656 96 7356 7550 37 16 42 68 77,56 7584 77 87 24 96 73 68 75,96 84 87 7573 77 2673 37 87 41 68 3784 77 87 24 96 73 68 7731 96 4950 37 16 42 68 7775 87 7550 37 16 42 37 6831 96 4984 77 87 24 96 73 68 75-56 9673 3739 73 3756 9612 64 37 28 75 73 41,56 3728 77 35 9656 9644 16 75 31 87 75 35 77 73 41 84 61.12 84 9644 16 96 35 56 75 9616 77 84 68 87 77 28 5787 96 73 61 736839 96 16 73 91,1235 75 49 56 4184 87 96 28 91 96 7356 96 26 96 28 87 96 56 56 3744 16 96 73 12 37 16 61 73 4149 77 44 77 84 56 37 1412 77 16 75 77 56 73.56 91 35 56 3768 77 6826 37 35 56 3731 57 84 73 16 96 9637 73 84 82 28 7784 26 77 73 57 12 77 73 41 84 61,91 31 75 16 77 73 41 84 616839 96 16 73 37 12 37 1426 77 73 96 16 7575 4950 37 16 37 28 68 77,12 84 73 91 44 77 96 731284 75 87 9149 77 44 77 84 56 37 1412 77 16 75 77 56 7337 73 64 37 28 77…

12 96 84 4137 68 16 91 35 77 82 22 75 1426 75 1612 56 96 49 77 44 56 3784 73 77 8756 9644 16 37 84 73 3739 91 35 75 26-12 16 77 35 28 96 31 56 57 26.44 37 28 37 49 16 96 12 77 73 4184 87 96 28 37 12 77 87 3712 84 96 647512 84 61.44 41 82 22 75 6444 75 12 3784 37 87 28 77 73 75 68 37

12-1273 37 26,39 73 3737 56 7556 9684 37 87 28 77 73 75 68 7512 37 12 84 96,7750 16 91 44 44 7749 77 64 12 77 73 7775 4912 37 96 56 56 37 1468 37 56 73 16 16 77 49 12 96 28 68 75,44 16 96 84 73 77 16 96 87 37 50 3750 37 84 73 75 56 75 39 56 37 50 3764 26 57 16 61-1273 37 26,39 73 3737 5612 37 12 84 9656 9644 37 16 73 41 9675 87 7512 87 77 28 96 87 96 94,75 87 7573 377528 16 91 50 37 961237 28 56 37 2687 75 94 96,7744 37 87 68 37 12 56 75 6849 28 96 42 56 96 1473 77 14 56 37 1444 37 87 75 94 75 75.12 84 9612 37 49 26 37 35 56 37,68 37 50 28 7791 84 87 37 12 87 96 56 56 37 50 3784 75 50 56 77 87 7756 96 7356 7791 84 87 37 12 87 96 56 56 37 2626 96 84 73 96.

23.

22 10 75 6247 1074 10 24 88 47 39 35 66 15 75 58 10 47 64 53 5385 66 35 10 69 62 28 10 24 5366 49 53 47 47 10 49 64 10 58 3928 22 88 17 10 79 47 88 1547 66 22 53.4447 10 85 17 10 28 53 24 75 443551 66 75 58 53 47 53 64 88.35 10 3572 62 28 10 24 6647 8817 10 69,4466 80 37 80 10 2469 49 88 75 3937 74 53 17 66 58 28 66 17 88 47 53 885385 66 35 66 15,22 37 28 75 58 28 10,35 66 58 66 17 62 8853 75 85 62 58 62 28 10 88 79 39,66 35 10 69 10 28 79 53 75 392849 10 28 47 6669 47 10 35 66 74 62 4274 88 75 58 10 42.79 53 17 66 35 53 8828 66 17 66 58 1072 62 24 5317 10 75 85 10 42 47 37 58 62,37 75 10 49 39 72 1037 58 66 47 37 24 102875 37 74 88 17 35 10 42.4428 66 79 88 242842 66 24 24,51 49 8858 37 74 10 47 47 62 8869 88 17 35 10 24 1069 62 72 35 6666 58 17 10 31 10 24 5364 28 88 58 625349 88 58 10 24 5353 47 58 88 17 39 88 17 10.37 49 53 28 53 58 88 24 39 47 66,47 6642 66 69 44 53 4747 8837 69 47 10 2474 88 47 44.66 4785 17 66 58 44 47 37 2417 88 51 53 75 58 17 10 64 53 66 47 47 37 9735 47 53 51 37.4428 69 44 2417 37 22 35 37,66 72 7 41 03 54 73 7 2485 88 17 662872 17 66 47 69 66 28 37 9722 88 17 47 53 24 39 47 53 64 3753,75 35 24 66 47 53 28 79 53 75 3947 10 49 17 10 75 35 17 62 58 62 74 5375 58 17 10 47 53 64 10 74 53,75 58 66 24 35 47 37 24 75 447585 88 17 28 66 1553 6974 47 66 31 88 75 58 28 1047 88 66 31 53 49 10 47 47 66 75 58 88 15,35 66 58 66 17 62 8885 66 49 75 58 88 17 88 51 10 24 5374 88 47 4425 58 66 1547 66 22 39 97.74 66 8853 74 44,42 66 17 42 8824 37 53 7572 66 17 42 88 75,72 62 24 6647 10 22 88 17 58 10 47 662835 47 53 51 88,5322 88 17 47 53 24 1088 80 8847 8837 75 85 88 24 5328 62 75 66 42 47 37 58 39.

24.

6152 16 36 26 14 5416 45 24 29 4595 1129 36 95 86 36 16 29 451452 49 75 36 4797 36 93 95 61 54 26 6197 3626 86 45 97 49 95 41 29 11 47.93 49 30 61 86 95 11 93 56 11 86 83 8995 36 47 49 1695 11 37 36 93 14 54 26 6195 1130 86 36 16 36 4721 86 11 33 49,2636 29 95 11 47 1495 1130 95 45 86 16 49 95 95 14 8993 30 36 16 14 29,33 11 54 29 14 891471 11 52 16 36 19 49 95 95 83 89,36 52 95 49 26 49 95 95 83 8952 11 54 98 26 86 16 11 93 36 89;75 93 49,29 11 2997 36 47 95 14 54 36 26 4147 95 49,26 86 36 61 54 1197 54 61 33 95 11 6126 29 11 47 49 89 29 11.21 86 3652 83 54 1126 11 47 11

6152 36 54 41 19 11 6129 36 47 95 11 86 1130 75 36 26 86 14 95 14 56 49.6186 36 54 29 95 45 5493 30 49 16 41,36 95 1197 36 93 93 11 54 11 26 41.97 36 93 97 36 86 36 54 29 36 4775 36 16 49 54 1154 98 26 86 16 11.3049 4952 49 71 33 11 54 36 26 86 95 36 4726 30 49 86 496145 71 95 11 5426 49 52 61.95 1145 71 29 36 8933 49 54 49 71 95 36 8929 16 36 30 11 86 1454 49 33 11 5461,97 36 26 86 11 16 49 30 19 14 891436 52 16 98 71 75 19 14 89,1416 11 71 75 54 61 93 83 30 11 5454 49 97 95 14 95 4595 1197 36 86 36 54 29 49.6145 26 54 83 19 11 5475 36 54 36 26.95 4926 36 30 26 49 4747 36 89-52 49 7136 52 49 16 86 36 95 36 30,95 49 97 16 14 61 86 95 83 89,97 36 37 36 33 14 8995 1147 11 75 95 14 86 36 78 36 95 95 45 9871 11 97 14 26 41.

-45 93 14 30 14 86 49 54 41 95 36,-26 29 11 71 11 5436 95,-95 11 2693 30 36 491447 8336 93 95 36.30 97 16 36 24 49 47,30 3626 95 4995 14 24 86 3695 4926 97 36 26 36 52 95 3630 83 71 30 11 86 4145 93 14 30 54 49 95 14 49.6116 36 52 29 3626 97 16 36 26 14 54:

-71 95 11 24 14 86,30 26 4921 86 3626 36 95?

-97 16 14 24 49 4797 36 26 54 49 93 95 14 8926 36 95.-33 49 26 86 36 4736 9597 36 29 11 71 11 5495 1197 45 26 86 36 89 97 45 71 83 16 49 29,

26 86 36 61 30 19 14 8995 1147 16 11 47 36 16 95 36 8929 16 83 19 29 4995 36 24 95 36 75 3626 86 36 54 14 29 11.-86 49 52 49 97 16 14 93 49 86 26 61,95 11 30 49 16 95 36 49,45 30 14 93 49 86 4147 95 36 33 49 26 86 30 3626 95 36 30,97 16 49 33 93 4924 49 4793 36 52 49 16 49 19 41 26 6193 3621 86 36 8995 36 24 14.29 11 29 36 4926 49 75 36 93 95 6124 14 26 54 3697 3686 30 36 49 47 4529 11 54 49 95 93 11 16 98?

25.

48 84 13 3394 13 48 42 33 46 82,84 13 82 4894 82 46 84 33 4213 88 82 84 16 46 1625 8250 17 481342 61 37 78 50 511682 42 13 82 84 16 46 1650 48 17 341376 82 25 82 1672 82 46 48 69 17 82 28 82,28 84 4851 75 4875 84 33 46 1646 33 84 33 17,75 33 37 82 13 17 341638 48 37 17 16 46 33.82 1713 58 94 25 33 69 58 13 33 4676 82 75 48 46 33 17 16 34,163476 82 25 33 69 58 13 33 4648 50 5113 94 48,38 42 8217 1648 94 42 781350 16 37 48.1376 37 16 28 82 37 64 17 4817 48 17 33 13 16 94 42 17 82 28 8272 58 46 8294 82 72 37 33 17 8213 94 48,38 42 8284 82 13 48 46 82 94 78 76 82 13 16 84 33 42 7851 75 4851 94 82 76 64 16 501638 42 8269 37 34 4217 58 17 4869 84 37 33 13 94 42 13 51 61 21 16 48:28 82 37 82 84 33,75 33 37 25 16 481688 82 46 82 84 17 58 4894 42 37 33 17 58,94 82 25 37 82 13 16 21 33,94 25 37 58 42 58 481369 48 50 17 58 8828 46 51 72 16 17 33 88,72 82 37 82 69 84 34 21 16 4850 82 37 3425 82 37 33 72 46 16,82 37 51 84 16 3413 82 91 17 58,16 17 94 42 37 51 50 48 17 42 5813 37 33 38 48 13 33 17 16 341650 51 69 58 25 16,76 46 48 17 16 42 48 46 78 17 58 8875 48 17 21 16 17,17 48 76 82 84 13 16 75 17 58 4869 13 48 69 84 581676 46 33 17 48 42 58,25 37 33 94 25 16,25 82 42 82 37 58 50 1676 82 46 78 69 51 61 42 94 3417 48 13 48 37 17 58 48,25 82 28 84 3376 16 64 51 4294 13 82 1650 48 37 69 25 16 48

25 33 37 42 16 17 58,37 33 94 42 48 17 16 341650 16 17 48 37 334 65 894 8213 94 48 50 1616 8894 82 25 37 82 13 48 17 17 58 50 1669 33 50 48 38 33 42 48 46 78 17 58 50 1694 13 82 91 94 42 13 33 50 16,94 48 37 48 72 37 34 17 58 8833 17 28 48 46 82 13,38 48 9188 46 48 72-88 13 33 46 331676 37 48 13 82 69 17 48 94 48 17 16 4828 82 94 76 82 84 33,37 33 69 84 33 38 5117 33 28 37 33 841364 25 82 46 33 88,19 16 28 51 37 5876 42 16 981698 33 37 48 91,88 37 33 17 34 21 16 48 94 341394 33 50 82 5094 48 37 84 98 4876 16 37 33 50 16 84,42 48 17 7872 58 25 33,17 3325 82 42 82 37 82 5076 82 25 82 16 42 94 3469 48 50 46 34,1637 58 72 58,17 3325 82 42 82 37 82 9194 42 82 16 42

72 58 25,76 51 94 42 58 17 1613 94 48 50 16 46 82 94 42 16 13 82 28 8272 82 28 33.82 1751 13 16 84 48 4613 48 21 1617 48 82 76 16 94 51 48 50 58 48,42 33 25 16 48,25 33 2551 46 16 98 58,82 94 13 48 21 48 17 17 58 4828 33 69 82 13 58 50 1637 82 75 25 33 50 16,1625 16 42 33,25 82 42 82 37 58 9151 50 16 37 33 48 4276 37 1669 13 51 25 33 8838 48 46 82 13 48 38 48 94 25 82 28 8228 82 46 82 94 33.

Пример решения курсовой работы

15 вариант

Скользящая перестановка

Текст для расшифровки: _ПАРИИВИАРЗ_БРА_ИСТЬЛТОЕК

Текст содержит 25 символов, т.е. записываем его в таблицу 5×5.

_	П	А	Р	И
И	В	И	А	Р
З	_	Б	***Р***	***А***
_	И	С	***Т***	***Ь***
Л	Т	О	***Е***	***К***

Расшифровку следует проводить меня порядок столбцов.

Воспользуемся таблицей сочетаемости букв. 4 и 5 столбцы идут друг за другом, т.к. биграммы РА, ТЬ и ЕК наиболее распространенные. 2 и 4 столбец идут друг за другом, т.к. биграммы ИТ и ТЕ тоже распространены. По выше перечисленным признакам не трудно догадаться, что столбцы будут располагаться в следующем порядке: 2,4,5,3,1. И зашифрованной фразой будет: ***При_аварии_разбить_стекло.***

В данном случае дешифровать текст можно было обычным методом перебора, не обращаясь к таблице сочетаемости букв.

Шифр двойной перестановки

Текст для расшифровки: ЗШАФИПРАЛОЕНЖ_ОЬН_ДАРВОНА.

Текст содержит 25 символов, т.е. записываем его в таблицу 5ˣ5.

З	Ш	А	Ф	И
П	Р	А	Л	О
Е	Н	Ж	_	О
Ь	Н	_	Д	А
Р	В	О	Н	А

Расшифровку следует проводить меня порядок столбцов и строк.

Глядя на зашифрованный текст по первым пяти символам можно сразу предположить, что столбцы меняются следующим образом: 1,3,2,5,4.

З	А	Ш	И	Ф
П	А	Р	О	Л
Е	Ж	Н	О	_
Ь	_	Н	А	Д
Р	О	В	А	Н

Глядя на вторую таблицу можно, также, без труда определить порядок строк: 2,4,3,1,5.

Расшифрованный текст: Пароль_надежно_зашифрован.

Шифр простой замены

Расшифрованный текст:

ЧЕМ ДАЛЬШЕ, ТЕМ СИЛЬНЕЕ ОН ЧУВСТВОВАЛ НЕШУТОЧНОЕ РАЗДРАЖЕНИЕ, ПОРОЮ ПЕРЕХОДИВШЕЕ В ПРИЛИВЫ ЗЛОСТИ-ОТТОГО, ЧТО ОНИ ЧЕТВЕРО СУТОК, ОБРАТИВШИСЬ В ЗРЕНИЕ И СЛУХ, ТОРЧАЛИ В ЧАЩОБЕ, КАК ДИКИЕ ОБЕЗЬЯНЫ ИЗ БРАЗИЛИИ, ОТТОГО, ЧТО ПОДВЕРНУЛСЯ ТУПОЙ КАЙМАН, С ОДИНАКОВЫМ УСЕРДИЕМ НАПАДАВШИЙ И НА ЛЕСНУЮ СВИНЬЮ, И НА ОТЛИЧНОГО ПАРНЯ С ДРУГОГО КОНТИНЕНТА А В ЭТО ВРЕМЯ ТЕ, НА БАЗЕ, ЖИЛИ В СВОЕ УДОВОЛЬСТВИЕ, СПАЛИ НА ЧИСТЕНЗЫЗИХ ПРОСТЫНКАХ В КОНДИЦИОНИРОВАННОЙ ПРОХЛАДЕ, ПРИНИМАЛИ ДУШ, ЖРАЛИ НА ЗАВТРАК ФРУКТЫ, ДЖЕМ И БИФШТЕКСЫ В ТРИ ПАЛЬЦА ТОЛЩИНОЙ, И ОКНА ТАК УЮТНО СВЕТИЛИСЬ, И МУЗЫКА ИГРАЛА, И ФУТБОЛ ПО ТЕЛЕВИЗОРУ

НИЧЕГО В ЭТОЙ ЗЛОСТИ НЕ БЫЛО ПЛОХОГО, НАОБОРОТ - ТАКОЙ НАСТРОЙ КАК РАЗ И ПРИДАЕТ БОЕВОГО КУРАЖА…

А ПОТОМ ПРИШЕЛ КОНЕЦ И ПОСТОРОННИМ МЫСЛЯМ И БЕЗДЕЛЬЮ. МОРСКОЙ ЗМЕЙ НАКОНЕЦ-ТО ПОДАЛ ЗНАК, КОТОРОГО ОНИ ЖДАЛИ ЧЕТВЕРО СУТОК, И ЭТО БЫЛО СЛОВНО МЕДНЫЙ РЕВ БОЕВОЙ ТРУБЫ, ЭТО ОЗНАЧАЛО, ЧТО НАЧАЛИСЬ РАБОТЫ, И НИЧЕГО УЖЕ НЕ ИЗМЕНИТЬ, НЕ ОСТАНОВИТЬ, НЕ ПЕРЕИГРАТЬ…

2.2.2. ЗАДАНИЕ НА КУРСОВУЮ РАБОТУ ПО ШИФРОВАНИЮ С СЕКРЕТНЫМ КЛЮЧОМ

КРИПТОАНАЛИЗ ШИФРОТЕКСТОВ ПОЛУЧЕННЫХ МЕТОДОМ ГАММИРОВАНИЯ

Заданием для данной лабораторной работы является отыскание открытого текса зашифрованного методом гаммирования при помощи сдвигового регистра с линейной обратной связью. Для сдачи работы необходимо предоставить текст файла отчета. После получения верного открытого текста необходимо по найденной части ключа вручную определить положение отводов в регистре при помощи алгоритма Берлекэмпа-Месси и представить таблицу вывода для проверки. Необходимо заметить, что это является обязательным шагом уже после нахождения верного открытого текста. Для промежуточных нахождений положений отводов в регистре алгоритм Берлекэмпа-Месси использовать необязательно, можно воспользоваться методом, основанным на нахождении обратной матрицы.

Общее описание лабораторной работы

Целью работы является приобретение практических навыков криптоанализа аддитивных шифров.

Результатом работы является получение осмысленного открытого текста из зашифрованного сообщения при помощи учебной программы, называемой «Криптоанализ аддитивного шифра LSR». Лабораторная работа представляет собой исполняемый файл LSR.exe (учебная программа) и набор из 25 вариантов задания (зашифрованный текст).

Общий вид окна учебной программы

Программа LSR.exe представляет собой исполняемый файл, который запускается двойным нажатием на пиктограмму

Рис. 23. Пиктограмма LSR

После чего на экране появляется диалоговое окно, представляющее собой окно лабораторной работы (рабочее окно).

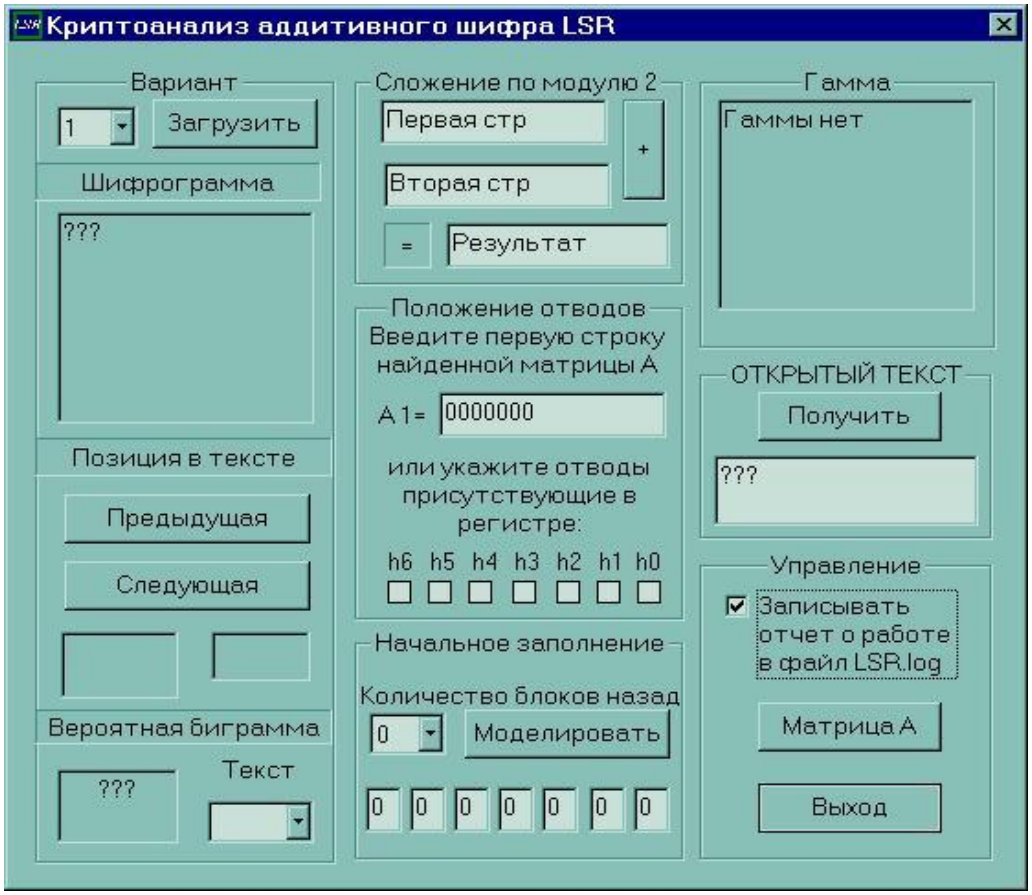


Рис. 24. Внешний вид окна LSR

Рабочее окно лабораторной работы разделено на 7 блоков, которые представляют собой отдельно последовательно выполняемые шаги лабораторной работы и блок управления. Работа последующих блоков базируется на результатах работы предыдущих.

Кратко перечислим и поясним эти блоки:

- Вариант. Блок предназначен для загрузки внешнего файла варианта в соответствии с выбранным номером, отображения текста задания (подзаголовок Шифрограмма) в зашифрованном виде в битовом представлении и выбора одной из наиболее вероятных биграмм (подзаголовок Вероятная биграмма). Кроме того в блоке находятся кнопки управления «Предыдущая» и «Следующая» для перехода к соответственно предыдущий и последующей позиции, которая является вероятной позицией для биграммы;

- Сложение по модулю два. Блок предназначен для отыскания части вероятной гаммы путем сложения по модулю два битового представления вероятной биграммы и битового представления выбранной части зашифрованного текста;
- Положение отводов. Блок предназначен для ввода строки матрицы А, которая определяет положение отводов в регистре, или указания положения отводов путем заполнения соответствующих полей. **Положение отводов определяется студентом используя подпрограмму**, которая вызывается нажатием кнопки «Матрица А». **Выполняющий составляет вектора S(1),…,S(8)** и подпрограмма, используя метод основанный на нахождении обратной матрицы (с помощью метода Гаусса), находит матрицу обратную к X1 и матрицу А (значение первой строки, которой необходимо для определения положения отводов).
- Начальное заполнение. Блок предназначен для поиска начального заполнения выбранного регистра в соответствии с частью вероятной гаммы. Блок позволяет моделировать работу регистра на некоторое число блоков назад (1 блок=8 шагов) и получать таким образом нужное начальное заполнение, которое так же представлено в этом блоке;
- Гамма. Блок предназначен для получения и отображения гаммы, которая получается используя вид регистра и его начальное заполнение;
- Открытый текст. Блок необходим для получения текстового представления открытого текста, который получен сложением шифрованного текста и гаммы по модулю 2 и последующей перекодировкой;
- Управление. Блок является вспомогательным. Он предназначен для управлением автоматическим созданием файла отчета, нахождения матрицы А (имеется кнопка «Матрицап А», вызывающая подпрограмму поиска матрицы А) и для завершения работы (в данном блоке имеется кнопка «Выход», предназначенная для завершения лабораторной работы и закрытия рабочего окна).

Требования к размещению файлов

Для запуска лабораторной работы необходимо наличие файла LSR.exe, для ее выполнения нужен файл соответсвующего варианта (всего 25 различных вариантов $\Rightarrow$ 25 файлов). Файлы вариантов должны располагаться в том же каталоге, что и LSR.exe. Заметим, что файл отчета lsr.log будет создаваться так же в том же каталоге.

Необходимые знания

Для успешного выполнения лабораторной работы требуются базовые знания в области аддитивных шифров, в частности общие понятия о принципе действия линейного сдвигового регистра, а также пользовательские навыки работы с ОС Windows. Изложенный ранее краткий теоретический материал является достаточным для выполнения лабораторной работы.

Загрузка варианта

Каждому студенту преподавателем назначается вариант, и в соответствии со своим вариантом студент выполняет лабораторную работу.

Для загрузки соответствующего варианта предназначено поле выбора и кнопка «Загрузить» в верхней части блока «Вариант»

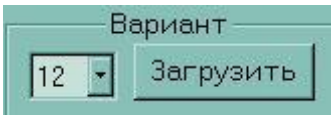


Рис. 25.Часть блока вариант

Выполняющий работу (студент) выбирает один из предложеных 25 номеров варианта и нажимает кнопку «Загрузить»

Рис. 26. Кнопка «Загрузить»

После нажатия кнопки в поле для чтения «Шифрограмма» появляется зашифрованный текст в битовом представлении или возникает сообщение об ошибке (см. Сообщения выдаваемые в процессе работы). Задачей выполняющего является расшифровка данного текста.

Рис. 27. Поле для чтения «Шифрограмма»

В поле для чтения «Шифрограмма» располагается двоичное представление зашифрованного текста. Каждые восемь бит в совокупности представляют собой одну закодированную букву. Ознакомиться с кодировкой можно в Приложении 1.

Всего в поле для чтения «Шифрограмма» представлено 16 закодированных букв (128 бит), таким образом зашифрованный текст представляет собой слово или фразу из 16 символов.

Выбор вероятных составляющих

Поскольку для дальнейшего расшифрования текста (а именно отыскания начального заполнения еще неопределенного регистра) нам требуется 2*L бит гаммы (L – разрядность регистра, в работе n=7 $\Rightarrow$ требуется 14 бит), то следующим шагом в выполнении работы является определение вероятной биграммы и ее положения в зашифрованном тексте. Для этого предназначено поле выбора «Вероятная биграмма»

Рис. 28. Поле «Вероятна биграмма»

На выбор выполняющему работу предлагается 8 биграмм (ЕН, ЕТ, НА, НИ, ПР, РА, СТ, ТО). Эти биграммы являются наиболее вероятными в русском языке, следовательно хотябы одна из них должна содержатся в зашифрованном сообщении (см. полную таблицу вероятностей биграмм в тексте в Приложении 2).

После выбора в поле «Текст» выроятной биграммы в соседнем поле для чтения появится битовое представление этой биграммы, кроме того тоже битовое представление появится в поле ввода «Вторая стр» блока «Сложение по модулю 2».

Рис. 29. Выбранная биграмма

На этом выбор вероятной биграммы закончен. Теперь необходимо определить ее положение в тексте. Будем последовательно перебирать все возможные положения данной биграммы при помощи двух управляющих кнопок «Предыдущая» и «Следующая» (подзаголовок Позиция в тексте).

Рис. 30. Позиция в тексте и управляющие кнопки

При нажатии на кнопку «Следующая» или «Предыдущая» в левом поле рис 7 появится часть шифрограммы, которая соответствует позициям, номера которых появятся в правом поле для чтения. Одновременно с этим поизойдет заполнение первого поля в блоке «Сложение по модулю 2» содержимым левого поля.

После того как выбрана биграмма и ее положение (то есть заполнены два верхних поля в блоке «Сложение по модулю 2»), в поле «=» блока «Сложение по модулю 2» появится результат сложения.

На этом определение вероятного местоположения вероятной биграммы и части вероятной гаммы закончен. Таким образом мы имеем предполагаемую биграмму, ее предполагаемое местоположение и, вероятно, часть ключа. Дальнейшие шаги покажут нам правильность или ошибочность выбора предполагаемых компонентов.

Нахождение вероятной части ключа

Данный шаг необходим для ручного сложения по модулю 2 собственных компонентов, то есть на предыдущем шаге вероятная часть ключа была найдена автоматически. Таким образом данное описание можно пропустить.

Для определения вероятной части ключа мы будем использовать блок «Сложение по модулю 2» с внесенными в него на предыдущем шаге начальными данными (вероятной биграммой и соответствующей ей части зашифрованного текста).

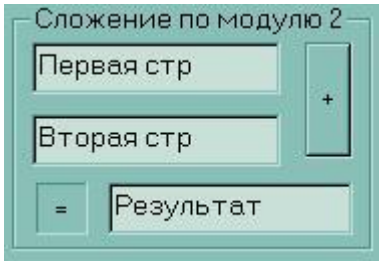


Рис. 31. Блок «Сложение по модулю 2»

Поскольку для определения вероятной части гаммы достаточно простого сложения по модулю два вероятной биграммы и соответствующей ей части зашифрованного текста, то для получения необходимо нажать кнопку «+».

Рис. 32. Кнопка «+» (сложить)

После чего в поле «=» появится искомая часть вероятной гаммы.

Рис. 33. Поле «=» - результат сложения

Таким образом мы определили 16 бит ключевой последовательности, которые нужны нам для отыскания положения отводов в регистре, начального заполнения регистра и, как следствие, всей гаммы и открытого текста. Строго говоря, 2 бита из этой последовательности являются избыточными, поскольку для определения положения отводов нужно 2*7=14 бит, а для получения начального заполнения всего 7 бит, но в связи с выбранной кодировкой символов приходится учитывать и эти 2 бита.

Определение положения отводов

Одним из ключевых шагов в выполнении работы является нахождение положения отводов в регистре. В данной работе предполагается определение положения отводов при

помощи метода основанного на нахождении обратной матрицы методом Гаусса, используя подпрограмму для обращения матрицы и нахождения матрицы А.

Для определения положения отводов выполняющему необходимо вызвать подпрограмму нахождения матрицы А, нажатием кнопки «Матрица А».

Рис. 34. Кнопка «Матрица А»

Затем в появившемся диалоговом окне необходимо заполнить поля представляющие собой поля для ввода векторов-столбцов S(1)…S(8) (см. Теоретическое введение).

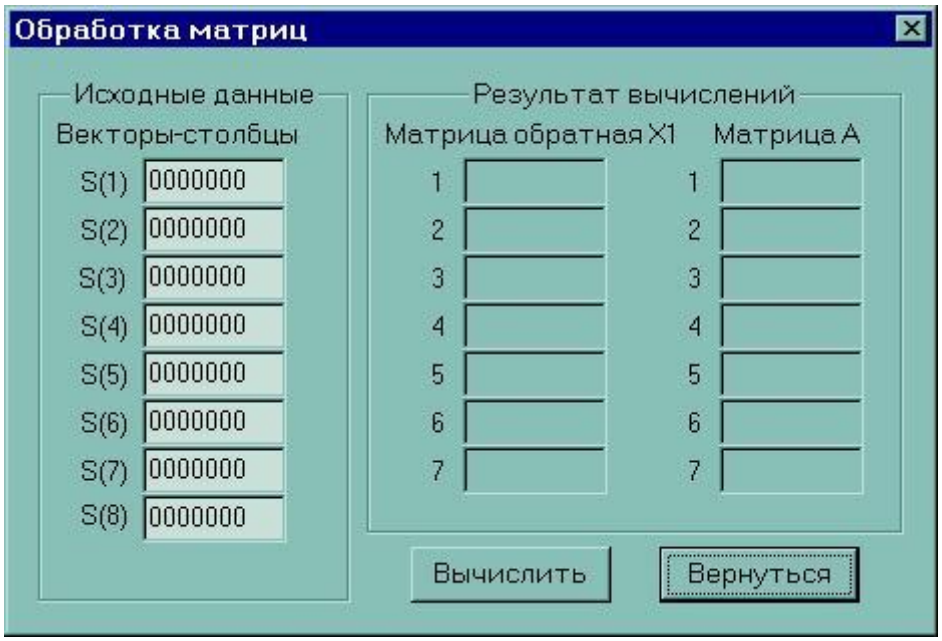


Рис. 35. Окно подпрограммы для нахождения матрицы А

После корректного заполнения вышеуказанных полей, необходимо нажать кнопку «Вычислить» и в соответствующих полях окна подпрограммы появятся строки соттветствующие матрицам X^{-1} и А.

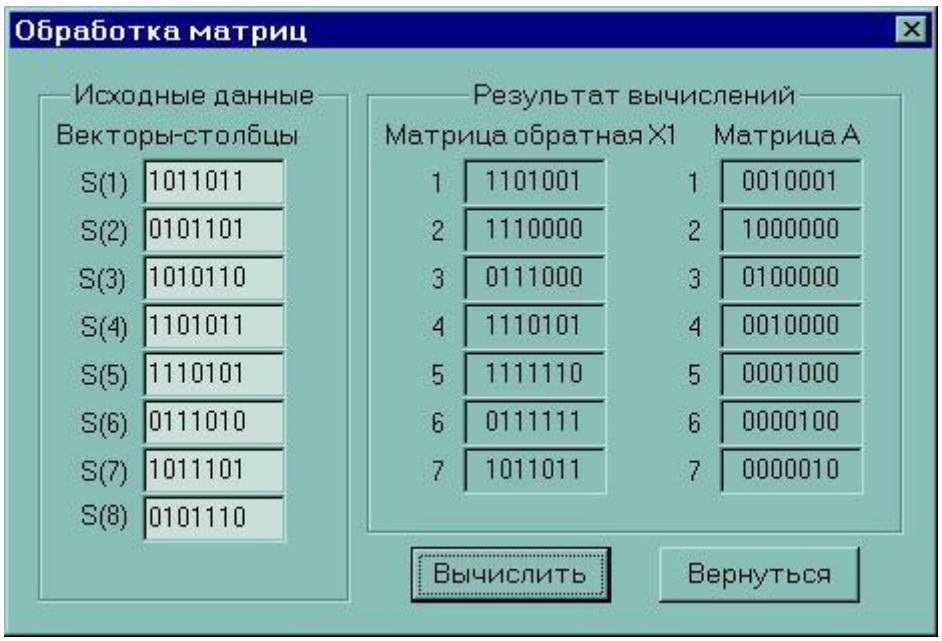


Рис. 36. Результат работы после нажатия на кнопку «Вычислить»

Следует отметить, что **матрица А должна иметь специальный вид**: первая строка – определяет положение отводов, в остальных строках под главной диаганалью находятся единицы, остальные нули. Если найденная матрица отличается по виду от вышеописанной, то была допущена ошибка на ранних шагах (например выбрана ошибочная биграмма). Строка 1 подраздела «Матрица А» является определяющей, то есть именно ее вид определяет положение отводов и именно ее необходимо заносить в поле А1 блока положение отводов, после выхода из подпрограммы (нажатием кнопки «Вернуться»).

Рис. 37. Блок положение отводов

Поскольку для определение отводов существует, по крайней мере, два способа определения положения отводов, то возможно 2 способа заполнения положения отводов. Рассмотрим эти способы.

1) Если отводы были определены при помощи нахождения обратной матрицы, то удобно ввести в поле «A1=» первую строку матрицы A, что будет являться заданием положения отводов и будет продублировано в нижней части блока.

Регистр по условию лабораторной работы является 7-разрядным, то есть первая строка матрицы A является последовательностью из 7 бит, каждый из которых говорит о наличии (если бит равен 1) или отсутствии (если бит равен 0) отвода в регистре.

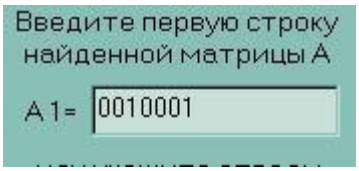


Рис. 38. Строковое задание положения отводов

2) Если положение отводов были найдены другим способом, то удобно непосредственно указать отводы присутствующие в регистре, то есть активировать чек-бокс соответствующий присутствующему отводу, введенные данные продублируются в строке «A1=»

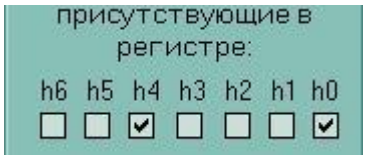


Рис. 39. Непосредственный выбор отводов

Необходимо внимательнее подходить к проблеме поиска отводов в регистре, так как неправильное определение положения отводов влечет за собой неправильный результат.

Поиск начального заполнения

Для того, чтобы расшифровать текст необходима гамма такой же длины как и зашифрованный текст. Для получения гаммы нам нужно знать начальное заполнение регистра. Для определения начального заполнения в лабораторной работе используется блок «Начальное заполнение».

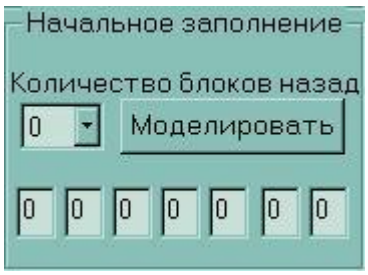


Рис. 40. Блок «Начальное заполнение»

Поскольку для получения начального заполнения необходимо промоделировать обратную работу регистра, то существует кнопка «Моделировать», при нажатии на которую происходит обратное моделирование работы регистра на заданное количество шагов, которое задается в поле выбора «Количество блоков назад».

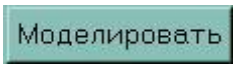


Рис. 41. Кнопка «Моделировать»

Поскольку нецелесообразно моделировать обратную работу на число шагов не кратное 8 (так как 1 символ закодирован 8 битами), то число шагов заменено числом блоков. То есть 1 блок = 8 шагов, и при моделировании на 1 блок производится обратная работа на 8 шагов. Выбор количества блоков назад ограничен 14 (для обеспечния отсутствия цикличности).

Выбор количества блоков на которое производится обратное моделирование важен для правильности определения начального заполнения. Количество блоков для обратного моделирования является первой цифрой в номере позиции вероятной биграммы (см. Подзаголовок «Позиция в тексте» блока «Вариант» правое поле для чтения). То есть если позиция представлена как 3-4 (то есть вероятная биграмма находится на позиции 3 и позиции 4), то обратное моделирование должно производиться на 3 блока назад.

После нажатия на кнопку «Моделировать» автоматически производится поиск начального заполнения регистра. Для этого используются первые 7 бит строки «=» блока «Сложение по модулю 2» и регистр из блока «Положение отводов» (точнее положение его отводов). Полученный результат отображается в схематичном представлении ячеек регистра, заполненных нулями или единицами.

Рис. 42. Схематичное представление ячеек регистра

Кроме того для удобства выполнения работы сразу после нажатия кнопки «Моделировать», если не произошло никаких ошибок заполняются поля в блоках «Гамма» и «Открытый текст». Таким образом после нажатия кнопки «Моделировать» **при правильном выборе вероятной биграммы, ее положения в тексте и правильного определения положения отводов получается открытый текст**.

Получение гаммы

Для расшифрования сообщения нам необходимо получить гамму, которая использовалась при зашифровке. Этот шаг выполняется автоматически при нажатии на кнопку «Моделировать» из блока «Начальное заполнение». Для контроля за правильностью гаммы предназначен блок «Гамма»

Рис. 43. Блок «Гамма»

Гамма представляет собой последовательность 128 двоичных символов, которые выводятся в поле для чтения «Гамма». Данная последовательность используется для последующего сложения по модулю 2 с шифрограммой и получения открытого текста в битовом представлении.

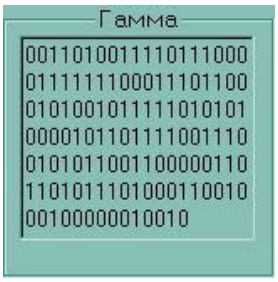


Рис. 44. Поле для чтения «Гамма»

Получение открытого текста

Открытый текст получается автоматически при нажатии на кнопку «Моделировать» блока «Начальное заполнение», однако для контроля предусмотрены дополнительный возможности.

Открытый текст представляется в программе перекодированным из битовой последовательности в символы и для этого используется блок «ОТКРЫТЫЙ ТЕКСТ».

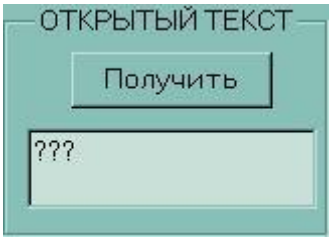


Рис. 45. Блок «Открытый текст»

Для получения открытого текста достаточно нажать кнопку «Получить». Программа автоматически произведет сложение гаммы и зашифрованного текста, а потом перекодирует битовый текст в символьный.

Рис. 46. Кнопка «Получить»

В результате в поле ввода появится некоторый текст, который либо представляет собой осмысленное сообщение (тогда работа успешно завершена), либо непонятный набор символов (увы, придется повторить некоторые шаги заново). Во втором случае наиболее вероятным местом ошибки является неправильно выбранное количество блоков для обратного моделирования (как следствие неправильные начальное заполнения и гамма). Если же вы уверены в своих действиях по выбору количества блоков, тогда неверно выбрана биграмма или ее положение (то есть придется вернуться к п 5.3.4), кроме того возможно неверное определение положения отводов (придется вернуться к п 5.3.5)

Если полученный открытый текст устраивает выполняющего то работа завершена.

Отчет о проделанной работе

Для контроля за выполнением работы предусмотрено специальное средство – отчет о проделанной работе. В данной лабораторной отчет представляется в форме файла отчета: файл отчета – необходим для предоставления проверяющему (преподавателю);

Форма отчета включаются путем выбора соответствующего элемента в блоке «Управление».

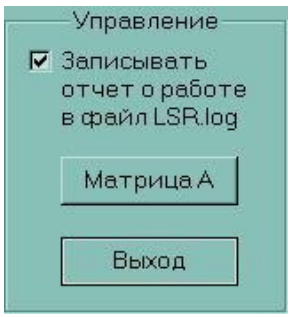


Рис. 47. Блок «Управление»

Выключатель «Записывать отчет о работе в файл LSR.log» включает\выключает режим записи произведенных действий в файл «lsr.log».

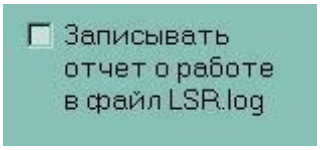


Рис. 48. Выключатель «Записывать отчет о работе в файл LSR.log»

При включении данного выключателя создается или перезаписываетя или дозаписывается (в зависимости от ситуации) файл «lsr.log», в который записываются действия пользователя по отысканию открытого текста.

Для составления отчета надо:

a) После запуска лабораторной работы включить переключатель «Записывать отчет о работе в файл LSR.log» (включен по умолчанию). Если уже существует lsr.log, то ответить на вопрос: «Переписывать?». Если такого файла нет, то он создастся;

b) Загрузить вариант. В файле появится запись «Начало LOG*********»;

c) Выполнить действия по поиску открытого текста;

d) Найти открытый текст.

e) Выйти из программы при помощи кнопки «Выход». В файле появится запись «Конец LOG*********».

Рис. 49. Кнопка «Выход»

В файле отчета будут задокументированны основные действия по поиску открытого текста. Отчет предоставляется в распечатанном виде от фразы «Начало LOG**********» до фразы «Конец LOG**********».

Сообщения выдаваемые в процессе работы

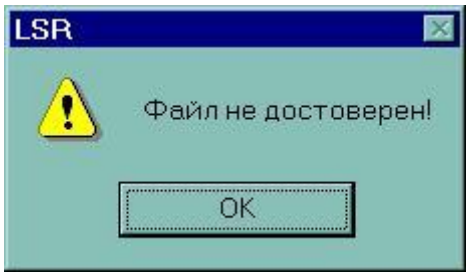
Во время выполнения лабораторной работы по мере возникновения исключительных ситуаций программа выдает сообщния, которые соответствуют определенному событию. Сообщения выводятся в отдельном окне. Программа перед продолжением работы ждет реакции пользователя на выведенное сообщение. Рассмотрим возможные сообщения.

Сообщения об ошибках

Это наиболее большая группа сообщений. Они возникают при вводе ошибочных или ложных данных в соответствующие поля ввода.

- *Файл не достоверен!*

Сообщение выдается, когда файл загружаемого варианта является недостоверным. То есть посчитанная контрольная сумма не совпадает с той которая записана в файле. Внешний вид окна сообщения:



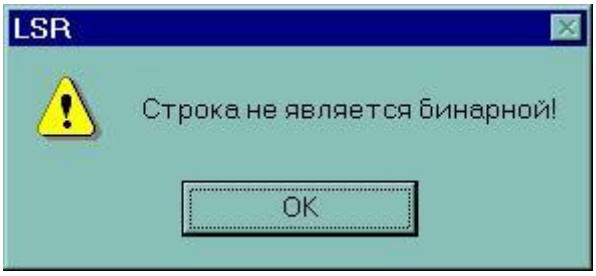
Действия пользователя:

- Нажать кнопку «ОК».

Найти правильный файл варианта или загрузить другой вариант.

- *Строка не является бинарной!*

Сообщение выдается при содержании в строке «=» блока «Сложение по модулю 2» хотя бы одной цифры отличной от нуля или единицы или при содержании в строке S1…S8 подпрограммы «Обработка матриц» хотя бы одной цифры отличной от нуля или единицы. Внешний вид окна сообщения:

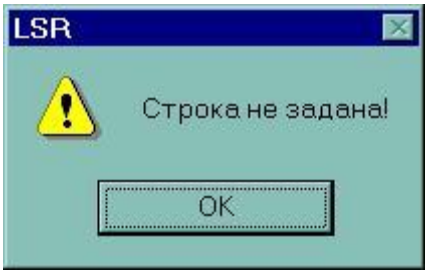


Действия пользователя:

- Нажать кнопку «ОК».
- Правильно заполнить строку «=» или строку S1…S8.

- *Строка не задана!*

Сообщение выдается, когда не задана (пустая) одна из двух строк (Первая стр или Вторая стр) в блоке «Сложение по модулю 2». Внешний вид окна сообщения:

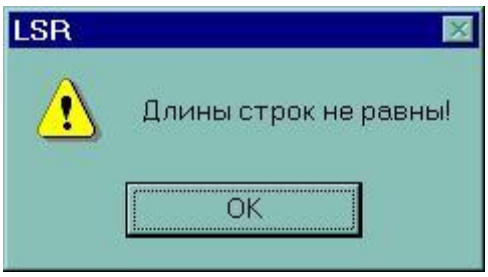


Действия пользователя:

- Нажать кнопку «ОК».
- Заполнить поля ввода «Первая стр» «Вторая стр».

- *Длины строк не равны!*

Сообщение выдается, когда длины строк складываемых в блоке «Сложение по модулю 2» различаются. Внешний вид окна сообщения:

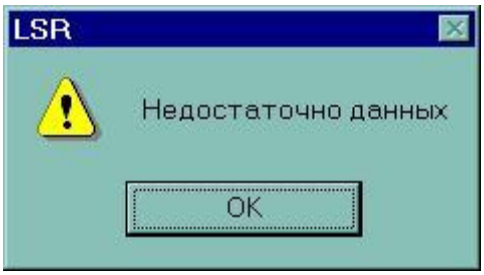


Действия пользователя:

- Нажать кнопку «ОК».
- Выравнять длину заполненных полей ввода «Первая стр» «Вторая стр».

- *Недостаточно данных*

Сообщение выдается, когда длина строки «=» блока «Сложение по модулю 2» меньше 14 бит или длина строки S1…S8 подпрограммы «Обработка матриц» менее 7 бит. Внешний вид окна сообщения:



Действия пользователя:

- Нажать кнопку «ОК».
- Увеличить длину последовательности данных в поле «=» или длину строк S1…S8.

- *Необходим 0 или 1*

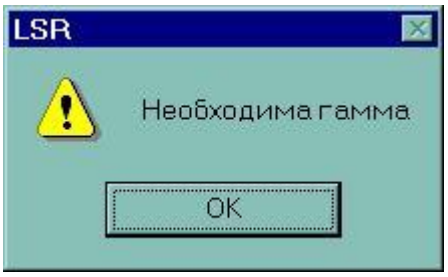
Сообщение выдается, когда одна из схематично изображенных ячеек регистра в блоке «Начальное заполнение» заполнена цифрой оличной от нуля ими единицы. Внешний вид окна сообщения:

Действия пользователя:

- Нажать кнопку «ОК».
- Правильно заполнить ячейки регистра.

- *Необходима гамма*

Сообщение выдается, когда необходимая гамма в поле «Гамма» не была получена, то есть не заполнено поле для чтения «Гамма». Внешний вид окна сообщения:



Действия пользователя:

- Нажать кнопку «ОК».
- Получить гамму нажатием кнопки «Получить гамму» в блоке «Гамма».

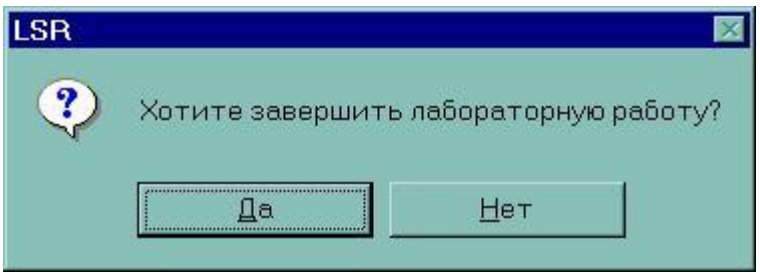
Сообщения-вопросы

Реакцией пользователя на сообщения данного типа должен стать выбор одного из предложенных вариантов ответа.

- *Хотите завершить лабораторную работу?*

Сообщение выдается при нажатии на кнопку «Выход» 

, то есть при желании выполняющего завершить выполнение работы. Внешний вид окна сообщения:

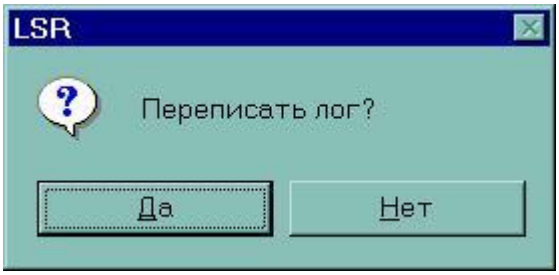


Действия пользователя:

- Нажать кнопку «Да», если действительно есть желание завершить лабораторную работу.
- Нажать кнопку «Нет», если нет желания завершать лабораторную работу.

- *Переписать лог?*

Сообщение выдается при включении режима записи файла-отчета, при условии, что файл уже существует. То есть при согласии на перезапись предыдущий вариант будет уничтожен. Внешний вид окна сообщения:



Действия пользователя:

- Нажать кнопку «Да», если необходимо создать новый отчет.
- Нажать кнопку «Нет» и отказаться от создания, если нужен файл старого отчета.

Критические ошибки

Система выдает сообщения данного типа, когда происходит ошибка препятствующая дальнейшему выполнению лабораторной работы.

- Не могу открыть файл!

Сообщение выдается в случае, когда программа не может в силу каких-либо причин открыть на чтение файл заданного варианта. Внешний вид окна сообщения:

Действия пользователя:

- Нажать кнопку «ОК».
- Рзрешить проблему доступа к файлу заданного варианта.

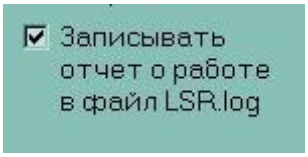
Пример

Рассмотрим для примера выполнение следующего задания:

Задание: Выриант №12

Решение: Начнем с нахождения открытого текста. Запускаем LSR.exe

a) Включаем выключатель записи варианта в файл.



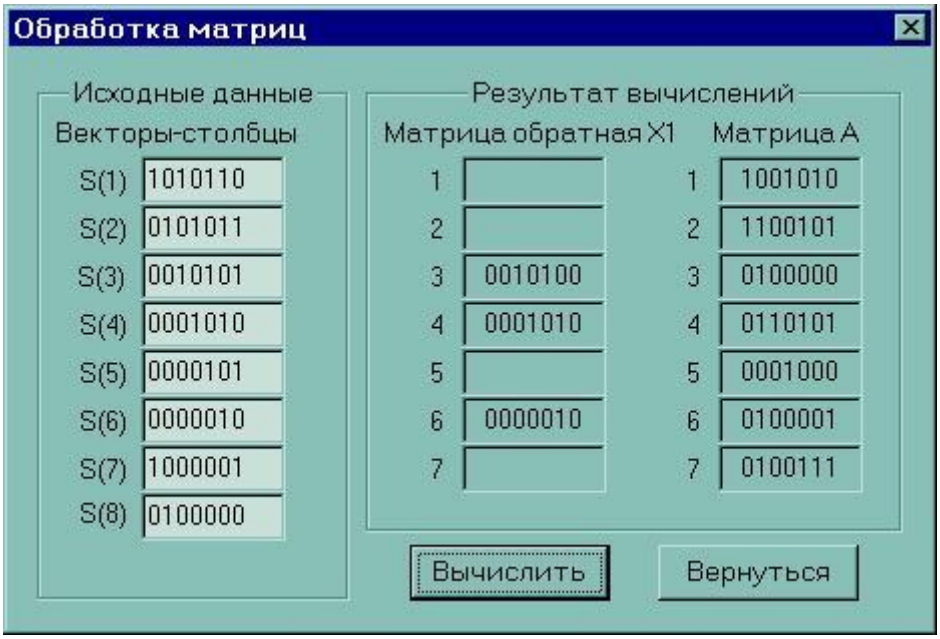
b) Загружаем файл для 12 варианта.

c) Выбираем вероятную биграмму – «ЕН». Получаем во второой строке блока «Сложение по модулю 2» строку «1100010111001101»

d) Предполагаем, что она стоит на месте 0-1. Таким образом, ничего не меняя, получаем в первой строке блока «Сложение по модулю 2» строку «0110101000001011»

e) Вероятная часть гаммы получена автоматически сложением двух строк.

f) Определим положение отводов в регистре при помощи метода основанного на нахождении обратной матрицы и введем первую строку матрицы А. Вызовем подпрограмму «Обработка матриц» кнопкой «Матрица А», заполним поля S1…S8 и нажмем кнопку «Вычислсть»



Как видно матрица A не имеет специального вида (см. выше), значит можно нажать кнопку «Вернуться» и выбрать следующее вероятное положение.

g) Выберем следующую позицию

Данная позиция также не даст положительных результатов.

Если продолжать выполнение, то мы переберем все возможные позиции вероятной биграммы (до 14-15) и не придем к удовлетворительному результату. Следовательно была ошибка в выборе биграммы.

h) Выберем новую биграмму и будем перебирать вероятные положения биграмм заново.

Перебирая положения и биграммы мы дойдем до вероятного положения биграммы 13-14 и биграммы ET. Остановимся на этом случае.

i) Вероятная часть гаммы найдена автоматически

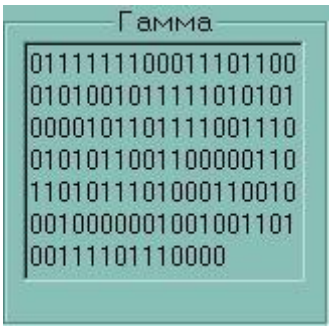
j) Определим положение отводов в регистре при помощи подпрограммы. То есть введем в поля ввода значения векторов S1…S8 (которые получаются из вероятной части ключа (см. поле ввода «=»)), нажмем кнопку «Вычислить» и получим значение строк обратной матрицы X^{-1} и значение строк матрицы A. В данном случае матрица A имеет специальный вид, значит первая строка представляет собой положение отводов в регистре.

k) Введем найденное положение отводов в блоке «Положение отводов»

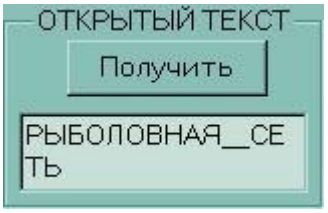
l) Промоделируем работу на 13 блоков назад и получим:

- Начальное заполнение регистра

- Гамму



- Открытый текст



Мы получили осмысленный текст и файл отчета «lsr.log», который содержит информацию о проделанной работе.

Теперь необходимо по части ключа «1001001101001111» с помощью алгоритма Берлекэмпа-Месси убедиться в правильности определения отводов регистра.

На вход алгоритма подаем битовую последовательность: «10010011010011», которая является частью ключа. На выходе мы получим минимальный регистр, который мог породить такую последовательность.

Составим таблицу для упрощения записей:

g_N	D	T(D)	C(D)	L	m	B(D)	N
-	-	-	1	0	-1	1	0
1	1	1	1+D	1	0	1	1
0	1	1+D	1	1	0	1	2
0	0	1+D	1	1	0	1	3
1	1	1	$1+D^3$	3	3	1	4
0	0	1	$1+D^3$	3	3	1	5
0	0	1	$1+D^3$	3	3	1	6
1	0	1	$1+D^3$	3	3	1	7
1	1	$1+D^3$	$1+D^3+D^4$	5	7	$1+D^3$	8
0	0	$1+D^3$	$1+D^3+D^4$	5	7	$1+D^3$	9
1	0	$1+D^3$	$1+D^3+D^4$	5	7	$1+D^3$	10

0	0	$1+D^3$	$1+D^3+D^4$	5	7	$1+D^3$	11
0	1	$1+D^3+D^4$	$1+D^3+D^4$	7	11	$1+D^3+D^4$	12
1	0	$1+D^3+D^4$	$1+D^3+D^7$	7	11	$1+D^3+D^4$	13
1	0	$1+D^3+D^4$	**$1+D^3+D^7$**	7	11	$1+D^3+D^4$	14

Таким образом мы получили, что ячейки регистра, породившего заданную последовательность, задаются формулой $1+D^3+D^7$, если привести это выражение к уравнению, задающему положение отводов, то получим $H(X)=X^7+X^4+1$. Следовательно положение отводов в регистре, найденное двумя способами, оказалось одинаковым.

На этом выполнение работы завершено.

Ответ: РЫБОЛОВНАЯ__СЕТЬ

Теперь необходимо распечатать файл отчета, приложить решение алгоритмом Берлекэмпа-Месси и сдать на проверку преподавателю.

2.2.3. ЗАДАНИЕ НА КУРСОВУЮ РАБОТУ ПО ШИФРОВАНИЮ С ОТКРЫТЫМ КЛЮЧОМ

КРИПТОАНАЛИЗ АЛГОРИТМА RSA [2]

Концепция криптографии с открытым ключом была предложена Уитфилдом Диффи (Whitfield Diffie) и Мартином Хеллманом (Martin Hellman), и, независимо от них, Ральфом Мерклом (Ralph Merkle). Основная идея заключается в том, чтобы использовать ключи парами, состоящими из ключа зашифрования и ключа расшифрования, которые невозможно вычислить один из другого.

В 1976 г. вышла основополагающая работа [4]. С этого времени было создано много алгоритмов, использующих концепцию открытых ключей. Алгоритм является общедоступным, нет необходимости в секретных каналах связи. Общая схема выглядит следующим образом:

1. Каждый пользователь генерирует пару ключей: один для шифрования, другой для дешифрования.

2. Каждый пользователь публикует свой ключ шифрования, размещает его в открытом для всех доступе. Второй ключ, соответствующий открытому, сохраняется в секрете.

3. Если пользователь *A* собирается послать сообщение пользователю *B*, он шифрует сообщение открытым ключом пользователя *B*.

4. Когда пользователь *B* получает сообщение, он дешифрует его с помощью своего личного (секретного) ключа. Другой получатель не сможет дешифровать сообщение, поскольку личный ключ *B* знает только *B*.

В 1978 г. появилась работа [4], в которой Рон Райвест (Ron Rivest), Ади Шамир (Adi Shamir) и Лен Адлеман (Len Adleman) предложили алгоритм с открытым ключом. Схема Райвеста–Шамира–Адлемана (RSA) получила широкое распространение.

Опишем процесс шифрования. Исходный текст должен быть переведен в числовую форму, этот метод считается известным. В результате этого текст представляется в виде одного большого числа. Затем полученное число разбивается на части (блоки) так, чтобы каждая из них была числом в промежутке
[0, N – 1] (о выборе N — см. ниже). Процесс шифрования одинаков для каждого блока. Поэтому мы можем считать, что блок исходного текста представлен числом x, $0 \le x \le N-1$.

Каждый абонент вырабатывает свою пару ключей. Для этого он генерирует два больших простых числа p и q, вычисляет произведение $N = p \cdot q$. Затем он вырабатывает случайное число e, взаимно простое со значением функции Эйлера от числа N, $\varphi(N) = (p-1)\cdot(q-1)$ и находит число d из условия
$e \cdot d = 1 (\mathrm{mod}\ \varphi(N))$. Так как $(e, \varphi(N)) = 1$, то такое число d существует и оно единственно. Пару (N, e) он объявляет открытым ключом и помещает в открытый доступ. Пара (N, d) является секретным ключом. Для расшифрования достаточно знать секретный ключ. Числа p, q, $\varphi(N)$ в дальнейшем не нужны, поэтому их можно уничтожить.

Пользователь *A*, отправляющий сообщение x абоненту *B*, выбирает из открытого каталога пару (N, e) абонента *B* и вычисляет шифрованное сообщение $y = x^e \pmod N$. Чтобы получить исходный текст, абонент B вычисляет $y^d \pmod N$. Так как $e \cdot d \equiv 1 (\mathrm{mod}\ \varphi(N))$, т. е. $e \cdot d = \varphi(N) \cdot k + 1$, где k – целое, то применяя теорему Эйлера, получим: следующее соотношение: $y^d \equiv (x^e)^d \equiv x^{ed} \equiv x^{\varphi(N)\cdot k+1} \equiv (x^{\varphi(N)})^k \cdot x \equiv x (\mathrm{mod}\ N)$. *Пример* 1. Пусть p = 7, q = 17. Тогда $N = 7 \cdot 17 = 119$, $\varphi(N) = 96$. Выбираем значение e: $e < 96$, $(e, 96) = 1$. Пусть в нашем случае e = 5. Находим d: $d = 1/e \pmod{96}$. Получаем d = 77, так как $77 \cdot 5 = 4 \cdot 96 + 1$. Открытый ключ (119,5), личный ключ (119,77). Пусть x = 19. Для зашифрования число 19 возводим в 5-ю степень по модулю 119, тогда имеем 19^5 = 2 476 099 и остаток от деления 2 476 099 на 119 равен 66. Итак, $y = 19^5 \bmod 119 = 66$, а расшифрование $x = 66^7 \bmod 119 = 19$.

О вычислениях

Как шифрование, так и расшифрование в RSA предполагают использование операции возведения целого числа в целую степень по модулю *N*. Если возведение в степень выполнять непосредственно с целыми числами и только потом проводить сравнение по модулю *N*, то промежуточные значения окажутся огромными. Здесь можно воспользоваться свойствами арифметики в классах вычетов $(a \bmod N)\cdot(b \bmod N) \bmod N = (ab) \bmod N$. Таким образом, можно рассмотреть промежуточные результаты по модулю *N*. Это делает вычисления практически выполнимыми.

О стойкости RSA

Безопасность алгоритма RSA основана на трудоемкости разложения на множители больших чисел. Современное состояние технических средств разложения на множители таково, что число, содержащее 193 десятичных знака, факторизовано в 2005 г. Следовательно, выбираемое *N* должно быть больше. Большинство общепринятых алгоритмов вычисления простых чисел p и q носят вероятностный характер.

О выборе чисел *p* и *q*

Для работы алгоритма RSA нужны простые числа. Наиболее приемлемым является генерация случайных чисел и последующая проверка их на простоту. Существуют вероятностные тесты, определяющие с заданной степенью достоверности факт простоты числа. Возникает вопрос, что произойдет, если числа окажутся составными? Можно свести вероятность такого события до приемлемого минимума, используя тесты на простоту. Кроме того, если такое событие произойдет, это будет быстро обнаружено — шифрование и расшифрование не будут работать.

Кроме разрядности *p* и *q*, к ним предъявляются следующие дополнительные требования:

– числа не должны содержаться в списках известных больших простых чисел;

– они не должны быть близкими, так как иначе можно воспользоваться для факторизации *N* методом Ферма и решить уравнение $(\frac{p+q}{2})^2 - N = (\frac{p-q}{2})^2$.

– в алгоритме RSA всегда есть эквивалентные по расшифрованию показатели степеней, например d и $d' = d + [p-1, q-1]$. При этом эквивалентных решений тем больше, чем

больше $(p-1, q-1)$. В лучшем случае $(p-1, q-1) = 2$,
$p = 2t + 1$, $q = 2s + 1$, где s, t – нечетные числа с условием $(s, t) = 1$.

Чтобы исключить возможность применения методов факторизации накладывают следующее ограничение: числа $p-1$, $p+1$, $q-1$, $q+1$ не должны разлагаться в произведение маленьких простых множителей, должны содержать в качестве сомножителя хотя бы одно большое простое число. В 1978 г. Райвест сформулировал наиболее сильные требования. Числа $p_1 = \frac{p-1}{2}$, $p_2 = \frac{p+1}{2}$, $q_1 = \frac{q-1}{2}$, $q_2 = \frac{q+1}{2}$ должны быть простыми, причем числа $p_1 - 1$ и $q_1 - 1$ не должны разлагаться в произведение маленьких простых.

О выборе параметров *e* и *d*

Рассмотрим вопрос о выборе экспонент шифрования и расшифрования. Так как значения e и d определяют время зашифрования и расшифрования, то можно назвать ряд ситуаций, в которых желательно иметь малое значение e и d. Например, при использовании системы RSA при защите электронных платежей с применением кредитных карточек естественным является требование использования небольших значений экспоненты d у владельца карточки и большого значения экспоненты e у центрального компьютера.

Однако выбор малых параметров e или d представляется небезопасным по ряду соображений. Если малым является секретный параметр d, то можно применить метод перебора малых значений до получения искомого числа d. А если малым является параметр e, то достаточно большое число открытых сообщений, удовлетворяющих неравенству $x < \sqrt[e]{N}$, будут зашифровываться простым возведением в степень $y = x^e \pmod N$ и поэтому их можно найти путем извлечения корня степени e.

Другая аналогичная ситуация может сложиться, когда у нескольких абонентов используется одинаковая экспонента e. Тогда становится возможна атака на основе китайской теоремы об остатках (см. ниже).

Подготовка текста к шифрованию

Сначала нужно каким-либо способом представить текст сообщения в виде упорядоченного набора чисел по модулю N. Это еще не процесс шифрования, а только подготовка к нему.

Пример 2. Для простоты предположим, что текст сообщения содержит слова, записанные только заглавными буквами. Первый шаг состоит в замене каждой буквы сообщения числом. Пусть наша таблица замен имеет вид:

0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7

8	9	0	1	2	3	4	5	6	7	8	9	0	1

Пробел между словами будем заменять числом 99.

Например, пусть открытый текст – это девиз «ПОЗНАЙ СЕБЯ». Тогда его цифровое представление имеет вид: 2524172310199927151141.

Пусть в нашем примере p = 149, q = 157, тогда N = 23393. Поэтому цифровое представление открытого текста нужно разбить на блоки, меньшие, чем 23393. Одно из таких разбиений выглядит следующим образом:

2524 – 1723 – 10199 – 9271 – 511 – 41.

Конечно, выбор блоков неоднозначен, но и не совсем произволен. Например, во избежание двусмысленностей, на стадии расшифровки не следует выделять блоки, начинающиеся с нуля.

При расшифровке сообщения получаем последовательность блоков, затем их соединяем вместе и получаем число. После этого числа заменяют буквами в соответствии с таблицей, приведенной выше.

Обратим внимание на то, что в этом примере каждую букву кодируем двузначным числом. Это сделано для предотвращения неоднозначности. Если бы мы пронумеровали буквы не по порядку, начиная с 1, т. е. А соответствует 1, Б соответствует 2 и т. д., то было бы непонятно, что обозначает блок 12: пару букв АБ или букву Л, двенадцатую букву алфавита. Конечно, для кодирования можно использовать любые однозначные соответствия между буквами и числами, например ASCII-кодировку, что чаще всего это и делается.

Продолжим пример: выбираем p = 149, q = 157, вычисляем $\varphi(N) = 23\,088$. Теперь нужно выбрать число e, взаимно простое с $\varphi(N)$. Наименьшее простое, не делящее $\varphi(N)$, равно 5. Положим e = 5. Зашифруем первый блок сообщения: вычисляем $2524^5 \bmod 23393 = 22752$; далее $1723^5 \bmod 23393 = 6198$.

$10199^5 \bmod 23393 = 14204$,

$9271^5 \bmod 23393 = 23191$,

$511^5 \bmod 23393 = 10723$,

$41^5 \bmod 23393 = 14065$.

Теперь шифрованный текст имеет вид

22752619814204231911072314065

В нашем примере $N = 23393$, $e = 5$. Применив алгоритм Эвклида к числам $\varphi(N) = 23088$ и $e = 5$, найдем $d = e^{-1} \bmod 23088 = 13853$. Значит для расшифровки блоков шифртекста мы должны возвести этот блок в степень 13583 по модулю 23393. В примере первый блок шифртекста – число 22752, тогда получим $22752^{13853} \bmod 23393 = 2524$.

Разбиение числа на блоки можно произвести различными способами. При этом *промежуточные* результаты зависят от способа разбиения, однако *конечный* результат – не зависит.

Атаки на алгоритм RSA

Для дешифрации необходимо по известным N, e и шифртексту y найти такое $x \in ((Z/N))^*$, что $y = x^e \bmod N$.

Попытаемся решить сравнение при конкретных y, затем использовать гомоморфность отображения $D(x)$.

Один из возможных способов следующий: пусть имеется набор пар $\{(x_1, y_1)...(x_k, y_k)\}$ с условием, что $x_i^e = y_i \bmod N$, $1 < y < N$, $(y, N) = 1$. Если каким-либо образом удалось представить y в виде $y = y_1^{s_1} \cdot ... \cdot y_k^{s_k} \bmod N$ с целыми s_k, то $x = x_1^{s_1} \cdot ... \cdot x_k^{s_k}$ будет решением сравнения $y = x^e \bmod N$.

Пример 3. В наличии имеется открытый ключ N = 31459, e = 5 и набор пар соответствующих друг другу исходных и зашифрованных сообщений: (23, 18707), (755, 26871), (631, 6384). Требуется расшифровать шифртекст y = 11 638. Для этого представим y в виде $y = 18\,707^{-1} \cdot 26\,871^3 \cdot 6\,384^{-2} = 11\,638$. Отсюда легко вычислить исходное сообщение: $x = 23^{-1} \cdot 755^3 \cdot 631^{-2} = 28\,260$.

Заметим, что этот подход не менее труден, чем поиск алгоритма решения сравнения $y = x^e \bmod N$.

Взлом RSA при неудачном выборе параметров криптосистемы

Само по себе использование RSA не обеспечивает безопасности. Дело еще в деталях реализации. Приведем ряд примеров. Для простоты вычислений будем работать с небольшими числами. Цель – показать особенности, не зависящие от размера.

Пример 4. Пусть пользователь выбрал N = 2047, e = 179, d = 411. Так как 2047 = 2389, а $\varphi(23)=22,\ \ \varphi(89)=88$ имеют наименьшее общее кратное 88, то любой обратный к 179 по модулю 88, например 59, будет действовать как d.

Пример 5. Число N = 536813567 является произведением простого числа Мерсенна 8191 и простого числа Ферма 65537. Это очень плохой выбор.

Пример 6. Число 23360947609 является очень плохим выбором для N из-за того, что два его простых делителя слишком близки к друг другу. Пусть $p > q$, тогда имеем $N=(\frac{p+q}{2})^2+(\frac{p-q}{2})^2$. Обозначим: $t=\frac{p+q}{2},\ \ S=\frac{p-q}{2}$. Так как S мало, то t – целое число, лишь немного большее $\sqrt{N}$, причем $t^2 - N$ является полным квадратом. Проверяем подряд целые числа $t > \sqrt{N}$**.** В нашем примере t_1 = 152843, t_2 = 152844, t_3 = 152845 и $t^3-N=804^2$, тогда $p=152\,845+804,$

p = 152845 – 804. Таким образом, мы с третьей попытки нашли p и q. Количество попыток, необходимых для факторизации N, можно при известных p и q вычислить по следующей формуле: $k=\sqrt{p\cdot q+(\frac{p-q}{2})^2}-\left[\sqrt{p\cdot q}\right]$, где [$x$] – операция округления x до ближайшего целого числа.

Атака повторным шифрованием

Строим последовательность: $y_1=y,\ \ y_i=y_{i-1}^e(\mathrm{mod}\ N),\ i>1$. Итак, $y_m=y^{e^m}(\mathrm{mod}\,N)$, а так как $\left(e,\varphi(N)\right)=1$, то существует такое натуральное число m, что $e^m\equiv 1(\mathrm{mod}\,\varphi(N))$. Но тогда $y^{e^m-1}\equiv 1(\mathrm{mod}\,N)$, отсюда следует, что $y^{e^m}\equiv y(\mathrm{mod}\,N)$, значит, y_{m-1} – решение сравнения $y=x^e\left(\mathrm{mod}\,N\right).$

Пример 7. Пусть у нас имеется открытый ключ N =84517 , e = 397 и зашифрованное им сообщение y = 8646. Необходимо найти исходный текст x. Возведем y в степень e и получим y_2 = 37043. Будем повторять операцию до тех пор, пока не получим $y_n = y$. y_{n-1} – искомое

сообщение: $y_3 = 5569$, $y_4 = 61833$,

$y_5 = 83891$, $y_6 = 16137$, $y_7 = 8646$. y_6 является решением сравнения $y = x^e \pmod N$, а, следовательно, искомым сообщением x.

Замечание. Анализ метода повторного шифрования хорошо показывает необходимость соблюдения требований на выбор p и q для обеспечения стойкости. В данном примере $d = 82\,225$. Неудачный выбор криптосистемы привел к тому, что атака методом повторного шифрования дала результат почти сразу, тогда как нахождение d потребовало бы на порядок больших вычислений.

Атака на основе Китайской теоремы об остатках.

Как отмечалось ранее, системы шифрования с открытыми ключами работают сравнительно медленно. Для повышения скорости шифрования RSA на практике используют малую экспоненту зашифрования.

Если выбрать число e небольшим или таким, чтобы в его двоичной записи было мало единиц, то процедуру шифрования можно значительно ускорить. Например, выбрав $e = 3$ (при этом ни $p - 1$, ни $q - 1$ не должны делиться на 3), мы сможем реализовать шифрование с помощью одного возведения в квадрат по модулю N и одного перемножения. Выбрав $e = 2^{16} - 1 = 65\,537$ – число, двоичная запись которого содержит только две единицы, мы сможем реализовать шифрование с помощью 16 возведений в квадрат по модулю N и одного перемножения. Если экспонента e выбирается случайно, то реализация шифрования по алгоритму RSA потребует s возведений в квадрат по модулю N и в среднем $s/2$ умножений по тому же модулю, где 5 – длина двоичной записи числа N. Вместе с тем выбор небольшой экспоненты e может привести к негативным последствиям. Дело в том, что у нескольких корреспондентов могут оказаться одинаковые экспоненты e.

Пусть, например, три корреспондента имеют попарно взаимно простые модули N_1, N_2, N_3 и общую экспоненту $e = 3$. Если еще один пользователь посылает им некое циркулярное сообщение x, то криптоаналитик противника может получить в свое распоряжение три шифрованных текста $y_i = x^3 (\mathrm{mod}\, N_i)$,

$i = 1, 2, 3$. Далее он может найти решение системы сравнений, лежащее в интервале $0 < y < N_1 \cdot N_2 \cdot N_3$

$$\begin{cases} y \equiv y_1 (\text{mod } N_1), \\ y \equiv y_2 (\text{mod } N_2), \\ y \equiv y_3 (\text{mod } N_3), \end{cases}$$

По китайской теореме об остатках такое решение единственно, а так как $x^3 < N_1, N_2, N_3$, то $y = x^3$. Значение x можно найти, вычислив кубический корень $x = \sqrt[3]{y}$.

Отметим, что выбор малой экспоненты расшифрования d также нежелателен в связи с возможностью определения d простым перебором. Известно также что если $d < \sqrt[4]{N}$, то экспоненту d легко найти, используя непрерывные дроби.

Пример 8. Три пользователя имеют модули $N_1 = 26549$, $N_2 = 45901$, $N_3 = 25351$. Все пользователи используют экспоненту $e = 3$. Всем пользователям было послано некое сообщение x, причем пользователи получили сообщения $y_1 = 5366$, $y_2 = 814$, $y_3 = 4454$. Найдем $M_0 = N_1 \cdot N_2 \cdot N_3 = 30893378827799$. Далее находим

$m_1 = N_2 \cdot N_3 = 1163636251$

$m_2 = N_1 \cdot N_3 = 673043699$

$m_3 = N_1 \cdot N_2 = 1218625649$

$n_1 = m_1^{-1} \bmod N_1 = 13533$

$n_2 = m_2^{-1} \bmod N_2 = 27930$

$n_3 = m_3^{-1} \bmod N_3 = 22354$

$S = y_1 \cdot n_1 \cdot m_1 + y_2 \cdot n_2 \cdot m_2 + y_3 \cdot n_3 \cdot m_3 = 84501028038745578 + 15301661957638980 + + 121332116653000684 = 221134806649385242$

$S \bmod M_0 = 1000000000$

$x = (S \bmod M_0)^{1/3} = 1000$ – исходное сообщение, отправленное пользователям.

Бесключевое чтение

Пусть два пользователя выбрали одинаковый модуль N и разные экспоненты e_1 и e_2. Если один пользователь посылает им некое циркулярное сообщение x, то криптоаналитик противника может получить в свое распоряжение два шифрованных текста $y_1 = x^{e_1} (\text{mod } N)$ и $y_2 = x^{e_2} (\text{mod } N)$. В таком случае криптоаналитик может получить исходное сообщение, используя расширенный алгоритм Евклида, находим r, s такие, что $re_1 + se_2 = 1$. Отсюда

получаем: $y_1^r y_2^s = x^{re_1+se_2} = x$

Пример 9. Два пользователя применяют общий модуль N = 137759, но разные взаимно простые экспоненты e_1 = 191 и e_2 = 233. Пользователи получили шифртексты y_1 = 60197 и y_2 = 63656, которые содержат одно и то же сообщение. Найдем исходное сообщение методом бесключевого чтения. Так как e_1 и e_2 взаимно просты, то найдем такие r и s, что $re_1 + se_2 = 1.$ С помощью расширенного алгоритма Евклида находим r = 61, s = –50. Искомое сообщение

$$x = y_1^r \cdot y_2^s = 60197^{61} \cdot 63656^{-50} = 1234$$

Выводы

Как видно из приведенных выше примеров (а также из примеров выполнения заданий лабораторных работ) выбор параметров криптосистемы является ответственной задачей. Параметры необходимо выбирать в строгом соответствии с требованиями. Существующими в настоящими время методами (и при использовании существующих в настоящее время вычислительных мощностей) атака на алгоритм и/или криптосистему возможна лишь при неудачном выборе параметров. В процессе выполнения заданий лабораторных работ вы убедитесь в обоснованности перечисленных требований к параметрам криптосистемы. В частности, необходимо обеспечить каждому пользователю уникальные значения p, q и уникальное значение e, удовлетворяющие требованиям, приведенным выше.

Пример выполнения лабораторной работы
с помощью программы BCalc

Исходные данные: N = 65815671868057; e = 7423489; C = 38932868535359. Найти

1. Вычисляем n = [sqrt(N)] + 1. В поле A помещаем N, в поле B – 2; нажимаем кнопку «D = A^(1/B)». В поле D заносится число 8112686, в первую строку таблицы – сообщение «[error]». Это свидетельствует, о том, что N не является квадратом целого числа.

2. $t_1 = n + 1$. Возводим число t_1 в квадрат: A: = 8112687, B: = 2, C: = 0 (возведение в квадрат будет производиться не по правилам модульной арифметики), нажимаем «$D = A\text{^}B \bmod C$» => $D = t_1$^2 = 65815690359969. Вычисляем

$w_1 = t_1$^2 – N. Для этого A:= t_1^2, B:= –N, затем нажимаем «$D = A + B$» => D =

= w_1 = 18491912. Проверяем, является ли w_1 квадратом целого числа: A:= w_1,

B:= 2, нажимаем «$D = A$^(1/B)» => в первой строке таблицы появляется сообщение «[error]», следовательно проделываем п. 2 заново с $t_2 = n + 2$ и так далее, пока не найдем, что некое w_i является квадратом целого числа.

3. При вычислении квадратного корня w_5 первая строка таблицы остается пустой, а D = sqrt(w_5) = 9132, что свидетельствует об успехе факторизации.

t_5 = 8112691.

4. Вычисляем $p = t_5$ + sqrt(w_5); A:= t_5, B:= sqrt(w_5), нажимаем «$D = A + B$» => $D = p$ = 8121823; $q = t_5$ – sqrt(w_5) = 8103559. Вычисляем

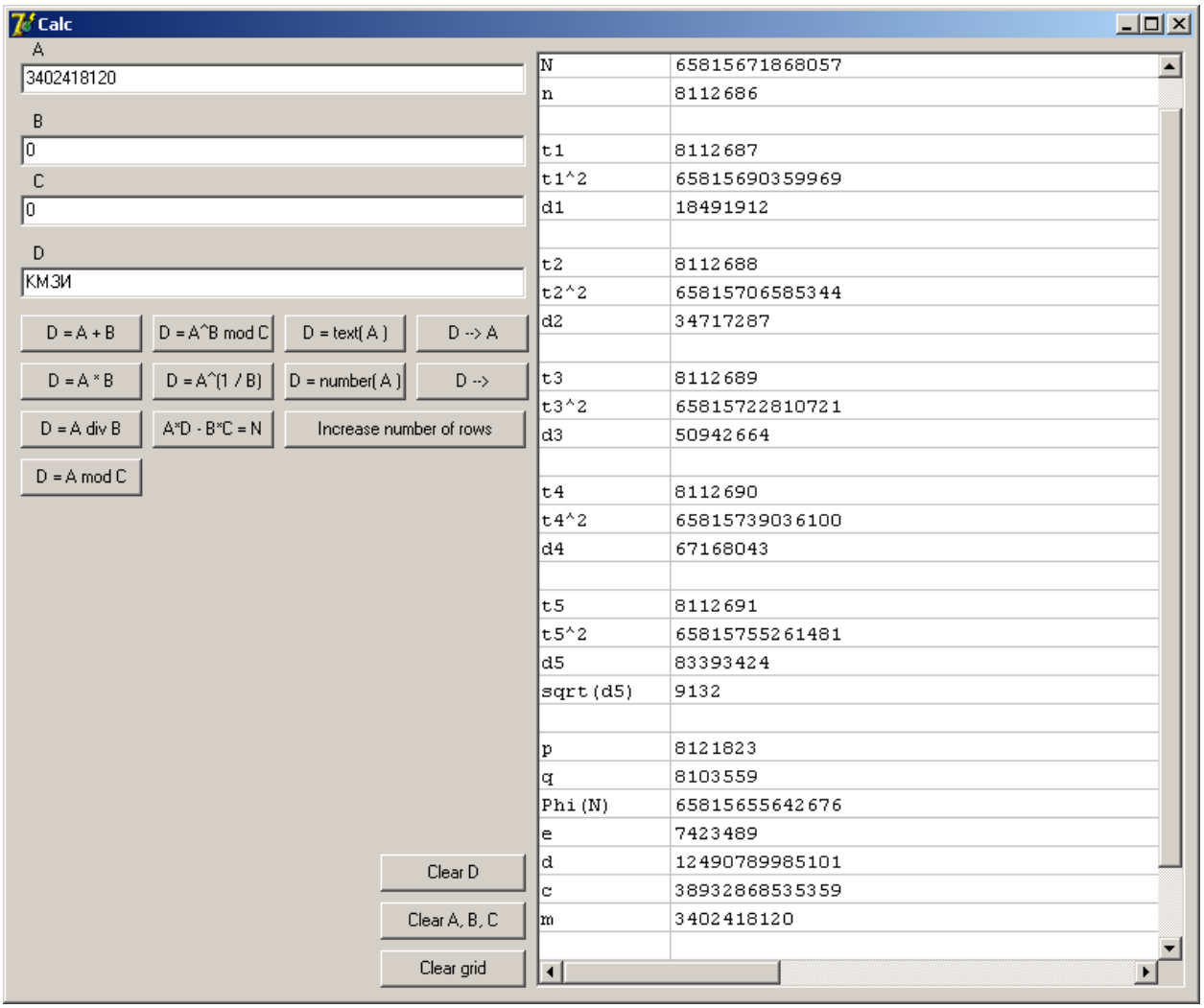
Phi(N) = (p – 1)(q – 1), A:= 8121822, B:= 8103558, нажимаем «$D = A \cdot B$» => D =

= Phi(N) = 65815655642676. Вычисляем d, как обратный к e: A:= e, B:= –1,

C:= Phi(N), нажимаем «D = A^B mod C» => $D = d$ = 12490789985101.

5. Производим дешифрацию шифрблока C: A:= C; B:= d; C:= N. Нажимаем «D = A^B mod C». В поле D находится исходное сообщение M = 3402418120. Переводим M в текстовый вид. Для этого A:= M, нажимаем «D = text(A)» => D = = «КМЗИ».

Снимок экрана с окном программы «BCalc» приведен ниже**.**



Лабораторная работа 2

Атака на алгоритм шифрования RSA методом повторного шифрования

Цель работы: изучить атаку на алгоритм шифрования RSA посредством повторного шифрования.

Ход работы:

– ознакомиться с теорией, изложенной в п. 1.2 («Атака повторным шифрованием»);

– получить вариант задания у преподавателя (табл. 2 приложения);

– по полученным исходным данным, используя метод перешифрования, определить порядок числа *e* в конечном поле $Z_{\varphi(N)}$;

– используя значение порядка экспоненты, получить исходный текст методом перешифрования;

– результаты и промежуточные вычисления оформить в виде отчета.

Примечание. Для выполнения практического задания рекомендуется использовать программу PS.exe, которая находится на диске, прилагаемом к методическим указаниям.

Пример выполнения лабораторной работы

с помощью программы PS

Исходные данные: N = 453819149023; e = 1011817; C = 442511634532.

1. Определить порядок экспоненты. Для этого необходимо ввести значение модуля в поле *N*, экспоненты в поле *e*, в поле *Y* записывается произвольное число, меньше чем *N*. После этого нужно нажать кнопку **Запуск повторного шифрования** и дождаться, пока в поле *X* появится значение, равное корню *e* степени от числа *Y* по модулю *N*, а в поле *i* – порядок *e* в конечном поле $Z_{\varphi(N)}$. В данном примере он составляет 435.

2. Дешифровать зашифрованный текст. Для этого нужно в область редактирования поля *C* поместить блоки зашифрованного текста, разделенные символом конца строки, значение модуля в поле *N*, экспоненты в поле *e* и порядка экспоненты в поле *i*. Затем нажать на кнопку **Дешифрация** и дождаться появления исходного текста в области редактирования *M*. Ответ – открытый текст – «null».

Лабораторная работа 3

Атака на алгоритм шифрования RSA

Методом бесключевого чтения

Цель работы: изучить атаку на алгоритм шифрования RSA посредством метода бесключевого чтения.

Ход работы:

– ознакомиться с теорией, изложенной в п. 1.2 («Бесключевое чтение»);

– получить вариант задания у преподавателя (табл. 3 приложения);

– по полученным данным определить значения r и s при условии, чтобы $e_1 \cdot r - e_2 \cdot s = 1$. Для этого необходимо использовать расширенный алгоритм Евклида;

– используя полученные выше значения r и s, записать исходный текст;

– результаты и промежуточные вычисления значений для любых трех блоков шифрованного текста оформить в виде отчета

Примечание. Для выполнения практического задания рекомендуется использовать программу BCalc.exe, которая находится на диске, приложенном к методическим указаниям.

Пример выполнения лабораторной работы

с помощью программы «BCalc»

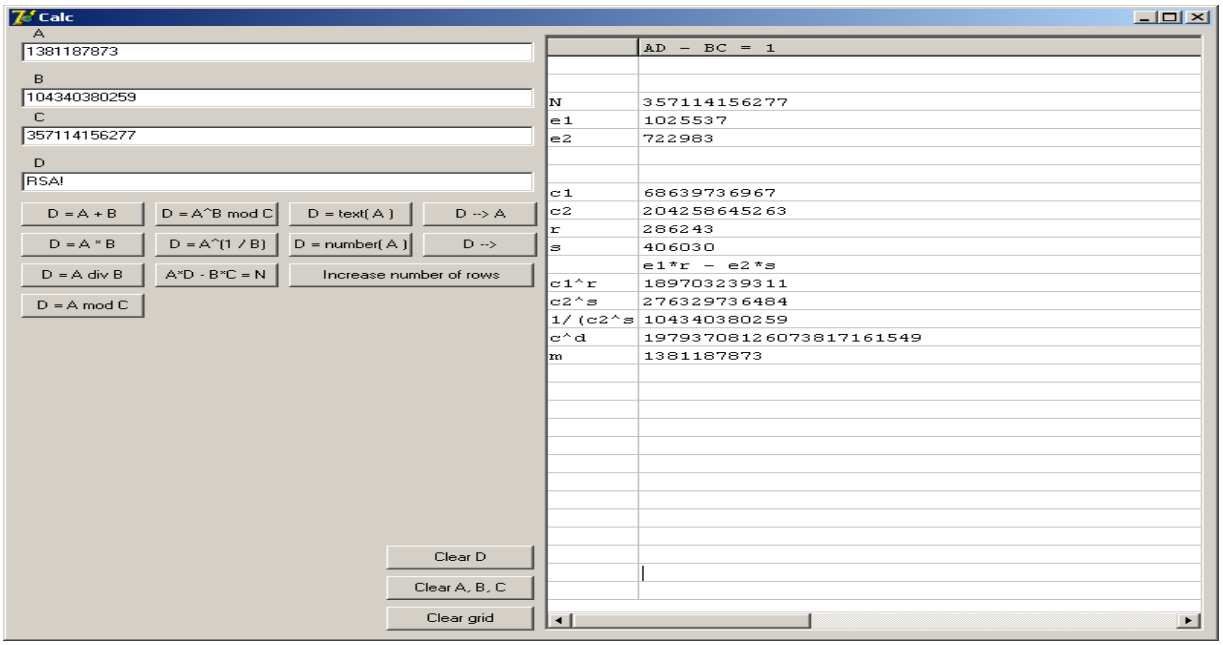
Исходные данные: $N = 357114156277$; $e_1 = 1025537$; $e_2 = 722983$;
$C_1 = 68639736967$; $C_2 = 204258645263$.

1. Решаем уравнение $e_1 \cdot r - e_2 \cdot s = \pm 1$. Для этого в поле A помещаем значение e_1, в поле B – значение e_2. Нажимаем кнопку «$A \cdot D - B \cdot C = N$», затем – кнопку $C = s = 406030$; $D = r = 286243$.

2. Производим дешифрацию: c_1 возводим в степень r, а c_2 – в степень $-s$ по модулю N, тогда $c_1 \wedge r = 189703239311$, $c_2 \wedge (-s) = 104340380259$.

После этого результаты перемножаем и получаем, что $m \wedge (e_1 \cdot r - e_2 \cdot s) =$
$= 19793708126073817161549$. Далее берем модуль от полученного значения: $(m \wedge (e_1 \cdot r - e_2 \cdot s) \bmod N) = 1381187873$ и преобразуем в текст «RSA!».

Ниже приведен снимок экрана с окном программы «BCalc».



Лабораторная работа 4

Атака на алгоритм шифрования RSA,

Основанный на китайской теореме об остатках

Цель работы: изучить атаку на алгоритм шифрования RSA посредством Китайской теоремы об остатках.

Ход работы:

– ознакомиться с теорией, изложенной в п. 1.2 («Атака на основе Китайской теоремы об остатках»);

– получить вариант задания у преподавателя (табл. 4 приложения). Экспонента для всех вариантов $e = 3$;

– используя Китайскую теорему об остатках, получить исходный текст;

– результаты и промежуточные вычисления значений для любых трех блоков шифрованного текста оформить в виде отчета

Примечание. Для выполнения практического задания рекомендуется использовать программу BCalc.exe, которая находится на диске, приложенном к методическим указаниям.

Пример выполнения лабораторной работы

с помощью программы «BCalc»

Исходные данные: $N_1 = 363542076673$; $N_2 = 728740902979$;
$N_3 = 522993716719$; $C_1 = 246562834516$; $C_2 = 291375746601$; $C_3 = 222724269731$.

Последовательно вычисляем следующие значения:

$M_0 = N_1 \cdot N_2 \cdot N_3 = 138555669564008119302694433926047373$;

$m_1 = N_2 \cdot N_3 = 381126913374147389205901$;

$m_2 = N_1 \cdot N_3 = 190130221862955939995887$;

$m_3 = N_1 \cdot N_2 = 264927981225542872108867$;

$n_1 = m_1\text{^} (-1) \bmod N_1 = 287993142707$;

$n_2 = m_2\text{^} (-1) \bmod N_2 = 106614970676$;

$n_3 = m_3\text{^} (-1) \bmod N_3 = 32171022265$;

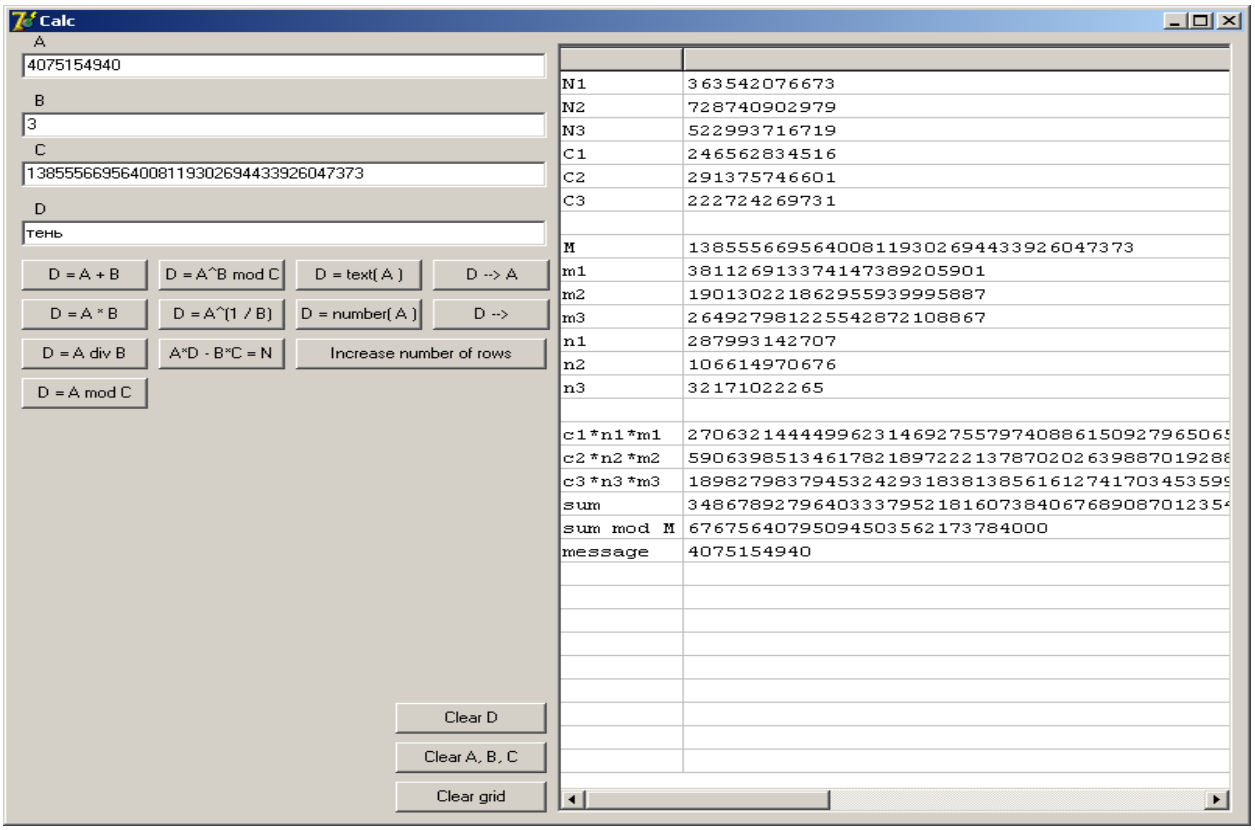
$S = c_1 \cdot n_1 \cdot m_1 + c_2 \cdot n_2 \cdot m_2 + c_3 \cdot n_3 \cdot m_3 = 348678927964033379521816073840676890870123543 29$;

$S \bmod M_0 = 676756407950945035621737840 00$;

$M = (S \bmod M_0)^{\wedge}(1/e) = 4075154940$;

text(M) = «тень».

Ниже приведен снимок экрана с окном программы «BCalc».



Пример криптоанализа алгоритма RSA

Атака на алгоритм шифрования rsa посредством

Метода Ферма

Основная идея заключается в том, чтобы использовать ключи парами, состоящими из ключа зашифрования и ключа расшифрования, которые невозможно вычислить один из другого.

В 1976 г. вышла основополагающая работа [4]. С этого времени было создано много алгоритмов, использующих концепцию открытых ключей. Алгоритм является общедоступным, нет необходимости в секретных каналах связи. Общая схема выглядит следующим образом:

1. Каждый пользователь генерирует пару ключей: один для шифрования, другой для дешифрования.

2. Каждый пользователь публикует свой ключ шифрования, размещает его в открытом для всех доступе. Второй ключ, соответствующий открытому, сохраняется в секрете.

3. Если пользователь A собирается послать сообщение пользователю B, он шифрует сообщение открытым ключом пользователя B.

4. Когда пользователь B получает сообщение, он дешифрует его с помощью своего личного (секретного) ключа. Другой получатель не сможет дешифровать сообщение, поскольку личный ключ B знает только B.

RSA-ключи генерируются следующим образом:

1. Выбираются два различных случайных простых числа p и q заданного размера (например, 1024 бита каждое).

2. Вычисляется их произведение $n = p \cdot q$, которое называется модулем.

3. Вычисляется значение функции Эйлера от числа n:

$$\varphi(n) = (p-1) \cdot (q-1).$$

4. Выбирается целое число e ($1 < e < \varphi(n)$), взаимно простое со значением функции $\varphi(n)$. Обычно в качестве e берут простые числа, содержащие небольшое количество единичных бит в двоичной записи, например, простые числа Ферма 17,257 или 65537.

- Число e называется открытой экспонентой
- Время, необходимое для шифрования с использованием быстрого возведения в степень, пропорционально числу единичных бит в e.
- Слишком малые значения e, например 3, потенциально могут ослабить безопасность схемы RSA

5. Вычисляется число d, мультипликативно обратное к числу e по модулю $\varphi(n)$, то есть число, удовлетворяющее сравнению:

$$d \cdot e \equiv 1 \pmod{\varphi(n)}.$$

- Число d называется секретной экспонентой. Обычно, оно вычисляется при помощи расширенного алгоритма Евклида.

6. Пара $\{e, n\}$ публикуется в качестве открытого ключа RSA

7. Пара $\{d, n\}$ играет роль закрытого ключа RSA и держится в секрете.

Вычисления

Как шифрование, так и расшифрование в RSA предполагают использование операции возведения целого числа в целую степень по модулю N. Если возведение в степень выполнять непосредственно с целыми числами и только потом проводить сравнение по модулю N, то промежуточные значения окажутся огромными. Здесь можно воспользоваться свойствами

арифметики в классах вычетов $(a \bmod N)\times(b \bmod N) \bmod N = (ab) \bmod N$. Таким образом, можно рассмотреть промежуточные результаты по модулю N. Это делает вычисления практически выполнимыми.

О выборе чисел p и q

Для работы алгоритма RSA нужны простые числа. Наиболее приемлемым является генерация случайных чисел и последующая проверка их на простоту. Существуют вероятностные тесты, определяющие с заданной степенью достоверности факт простоты числа. Возникает вопрос, что произойдет, если числа окажутся составными? Можно свести вероятность такого события до приемлемого минимума, используя тесты на простоту. Кроме того, если такое событие произойдет, это будет быстро обнаружено — шифрование и расшифрование не будут работать.

Кроме разрядности p и q, к ним предъявляются следующие дополнительные требования:

– числа не должны содержаться в списках известных больших простых чисел;

– они не должны быть близкими, так как иначе можно воспользоваться для факторизации N методом Ферма и решить уравнение $(\frac{p+q}{2})^2 - N = (\frac{p-q}{2})^2$.

– в алгоритме RSA всегда есть эквивалентные по расшифрованию показатели степеней, например d и $d' = d + [p-1, q-1]$. При этом эквивалентных решений тем больше, чем больше (p – 1, q – 1). В лучшем случае (p – 1, q – 1) = 2,p = 2t + 1, q = 2s + 1, где s, t – нечетные числа с условием (s, t) = 1.

Чтобы исключить возможность применения методов факторизации накладывают следующее ограничение: числа p – 1, p + 1, q – 1, q + 1 не должны разлагаться в произведение маленьких простых множителей, должны содержать в качестве сомножителя хотя бы одно большое простое число. В 1978 г. Райвест сформулировал наиболее сильные требования. Числа $p_1 = \frac{p-1}{2},\ p_2 = \frac{p+1}{2},\ \ q_1 = \frac{q-1}{2},\ \ q_2 = \frac{q+1}{2}$ должны быть простыми, причем числа $p_1 – 1$ и $q_1 – 1$ не должны разлагаться в произведение маленьких простых.

О выборе параметров e и d

Рассмотрим вопрос о выборе экспонент шифрования и расшифрования. Так как значения e и d определяют время зашифрования и расшифрования, то можно назвать ряд ситуаций, в которых желательно иметь малое значение e и d. Например, при использовании системы RSA при защите электронных платежей с применением кредитных карточек естественным

является требование использования небольших значений экспоненты d у владельца карточки и большого значения экспоненты e у центрального компьютера.

Однако выбор малых параметров e или d представляется небезопасным по ряду соображений. Если малым является секретный параметр d, то можно применить метод перебора малых значений до получения искомого числа d. А если малым является параметр e, то достаточно большое число открытых сообщений, удовлетворяющих неравенству $x < \sqrt[e]{N}$, будут зашифровываться простым возведением в степень $y = x^e \pmod N$ и поэтому их можно найти путем извлечения корня степени e.

Другая аналогичная ситуация может сложиться, когда у нескольких абонентов используется одинаковая экспонента e. Тогда становится возможна атака на основе китайской теоремы об остатках (см. ниже).

Ход работы

1. Вычисляем n = [sqrt(N)] + 1. В поле A помещаем N, в поле B – 2; нажимаем кнопку «D = A^(1/B)». В поле D заносится число 8112686, в первую строку таблицы – сообщение «[error]». Это свидетельствует, о том, что N не является квадратом целого числа.

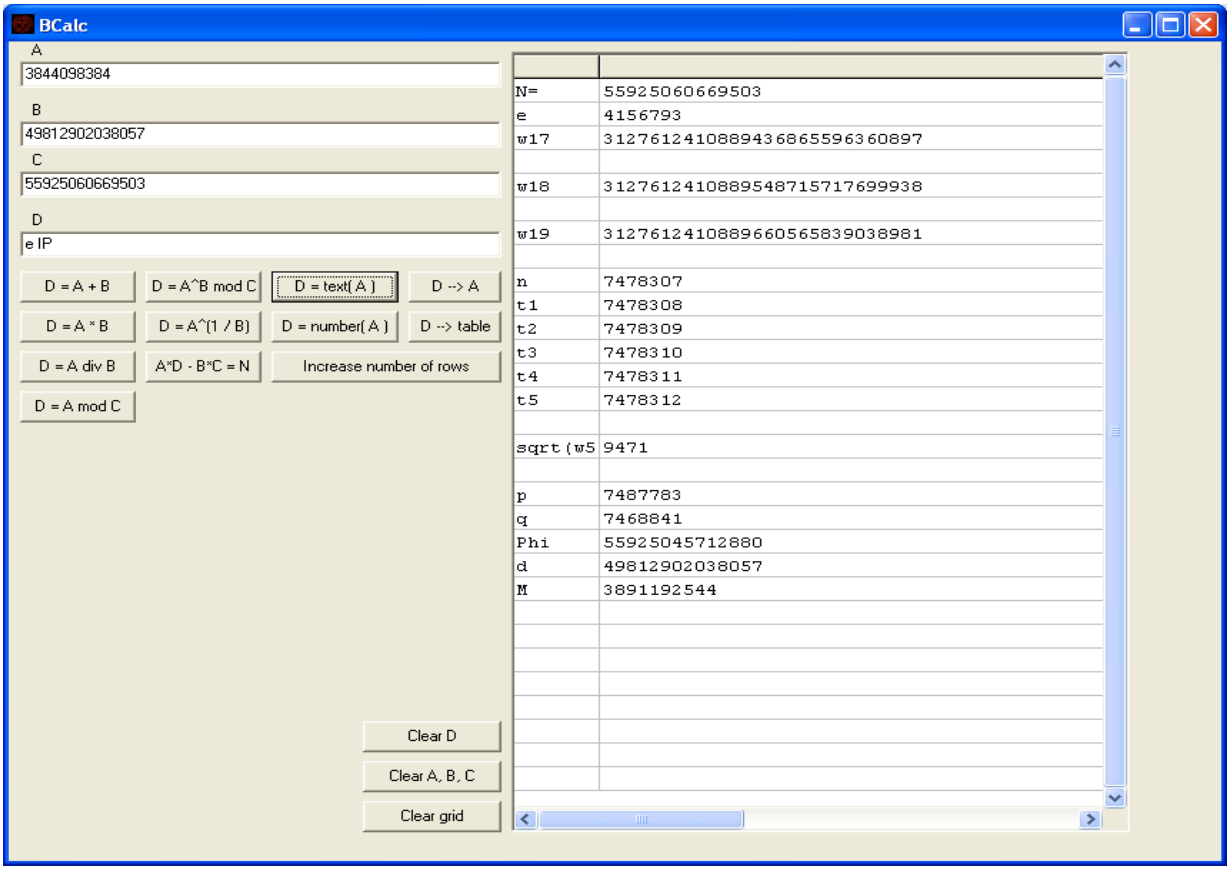
2. $t_1 = n + 1$. Возводим число t_1 в квадрат: A: = 8112687, B: = 2, C: = 0 (возведение в квадрат будет производиться не по правилам модульной арифметики), нажимаем «$D = A\text{^}B \bmod C$» => $D = t_1$^2 = 65815690359969. Вычисляем
$w_1 = t_1\text{^}2 - N$. Для этого A:= t_1^2, B:= –N, затем нажимаем «$D = A + B$» => D =
= w_1 = 18491912. Проверяем, является ли w_1 квадратом целого числа: A:= w_1,
B:= 2, нажимаем «D = A^(1/B)» => в первой строке таблицы появляется сообщение «[error]», следовательно проделываем п. 2 заново с $t_2 = n + 2$ и так далее, пока не найдем, что некое w_i является квадратом целого числа.

3. При вычислении квадратного корня w_5 первая строка таблицы остается пустой, а D = sqrt(w_5) = 9132, что свидетельствует об успехе факторизации.
t_5 = 8112691.

4. Вычисляем $p = t_5$ + sqrt(w_5); A:= t_5, B:= sqrt(w_5), нажимаем «$D = A + B$» => $D = p$ = 8121823; $q = t_5$ – sqrt(w_5) = 8103559. Вычисляем
Phi(N) = (p – 1)(q – 1), A:= 8121822, B:= 8103558, нажимаем «$D = A \cdot B$» => D =
= Phi(N) = 65815655642676. Вычисляем d, как обратный к e: A:= e, B:= –1,
C:= Phi(N), нажимаем «$D = A\text{^}B \bmod C$» => $D = d$ = 12490789985101.

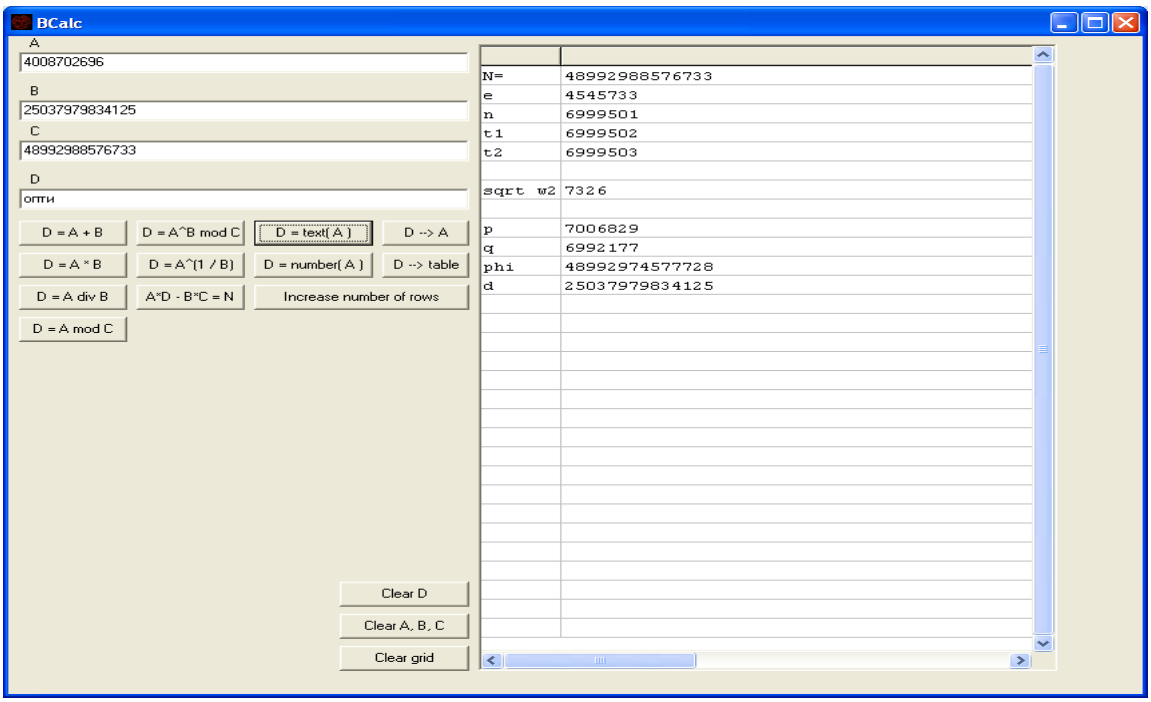
5. Производим дешифрацию шифрблока C: A:= C; B:= d; C:= N. Нажимаем «$D = A\text{^}B \bmod C$». В поле D находится исходное сообщение M = 3402418120. Переводим M в текстовый вид. Для этого A:= M, нажимаем «D = text(A)» => D = = «КМЗИ».

Вариант №20



Ответ: «зования протокола TCP: фрагментация на уровне IP»

Вариант №23.



Ответ: «оптимальным MTU на уровне DLC маленький

Как видно из приведенных выше примеров (а также из примеров выполнения заданий лабораторных работ) выбор параметров криптосистемы является ответственной задачей. Параметры необходимо выбирать в строгом соответствии с требованиями. Существующими в настоящими время методами (и при использовании существующих в настоящее время вычислительных мощностей) атака на алгоритм и/или криптосистему возможна лишь при неудачном выборе параметров. В процессе выполнения заданий лабораторных работ вы убедитесь в обоснованности перечисленных требований к параметрам криптосистемы. В частности, необходимо обеспечить каждому пользователю уникальные значения p, q и уникальное значение e, удовлетворяющие требованиям, приведенным выше

2.3. ПЕРЕЧЕНЬ ИНДИВИДУАЛЬНЫХ ЗАДАНИЙ НА КУРСОВЫЕ РАБОТЫ ПО КОДИРОВАНИЮ И ШИФРОВАНИЮ ИНФОРМАЦИИ В СИСТЕМАХ СВЯЗИ

№ п/п	Темы курсовых работ
1.	Аппаратно-программный комплекс визуализации и исследования метода свёрточного декодирования на основе последовательного алгоритма
2.	Аппаратно-программный комплекс для исследования и визуализации «КОДЕР КОДА ХЕММИНГА»
3.	Аппаратно-программный комплекс для визуализации и исследования алгоритма Витерби для декодирования сверточного кода
4.	Аппаратно-программный комплекс для визуализации и исследование кодов Рида-Соломона в каналах с независимыми ошибками на базе MATLAB
5	Аппаратно-программный комплекс для визуализации и исследования алгоритма Лемпеля - Зива
6.	Аппаратно-программный комплекс для визуализации и исследования кодов Боуза-Чоудхури-Хоквенгема (БЧХ) с использованием MATLAB
7.	Аппаратно-программный комплекс для визуализации и исследования Турбо кодов
8.	Аппаратно-программный комплекс для визуализации и исследование процессов кодирования источника и полосовой модуляции/демодуляции в среде LabView
9.	Аппаратно-программный комплекс для визуализации и исследования процессов кодирования источника и полосовой модуляции/демодуляции в среде LabView

10.	Аппаратно-программный комплекс для исследования, визуализации Методы сжатия с потерей информации. Кодирование преобразований. Стандарт сжатия JPEG. Фрактальный метод
11.	Аппаратно-программный комплекс для визуализации и исследования кодирования источника дискретных сообщений методом Шеннона-Фано
12.	Аппаратно-программный комплекс для визуализации и исследования методов канального кодирования/декодирования в беспроводных системах цифрового вещания и связи. Коды LDPC
13.	Аппаратно-программный комплекс для визуализации и исследования кодов Рида-Маллера
14.	Разработка программного комплекса для исследования методов аналогового скремблирования на базе LabVIEW
15.	Аппаратно-программного комплекса для исследования и визуализации методов канального кодирования/декодирования в беспроводных системах цифрового вещания и связи. Коды LDPC
16.	Разработка программного комплекса для исследования алгоритма ассиметричного шифрования Эль-Гамаля
17.	Разработка программного комплекса для исследования средств сжатия информации на базе вейвлет-фрактальных преобразований
18.	Российский алгоритм функции хэширования ГОСТ Р 34.11-94 и его программная реализация
19.	Методы оценки качества алгоритмов поточного шифрования и программная реализация статистических тестов НИСТ
20.	Алгоритм шифрования данных DES и его программная реализация
22.	Алгоритм ассиметричного шифрования Диффи-Хеллмана и его программная реализация
23.	Алгоритм шифрования данных AES и его программная реализация
24.	Разработка программного комплекса для исследования методов аналогового скремблирования на базе LabView

28.	Алгоритм цифровой подписи RSA и его программная реализация

Наличие большого числа тем способствует учету индивидуальных особенностей студента и стимулирует его интерес к выполняемой курсовой работе. Студентам с хорошей базовой подготовкой рекомендуется выбирать более сложные темы, связанные дисциплинами, изучаемыми на последующих курсах.

3 СОДЕРЖАНИЕ РАБОТЫ

3.1 Общие сведения

После получения задания студент последовательно выполняет следующее:

- анализ технического задания,
- постановка задачи,
- аналитический обзор литературы,
- сравнительный анализ методов решения задачи,
- выбор и обоснования метода решения задачи,
- выбор и обоснование используемого программного обеспечения,
- разработка технического проекта,
- анализ результатов проектирования,
- оформление пояснительной записки,
- подготовка компьютерной презентации курсовой работы,
- защита работы перед комиссией.

3.2 Структура пояснительной записки

Объем текстового документа подготавливаемого студентом в процессе выполнения курсового проектирования составляет приблизительно 20-30 страниц машинописного текста формата А4.

В текстовый документ последовательно включаются следующие части:

- титульный лист,
- реферат,
- задание,
- список условных сокращений и обозначений (при необходимости),
- содержание,
- введение,
- основная часть,

- заключение,
- литература,
- приложения.

Примеры оформления титульного листа, задания, приведены соответственно в Приложениях А, Б.

3.3 Титульный лист

Титульный лист выполняется студентом аналогично примеру оформления, приведенному в Приложении А [3].

3.4 Реферат

Реферат выполняется в соответствии с Приложением Б и размещается на отдельной странице.

Реферат должен содержать

- сведения о количестве страниц, иллюстраций, таблиц, использованных источников, приложений, листов графического материала;
- ключевые слова,
- текст реферата.

Текст реферата должен отражать:

- объект разработки или исследования;
- цель работы;
- назначение работы и область применения;
- метод исследования и программно-аппаратное обеспечение для разработки;
- полученные результаты и их новизну;
- основные технико-эксплуатационные характеристики алгоритма и программы;
- степень внедрения (по возможности);
- рекомендации по внедрению;
- предположения и рекомендации о развитии объекта разработки;
- дополнительные сведения.

Если курсовой проект не содержит сведений о какой-либо из перечисленных выше частей реферата, то она опускается. При этом последовательность изложения сохраняется.

3.5 Содержание

Содержание содержит рубрикацию и наименование разделов отчета и должно отражать все материалы, представленной к защите работы.

3.6 Введение

В разделе «Введение» указывается цель работы, ее назначение и область применения. Указывается значение работы для науки (техники) и, возможно, экономическая целесообразность разработки.

3.7 Основная часть

3.7.1 Структура основной части

В основной части отражается работа студента по выполнению индивидуального задания. Основная часть, как правило, содержит следующие разделы:

- анализ задания,
- постановка задачи,
- разработка концепции информационной безопасности,
- сравнительный анализ технологий решения поставленной задачи,
- сравнительный анализ математических методов решения поставленной задачи,
- варианты построения системы,
- разработка структурной схемы системы,
- выбор и обоснование используемого оборудования,
- выбор и обоснование используемого программного обеспечения (протоколов),
- вопросы эксплуатации системы,
- анализ защищенности информационной системы.

В соответствии с индивидуальным заданием некоторые разделы основной части могут быть объединены или опущены.

3.7.2 Анализ задания и постановка задачи

В этом разделе рассматривается основание для разработки системы и ставится цель и задачи курсового проектирования. Приводится описание и математическая модель решаемой задачи. Анализируются требования к функциональным характеристикам разрабатываемой системы. Определяются критерии эффективности. Выполняется анализ технических ограничений на разработку.

3.7.3 Информационная безопасность системы

В разделе рассматриваются вопросы обеспечения информационной безопасности разрабатываемой системы. Формулируются основные задачи обеспечения информационной безопасности. Анализируются угрозы безопасности защищаемой информации и возможные каналы несанкционированного доступа. Формулируются требования к системе защиты информации.

3.7.4 Сравнительный анализ технологий решения поставленной задачи

В разделе выполняется обзор технологий решения поставленной задачи. Выполняется анализ современного состояния решаемой научно-технической проблемы. Производится аналитический обзор литературы по теме. Рекомендуется выполнить патентные исследования по теме проектирования. Должен быть выполнен сравнительный анализ технологий проектирования. Раздел завершается выбором и обоснованием технологии решения задачи.

3.7.5 Сравнительный анализ методов решения задачи

В разделе выполняется обзор математических методов решения поставленной задачи. Должен быть выполнен сравнительный анализ методов

решения поставленной задачи. Приводится описание объектов и процессов в проектируемой системе. Рассматриваются математические модели объектов и процессов. Раздел завершается выбором и обоснованием математического метода решения задачи.

3.7.6 Варианты построения системы

В разделе «Варианты построения системы» анализируются различные варианты создания системы в рамках выбранного метода проектирования. Раздел завершается разработкой структурной (функциональной) схемы системы.

3.7.7 Выбор и обоснование используемого оборудования

На основе полученной ранее топологии системы и заданных ограничений на разработку выполняется выбор используемого оборудования. Каждое техническое решение должно обосновываться и сопровождаться необходимыми расчетами. Раздел завершается разработкой спецификации оборудования.

3.7.8 Выбор и обоснование используемого программного обеспечения

В разделе производится сравнительный анализ современного программного обеспечения, которое может быть установлено в разрабатываемой системе. Выполняется выбор и обоснование используемого программного обеспечения с учетом ограничений на разработку. В случае необходимости обосновывается использование протоколов обмена информацией. Раздел завершается списком используемых программных продуктов.

3.7.9 Эксплуатация системы

В разделе рассматриваются вопросы внедрения, тестирования, проведения регламентных работ, администрирования, модернизации и в перспективе утилизации разработанной системы. Особое внимание уделяется разработке организации службы безопасности на предприятии. Приводится структура системы безопасности на предприятии. Предлагаются защитные механизмы, меры и средства обеспечения безопасности предприятия.

3.7.10 Анализ способности системы противостоять отдельным угрозам

В разделе производится оценка способности разработанной системы противостоять отдельным угрозам. Угрозы безопасности классифицируются и сводятся в отдельную таблицу. Для удобства анализа разработанной системы вводится так называемая матрица безопасности [46,47]. В заключении делается вывод о решении (либо о частичном решении) комплексной проблемы информационной безопасности. Раздел завершается комплексом организационно-технических мер по обеспечению безопасности системы.

3.8 Заключение

Заключение должно содержать краткие выводы по наиболее важным результатам выполненной работы. Следует выполнить оценку полноты решения поставленных задач и дать рекомендации по дальнейшему использованию выполненной работы.

3.9 Литература

В разделе «Литература» включаются все источники, использованные студентом в процессе выполнения работы (книги, журналы, статьи, конспекты лекций, источники в Интернет и др.). В тексте обязательны ссылки на все использованные источники.

3.10 Приложения

Приложения рекомендуется выносить материалы иллюстративного и вспомогательного характера. Приложения к курсовой работе по информатике могут содержать следующие материалы:

- термины и определения,
- список каталогов и файлов, прилагаемых на компакт диске,
- структурная схема системы,
- спецификация оборудования,
- режим работы обслуживающего персонала,
- протоколы испытаний программы,
- акты внедрения программы.

4 ТРЕБОВАНИЯ К ОФОРМЛЕНИЮ

4.1Общие требования

4.1.1 При оформлении курсовой работы следует пользоваться стандартом вуза ОС ТУСУР [3].

4.1.2 Текстовые документы (ТД) должны быть выполнены на белой бумаге формата А4 (210х297 мм) с одной стороны листа с применением печатающих или графических устройств

вывода ЭВМ: межстрочный интервал одинарный или полуторный, высота букв и цифр не менее 1,8 мм, цвет - черный. Рекомендуется использовать следующие шрифты: Times New Roman Cyr 13, Times New Roman 12, Arial 12.

4.1.3. Иллюстрации, таблицы и распечатки с ЭВМ допускается выполнять на листах формата А3, при этом они должны быть сложены на формат А4 "гармоникой" по ГОСТ 2.501.

4.1.1 Текст следует выполнять, соблюдая размеры полей: левое - не менее 30 мм, правое - не менее 10 мм, верхнее - не менее 15 мм, нижнее - не менее 20 мм.

4.1.2 Абзацы в тексте начинают отступом, равным 10-15 мм.

4.1.3 Опечатки, описки, графические неточности, обнаруженные в процессе выполнения ТД, допускается исправлять аккуратным заклеиванием или закрашиванием белой краской и нанесением на том же месте и тем же способом исправленного текста. Повреждение листов ТД, помарки и следы не полностью удалённого текста не допускаются.

4.1.4 ТД должен быть сшит (переплетен) и иметь обложку.

4.2 Требования к тексту

4.2.1 В ТД должны применяться термины, обозначения и определения, установленные стандартами по соответствующему направлению науки, техники и технологии, а при их отсутствии - общепринятые в научно-технической литературе.

4.2.2 В ТД не допускается:

- применять для одного и того же понятия различные научно -технические термины, близкие по смыслу (синонимы), а также иностранные слова и термины при наличии равнозначных слов и терминов в русском языке;
- применять произвольные словообразования;
- применять индексы стандартов (ГОСТ, ГОСТ Р, ОСТ и т.п.), технических условий (ТУ) и других документов без регистрационного номера.
- использовать в тексте математические знаки и знак 0 (диаметр), а также знаки № (номер) и % (процент) без числовых значений.

4.3 Деление текста

4.3.1 Текст разделяют на разделы, подразделы, пункты. Пункты, при необходимости, могут быть разделены на подпункты.

4.3.2 Каждый раздел ТД рекомендуется начинать с нового листа (страницы).

4.3.3 Разделы должны иметь порядковые номера в пределах всего ТД, обозначенные арабскими цифрами и записанные с абзацного отступа. Подразделы и пункты должны иметь нумерацию в пределах каждого раздела или подраздела, подпункты - в пределах пункта. Отдельные разделы могут не иметь подразделов и состоять непосредственно из пунктов.

4.3.4 Если раздел или подраздел состоит из одного пункта, этот пункт также нумеруется.

4.3.5 Точка в конце номеров разделов, подразделов, пунктов, подпунктов не ставится.

4.4 Заголовки

4.4.1 Разделы, подразделы должны иметь заголовки. Пункты, как правило, заголовков не имеют.

4.4.2 Заголовки должны четко и кратко отражать содержание разделов, подразделов.

4.4.3 Заголовки следует выполнять с абзацного отступа с прописной буквы без точки в конце, не подчеркивая. В начале заголовка помещают номер соответствующего раздела, подраздела, пункта.

4.4.4 Переносы слов в заголовках не допускаются. Если заголовок состоит из двух предложений, их разделяют точкой.

4.4.5 Расстояние между заголовком и текстом должно быть равно удвоенному межстрочному расстоянию; между заголовками раздела и подраздела - одному межстрочному расстоянию

4.5 Таблицы

4.5.1 Таблицы применяют для лучшей наглядности и удобства сравнения показателей.

4.5.2 Таблицы слева, справа и снизу, как правило, ограничивают линиями. Головка таблицы должна быть отделена линией от остальной части таблицы. Разделять заголовки и подзаголовки боковика и граф диагональными линиями не допускается. Высота строк таблицы должна быть не менее 8 мм.

4.5.3 Все таблицы нумеруют в пределах раздела арабскими цифрами.

4.5.4 Над левым верхним углом таблицы помещают надпись: «Таблица» с указанием номера таблицы, например: «Таблица 2.1» (первая таблица второго раздела), «Таблица В.5» (пятая таблица приложения В).

4.5.5 Таблица может иметь название. Название таблицы должно отражать содержание, быть точным, кратким. Если таблица имеет название, то его помещают после номера таблицы через тире, с прописной буквы.

4.5.6 На все таблицы должны быть ссылки в тексте.

4.5.7 Таблицу следует располагать в ТД непосредственно после абзаца, где она упоминается впервые, или на следующем листе (странице).

4.6 Иллюстрации

4.6.1 Иллюстрации помещаются в ТД для пояснения текста и должны быть выполнены в соответствии с требованиями государственных стандартов.

4.6.2 Иллюстрации, на которых изображаются графики (диаграммы), должны быть выполнены в соответствии с Р 50-77-88 Рекомендации. ЕСКД.

4.6.3 Иллюстрации следует выполнять на бумаге или пленке того же формата, что и текст, с соблюдением тех же полей, что и для текста. Допускается наклеивание отдельно выполненных изображений на форматный лист. Цвет изображений, как правило, черный на белом фоне.

4.6.4 В тексте все иллюстрации (фотографии, схемы, чертежи и пр.) именуются рисунками.

4.6.5 Рисунки нумеруются в пределах раздела (приложения) арабскими цифрами, например: «Рисунок 3.2» (второй рисунок третьего раздела); «Рисунок А.2» (второй рисунок приложения А).

4.6.6 Рисунок может иметь тематическое наименование и пояснительные данные (подрисуночный текст).

4.6.7 Слово «рисунок», его номер и тематическое наименование (при наличии) помещают ниже изображения и пояснительных данных симметрично иллюстрации.

4.7 Формулы

4.7.1 Формулы следует выделять из текста в отдельную строку.

4.7.2 Значения символов и числовых коэффициентов, входящих в формулу, должны быть приведены непосредственно под формулой. Значение каждого символа дают с новой строки в той последовательности, в какой они приведены в формуле. Первая строка расшифровки должна начинаться со слова "где" без двоеточия после него.

4.8 Ссылки

4.8.1 В ТД приводят ссылки:

- на данную работу;
- на использованные источники.

4.8.2 При ссылках на данную работу указывают номера структурных частей текста, формул, таблиц, рисунков, обозначения чертежей и схем, а при необходимости - также графы и строки таблиц и позиции составных частей изделия на рисунке, чертеже или схеме.

4.8.3 При ссылках на структурные части текста указывают номера разделов (со словом «раздел»), приложений (со словом «приложение»), подразделов, пунктов, подпунктов, перечислений, например: «...в соответствии с разделом 2»; «... согласно 3.1»; «... по 3,1.1»; «... в соответствии с 4.2.2, перечисление б»; приложение Л; «... как указано в приложении М».

4.8.4 Ссылки в тексте на номер формулы дают в скобках, например: «...согласно формуле (В.1)»; «...как следует из выражения (2.5)».

4.8.5 Ссылки в тексте на таблицы и иллюстрации оформляют по типу: «таблица 4.3»; «. . в таблице 1.1, графа 4»; (рисунок 2.11); «...в соответствии с рисунком 1.2»; «.. как показано на рисунке Г.7, поз. 12 и 13».

4.8.6 При ссылке в тексте на использованные источники следует приводить порядковые номера по списку использованных источников, заключенные в квадратные скобки, например: «.. как указано в монографии [10]»; «... в работах [11, 12, 15-17]».

4.8.7 При необходимости в дополнение к номеру источника указывают номер его раздела, подраздела, страницы, иллюстрации, таблицы, например: [12, раздел 2]; [18, подраздел 1.3, приложение А]; [19, с.25, таблица 8.3].

4.9 Сокращения

4.9.1 При многократном упоминании устойчивых словосочетаний в тексте следует использовать аббревиатуры или сокращения.

4.9.2 При первом упоминании должно быть приведено полное название с указанием в скобках сокращенного названия или аббревиатуры. При последующих упоминаниях следует употреблять сокращенное название или аббревиатуру.

4.9.3 Расшифровку аббревиатур и сокращений, установленных государственными стандартами (ГОСТ 2.316, ГОСТ 7.12) и правилами русской орфографии, допускается не приводить, например: ЭВМ, НИИ, АСУ, с. (страница), т.е. (то есть), вуз (высшее учебное заведение) и др.

5. РЕКОМЕНДАЦИИ ПО ОРГАНИЗАЦИИ РАБОТЫ СТУДЕНТОВ

Для того чтобы успешно выполнить индивидуальное задание, необходимо регулярно и систематически работать в течение семестра. Следует посещать консультации, рационально и равномерно распределять свое рабочее время.

Для работы следует завести рабочую тетрадь объемом 40-50 листов. В рабочей тетради (РТ) необходимо регулярно фиксировать:

- календарный график работы и его реализацию,
- используемые литературные источники, включая источники в Интернет (В конце РТ отводится несколько страниц для регистрации литературных источников, с которыми работает студент),
- краткую информацию по используемым литературным источникам,
- список задач, которые должны быть решены в процессе проектирования,
- основные вопросы, возникающие в процессе работы,
- расчетные формулы, интересные факты, описание используемых данных,
- оглавления текстовых документов, подготавливаемых в процессе работы,

- контрольные примеры и результаты тестирования.

После получения индивидуального технического задания студе выполняет его тщательный анализ. Необходимо осознать суть решаемой течение семестра задачи, выяснить ее назначение. Студент начина составлять индивидуальный календарный план, уточняет дату еда законченной курсовой работы на кафедру, выясняет сроки защиты курсов работы перед комиссией. Следует сходить в библиотеку и познакомиться источниками разработки и государственными стандартами по оформлении программного обеспечения [2-27]. Рекомендуется ознакомиться дополнительной литературой [28-63].

При разработке проекта следует учитывать требования к курсовому проектированию приведенные в шкале рейтинга по дисциплин (Приложение В).

Выполненный курсовой проект в установленные техническим задание сроки сдается на проверку. В течение одной недели преподаватель проверя работу и выносит решение либо о допуске к защите, либо об ее доработке После получения допуска к защите выполняется защита перед комиссией При отсутствии существенных замечаний допускается защита пере преподавателем.

Во время защиты студент за 5-7 минут докладывает о результатах полученных им при выполнении курсовой работы:

- наименование работы,
- назначение и цель работы,
- основные решаемые задачи,
- выбор технологии решения задачи,
- выбор метода решения,
- основные результаты,
- отличительные особенности работы.

В докладе следует уделить наибольшее внимание самым важным и интересным моментам работы. Рекомендуется не уделять значительно внимания второстепенным проблемам.

После окончания доклада студент отвечает на вопросы членов комиссии и всех присутствующих.

После окончания защиты курсовая работа сдается на кафедру для хранения.

5.3 Смотр-конкурс студенческих работ

5.3.1 Общие сведения Курсовые проекты, имеющие исследовательский характер, могут быть представлены на смотр-конкурс студенческих работ. В этом случае преподаватель пишет отзыв о работе, а студент готовит необходимые конкурсные документы.

5.3.2 Награждение победителей Победители смотров-конкурсов студенческих работ, как правил награждаются грамотами и получают денежные премии.

5.3.3 Критерии оценки работ Смотры-конкурсы студенческих работ проводятся по различны направлениям. Но, как правило, уровень работ, поданных на конку] оценивается по следующим критериям:

- актуальность работы,
- практическая значимость работы,
- достоверность результатов,
- новизна,
- уровень использования учебной, специальной и научной литературы,
- уровень использования вычислительной техники,
- оригинальные технические решения,
- оформление работы,
- содержание работы,
- личный вклад автора,
- наличие публикаций по теме работы,
- обсуждение результатов работы на студенческих и научны: конференциях,
- отсутствие грамматических, стилистических и орфографичесю ошибок.

ЛИТЕРАТУРА

1. Банкет В.Л. Помехоустойчивое кодирование в телекоммуникационных системах: учебн. пособие. - Одесса: ОНАС им А.С. Попова, 2011. - 104 с.

2. Алгоритм RSA : метод. указания к выполнению лабораторных работ для студентов спец. 090105 «Комплексное обеспечение информационной безопасности автоматизированных систем» очной формы обучения / сост.: О. Н. Жданов, И. А. Лубкин ; Сиб. гос. аэрокосмич. ун-т. – Красноярск, 2007. – 38 с.

3.Чернышев А.А. ОС ТУСУР 01-2013 «Работы студенческие по направлениям подготовки и специальностям технического профиля. Общие требования и правила оформления». Томск, 2013. Режим доступа: http://www.tusur.ru/export/sites/ru.tusur.new/ru/education/

documents/inside/tech_01-2013_new.pdf2. ГОСТ Р 7.0.5-2008 Система стандартов по информации, библиотечному и издательскому делу. Библиографическая ссылка. Общие требования и правила составления.

4. ГОСТ Р 7.0.11-2011 Система стандартов по информации, библиотечному и издательскому делу. Диссертация и автореферат диссертации. Структура и правила оформления.

5. ГОСТ 2.105-95 Единая система конструкторской документации. Общие требования к текстовым документам.

6. ГОСТ 2.106-96. Единая система конструкторской документации. Текстовые документы.

7. ГОСТ 2.201-80 Единая система конструкторской документации. Обозначение изделий и конструкторских документов.

8. ГОСТ 2.501-88 Единая система конструкторской документации. Правила учета и хранения.

9. ГОСТ 2.316-2008 Единая система конструкторской документации. Правила нанесения на чертежах надписей, технических требований и таблиц;

10. ГОСТ 3.1201-85 Единая система технологической документации. Система обозначения технологической документации;

11. ГОСТ 7.1 -2003 Система стандартов по информации, библиотечному и издательскому делу. Библиографическая запись. Библиографическое описание. Общие требования и правила составления;

12. ГОСТ 7.9-95 (ИСО 214-76) Система стандартов по информации, библиотечному и издательскому делу. Реферат и аннотация. Общие требования;

13. ГОСТ 7.12-93 Система стандартов по информации, библиотечному и издательскому делу. Библиографическая запись. Сокращение слов на русском языке. Общие требования и правила;

14. ГОСТ 7.32-2001. Межгосударственный стандарт. Система стандартов по информации, библиотечному и издательскому делу. Отчет о научно-исследовательской работе. Структура и правила оформления;

15. ГОСТ 8.417-2002 Государственная система обеспечения единства измерений. Единицы величин;

16. ГОСТ 19.103-77 Единая система программной документации. Обозначения программ и программных документов;

17. ГОСТ 34.201-89 Информационная технология. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем;

18. ОК 012-93 Общероссийский классификатор изделий и конструкторских документов (классификатор ЕСКД);

19. Р 50-77-88 Рекомендации. Единая система конструкторской документации. Правила выполнения диаграмм.

20. Голиков А.М. Методы шифрования информации в сетях и системах радиосвязи: Сборник лабораторных работ. – Томск: Томск. гос. ун-т систем управления и радиоэлектроники, 2012. – 333 с. Режим доступа: http://edu.tusur.ru/training/publications/1051

21. Кодирование и шифрование информации в системах связи Часть 2. Шифрование. Учебное пособие для специалитета: 210601.65 Радиоэлектронные системы и комплексы

Курс лекций, компьютерный практикум, задание на самостоятельную работу / А.М.Голиков. – Томск: Томск. гос. ун-т систем упр. и радиоэлектроники, 2016. – 490 с. Режим доступа: http://edu.tusur.ru/training/publications/6091

ПРИЛОЖЕНИЕ А

ПРИМЕР ОФОРМЛЕНИЯ ТИТУЛЬНОГО ЛИСТА

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ

Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования

ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИСТЕТ СИСТЕМ УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ

Кафедра радиотехнических систем

РАЗРАБОТКА ПРОГРАММНОГО КОМПЛЕКСА ДЛЯ ИССЛЕДОВАНИЯ И ВИЗУАЛИЗАЦИИ ЦИКЛИЧЕСКОГО ИЗБЫТОЧНОГО КОДА И КАСКАДНЫХ КОДОВ НА БАЗЕ MATLAB SIMULINK

Пояснительная записка к курсовой работе по дисциплине «Кодирование и шифрование информации в системах связи»

Выполнил: Студент гр.122-2

_____Н.В. Макаров

_____2016 г.

Проверил: Доцент кафедры РТС

_____Голиков А.М.

_____2015г.

2016 г.

ПРИЛОЖЕНИЕ А

ПРИМЕР ЗАДАНИЯ КУРСОВУЮ РАБОТУ

Министерство образования и науки Российской Федерации

Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования

Томский государственный университет систем управления и радиоэлектроники

КАФЕДРА РАДИОТЕХНИЧЕСКИХ СИСТЕМ

ТЕХНИЧЕСКОЕ ЗАДАНИЕ

на выполнение курсового проекта по курсу

«Кодирование и шифрование информации в системах связи»

студенту гр. _122-2_ __Н.В. Макарову

1. Наименование проекта: **Проектирование программного комплекса для исследования и визуализации Циклического избыточного кода** (англ. *Cyclic redundancy check, CRC*)» **и Каскадных кодов на базе MATLAB Simulink 2015**

2. ***Цель проекта:*** Проектирование и испытание учебного программного комплекса

3. Назначение проекта: Проектирование программного комплекса для исследования и визуализации Циклического избыточного кода (англ. *Cyclic redundancy check, CRC*)» и Каскадных кодов на базе MATLAB Simulink 2015

4. ***Содержание работы по проекту:***

4.1. Аналитический обзор существующих методов и средств

4.2. Разработка структурной схемы программного комплекса

4.2. Разработка алгоритмов программ

4.3. Разработка программного интерфейса для исследования характеристик и визуализации основных преобразований

4.4. Разработка методики и проведение исследования основных технических характеристик, анализ результатов исследования

5. ***Форма отчетности*** _Пояснительная записка к работе объемом не менее 30 листов формата А4, схемы структурные и функциональные в соответствии с ГОСТ, CD-диск с ПО, результатами испытаний и описанием учебного программного комплекса

Руководитель проекта _*Голиков А.М., доцент кафедры РТС*_____

(Фамилия, имя, отчество, должность руководителя)

Подпись руководителя проекта _____

Сдача задания _____

Подпись студента_____