А.М. Голиков

КРИПТОГРАФИЯ

Методические указания по курсовой работе для студентов специальности 090106 «Информационная безопасность телекоммуникационных систем»

Томск

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ

Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования

ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИСТЕТ СИСТЕМ УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ

УТВЕРЖДАЮ
Заведующий кафедрой РТС

_____ Г.С. Шарыгин
“____” _____ 2008 г.

КРИПТОГРАФИЯ

Методические указания по курсовой работе
для студентов специальности
090106 «Информационная безопасность телекоммуникационных систем»

Разработчики

Доцент каф. РТС, к.т.н.

_____ А.М. Голиков

“____” _____ 2008г.

2008

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

А.М.Голиков Криптография. Методические указания по выполнению курсовой работы для студентов специальности 090106 Информационная безопасность телекоммуникационных систем. - Томск: Том. гос. ун-т систем управления и радиоэлектроники, 2008. – 24 с.

Приводятся указания по выполнению курсовой работы по дисциплине «Криптографические методы и средства защиты информации» для студентов специальности 090106 - Информационная безопасность телекоммуникационных систем.

СОДЕРЖАНИЕ

1 ЦЕЛЬ И ЗАДАЧИ КУРСОВОЙ РАБОТЫ

Цель курсовой работы по дисциплине «Криптография» состоит в развитии и закреплении навыков решения задач по защите информации с использованием криптографических методов.

Особое внимание уделяется разработке и анализу программ реализующих стандартные криптографические алгоритмы.

В процессе самостоятельной работы студента (под руководством преподавателя) решаются следующие задачи:

- получение навыков программирования криптографических алгоритмов;

- развитие системного и алгоритмического мышления;

- получение навыков разработки программной документации;

- усвоение комплекса организационных мер и приемов при выполнении работ большого объема;

- развитие навыков самостоятельного поиска и использования справочной литературы (включая источники в Интернет);

- приобретение навыков использования современных информационных технологий для подготовки презентаций;

- приобретение навыков публичных выступлений перед аудиторией.

Курсовая работа выполняется по индивидуальным заданиям. Общее руководство осуществляет преподаватель. За принятые в работе решения, правильность функционирования программ, качество подготовки текстовых документов, а также за своевременность подготовки и защиты курсовой работы в целом отвечает студент. В процессе выполнения работы студент должен правильно организовать свой труд, регулярно работать над заданием, проявлять максимум инициативы и самостоятельности для решения поставленных задач.

2 ТЕМАТИКА КУРСОВЫХ РАБОТ

Тематика работ определяется программой курса, связана с предыдущими и последующими дисциплинами и включает в себя следующие темы.

1. Цифровая подпись RSA.
2. Криптосистема RSA.
3. Алгогоритм Rijndael.
4. Моделирование имитозащищенного канала связи
5. Криптосистема Меркля- Хеллмана.
6. Стандарт цифровой подписи DSS.
7. Стандарт цифровой подписи ГОСТ Р 34.10-94.
8. Алгоритм аутентификации информации
9. Метод простой перестановки с использованием ключа.
10. Метод перестановки, усложнённый по матрице.
11. Метод перестановки, усложнённый по графу.
12. Шифрование с помощью датчика псевдослучайных чисел с использованием алфавита из таблицы.
13. Шифрование открытым ключом.
14. Аппаратно-программый комплекс криптографической защиты на базе алгоритма AES.
15. Криптошлюз на базе российского алгоритма криптографической защиты ГОСТ 28147-89 и его аппаратная реализация.
16. Аппаратно-программный комплекс сокрытия информации на базе методов стеганографии.
17. Быстродействующий цифровой скремблер.
18. Аппаратно-программный комплекс для реализации российского алгоритма электронной цифровой подписи.
19. Технология ЭЦП и PKI для филиальной сети банка.
20. Высокоскоростная система шифрования на базе поточных шифров.

3. СОДЕРЖАНИЕ КУРСОВАЙ РАБОТЫ

3.1 Общие сведения

В результате выполнения курсовой работы студент должен получить навыки разработки и анализа известных криптографических алгоритмов.

После получения задания студент последовательно выполняет следующее:

- анализ технического задания,
- постановка задачи,
- сравнительный анализ математических методов решения задачи,
- выбор и обоснования метода решения задачи,
- выбор и обоснование использования программного обеспечения,
- разработка алгоритма решения задачи,
- разработка программы решения задачи,
- верификация программы,
- разработка программной документации,
- подготовка компьютерной презентации курсовой работы,
- защита работы перед комиссией.

Следует сходить в библиотеку и познакомиться с источниками разработки и дополнительной литературой [1-34].

3.2 Структура курсовой работы

Объем текстового документа подготавливаемого студентом в процессе выполнения курсовой работы 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.

3.3 Титульный лист

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

3.4 Реферат

Реферат выполняется в соответствии с ГОСТ 7.9-95 и размещается на отдельной странице.

Реферат должен содержать [1,3]:

- 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 курсовая работа 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,
- сравнительный анализ математических методов решения поставленной задачи,
- описание криптографического алгоритма,
- описание алгоритма программы,
- описание программы,
- верификация программы,
- анализ результатов проектирования.

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 программы и ставится цель и задачи курсовой работы. Приводится описание и математическая модель решаемой задачи. Выполняется анализ технических ограничений на разработку. Обосновывается выбор используемых аппаратных и программных средств.

3.7.3 Сравнительный анализ методов решения задами

В разделе выполняется обзор математических методов решения поставленной задачи. Должен быть выполнен сравнительный анализ методов по предполагаемому быстродействию, точности, возможности оптимизации, трудоемкости разработки, требуемым вычислительным затратам. Раздел завершается выбором и обоснованием математического метода решения задачи.

3.7.4 Описание алгоритма

В разделе «Описание алгоритма» приводится алгоритм решения поставленной задачи в соответствии с индивидуальным заданием. Алгоритм приводится с необходимыми пояснениями. Описание алгоритма должно иллюстрироваться перечнем используемых переменных и схемой алгоритма программы. Схема алгоритма выполняется строго по ГОСТ 19.701-90 ЕСПД. В случае разработки сложной программной системы, как правило, в соответствии с заданием необходимо разработать схему алгоритма не для всей программы, а только для её определенного блока.

3.7.5 Описание программы

В разделе выполняется описание программного обеспечения, разработанного студентом.

Раздел «Описание программы» должен содержать следующие сведения:

- наименование программы,
- назначение программы, классы решаемых задач.
- программное обеспечение, необходимое для функционирования программы,
- вспомогательное программное обеспечение, языки программирования, на которых написана программа,
- функциональное назначение, ограничения на применение,
- структура программы с описанием функций составных частей,
- связи программы с другими программами,
- описание входных и выходных данных (количество, тип, формат).

В раздел рекомендуется включать таблицу соответствия переменных алгоритма и программы.

В разделе обязательно должна присутствовать функциональная схема программы, содержащая все разработанные функции.

Рекомендуется описание программы иллюстрировать пояснительными примерами, таблицами, схемами и графиками.

3.7.6 Верификация разработанного программного обеспечения

В разделе должна быть приведена методика тестирования разработанного программного обеспечения. Должны быть приведены тестирующие примеры. В каждом контрольном примере обязательно должно указываться, какую часть программы, функциональной схемы, модуля, функции данный пример тестирует. Приводятся входные данные и выходные результаты, обеспечивающие тестирование. Рекомендуется все тестовые примеры объединить в таблицу.

Должно быть доказано, что разработанное программное обеспечение работает правильно (Полностью соответствует техническому заданию).

3.7.7 Руководство пользователя

Раздел «Руководство пользователя» содержит описание программы, ориентированной на потребителя. Раздел должен быть написан таким образом, чтобы

потребитель разработанного программного обеспечения мог использовать его без другой документации.

Раздел «Руководство пользователя» должен содержать следующие сведения:

- назначение программы,
- требования к программному и аппаратному обеспечению,
- описание интерфейса,
- описание элементов управления,
- примеры окон диалога,
- требования к входным данным,
- форматы результатов,
- тестовые примеры (должны отличаться от примеров приведенных в разделе3.7.6).
- сообщения пользователю,
- методика настройки программы,
- описание действий пользователя при наличии сбоев в работе программы.

Раздел «Руководство пользователя» может быть вынесен в приложение.

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.

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 (Примеры библиографического описания источников см. в разделе «Литература» настоящих методических указаний).

3.10 Приложения

Приложения рекомендуется выносить материалы иллюстративного и вспомогательного характера.

Приложения к курсовой работе могут содержать следующие материалы:

- схемы алгоритмов,
- листинги программ,
- термины и определения,
- список каталогов и файлов, прилагаемых на компакт диске,
- протоколы испытаний программы,

- акты внедрения программы.

4 ТРЕБОВАНИЯ К ОФОРМЛЕНИЮ

4.1 Общие требования

4.1.1 При оформлении курсовой работы следует пользоваться стандартом вуза ОС ТУСУР 6.1-97 [1].

4.1.2 Текстовые документы (ТД) должны быть выполнены на белой бумаге формата А4 по ГОСТ 2.301 (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 ГОСТ 2.301, при этом они должны быть сложены на формат А4 "гармоникой" по ГОСТ 2.501.

4.1.4 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.

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

4.1.6 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.

4.1.7 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 одною 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», ею 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 иллюстрация 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.

ЛИТЕРАТУРА

1. Чернышев А.А. ОС ТУСУР 6.1-97 «Работы студенческие учебные и выпускные квалификационные. Общие требования и правила оформления». Томск, 2002.

2. ГОСТ 7.1-84 Система стандартов по информации, библиотечному и издательскому делу (ССИБИД). Библиографическое описание документа. Общие требования и правила составления.

3. ГОСТ 7.9-95 ССИБИД. Реферат и аннотация.

4. ГОСТ 7.12-93 ССИБИД. Сокращения русских слов и словосочетаний в библиографическом описании произведений печати.

5. ГОСТ 19.001-77 Единая система программной документации (ЕСПД). Общие положения.

6. ГОСТ 19.101-77 ЕСПД. Виды программ и программных документов.

7. ГОСТ 19.102-77 ЕСПД. Стадии разработки.

8. ГОСТ 19.103-77 ЕСПД. Обозначения программ и программных документов.

9. ГОСТ 19.104-78 ЕСПД. Основные надписи.

10. ГОСТ 19.105-78 ЕСПД. Общие требования к программным документам. И.ГОСТ 19.106-78 ЕСПД. Требования к программным документам
выполненным печатным способом. 12.ГОСТ 19.201-78 ЕСПД. Техническое задание. Требования к содержанию и оформлению.

13. ГОСТ 19.201-78 ЕСПД. Спецификация. Требования к содержанию и оформлению.

14. ГОСТ 19.301-79 ЕСПД. Программа и методика испытаний. Требования к содержанию и оформлению.

15. ГОСТ 19.401-78 ЕСПД. Текст программы. Требования к содержанию и оформлению.

16. ГОСТ 19.402-78 ЕСПД. Описание программы.

17. ГОСТ 19.404-79 ЕСПД. Пояснительная записка. Требования к содержанию и оформлению.

18. ГОСТ 19.502-78 ЕСПД. Описание применения. Требования к содержанию и оформлению.

19. ГОСТ 19.503-79 ЕСПД. Руководство системного программиста. Требования к содержанию и оформлению.

20. ГОСТ 19.504-79 ЕСПД. Руководство программиста. Требования к содержанию и оформлению.

21. ГОСТ 19.505-79 ЕСПД. Руководство оператора. Требования к содержанию и оформлению.

22. ГОСТ 19.508-79 ЕСПД. Руководство по техническому обслуживанию. Требования к содержанию и оформлению.
23. ГОСТ 19.701-90 ЕСПД. Схемы алгоритмов, программ, данных и систем. Обозначения условные и правила выполнения.
24. ГОСТ 19.871-90 ЕСПД. Обеспечение систем обработки информации программное. Термины и определения.
25. Соколов, А.В. Защита информации в распределенных корпоративных сетях и системах - М.: ДМК Пресс, 2002. - 656 с:

26. Щеглов, А.Ю. Защита компьютерной информации от несанкционированного доступа: производственно-практическое издание - СПб.: Наука и техника, 2004. - 384с.
27. Леонтьев, Б.К. Компьютерный "террор": Методы взлома информационных систем и компьютерных сетей: справочное издание -М.: Познавательная книга плюс, 2002. - 559с.
28.Орлов, С.А. Технологии разработки программного обеспечения.
Разработка сложных программных систем: Учебное пособие для вузов.
- СПб.: Питер, 2002. - 464 с. 29.«Введение в криптографию»: /Под общей редакцией В.В.Ященко. - М.:
«МЦНМО», «ЧеРо», 1998, 272с. ЗО.В.Жельников. «Криптография от папируса до компьютера». - М.:
«Мир», 1996.
31. А.Саломаа. «Криптография открытым ключом». - М.: «Мир», 1995.
32. Рябко Б.Я., Фионов А.Н.. Криптографические методы защиты информации: Учебное пособие для вузов. – М.: Горячая линия-Телеком, 2005. – 229 с.
33. Изучение стандарта криптографической защиты aes (advanced encryption standart): Лабораторная работа / Голиков А. М. – 2007. 41 с. (http://edu.tusur.ru/training/publications/1012)
34. Защита данных с помощью pgp: Лабораторная работа / Голиков А. М. – 2007. 46 с. (http://edu.tusur.ru/training/publications/1013)

ПРИЛОЖЕНИЕ А

(справочное)

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 УЧЕБНОГО АППАРАТНО-ПРОГРАММНОГО КОМПЛЕКС ДЛЯ ИССЛЕДОВАНИЯ И ВИЗУАЛИЗАЦИИ РАБОТЫ КРИПТОШЛЮЗА AES НА БАЗЕ ПО MATLAB

Курсовая работа по дисциплине «Криптография»

Студент гр. 1С8

_____ Ю.Д. Кузьменко

«_____» _____20___ г.

Руководитель

Доцент каф. РТС, к.т.н.

_____ А.М. Голиков

“____” _____ 20___г.

2008

ПРИЛОЖЕНИЕ В

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

ЗАДАНИЕ

на курсовую работу по курсу «Криптография»

студенту гр. 1с8 Кузьменко Ю. Д.

1. Наименование курсовой работы: Разработка учебного аппаратно-программного комплекс для исследования и визуализации работы криптошлюза AES на базе ПО MATLAB

2. Цель работы: Учебный аппаратно-программного комплекс позволит проводить как исследование и визуализацию работы криптошлюза AES, так и осуществить его дальнейшую аппаратную реализацию на современной базе

3. Назначение работы и область применения: Учебный аппаратно-программный комплекс предназначен для исследования и визуализации работы аппаратного криптошлюза AES на базе ПО MATLAB и дальнейшей его аппаратной реализации.

4. Основные условия работы и показатели назначения системы

4.1 Алгоритм шифрования AES (Rijndael).

4.2 Реализация алгоритма шифрования – аппаратно-программная

4.3 Скорость шифрования в абонентском режиме от 210КБ/с и выше

4.4 Длина шифруемого блока данных – 128 бит

4.5 Длина ключа шифрования – 128 бит (256 бит)

4.6 Программное обеспечение MATLAB

5. Содержание пояснительной записки курсовой работы (оглавление)

5.1 Математическая основа алгоритмов шифрования и режимов работы AES

5.2 Алгоритмы реализации методов шифрования, расшифрования, исследования и визуализации AES

5.3. Разработка ПО комплекса в среде MATLAB

5.4 Разработка и испытание методик шифрования, расшифрования, исследования и визуализации AES

5.5. Разработка задания для лабораторных исследований и рекомендаций для аппаратно-программной реализации криптошлюза AES на современной аппаратной базе, выработка максимально достижимых технических характеристик криптошлюза.

6. Перечень графического материала (с обязательным указанием чертежей)

6.1 Структурная схема аппаратно-программного комплекса

6.2 Блок схемы алгоритмов методов шифрования, расшифрования, исследования и визуализации AES

6.3.Блок схемы ПО комплекса в среде MATLAB

7.Форма отчетности.

Пояснительная записка, графический материал (п.6), CD_программного комплекса и технической документации, презентация курсовой работы для защиты

Руководитель проекта доцент каф. РТС Голиков А.М_____

(Ф.И.О., должность, место работы)

Подпись руководителя _____

Задание принял к исполнению (дата): «__» _____Подпись студента _____