Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего профессионального образования
«Томский государственный университет систем управления и радиоэлектроники»

Кафедра электронных приборов

Информационные технологии в электронике

КРИПТОГРАФИЧЕСКОЕ ПРЕОБРАЗОВАНИЕ ИНФОРМАЦИИ

Методические указания к лабораторной работе
для студентов направления «Электроника и микроэлектроника»
(специальность «Электронные приборы и устройства»

2012

Колегов Алексей Анатольевич

Криптографическое преобразование информации = Информационные технологии в электронике: методические указания к лабораторной работе для студентов направления «Электроника и микроэлектроника» (специальность «Электронные приборы и устройства» / А.А. Колегов; Министерство образования и науки Российской Федерации, Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования Томский государственный университет систем управления и радиоэлектроники, Кафедра электронных приборов. - 2-е изд. - Томск: ТУСУР, 2012. - 25 с.

Целью данной лабораторной работы является ознакомление с некоторыми методами криптографического преобразования информации

Криптографические методы являются специфическим способом защиты процессов переработки информации, они имеют многовековую историю развития и применения. Более того, сформировалось самостоятельное научное направление — криптология, изучающая и разрабатывающая научно-методологические основы, способы, методы и средства криптографического преобразования информации.

Предназначено для студентов очной и заочной форм, обучающихся по направлению «Электроника и микроэлектроника» (специальность «Электронные приборы и устройства») по дисциплине «Информационные технологии в электронике».

Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего профессионального образования
«Томский государственный университет систем управления и
радиоэлектроники»

Кафедра электронных приборов

УТВЕРЖДАЮ
Зав.кафедрой ЭП
_____С.М. Шандаров
«___» _____ 2012 г.

Информационные технологии в электронике

КРИПТОГРАФИЧЕСКОЕ ПРЕОБРАЗОВАНИЕ ИНФОРМАЦИИ

Методические указания к лабораторной работе
для студентов направления «Электроника и микроэлектроника»
(специальность «Электронные приборы и устройства»

Разработчик
_____А.А.. Колегов
«____»_____2012 г

2012

Содержание

1 Введение

Целью данной лабораторной работы является ознакомление с некоторыми методами криптографического преобразования информации

Криптографические методы являются специфическим способом защиты процессов переработки информации, они имеют многовековую историю развития и применения. Более того, сформировалось самостоятельное научное направление — криптология, изучающая и разрабатывающая научно-методологичес-кие основы, способы, методы и средства криптографического преобразования информации.

2 Теоретическая часть

2.1 Основные понятия, определения, композиции и синтез шифров

В настоящее время криптографические методы в различных системах могут применяться как для защиты процессов переработки информации, обрабатываемой в ЭВМ или хранящейся в различного типа ЗУ, так и для закрытия информации, передаваемой между различными элементами системы по линиям связи. Криптографическое преобразование как метод предупреждения несанкционированного доступа к информации имеет многовековую историю. Разработано множество различных методов шифрования, созданы теоретические и практические основы их применения. Большинство этих методов может быть успешно использовано и для закрытия информации.

Криптология разделяется на два направления: криптография и криптоанализ. Цели этих направлений прямо противоположны.

Криптография занимается поиском и исследованием математических методов преобразования информации.

Сфера интересов *криптоанализа* — исследование возможности расшифровывания информации без наличия ключей.

Современная криптография включает в себя четыре крупных раздела:

- симметричные криптосистемы;
- криптосистемы с открытым ключом;
- системы электронной подписи;
- управление ключами.

Основными направлениями использования криптографических методов являются: передача конфиденциальной информации по каналам связи (например, электронная почта), установление подлинности передаваемых сообщений, хранение информации (документов, баз данных) на носителях в зашифрованном виде.

Методы криптографического преобразования информации могут быть классифицированы на четыре большие группы:

- шифрование-дешифрование;
- кодирование;
- стеганография;
- сжатие-расширение.

Рассмотрим основные понятия методологии криптографии.

Алфавит — конечное множество используемых для кодирования информации знаков.

В качестве примеров алфавитов, используемых в современных ИС, можно привести следующие:

- алфавит Z_{32} — 32 буквы русского алфавита и пробел;
- алфавит Z_{256} — символы, входящие в стандартные коды ASCII и КОИ-8;
- бинарный алфавит — $Z_2 = \{0,1\}$;
- восьмеричный или шестнадцатеричный алфавит;

Текст — упорядоченный набор из элементов алфавита.

Шифрование — преобразовательный процесс: исходный текст, который носит также название открытого текста, заменяется шифрованным текстом рис. 2.1.

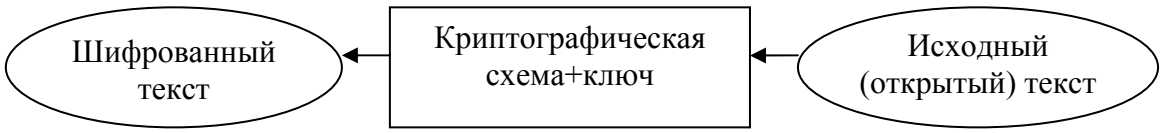

Рисунок 2.1 — Схема процедуры шифрования текста

Дешифрование — процесс, обратный шифрованию. На основе ключа шифрованный текст преобразуется в исходный.

Ключ — информация, необходимая для беспрепятственного шифрования и дешифрования текстов.

Криптографическая система представляет собой семейство *T* преобразований открытого текста. Члены этого семейства индексируются или обозначаются символом *k*; параметр *k* является ключом.

Пространство ключей K — это набор возможных значений ключа. Обычно ключ представляет собой последовательный ряд букв алфавита.

Криптосистемы подразделяют на симметричные и с открытым ключом.

В *симметричных криптосистемах* и для шифрования, и для дешифрования используется один и тот же ключ.

В *системах с открытым ключом* используют два ключа — открытый и закрытый, которые математически связаны друг с другом.

Информация шифруется с помощью открытого ключа, который доступен всем желающим, а расшифровывается с помощью закрытого ключа, известного только получателю сообщения.

Термины «распределение ключей» и «управление ключами» относятся к процессам системы обработки информации, содержанием которых являются составление и распределение ключей между пользователями.

Электронной (*цифровой*) *подписью* называется присоединяемое к тексту его криптографическое преобразование, которое позволяет при получении текста другим пользователем проверить авторство и подлинность сообщения.

Для современных криптографических систем защиты процессов переработки информации сформулированы следующие общепринятые требования:

– зашифрованное сообщение должно поддаваться чтению только при наличии ключа;

– число операций, необходимых для определения использованного ключа шифрования по фрагменту шифрованного сообщения и соответствующего ему открытого текста, должно быть не меньше общего числа возможных ключей;

– число операций, необходимых для расшифровывания информации путем перебора всевозможных ключей, должно иметь строгую нижнюю оценку и выходить за пределы возможностей современных компьютеров (с учетом возможности использования сетевых вычислений);

– знание алгоритма шифрования не должно влиять на надежность защиты;

– незначительное изменение ключа должно приводить к существенному изменению одного и того же ключа;

– структурные элементы алгоритма шифрования должны быть неизменными;

– дополнительные биты, вводимые в сообщение в процессе шифрования, должны быть полностью и надежно скрыты в шифрованном тексте;

– длина шифрованного текста должна быть равной длине исходного текста;

– не должно быть простых и легко устанавливаемых зависимостей между ключами, последовательно используемыми в процессе шифрования;

– любой ключ из множества возможных должен обеспечивать надежную защиту информации;

– алгоритм должен допускать как программную, так и аппаратную реализацию, при этом изменение длины ключа не должно вести к качественному ухудшению алгоритма шифрования.

Таким образом, под кодированием понимается такой вид криптографического закрытия, когда некоторые элементы защищаемых данных (это не обязательно отдельные символы) заменяются заранее выбранными кодами (цифровыми, буквенными, буквенно-цифровыми сочетаниями и т.п.). Этот метод имеет две разновидности: смысловое и символьное кодирование.

При *смысловом кодировании* кодируемые элементы имеют вполне определенный смысл (слова, предложения, группы предложений).

При *символьном кодировании* кодируется каждый символ защищаемого сообщения. Символьное кодирование по существу совпадает с шифрованием заменой.

При кодировании замене подвергаются смысловые элементы информации, поэтому для каждого специального сообщения в общем случае необходимо использовать свою систему кодирования.

В последнее время разработаны специальные коды для сокращения объема информации при записи ее в ЗУ. Специфика этих кодов заключается в том, что для записи часто встречающихся символов используются короткие двоичные коды, а для записи редко встречающихся — длинные. Примером такого кода для английского языка может служить код Хаффмена.

Такое кодирование имеет криптографическую стойкость на уровне шифрования простой заменой.

При смысловом кодировании основной кодируемой единицей является смысловой элемент текста. Для кодирования составляется специальная таблица кодов, содержащая перечень кодируемых элементов и соответствующих им кодов, например:

Автоматизированные системы управления…….001
Автоматизация управления ..……002
Осуществляет …….415
Позволяет ……632

Тогда предложение «Автоматизированные системы управления позволяют осуществлять автоматизацию управления» после кодирования будет иметь следующий вид: 001 632 415 002.

Под шифрованием (дешифрованием) понимается такой вид криптографического закрытия (раскрытия), при котором преобразованию подвергается каждый символ защищаемого сообщения. Методы шифрования и дешифрования подразделяют на два класса: с симметричным ключом и системы с открытыми ключами. Все известные способы шифрования с симметричными ключами можно разбить на пять

групп: подстановка (замена), перестановка, аналитическое преобразование, гаммирование и комбинированное шифрование (дешифрование).

Каждый из этих способов может иметь несколько разновидностей.

В методах шифрования с симметричными ключами способом замены применяются алгоритмы прямой замены, многоалфавитной подстановки или полиалфавитной замены. Это наиболее простой вид преобразований, заключающийся в замене символов исходного текста на другие (того же алфавита) по более или менее сложному правилу.

Для обеспечения высокой криптостойкости требуется использование больших ключей, кроме того, применяется модифициованная матрица шифрования.

Метод перестановки — несложный метод криптографического преобразования. Он используется, как правило, в сочетании с другими методами.

Аддитивные методы (гаммирование) заключается в наложении на исходный текст некоторой псевдослучайной последовательности, генерируемой на основе ключа.

Блочные шифры относятся к комбинированным методам и представляют собой последовательность (с возможным повторением и чередованием) основных методов преобразования, применяемую к блоку (части) шифруемого текста. Блочные шифры на практике встречаются чаще, чем «чистые» преобразования того или иного класса в силу их более высокой криптостойкости. Российские и американские стандарты шифрования основаны именно на этом классе шифров.

2.2 Шифрование методами замены (подстановки)

Этот вид шифрования подразумевает, что символы шифруемого текста заменяются с другими символами, взятыми из одного (одно- или моноалфавитная подстановка) или нескольких (много- или полиалфавитная подстановка) алфавитов.

Самой простой разновидностью является прямая (простая) замена, когда буквы шифруемого сообщения заменяются другими буквами того же самого алфавита. Таблица замены текста с английским алфавитом может иметь следующий вид (табл. 2.1).

Таблица 2.1 — Символы шифрования при простой замене

Исходные символы	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
замена	S	P	X	L	R	Z	I	M	A	Y	E	D	W	T	B	G	V	N	J	O	C	F	H	Q	U	K

Используя ее, можно зашифровать любой текст, однако такой шифр имеет низкую стойкость, т.к. зашифрованный текст в большинстве случаев имеет те же статистические характеристики, что и исходный. К тому же, если объем зашифрованного текста намного больше, чем одна строка, то частоты появления букв в зашифрованном тексте будут еще ближе к частотам появления букв в английском алфавите и расшифровка окажется еще проще. Поэтому простую замену используют лишь в тех случаях, кода шифруемый текст короток.

Для повышения стойкости шифра используют полиалфавитные подстановки, в которых для замены символов исходного текста используются символы нескольких алфавитов. Существует несколько разновидностей полиалфавитной подстановки, наиболее известными из которых являются одно- (обыкновенная и монофоническая) и многоконтурная.

При *полиалфавитной одноконтурной обыкновенной подстановке* замена символов происходит последовательно и циклически, т.е. первый символ заменяется соответствующим символом первого алфавита, второй — символом второго алфавита, и так до тех пор, пока не будут использованы все выбранные алфавиты. После этого использование алфавитов повторяется.

Другой разновидностью метода замены является схема шифрования Вижинера. Таблица Вижинера представляет собой квадратную матрицу с n^2 элементами, где n — число символов используемого алфавита. В табл. 2.2 представлена таблица Вижинера для русского алфавита. Каждая строка получена циклическим сдвигом алфавита на один символ. Для шифрования выбирается буквенный ключ, в соответствии с которым формируется рабочая матрица шифрования. При этом из полной таблицы выбирается первая строка и те строки, первые буквы которых соответствуют буквам ключа. Первой размещается строка, а под нею — строки, соответствующие буквам ключа в порядке следования этих букв в ключе.

Процесс шифрования осуществляется следующим образом:

1) под каждой буквой шифруемого текста записываются буквы ключа. Ключ при этом повторяется необходимое число раз;

2) каждая буква шифруемого текста заменяется по подматрице буквами, находящимися на пересечении линий, соединяющих буквы шифруемого текста в первой строке подматрицы и находящиеся под ними буквы ключа;

3) полученный текст может разбиваться на группы по несколько знаков.

Таблица 2.2 — Таблица Вижинера для русского алфавита

а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ы	ъ	э	ю	я
б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ы	ъ	э	ю	я	а
в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ы	ъ	э	ю	я	а	б
г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ы	ъ	э	ю	я	а	б	в
д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ы	ъ	э	ю	я	а	б	в	г
е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ы	ъ	э	ю	я	а	б	в	г	д
ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ы	ъ	э	ю	я	а	б	в	г	д	е
з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ы	ъ	э	ю	я	а	б	в	г	д	е	ж
и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ы	ъ	э	ю	я	а	б	в	г	д	е	ж	з
й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ы	ъ	э	ю	я	а	б	в	г	д	е	ж	з	и
к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ы	ъ	э	ю	я	а	б	в	г	д	е	ж	з	и	й
л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ы	ъ	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к
м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ы	ъ	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л
н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ы	ъ	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м
о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ы	ъ	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н
п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ы	ъ	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о
р	с	т	у	ф	х	ц	ч	ш	щ	ь	ы	ъ	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п
с	т	у	ф	х	ц	ч	ш	щ	ь	ы	ъ	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р
т	у	ф	х	ц	ч	ш	щ	ь	ы	ъ	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с
у	ф	х	ц	ч	ш	щ	ь	ы	ъ	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т
ф	х	ц	ч	ш	щ	ь	ы	ъ	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у
х	ц	ч	ш	щ	ь	ы	ъ	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф
ц	ч	ш	щ	ь	ы	ъ	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х
ч	ш	щ	ь	ы	ъ	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц
ш	щ	ь	ы	ъ	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч
щ	ь	ы	ъ	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш
ь	ы	ъ	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ
ы	ъ	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь
ъ	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ы
э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ы	ъ
ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ы	ъ	э
я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ы	ъ	э	ю

Пусть, например, требуется зашифровать сообщение:

МАКСИМАЛЬНО ДОПУСТИМОЙ ЦЕНОЙ ЯВЛЯЕТСЯ ПЯТЬСОТ РУБ. ЗА ШТУКУ.

В соответствии с первым правилом записываем под каждой буквой шифруемого текста буквы ключа. Получаем зашифрованный текст:

САЛЬЕРИСАЛЬ ЕРИСАЛЬЕРИ САЛЬЕ РИСАЛЬЕР ИСАЛЬЕР ИСАЛЬ ЕРИСА.

Затем осуществляем непосредственное шифрование в соответствии со вторым правилом: берем первую букву шифруемого текста (М) и соответствующую ей букву ключа (С); по букве шифруемого текста (М) входим в рабочую матрицу шифрования и выбираем под ней букву, расположенную в строке, соответствующей букве ключа (С), — в нашем примере такой буквой является Э; выбранную таким образом букву помещаем в шифрованный текст. Эта процедура циклически повторяется до зашифровывания всего текста.

Пример такой рабочей матрицы шифрования с использованием ключа «Сальери» приведен в табл. 2.3. Эксперименты показали, что при использовании такого метода статистические характеристики исходного текста практически не проявляются в зашифрованном сообщении. Здесь мы имеем полиалфавитную подстановку, причем число используемых алфавитов определяется числом букв в слове ключа. Поэтому стойкость такой замены определяется произведением стойкости прямой замены на число используемых алфавитов, т.е. на число букв в ключе.

Таблица 2.3 — Рабочая матрица

а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ы	ъ	э	ю	я
с	т	у	ф	х	ц	ч	ш	щ	ь	ы	ъ	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р
а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ы	ъ	э	ю	я
л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ы	ъ	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к
ь	ы	ъ	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ
е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ы	ъ	э	ю	я	а	б	в	г	д
р	с	т	у	ф	х	ц	ч	ш	щ	ь	ы	ъ	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п
и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ы	ъ	э	ю	я	а	б	в	г	д	е	ж	з

Дешифровка текста производится в следующей последовательности:

1) над буквами зашифрованного текста последовательно надписываются буквы ключа, причем ключ повторяется необходимое число раз;

2) в строке подматрицы Вижинера соответствующей букве ключа отыскивается буква, соответствующая знаку зашифрованного текста. Находящаяся под ней буква первой строки подматрицы и будет буквой исходного текста;

3) полученный текст группируется в слова по смыслу.

Одним из недостатков шифрования по таблице Вижинера является то, что при небольшой длине ключа надежность шифрования остается невысокой, а формирование длинных ключей сопряжено с трудностями.

Для повышения стойкости шифрования можно использовать усовершенствованные варианты таблиц Вижинера, например следующий алгоритм модификации метода:

1) во всех (кроме первой) строках таблицы буквы располагаются в произвольном порядке;

2) в качестве ключа используются случайные последовательности чисел;

3) из таблицы Вижинера выбираются десять произвольных строк, которые кодируются натуральными числами от 0 до 10.

Эти строки используются в соответствии с чередованием цифр в выбранном ключе.

Вариант системы подстановок Вижинера при $m = 2$ называется *системой Вернама*. В ней ключ $k = (k_0, k_1,\ldots,k_k - 1)$ записывается на бумажной ленте, а каждая буква исходного текста переводится с использованием кода Бодо в пятибитовый символ. К исходному тексту Бодо добавлялся ключ (по модулю 2). Это считывающее устройство Вернама и оборудование для шифрования использовалось в свое время корпусом связи армии США.

Полиалфавитная одноконтурная монофоническая подстановка является частным случаем рассмотренной подстановки. Особенность этого метода состоит в том, что число и состав алфавитов выбираются таким образом, чтобы частоты появления всех символов в зашифрованном тексте были одинаковыми. При таком положении затрудняется криптоанализ зашифрованного текста с помощью его статической обработки. Выравнивание частот появления символов достигается за счет того, что для часто встречающихся символов исходного текста предусматривается использование большего числа заменяющих элементов, чем для редко встречающихся символов. Пример матрицы монофонического шифра для английского алфавита показан в табл. 2.4. Шифрование осуществляется так же, как и при простой замене, с той лишь разницей, что после шифрования каждого знака соответствующий ему столбец алфавитов циклически сдвигается вверх на одну позицию. Таким образом, столбцы алфавита как бы образуют независимые друг от друга кольца, поворачиваемые вверх на один знак каждый раз после шифрования соответствующего знака.

Полиалфавитная многоконтурная подстановка заключается в том, что для шифрования используется циклически несколько наборов (контуров) алфавитов, причем каждый контур в общем случае имеет свой индивидуальный период применения. Этот период исчисляется, как правило, числом знаков, после зашифровки которых меняется контур алфавитов. Частным случаем многоконтурной полиалфавитной подстановки является замена по таблице Вижинера, если для шифрования используется несколько ключей, каждый из которых имеет свой период применения.

Таблица 2.4 — Матрица монофонического шифра для английского алфавита

	Алфавит открытого текста																									
Алфавит шифротекста	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	f	N	Q	.	G	т	D	,	A	e	L	-	R	(	C	x	I	Z	V	–	W	S	h	u	K	t
	*	N	Q	b	+	[	D	p	)	e	L	O	R	y	/	x	I	=	$	i	W	S	h	u	K	t
	k	N	Q	i	]	W	D	r	q	e	L	и	R	(	#	x	I	a	d	:	W	S	h	u	K	t
	f	N	Q	.	1	т	D	,	A	e	L	A	R	y	П	x	I	Z	V	C	W	S	h	u	K	t
	*	N	Q	b	G	[	D	p	)	e	L	O	R	(	C	x	I	=	$	–	W	S	h	u	K	t
	R	N	Q	i	+	W	D	r	q	e	L	и	R	y	/	x	I	a	d	i	W	S	h	u	K	t
	F	N	Q	.	]	т	D	,	A	e	L	A	R	(	#	x	I	Z	V	:	W	S	h	u	K	t
	*	N	Q	b	1	[	D	p	)	e	L	O	R	y	П	x	I	=	$	C	W	S	h	u	K	t
	K	N	Q	i	G	W	D	r	q	e	L	и	R	(	C	x	I	a	d	–	W	S	h	u	K	t
	F	N	Q	.	+	т	D	,	A	e	L	O	R	y	/	x	I	Z	V	i	W	S	h	u	K	t
	*	N	Q	b	]	[	D	p	)	e	L	A	R	(	#	x	I	=	$	:	W	S	u	u	K	t
	K	N	Q	i	1	W	D	r	q	e	L	и	R	y	П	x	I	a	d	C	W	S	h	u	K	t

Общий принцип шифрования подстановкой может быть представлен следующей формулой:

$$R_i = S_i + w \bmod(k - 1),$$

где R_i — символ зашифрованного текста; S_i — символ исходного текста; w — целое число в диапазоне $0\ldots(k - 1)$; k — число символов используемого алфавита.

Если w фиксировано, то формула описывает моноалфавитную подстановку; если w выбирается из последовательности w_1, w_2,…, w_n, то получается полиалфавитная подстановка с периодом n.

Если в полиалфавитной подстановке $n > m$ (где m — число знаков шифруемого текста) и любая последовательность w_1, w_2,…, w_n используется только один раз, такой шифр является теоретически нераскрываемым. Такой шифр получил название шифра Вермэна.

2.3 Шифрование с симметричными ключами методами перестановки

Этот вид шифрования подразумевает, что символы шифруемого текста внутри шифруемого блока символов переставляются по определенным правилам. Наиболее часто встречаются в автоматизированных системах следующие разновидности этого метода.

Самая простая перестановка — написать исходный текст задом наперед и одновременно разбить шифрограмму на пятерки букв. Например, из фразы ПУСТЬ БУДЕТ ТАК, КАК МЫ ХОТЕЛИ получится такой шифротекст:

ИЛЕТО ХЫМКА ККАТТ ЕДУБЬ ТСУП.

В последней группе (пятерке) не хватает одной буквы. Значит, прежде чем шифровать исходное выражение, следует его дополнить незначащей буквой (например, О) до числа, кратного пяти:

ПУСТЬ-БУДЕТ-ТАККА-КМЫХО-ТЕЛИО.

Тогда шифрограмма, несмотря на столь незначительное изменение, будет выглядеть по-другому:

ОИЛЕТ ОХЫМК АККАТ ТЕДУБ ЬТСУП.

Кажется, ничего сложного, но при расшифровке появятся серьезные неудобства.

Другую разновидность этого метода можно представить как метод усложненной перестановки по таблице следующим шифром (табл. 2.5). Исходную фразу следует писать в несколько строк, например по пятнадцать букв в каждой, дополнив последнюю строку свободно выбранными буквами.

Таблица 2.5 — Символы шифрования при усложненной замене по строкам

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
П	У	С	Т	Ь	Б	У	Д	Е	Т	Т	А	К	К	А
К	М	Ы	Х	О	Т	Е	Л	И	К	Л	М	Н	О	П

Затем вертикальные столбцы разбивают на пятерки букв и последовательно записывают в строку. Получают зашифрованный текст:

ПКУМС ЫТХЬО БТУЕД ЛЕИТК ТЛАМК НКОАП.

Другой вариант этого шифра предусматривает предварительную процедуру записи исходной фразы в столбцы (табл. 2.6).

Таблица 2.6 — Символы шифрования при усложненной замене по столбцам

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
П	С	Ь	У	Е	Т	К	А	М	Х	Т	Л	А	В	Д
У	Т	Б	Д	Т	А	К	К	Ы	О	Е	И	Б	Г	Е

Затем строки разбивают на пятерки

ПСЬУЕ ТКАМХ ТЛАВД УТБДТ АККЫО ЕИБГЕ.

Матричный шифр перестановки можно построить, если укоротить строки, соответственно увеличив их число в таблице. В результате получится прямоугольник-решетка, в который записывают исходный текст. При этом получают другую форму зашифрованного текста. В этом случае адресату и отправителю посланий необходимо сформулировать условия записи и дешифрования решетки, так как она может иметь различную длину и высоту. Записывать текст в решетку можно по строкам,

столбцам, прямой или обратной спирали, диагоналями, причем шифровать и дешифровать можно в различных направлениях.

Для примера возьмем решетку 6х6 (причем число строк может увеличиваться или уменьшаться в зависимости от длины исходного сообщения) и заполним ее по строкам (табл. 2.7).

Таблица 2.7 — Матричная перестановка символов

П	У	С	Т	Ь	Б
У	Д	Е	Т	Т	А
К	К	А	К	М	Ы
Х	О	Т	Е	Л	И
А	Б	В	Г	Д	Е
М	Л	К	И	З	Ж

Если шифровать по стрелкам (диагоналям) сверху вниз с левого верхнего угла, то в итоге получится такая шифрограмма:

П УУ СДК ТЕКХ ЬТАОА БТКТБМ АМЕВЛ ЫЛГК ИДИ ЕЗ Ж.

Для окончательного оформления шифротекст может быть разбит на группы по шесть символов:

ПУУСДК ТЕКХЬТ АОАБТК ТБМАМЕ ВЛЫЛГК ИДИЕЗЖ.

Часто используют перестановки с ключом. Тогда правила заполнения решетки и шифрования из нее упрощаются. Единственное, что надо помнить и знать, — это ключ, которым может быть любое слово.

Возьмем, например, слово РАДИАТОР. Применяем следующий алгоритм кодировки букв. По алфавиту буква А получает номер 1, вторая буква А — 2, следующая по алфавиту буква Д — 3, потом И — 4, О — 5, первая буква Р — 6, вторая Р — 7 и буква Т — 8.

Заполним решетку (табл. 2.8).

Таблица 2.8 — Перестановка символов с ключом

Р	А	Д	И	А	Т	О	Р
6	1	3	4	2	8	5	7
П	У	С	Т	Ь	Б	У	Д
Е	Т	Т	А	К	К	А	К
М	Ы	Х	О	Т	Е	Л	И
О							

Записываем столбики в соответствии с номерами букв ключа:
УТЫ ЬКТ СТХ ТАО УАЛ ПЕМО ДКИ БКЕ.
Затем последовательность опять разбиваем на пятерки:
УТЫЬК ТСТХТ АОУАЛ ПЕМОД КИБКЕ.

Развитием этого шифра является шифр перестановки колонок с пропусками (табл. 2.9), которые располагаются в решетке тоже в соответствии с ключом (в нашем случае через 6-1-3-4-2-8-5-7… символов).

Таблица 2.9 — Перестановка символов с пропусками

Р	А	Д	И	А	Т	О	Р
6	1	3	4	2	8	5	7
П	У	С	Т	Ь	Б	=	У
=	Д	Е	Т	=	Т	А	К
К	=	Х	О	=	Т	Е	Л
И	К	Л	М	=	О	П	Р

Шифрограмма получается следующей:
УДК Ь СЕХЛ ТТОМ АЕП ПКИ УКЛР БТТО.

2.4 Шифрование с симметричными ключами при помощи аналитических преобразований

С помощью этого вида шифрования информация закрывается достаточно надежно. Для этого можно использовать метод алгебры матриц, например умножение матрицы на вектор по следующему правилу:

$$\overline{\tilde{N}} = A \times \overline{B}; \qquad \sum_{j=1}^{N} a_{ij} b_j .$$

Если матрицу $A(a_{ij})$ использовать в качестве ключа, а в место компонента вектора $B = (b_j)$ подставить символы текста, то компоненты вектор $C = (c_j)$ будут представлять собой символы зашифрованного текста.

Приведем пример, взяв в качестве ключа квадратную матрицу третьего порядка:

$$A = \begin{pmatrix} 14 & 8 & 3 \\ 8 & 5 & 2 \\ 3 & 2 & 1 \end{pmatrix}.$$

Заменим буквы алфавита цифрами, соответствующими их порядковому номеру в алфавите: А = 0, Б = 1, В = 2 и т.д. Тогда отрывку текста ВАТАЛА будет соответствовать последовательность чисел 2, 0, 19,

0, 12, 0. По принятому алгоритму шифрования выполним необходимые действия:

$$\overline{C} = A \times \overline{B} = \begin{pmatrix} 14 & 8 & 3 \\ 8 & 5 & 2 \\ 3 & 2 & 1 \end{pmatrix} \times \begin{pmatrix} 2 \\ 0 \\ 19 \end{pmatrix} = \begin{pmatrix} 85 \\ 54 \\ 25 \end{pmatrix};$$

$$\overline{C} = A \times \overline{B} = \begin{pmatrix} 14 & 8 & 3 \\ 8 & 5 & 2 \\ 3 & 2 & 1 \end{pmatrix} \times \begin{pmatrix} 0 \\ 12 \\ 0 \end{pmatrix} = \begin{pmatrix} 96 \\ 60 \\ 24 \end{pmatrix}.$$

При этом зашифрованный текст будет иметь следующий вид:

85, 54, 25, 96, 60 , 24.

Дешифрование осуществляется с использованием того же правила умножения матрицы на вектор, только в качестве ключа берется матрица, обратная той, с помощью которой осуществляется шифрование, а в качестве вектора-сомножителя — соответствующие фрагменты символов закрытого текста. Тогда значениями вектора-результата будут цифровые эквиваленты знаков открытого текста.

Матрицей, обратной данной A, называется матрица A^{-1}, получающаяся из присоединенной матрицы делением всех ее элементов на определитель данной матрицы. В свою очередь, *присоединенной* называется матрица, составленная из алгебраических дополнений A_{ij} к элементам данной матрицы, которые вычисляются по следующей формуле:

$$A_{ij} = (-1)^{i+j} \Delta_{ij},$$

где Δ_{ij} — определитель матрицы, получаемой вычеркиванием i-й строки и j-го столбца исходной матрицы A.

Определителем матрицы называется алгебраическая сумма $n!$ членов (для определителя n-го порядка), составленная следующим образом: членами служат всевозможные произведения n элементов матрицы, взятых по одному в каждой строке и в каждом столбце, причем член суммы берется со знаком «+», если его индексы составляют четную подстановку, и со знаком «–» в противоположном случае. Для матрицы третьего порядка, например, определитель

$$\Delta = a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} - a_{11}a_{23}a_{32} - a_{12}a_{21}a_{33} - a_{13}a_{22}a_{31}.$$

Тогда процесс дешифровки текста будет выглядеть следующим образом:

$$A^{-1}\times\overline{C}=\begin{pmatrix}1 & -2 & 1\\ -2 & 5 & -4\\ 1 & -4 & 6\end{pmatrix}\times\begin{pmatrix}85\\ 54\\ 25\end{pmatrix}=\begin{pmatrix}1\cdot 85-2\cdot 54+1\cdot 25\\ -2\cdot 85+5\cdot 54-4\cdot 25\\ 1\cdot 85-4\cdot 54+6\cdot 25\end{pmatrix}=\begin{pmatrix}2\\ 0\\ 19\end{pmatrix};$$

$$A^{-1}\times\overline{C}=\begin{pmatrix}1 & -2 & 1\\ -2 & 5 & -4\\ 1 & -4 & 6\end{pmatrix}\times\begin{pmatrix}96\\ 60\\ 24\end{pmatrix}=\begin{pmatrix}1\cdot 96-2\cdot 60+1\cdot 24\\ -2\cdot 96+5\cdot 60-4\cdot 24\\ 1\cdot 96-4\cdot 60+6\cdot 24\end{pmatrix}=\begin{pmatrix}0\\ 12\\ 0\end{pmatrix}.$$

Таким образом, получена последовательность чисел раскрытого текста: 2, 0, 19, 0, 12, 0, что соответствует исходному тексту. Этот метод шифрования является формальным, что позволяет легко реализовывать его программными средствами.

2.5 Шифрование аддитивными методами (гаммирование)

Этот вид шифрования предусматривает последовательное сложение символов шифруемого текста с символами некоторой специальной последовательностью, которая называется *гаммой*. Иногда его представляют как наложение гаммы на исходный текст, поэтому он получил название *гаммирование*.

Процедуру наложения гаммы на исходный текст можно осуществить двумя способами. При первом способе символы исходного текста и гаммы заменяются цифровыми эквивалентами, которые затем складываются по модулю k, где k — число символов в алфавите, т.е.

$$R_i=(S_i+G)\bmod(k-1),$$

где R_i, S_i, G — символы соответственно зашифрованного исходного текста и гаммы.

При втором методе символы исходного текста и гаммы представляются в виде двоичного кода, затем соответствующие разряды складываются по модулю 2. Вместо сложения по модулю 2 при гаммировании можно использовать и другие логические операции, например преобразование по правилу логической эквивалентности (рис. 2.2, *а*) или логической неэквивалентности (рис. 2.2, *б*). Такая замена равносильна введению еще одного ключа (рис. 2.2, *в*), которым является выбор правила формирования символов зашифрованного сообщения из символов исходного текста и гаммы.

Гамма	Текст 0	Текст 1
0	0	1
1	1	0

а

Гамма	Текст 0	Текст 1
0	1	0
1	0	1

б

Шифруемый текст	Б	У	Д	Ь …	
	000001	010100	000100	011110	
Знаки гаммы	7	1	8	2 …	
	000111	000001	001000	000010	
Шифрованный текст	010101	100001	111010	100010	

в

а — по правилу логической эквивалентности; *б* — по правилу логической неэквивалентности; *в* — формирование сигналов зашифрованного сообщения из символов зашифрованного текста и гаммы

Рисунок 2.2 — Пример шифрования гаммированием

Стойкость шифрования методом гаммирования определяется главным образом свойствами гаммы: длительностью периода и равномерностью статистических характеристик. Последнее свойство обеспечивает отсутствие закономерностей в появлении различных символов в пределах периода. Обычно разделяют две разновидности гаммирования — с конечной и бесконечной гаммами. При хороших статистических свойствах гаммы стойкость шифрования определяется только длиной периода гаммы. При этом если длина периода гаммы превышает длину шифруемого текста, то такой шифр теоретически является абсолютно стойким, т.е. его нельзя вскрыть при помощи статистической обработки зашифрованного текста. Это, однако, не означает, что дешифрование такого текста вообще невозможно: при наличии некоторой дополнительной информации исходный текст может быть частично или полностью восстановлен даже при использовании бесконечной гаммы.

В качестве гаммы может быть использована любая последовательность случайных символов, например последовательность цифр числа π, числа **e** (основание натурального логарифма) и т.п. При шифровании с помощью ЭВМ последовательность гаммы может формироваться с помощью датчика псевдослучайных чисел (ПСЧ). В настоящее время разработано несколько алгоритмов работы таких датчиков, которые обеспечивают удовлетворительные характеристики гаммы.

2.5 Комбинированные методы шифрования с симметричными ключами

Эти методы являются достаточно эффективным средством повышения стойкости шифрования. Они заключаются в применении различных способов шифрования исходного текста одновременно или последовательно.

Как показали исследования, стойкость комбинированного шифрования S_k не ниже произведения стойкостей используемых способов S_i, т.е.

$$S_k \geq \prod_i S_i .$$

Комбинировать можно любые методы шифрования и в любом количестве, однако на практике наибольшее распространение получили следующие комбинации: 1) подстановка + гаммирование; 2) перестановка + гаммирование; 3) гаммирование + гаммирование; 4) подстановка + перестановка. Типичным примером комбинированного шифра является национальный стандарт США криптографического закрытия данных (DES).

3 Экспериментальная часть

3.1 Задание на работу

Задание 3.1. Таблица Вижинера

Реализовать средствами языка PASCAL программу шифрования данных. В качестве данных используется ФИО студента. Ключи для шифрования приведены в таблице 3.1.

Таблица 3.1 — Варианты заданий

№ Варианта	Ключ
1	Леонардо
2	Рафаэль
3	Донателло
4	Шекспир
5	Платон
6	Аристотель
7	Сократ
8	Ахиллес
9	Моцарт
10	Амадеус

Программа должна выводить на экран данные, подлежащие шифрованию, рабочую матрицу и зашифрованный текст. Шифрограмму записать в файл.

Задание 3.2 Перестановка символов с ключом

Реализовать средствами языка PASCAL программу шифрования данных. В качестве данных используется ФИО студента. Ключи для шифрования приведены в таблице 3.11.

Программа должна выводить на экран данные, подлежащие шифрованию, заполненную решетку и шифрограмму. Шифрограмму записать в файл.

Задание 3.3 Аналитические преобразования

Реализовать средствами языка PASCAL программу шифрования данных. В качестве данных используется фамилия студента. Ключи для шифрования приведены в таблице 3.2

Таблица 3.2 — Варианты заданий

№ Варианта	Ключ
1	$\begin{pmatrix} 2 & 8 & 1 \\ 3 & 15 & 8 \\ 4 & 2 & 7 \end{pmatrix}$
2	$\begin{pmatrix} 3 & 15 & 8 \\ 2 & 8 & 1 \\ 4 & 2 & 7 \end{pmatrix}$
3	$\begin{pmatrix} 19 & 3 & 4 \\ 9 & 13 & 12 \\ 4 & 1 & 2 \end{pmatrix}$
4	$\begin{pmatrix} 9 & 5 & 4 \\ 18 & 7 & 15 \\ 3 & 5 & 1 \end{pmatrix}$

Окончание табл. 3.2

№ Варианта	Ключ
5	$\begin{pmatrix} 10 & 8 & 1 \\ 13 & 6 & 18 \\ 14 & 3 & 5 \end{pmatrix}$
6	$\begin{pmatrix} 3 & 18 & 5 \\ 8 & 15 & 8 \\ 9 & 12 & 17 \end{pmatrix}$
7	$\begin{pmatrix} 5 & 7 & 11 \\ 4 & 15 & 18 \\ 5 & 3 & 2 \end{pmatrix}$
8	$\begin{pmatrix} 4 & 13 & 1 \\ 8 & 11 & 9 \\ 7 & 1 & 17 \end{pmatrix}$
9	$\begin{pmatrix} 14 & 4 & 3 \\ 3 & 10 & 6 \\ 5 & 1 & 13 \end{pmatrix}$
10	$\begin{pmatrix} 1 & 7 & 6 \\ 2 & 8 & 4 \\ 14 & 12 & 17 \end{pmatrix}$

Нумерацию букв алфавита начинать с 0. Программа должна выводить на экран данные, подлежащие шифрованию, ключ и шифрограмму. Шифрограмму записать в файл.

Задание 3.4 Гаммирование

Реализовать средствами PASCAL программу шифрования данных. В качестве данных используется фамилия студента. Буквы перевести в двоичный эквивалент, соответствующий номерам букв в алфавите. Нумерацию букв в алфавите начинать с 0. В качестве гаммы использовать последовательность нечетных чисел, использовать 6 разрядов. Программа должна выводить на экран таблицу, аналогичную таблице на рис. 2.2, *в*. Шифрограмму записать в файл.

3.2 Содержание отчета

Отчет должен содержать:
1. Титульный лист.
2. Цель.
3. Название используемого метода.
4. Алгоритм используемого метода.
5. Листинг программы.
6. Результат работы программы.
7. Выводы.

Список литературы

1. Мельников В.П., Клейменов С.А., Петраков А.М. Информационная безопасность: Учебное пособие для сред. проф. образования. — М.: Издательский центр «Академия», 2005. — 336 с.

Учебное пособие

Колегов А.А.

Криптографическое преобразование информации

Методические указания к лабораторной работе
по дисциплине «Информационные технологии в электронике»

Усл. печ. л. _____Препринт
Томский государственный университет
систем управления и радиоэлектроники
634050, г.Томск, пр.Ленина, 40