Программа учебной дисциплины
«Криптографические методы защиты информации»

Утверждена
Академическим советом ООП
Протокол № 2 от 19.04.2017 г.

Автор	Бабаш Александр Владимирович
Число кредитов	6
Контактная работа (час.)	72
Самостоятельная работа (час.)	156
Курс	1 курс, магистерская программа: «Управление информационной безопасностью»
Формат изучения дисциплины	без использования онлайн курса

I. ЦЕЛЬ, РЕЗУЛЬТАТЫ ОСВОЕНИЯ ДИСЦИПЛИНЫ И ПРЕРЕКВИЗИТЫ

Целями освоения дисциплины «Криптографические методы защиты информации» является получение знаний и выработка компетенций в области криптографической защиты информации в организациях.

В результате освоения дисциплины студент должен

знать:

- основания криптографической защиты информации в организации;
- основные понятия и требования криптографической защиты информации;

уметь:

- выявлять специфику криптографических угроз информационной безопасности по ряду категорий информации;
- выделять основания и объекты защиты информации, определять основания и процедуру осуществления криптографической защиты информации;

владеть:

- навыками определения криптографической стойкости шифрсистем;
- навыками обоснования выбора криптографических средств для защиты информации.

Дисциплина «Криптографические методы защиты информации» относится к вариативной части блока дисциплин, обеспечивающих подготовку магистров по программе: «Управление информационной безопасностью».
Изучение данной дисциплины базируется на следующих дисциплинах:

- «Математический анализ»;
- «Общая, линейная и высшая алгебра»;
- «Теория вероятностей и математическая статистика»;
- «Теория чисел»;
- «Математическая логика»;
- «Дискретная математика».

Для освоения учебной дисциплины, студенты должны владеть следующими знаниями и компетенциями:

- основами математического аппарата для решения задач прикладной математики;
- применять понятийно-категориальный аппарат, основные теоремы прикладной математики в профессиональной деятельности;
- ориентироваться в системе законодательства и нормативных правовых актов, регламентирующих сферу применения криптографических методов защиты информации для обеспечения информационной безопасности;
- использовать основные понятия и теоремы прикладной математики в профессиональной и общественной деятельности;
- защищать права на интеллектуальную собственность;
- навыками философского мышления для выработки системного, целостного взгляда на проблемы общества;
- навыками публичной речи, аргументации, ведения дискуссии.

Основные положения дисциплины должны быть использованы в дальнейшем при подготовке выпускной квалификационной работы по магистерской программе: «Управление информационной безопасностью».

II. СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

Тема 1. Исторический очерк развития криптографии

Рассматривается ряд конкретных примеров шифров и их применения, известных начиная с античных времен и до современного периода времени. Краткая характеристика рассматриваемых шифров.

Литература

1. Бабаш А. В. Криптографические методы защиты информации. Учебно-методическое пособие / Издание 2-е исправленное и дополненное. Т. 1. М. : ИНФРА-М, РИОР, 2014.
2. Бабаш А. В., Баранова Е. К. Криптографические методы защиты информации: учебник. М. : КноРус, 2016.
3. Баранова Е. К., Бабаш А. В. Криптографические методы защиты информации. Лабораторный практикум. + CD/ Учебное пособие. М. : КноРус, 2015.

Тема 2. Математические основы криптографии. Основные понятия криптографии

Операции над множествами. Бинарные отношения на множестве Бинарные операции на множестве. Алгебраические структуры (группы, кольца и т.д.). Криптография. Конфиденциальность. Целостность. Аутентификация. Цифровая подпись.
Управление секретными ключами. Предварительное распределение ключей. Пересылка ключей. Открытое распространение ключей. Схема разделения секрета.
Инфраструктура открытых ключей. Сертификаты. Центры сертификации.
Формальные модели шифров.
Модели открытых текстов. Математические модели открытого текста. Критерии распознавания открытого текста.

Литература

1. Бабаш А. В. Криптографические методы защиты информации. Учебно-методическое пособие / Издание 2-е исправленное и дополненное. Т. 1. М. : ИНФРА-М, РИОР, 2014.
2. Бабаш А. В., Баранова Е. К. Криптографические методы защиты информации: учебник. М. : КноРус, 2016.
3. Баранова Е. К., Бабаш А. В. Криптографические методы защиты информации. Лабораторный практикум. + CD/ Учебное пособие. М. : КноРус, 2015.

Тема 3. Классификация шифров по различным признакам

Математическая модель шифра простой замены. Классификация шифров замены.

Литература

1. Бабаш А. В. Криптографические методы защиты информации. Учебно-методическое пособие / Издание 2-е исправленное и дополненное. Т. 1. М. : ИНФРА-М, РИОР, 2014.
2. Бабаш А. В., Баранова Е. К. Криптографические методы защиты информации: учебник. М. : КноРус, 2016.
3. Баранова Е. К., Бабаш А. В. Криптографические методы защиты информации. Лабораторный практикум. + CD/ Учебное пособие. М. : КноРус, 2015.

Тема 4. Шифры перестановки

Маршрутные перестановки. Элементы криптоанализа шифров перестановки.

Литература

1. Бабаш А. В. Криптографические методы защиты информации. Учебно-методическое пособие / Издание 2-е исправленное и дополненное. Т. 1. М. : ИНФРА-М, РИОР, 2014.
2. Бабаш А. В., Баранова Е. К. Криптографические методы защиты информации: учебник. М. : КноРус, 2016.
3. Баранова Е. К., Бабаш А. В. Криптографические методы защиты информации. Лабораторный практикум. + CD/ Учебное пособие. М. : КноРус, 2015.

Тема 5. Шифры замены

Поточные шифры простой замены. Элементы криптоанализа поточного шифра простой замены. Блочные шифры простой замены. Многоалфавитные шифры замены. Многоалфавитные шифры замены.

Литература

1. Бабаш А. В. Криптографические методы защиты информации. Учебно-методическое пособие / Издание 2-е исправленное и дополненное. Т. 1. М. : ИНФРА-М, РИОР, 2014.
2. Бабаш А. В., Баранова Е. К. Криптографические методы защиты информации: учебник. М. : КноРус, 2016.
3. Баранова Е. К., Бабаш А. В. Криптографические методы защиты информации. Лабораторный практикум. + CD/ Учебное пособие. М. : КноРус, 2015.

Тема 6. Шифры гаммирования

Табличное гаммирование. О возможности восстановления вероятностей знаков гаммы. Восстановление текстов, зашифрованных неравновероятной гаммой. Повторное использование гаммы. Элементы криптоанализа шифра Виженера.
Ошибки шифровальщика.

Литература

1. Бабаш А. В. Криптографические методы защиты информации. Учебно-методическое пособие / Издание 2-е исправленное и дополненное. Т. 1. М. : ИНФРА-М, РИОР, 2014.
2. Бабаш А. В., Баранова Е. К. Криптографические методы защиты информации: учебник. М. : КноРус, 2016.
3. Баранова Е. К., Бабаш А. В. Криптографические методы защиты информации. Лабораторный практикум. + CD/ Учебное пособие. М. : КноРус, 2015.

Тема 7. Надежность шифров

Энтропия и избыточность языка. Расстояние единственности.
Стойкость шифров. Теоретическая стойкость шифров. Практическая стойкость шифров. Вопросы имитостойкости шифров. Шифры, не распространяющие искажений.

Литература

1. Бабаш А. В. Криптографические методы защиты информации. Учебно-методическое пособие / Издание 2-е исправленное и дополненное. Т. 1. М. : ИНФРА-М, РИОР, 2014.
2. Бабаш А. В., Баранова Е. К. Криптографические методы защиты информации: учебник. М. : КноРус, 2016.
3. Баранова Е. К., Бабаш А. В. Криптографические методы защиты информации. Лабораторный практикум. + CD/ Учебное пособие. М. : КноРус, 2015.

Тема 8. Блочные системы шифрования

Принципы построения блочных шифров. Примеры блочных шифров – американский стандарт шифрования данных DES, стандарт шифрования данных ГОСТ 28147-89. Режимы использования блочных шифров. Комбинирование алгоритмов блочного шифрования.
Элементы криптоанализа алгоритмов блочного шифрования.
Рекомендации по использованию алгоритмов блочного шифрования.

Литература

1. Бабаш А. В. Криптографические методы защиты информации. Учебно-методическое пособие / Издание 2-е исправленное и дополненное. Т. 1. М. : ИНФРА-М, РИОР, 2014.
2. Бабаш А. В., Баранова Е. К. Криптографические методы защиты информации: учебник. М. : КноРус, 2016.
3. Баранова Е. К., Бабаш А. В. Криптографические методы защиты информации. Лабораторный практикум. + CD/ Учебное пособие. М. : КноРус, 2015.
4. Шнайер Брюс. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. – М.: Триумф, 2002.

Тема 9. Поточные системы шифрования

Синхронизация поточных шифрсистем. Принципы построения поточных шифрсистем. Примеры поточных шифрсистем – шифрсистема А5, шифрсистема Гиффорда.
Линейные регистры сдвига.
Алгоритм Берлекемпа-Месси.
Усложнение линейных рекуррентных последовательностей. Фильтрующие генераторы. Комбинирующие генераторы. Композиции линейных регистров сдвига. Схемы с динамическим изменением закона рекурсии. Схемы с элементами памяти.
Элементы криптоанализа поточных шифров.

Литература

1. Бабаш А. В. Криптографические методы защиты информации. Учебно-методическое пособие / Издание 2-е исправленное и дополненное. Т. 1. М. : ИНФРА-М, РИОР, 2014.
2. Бабаш А. В., Баранова Е. К. Криптографические методы защиты информации: учебник. М. : КноРус, 2016.
3. Баранова Е. К., Бабаш А. В. Криптографические методы защиты информации. Лабораторный практикум. + CD/ Учебное пособие. М. : КноРус, 2015.
4. Варфоломеев А.А., Жуков А.Е., Пудовкина М.А. Поточные криптосистемы. Основные свойства и методы анализа стойкости. – М.: Изд-во МИФИ, 2000.

Тема 10. Системы шифрования с открытыми ключами

Шифрсистема RSA. Шифрсистема Эль-Гамаля. Шифрсистема Мак-Элиса. Шифрсистемы на основе «проблемы рюкзака».

Литература

1. Бабаш А. В. Криптографические методы защиты информации. Учебно-методическое пособие / Издание 2-е исправленное и дополненное. Т. 1. М. : ИНФРА-М, РИОР, 2014.
2. Бабаш А. В., Баранова Е. К. Криптографические методы защиты информации: учебник. М. : КноРус, 2016.
3. Баранова Е. К., Бабаш А. В. Криптографические методы защиты информации. Лабораторный практикум. + CD/ Учебное пособие. М. : КноРус, 2015.
4. Смарт Н. Криптография. – М.: Техносфера, 2006.

Тема 11. Идентификация

Фиксированные пароли (слабая идентификация). Правила составления паролей. Усложнение процедуры проверки паролей. «Подсоленные» пароли. Парольные фразы.
Атаки на фиксированные пароли. Повторное использование паролей. Тотальный перебор паролей. Атаки с помощью словаря. Личные идентификационные номера. Одноразовые пароли.
«Запрос-ответ» (сильная идентификация). «Запрос-ответ» с использованием симметричных алгоритмов шифрования. «Запрос-ответ» с использованием асимметричных алгоритмов шифрования.
Протоколы с нулевым разглашением. Атаки на протоколы идентификации.

Литература

1. Бабаш А. В. Криптографические методы защиты информации. Учебно-методическое пособие / Издание 2-е исправленное и дополненное. Т. 1. М. : ИНФРА-М, РИОР, 2014.
2. Бабаш А. В., Баранова Е. К. Криптографические методы защиты информации: учебник. М. : КноРус, 2016.
3. Баранова Е. К., Бабаш А. В. Криптографические методы защиты информации. Лабораторный практикум. + CD/ Учебное пособие. М. : КноРус, 2015.
4. Смарт Н. Криптография. – М.: Техносфера, 2006.

Тема 12. Криптографические хеш-функции

Функции хеширования и целостность данных. Ключевые функции хеширования.
Бесключевые функции хеширования. Целостность данных и аутентификация сообщений.
Возможные атаки на функции хеширования.

Литература

1. Бабаш А. В. Криптографические методы защиты информации. Учебно-методическое пособие / Издание 2-е исправленное и дополненное. Т. 1. М. : ИНФРА-М, РИОР, 2014.
2. Бабаш А. В., Баранова Е. К. Криптографические методы защиты информации: учебник. М. : КноРус, 2016.
3. Смарт Н. Криптография. – М.: Техносфера, 2006.

Тема 13. Цифровые подписи

Общие положения. Цифровые подписи на основе шифрсистем с открытыми ключами. Цифровая подпись Фиата-Шамира. Цифровая подпись Эль-Гамаля. Одноразовые цифровые подписи.

Литература

1. Бабаш А. В. Криптографические методы защиты информации. Учебно-методическое пособие / Издание 2-е исправленное и дополненное. Т. 1. М. : ИНФРА-М, РИОР, 2014.
2. Бабаш А. В., Баранова Е. К. Криптографические методы защиты информации: учебник. М. : КноРус, 2016.
3. Смарт Н. Криптография. – М.: Техносфера, 2006.

Тема 14. Протоколы распределения ключей

Передача ключей с использованием симметричного шифрования. Двусторонние протоколы. Трехсторонние протоколы. Передача ключей с использованием асимметричного шифрования. Протоколы без использования цифровой подписи. Протоколы с использованием цифровой подписи. Сертификаты открытых ключей.Открытое распределение ключей.
Предварительное распределение ключей. Схемы предварительного распределения ключей в сети связи. Схемы разделения секрета.
Способы установления ключей для конференц-связи.
Возможные атаки на протоколы распределения ключей.

Литература

1. Бабаш А. В. Криптографические методы защиты информации. Учебно-методическое пособие / Издание 2-е исправленное и дополненное. Т. 1. М. : ИНФРА-М, РИОР, 2014.
2. Бабаш А. В., Баранова Е. К. Криптографические методы защиты информации: учебник. М. : КноРус, 2016.
3. Смарт Н. Криптография. – М.: Техносфера, 2006.

Тема 15. Управление ключами

Жизненный цикл ключей. Услуги, предоставляемые доверенной третьей стороной. Установка временных меток. Нотаризация цифровых подписей.

Литература

1. Бабаш А. В. Криптографические методы защиты информации. Учебно-методическое пособие / Издание 2-е исправленное и дополненное. Т. 1. М. : ИНФРА-М, РИОР, 2014.
2. Бабаш А. В., Баранова Е. К. Криптографические методы защиты информации: учебник. М. : КноРус, 2016.
3. Баранова Е. К., Бабаш А. В. Криптографические методы защиты информации. Лабораторный практикум. + CD/ Учебное пособие. М. : КноРус, 2015.
4. Шнайер Брюс. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. – М.: Триумф, 2002.

Образовательные технологии

В рамках проведения семинаров разбираются задачи по темам лекций, рассматриваются и анализируются ситуационные задачи, выполняются практические работы по индивидуальным заданиям.

III. ОЦЕНИВАНИЕ

Оценки за работу на семинарских занятиях преподаватель выставляет в рабочую ведомость. Накопленная оценка по 10-ти балльной шкале за работу на семинарских занятиях определяется перед промежуточным или итоговым контролем – $O_{аудиторная}$.
Оценки за самостоятельную работу студента преподаватель выставляет в рабочую ведомость. Накопленная оценка по 10-ти балльной шкале за самостоятельную работу определяется перед промежуточным или итоговым контролем – $O_{сам.работа}$.

Накопленная оценка за текущий контроль учитывает результаты студента по текущему

контролю следующим образом:

$$О_{текущий} = 0,2 \cdot О_{аудиторная} + 0,8 \cdot О_{сам.работа}.$$

Способ округления накопленной оценки текущего контроля производится по правилам арифметики округления.

Результирующая оценка за итоговый контроль выставляется по следующей формуле, где $О_{итоговый\ тест}$ – оценка за итоговую письменную работу:

$$О_{итоговая\ \_} = 0,4 \cdot О_{итоговый\ тест} + 0,6 \cdot О_{текущий}.$$

Способ округления накопленной оценки итогового контроля производится по правилам арифметики округления.

IV. ПРИМЕРЫ ОЦЕНОЧНЫХ СРЕДСТВ

Оценочные средства для текущего контроля студента

Примеры тем для рефератов

1. Возможные атаки на алгоритм DES.
2. Достоинства и недостатки систем поточного шифрования по сравнению с блочными шифрами.
3. Атаки, которые могут быть использованы при нападении на протоколы идентификации.
4. Назначение и структура сертификата открытого ключа.

Вариант тестового задания

1. Всякий источник сообщений можно моделировать списком допустимых (т.е. встречающихся в каких-либо текстах) k-грамм при k=1,2,3,… Какие из приведенных k-грамм не являются допустимыми в русском языке? (несколько верных ответов)

1) “ШЕЕ”;
2) “ЖФ”;
3) “АУ”;
4) “ЮЪХ”;
5) “ЖЬН”.

2. Криптограмма получена в результате простой замены:

«ВГАДЮБКГЖЯАО МЮБ ЕДБЕБЗ ЛЖФАЮТ АЬЯБГЫЖРАА»

Ключ-подстановка:

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	Ъ	Ы	Ь	Э	Ю	Я
Ж	З	Х	К	И	Ц	Ч	Л	А	В	Ъ	Ы	Ь	Б	Д	Г	Е	Ю	Э	Я	П	Р	У	С	Ф	Ш	Т	Щ	М	Н	О

Восстановленный исходный текст:

1) «КРИПТОЛОГИЯ ЭТО НАУКА О ЗАЩИТЕ ИНФОРМАЦИИ»;
2) «КРИПТОГРАФИЯ ЭТО СПОСОБ ЗАЩИТЫ ИНФОРМАЦИИ»;
3) «КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ».

3. Что означает термин «многократное шифрование» применительно к блочным шифрам?

1) повторное применение алгоритма шифрования к шифртексту с теми же ключами;
2) шифрование одного и того же блока открытого текста несколько раз с несколькими ключами;
3) увеличение числа этапов шифрования открытого текста.

4. Гаммирование чаще всего осуществляется: (несколько верных ответов)

1) по модулю 2, если открытый текст представляется в виде бинарной последовательности;
2) по модулю 256, если открытый текст представляется в виде последовательности байтов;
3) по модулю 16, если открытый текст представлен в цифровом виде;
4) по модулю 10, если открытый текст представлен в виде последовательности цифр, что иногда делается в ручных системах шифрования.

5. Основой построения большинства поточных шифров являются:

1) генераторы псевдослучайных чисел, в частности, различные комбинации регистров сдвига;
2) схемы суммирования по mod 16;
3) таблицы подстановок.

6. Зашифрованный методом перестановки открытый текст: «Сертификаты ключей ЭЦП»***, при ключе длинной 7, и перестановке: {4132756}, имеет вид:***

1) тСреиифыктал кйюечЦ Э П ;
2) юклчТи ЭСЦ еиртфаикт ы ;
3) чКилют рСекиафиЭтПы Ц .

7. Зашифровать слово «выборочность» ***методом перестановки с ключом {3142}:***

1) бвоычрнотоьс ;
2) ыовбрчоонсьт ;
3) ывброончотсь .

8. Зашифровать открытый текст – «field» ***методом Виженера, ключ –*** «moon» ***(алфавит – латиница):***

1) rwcup
2) rwsyp
3) rvsyp

9. Частотный анализ может эффективно применяться для дешифрования шифров:

1) перестановки;
2) многоалфавитной замены;
3) простой замены.

10. Какие меры практической стойкости шифра относительно метода криптоанализа вы можете выделить: (несколько верных ответов)

1) вероятность дешифрования за время, не превосходящее T;
2) среднее время, необходимое для дешифрования шифра;
3) скорость дешифрования шифра.

11. Какие шифры можно называть имитостойкими?

1) шифры, обладающие свойством противостоять разрастанию ошибок при расшифровании текстов;
2) шифры, обладающие свойством противостоять попыткам навязывания ложной информации.

12. Какие шифры можно называть помехоустойчивыми?

1) шифры, обладающие свойством противостоять разрастанию ошибок при расшифровании текстов;
2) шифры, обладающие свойством противостоять попыткам навязывания ложной информации.

13. Разрастание числа ошибок означает что

1) ошибка в одной букве, допущенная при шифровании, приводит к большому числу ошибок в расшифрованном тексте;
2) ошибка в одной букве, допущенная при расшифровании, приводит к последующим ошибкам.

14. Шифр считается совершенным,

1) если он не поддается дешифрованию;
2) если положение противника, стремящегося к его дешифрованию, не облегчается в результате перехвата шифртекста;
3) если требуются большие затраты или мала вероятность успеха его дешифрования.

15. Шифр считается практически стойким,

1) если он не поддается дешифрованию;
2) если положение противника, стремящегося к его дешифрованию, не облегчается в результате перехвата шифртекста;
3) если требуются большие затраты или мала вероятность успеха его дешифрования.

16. Степень неоднозначности восстановления открытого текста при дешифровании

1) возрастает при уменьшении материала;
2) снижается при уменьшении материала.

Вариант контрольного задания

Вариант 1

1. Найдите произведение подстановок.

$G1 \cdot G2 = ?$

$G1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 5 & 4 & 6 & 2 \end{pmatrix}$; $G2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 6 & 1 & 5 & 3 \end{pmatrix}$.

2. Найдите обратную подстановку к данной.

$G = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 3 & 1 & 4 \end{pmatrix}$ $G^{-1} = ?$

3. Определите порядок подстановки.

$G = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 2 & 5 & 3 \end{pmatrix}$

4. Вычислить сумму 4 и 5 по модулю n. Множество {1,2,3,4,5,6,7}
5. Вычислить произведение 6 и 7 по модулю n. Множество {1,2,3,4,5,6,7}.
6. Множество{0,1,2,3,4,5,6}.Является ли элемент «5» обратимым по сложению? Если да, то какой элемент обратный?
7. Множество {0,1,2,3,4,5,6}.Является ли элемент «0» обратимым по умножению? Если да, то какой элемент обратный?

Примеры задач

Задача 1

Зашифровать текст при помощи шифра простой замены, при имеющемся ключе. Пропуски не шифруются.

Текст: «КРИПТОГРАФИЯ ЭТО СПОСОБ ЗАЩИТЫ ИНФОРМАЦИИ».

Ключ:

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	Ъ	Ы	Ь	Э	Ю	Я
Ж	З	Х	К	И	Ц	Ч	Л	А	В	Ъ	Ы	Ь	Б	Д	Г	Е	Ю	Э	Я	П	Р	У	С	Ф	Ш	Т	Щ	М	Н	О

Задача 2

Расшифровать текст при помощи шифра простой замены, при имеющемся ключе шифрования.

Текст: «ВГАДЮБКГЖЯАО МЮБ ЕДБЕБЗ ЛЖФАЮТ АЬЯБГЫЖРАА»

Ключ-подстановка:

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	Ъ	Ы	Ь	Э	Ю	Я
Ж	З	Х	К	И	Ц	Ч	Л	А	В	Ъ	Ы	Ь	Б	Д	Г	Е	Ю	Э	Я	П	Р	У	С	Ф	Ш	Т	Щ	М	Н	О

Задача 3

Зашифровать текст при помощи шифра перестановки при имеющемся ключе.

Текст: «КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА»

Ключ:

1	2	3	4	5	6
5	3	4	1	6	2

Задача 4

Расшифровать текст, зашифрованный шифром перестановки, имея ключ

Текст: «ПОРИКТФЧРАГИА СКЕЯИААЩЗТ»

Ключ:

1	2	3	4	5	6
5	3	4	1	6	2

Задача 5

Зашифровать текст с помощью шифра случайного гаммирования, считая, что буквы алфавита пронумерованы от 0 до 32 соответственно. Зная определенную гамму.

А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	
17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	

Текст: «КРИПТОГРАФИЯ»

Задача 6

Расшифровать криптограмму, полученную с помощью метода случайного гаммирования, считая, что буквы алфавита пронумерованы от 0 до 32 соответственно. Зная определенную гамму.

А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	
17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	

Текст: «ХСЩРАБЛЮТЕЧЙ»

Гамма(ключ):

11	1	17	1	14	19	9	14	19	17	15	11

Оценочные средства для промежуточной аттестации по курсу

Вопросы для оценки качества освоения дисциплины

1. Приведите примеры шифров, применявшихся еще до нашей эры
2. Приведите пример шифра, для которого сам открытый текст является ключом
3. Какие шифры являются омофонами, в чем их преимущество перед шифрами простой замены
4. Что является ключом шифра Виженера
5. Являлись ли трафареты, которые использовали А. Грибоедов и Ришелье для передачи тайных сообщений, средствами шифрования
6. Приведите пример шифра, допускающего неоднозначное зашифрование
7. Какими шифрами пользовались Цезарь, Галилей, Наполеон, Ришелье
8. В чем состоит правило Керхгоффса, почему это правило является общепризнанным в криптографии
9. Чем отличаются принципы шифрования в аналоговой телефонии от принципов шифрования телеграфных сообщений
10. Чем отличаются симметричные шифрсистемы от асимметричных шифрсистем
11. Когда родилась криптография с открытыми ключами и первая реальная система шифрования
12. Каких выдающихся криптографов XX в. Вы знаете
13. Чем отличаются подходы к обеспечению безопасности информации в криптографии и в методах сокрытия информации
14. Какими методами обеспечивается конфиденциальность информации
15. Что такое целостность информации
16. Для каких аспектов информационного взаимодействия необходима аутентификация
17. Какие средства используются для обеспечения невозможности отказа от авторства
18. В чем суть предварительного распределения ключей
19. В чем разница между обычным и открытым распределением ключей
20. Для чего нужны схемы разделения секрета
21. Что такое сертификат открытого распределения ключей
22. Каковы функции центра сертификации ключей
23. Чем отличаются алгебраическая и вероятностная модели шифра
24. С какими целями в криптографии вводятся модели открытых текстов
25. Как подсчитать вероятность данного открытого текста в модели первого приближения
26. Какие подходы используются для распознавания открытых текстов
27. С какими примерами шифров замены и перестановки вы познакомились в историческом обзоре
28. Существуют ли шифры, не являющиеся ни шифрами замены, ни шифрами перестановки
29. Приведите пример шифра многозначной замены
30. Может ли блочный шифр быть шифром разнозначной замены

31. Приведите пример шифра перестановки, который может рассматриваться и как блочный шифр замены
32. Как определить по криптограмме, полученной с помощью шифра вертикальной перестановки, число коротких столбцов заполненного открытым текстом основного прямоугольника
33. Какие свойства открытого текста используются при вскрытии шифра вертикальной перестановки
34. Какие шифры называются шифрами простой замены
35. Что является ключом шифра простой замены, каково максимально возможное число ключей шифра простой замены
36. Что более целесообразно для надежной защиты информации: архивация открытого текста с последующим зашифрованием или шифрование открытого текста с последующей архивацией
37. Имеет ли шифр Плейфера эквивалентные ключи, то есть такие ключи, на которых любые открытые тексты шифруются одинаково
38. Предположим, что матричный шифр Хилла используется для зашифрования открытого текста, представленного в виде двоичной последовательности, сколько ключей имеет такой шифр
39. Является ли надежным шифрование литературного текста с помощью модульного гаммирования, использующего гамму, два знака которой имеют суммарную вероятность, совпадающую с суммарной вероятностью остальных знаков
40. Почему наложение на открытый текст гаммы, представляющей собой периодическую последовательность небольшого периода, не дает надежной защиты
41. Почему недопустимо использовать дважды одну и ту же гамму для зашифрования разных открытых текстов
42. Почему в качестве гаммы нецелесообразно использовать текст художественного произведения
43. Как определяется энтропия и избыточность языка
44. Как можно качественно охарактеризовать избыточность языка
45. Какие тексты на русском языке имеют большую избыточность: литературные или художественные
46. Почему неопределенность шифра по открытому тексту (или по ключу) можно рассматривать как меру теоретической стойкости шифра
47. Как зависит расстояние единственности для шифра от энтропии языка
48. Найдите расстояние единственности для шифра Виженера, который используется для шифрования технических текстов на русском языке с избыточностью 0,8
49. Какие атаки используются в криптоанализе
50. Каким образом априорные вероятностные распределения на множествах открытых текстов и ключей индуцируют вероятностное распределение на множестве шифрованных текстов
51. Какой шифр называется совершенным (для атаки на основе шифртекста)
52. В каком случае шифр модульного гаммирования является совершенным (для атаки на основе шифртекста)
53. Верно ли, что лишь шифры табличного гаммирования являются совершенными
54. Чем отличаются понятия теоретической и практической стойкости шифра
55. Что такое имитостойкость шифра, что может служить мерой имитостойкости шифра, является ли шифр гаммирования имитостойким
56. Что такое совершенная имитостойкость шифра
57. Является ли шифр гаммирования шифром, не размножающим искажения типа «замена знаков», искажения типа «пропуск знаков»
58. Каковы с точки зрения криптографии преимущества и недостатки перехода к шифрованию сообщений в алфавитах большой мощности
59. Как реализуется предложенный К. Шенноном принцип «перемешивания» при практической реализации алгоритмов блочного шифрования
60. Каковы основные недостатки алгоритма DES, и каковы пути их устранения
61. Как связан «парадокс дней рождения» с криптографическими качествами блочных шифров в режиме простой замены
62. В каких случаях можно рекомендовать использование блочного шифра в режиме простой

замены

63. От каких потенциальных слабостей позволяет избавиться использование блочных шифров в режимах шифрования с обратной связью
64. Почему возникает проблема синхронизации поточных шифров
65. Что с точки зрения криптографического алгоритма определяет управляющий блок
66. Какой необходимый минимум функциональных возможностей должен быть заложен в шифрующем блоке
67. За счет чего можно обеспечить стойкость алгоритма шифрования при повторном использовании ключей
68. Какие причины обусловили широкое использование линейных регистров сдвига в качестве управляющих блоков поточных шифрсистем
69. Для каких целей применяются усложнения линейных рекуррентных последовательностей
70. Какие существуют типы генераторов Макларена-Марсальи
71. Какие два разных способа шифрования аналоговых сигналов вы знаете
72. Какие преобразования используются при скремблировании аналоговых сигналов
73. В чем (с точки зрения надежности защиты) состоят слабости преобразований сигналов в частотной области, во временной области
74. Какая фундаментальная теорема лежит в основе цифровой обработки сигналов
75. Какой метод шифрования аналоговых сигналов обеспечивает гарантированную стойкость
76. В чем состоят преимущества систем с открытыми ключами перед симметричными шифрсистемами
77. Сложностью какой математической задачи определяется стойкость системы RSA
78. К какому типу принадлежит схема шифрования, используемая в системе Эль-Гамаля, в чем ее преимущества
79. Чем вызваны трудности в практической реализации системы Мак-Элиса
80. На какие группы могут быть разбиты алгоритмы идентификации
81. В чем состоят недостатки систем с фиксированными паролями
82. За счет чего повышается надежность идентификации при использовании плстиковой карты и личного идентификационного номера
83. Каковы возможные схемы использования одноразовых паролей
84. Для каких целей используется временная метка в протоколах типа «запрос-ответ»
85. Чем могут быть заменены временные метки в протоколах типа «запрос-ответ»
86. Какая идея лежит в основе протоколов с нулевым разглашением
87. Для каких целей применяются хеш-функции
88. Перечислите основные требования, предъявляемые к хеш-функциям
89. Почему нельзя использовать в качестве хеш-функций линейные отображения
90. Сравните требования, предъявляемые к ключевым и бесключевым хеш-функциям
91. Можно ли использовать в качестве бесключевой хеш-функции ключевую хеш-функцию с фиксированным ключом
92. Что общего между обычной и цифровой подписями, чем они различаются
93. Какие задачи позволяет решить цифровая подпись
94. В чем заключается принципиальная сложность в практическом применении систем цифровой подписи
95. Почему в криптографических системах, основанных на открытых ключах, нельзя использовать одинаковые ключи для шифрования и цифровой подписи
96. Каковы преимущества централизованного распределения ключей
97. Какие шифры нельзя использовать в протоколе Шамира
98. Каков недостаток протокола Нидхэма-Шрёдера
99. С какой целью вводится второй сервер в протоколе Kerberos

V. РЕСУРСЫ

Основная литература

1. Агрaновский А. В., Хади Р. А. Практическая криптография. Алгоритмы и их программирование (+ CD-ROM). СПб, СОЛОН-Пресс, 2002.
3. Бабаш А.В., Шанкин Г.П. Криптография. / Под редакцией В.П.Шерстюка, Э.А. Применко. – М.: СОЛОН-Р, 2002. – 512 с.
4. Бабаш А.В. Криптографические и теоретико-автоматные аспекты современной защиты информации. Том 1 – М.: Изд.центр ЕАОИ, 2009. – 414 с.
5. Бабаш А.В., Баранова Е.К. Криптографические методы защиты информации. М.: КНОРУС, 2016. – 190 с.
6. Баранова Е.К., Бабаш А.В. Криптографические методы защиты информации. Лабораторный практикум: учеб.пособие (+CD-ROM) – М.: КНОРУС, 2015. . – 200 с.
7. Вельшенбах М. Криптография на Си и С++ в действии (+CD-ROM). – М.: Триумф, 2004.
8. Зубов А. Ю. Криптографические методы защиты информации.–М.: Гелиос АРВ, 2005. –192с.
9. Коутинхо С. Введение в теорию чисел. Алгоритм RSA. – М.: Постмаркет, 2001. – 328 с.
10. Молдовян А. А., Молдовян Н. А., Советов Б. Я. Криптография. Учебник для вузов – М.: Лань, 2005.
11. Осипян В.О., Осипян К.В. Криптография в задачах и упражнениях. – М.: Гелиос АРВ, 2004.
12. Смарт Н. Криптография. – М.: Техносфера, 2006. – 528 с.
13. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. – М.: Триумф, 2002.
14. Руководящие документы ФСТЭК РФ. [Электронный ресурс] URL: http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty#

Дополнительная литература

1. Анохин М.И., Варновский Н.П., Сидельников В.М., Ященко В.В. Криптография в банковском деле. – М.: Изд-во МИФИ, 1997.
2. Бабаш А.В., Глухов М.М., Шанкин Г.П. О преобразованиях множества слов в конечном алфавите, не размножающих искажений // Дискретная математика. – 1997. – Т. 9. - № 3.
3. Биллингслей П. Эргодическая теория и информация. – М.: Мир, 1969.
4. Варфоломеев А.А., Пеленицын М.Б. Методы криптографии и их применение в банковских технологиях. – М.: Изд-во МИФИ, 1995.
5. Варфоломеев А.А., Домнина О.С., Пеленицын М.Б. Управление ключами в системах криптографической защиты банковской информации. – М.: Изд-во МИФИ, 1996.
6. Варфоломеев А.А., Жуков А.Е., Пудовкина М.А. Поточные криптосистемы. Основные свойства и методы анализа стойкости. – М.: Изд-во МИФИ, 2000.
7. Гнеденко Б.В. Курс теории вероятностей.- М.: Наука, 1988.
8. Диффи У., Хеллман М.Э. Защищенность и имитостойкость. Введение в криптографию // ТИИЭР. – 1979.- Т. 67. - №3.
9. Зубов А.Ю. Математика кодов аутентификации. - М.: «Гелиос АРВ», 2007.
10. Кнут Д. Искусство программирования для ЭВМ.– М.: Мир, – Т. 2. - 1977; Т. 3. – 1978.
11. Лидл Р., Нидеррайтер Г. Конечные поля. Т 1, 2. – М.: Мир,1988.
12. Сборник задач по алгебре / Под ред. А.И. Кострыкина. – М.: Наука, 1987.
13. Саломаа А. Криптография с открытым ключом. – М.: Мир, 1996.

14. Симмонс Г. Дж. Обзор методов аутентификации информации // ТИИЭР. – 1988. – Т. 76. – № 5.
15. Неф М., Штройле П., Хартман В. Опасности в Интернете: Способы защиты для пользователей. - М.: Редакция «ОПиПМ», Научное издательство «ТВП», 2006.
16. Перельман Я.И. Занимательная астрономия. – М.: Наука, 1966.
17. Проскурин В.Г. Защита программ и данных. – М.: Издательский центр «Академия», 2011.
18. Смит Р.Э. Аутентификация: от паролей до открытых ключей. – Москва, Санкт-Петербург, Киев: Вильямс, 2002.
19. Соболева Т.А. Тайнопись в истории России. – М.: «Международные отношения», 1994.
20. Холл М. Комбинаторика.- М.: Наука, 1970.
21. Хоффман Л. Современные методы защиты информации. – М.: Радио и связь, 1980.
22. Шеннон К. Теория связи в секретных системах // В кн.: Работы по теории информации и кибернетике.- М.: Наука, 1963.
23. Шнайер Б. Прикладная криптография. – М.: «Издательство ТРИУМФ», 2002.
24. Яглом А.М., Яглом И.М. Вероятность и информация. – М.: Наука, 1973.
25. Введение в криптографию / Под общ. ред. В.В.Ященко. – М.: МЦНМО, «ЧеРо», 1998.
26. Becket B. Introduction to cryptology and PC security. – McGrow-Hill, London, 1997.
27. Blom R. Nonpablic key distribution // Advances in Cryptology. – Proceedings of EUROCRYPT'82. Plenum. New York. – 1983. – pp. 231-236.
28. Callas N.P. An application of computers in cryptography // Cryptologia, October, 1978.
29. Diffie W., Hellman M.E. New directions in cryptography // IEEE Trans. on Inf. Theory. – 1976. – IT-22.
30. Dyer M., Fenner T., Frieze A., Thomason A. On key storage in secure networks // J. Cryptology. – 1995. - № 8. – pp. 189-200.
31. Friedman W.F. The index of coincidence and its applications in cryptanalysis. – Aegoen Park Press, Laguna Hills CA, 1920.
32. Friedman W.F., Callimahos D. Military cryptanalysis. Part I. Vol. 2. – Aegoen Park Press, Laguna Hills CA, 1985.
33. El Gamal T. A public-key cryptosystem and a signature scheme based on discrete logariphms // IEEE Trans. Inf. Theory. – 1985. – IT-31. - № 4
34. Merkle R.C., Hellman M.E. On the security of multiple encryption // Communications of the ACM. – 1981. – Vol. 24.
35. Jacobsen T. A Fast method for cryptanalysis of substitution cipher // J. Cryptologia. – 1995. - XIX. - № 3.
36. Kahn D. The codebreakers. The story of secret writing. - Macmillan, N.Y., 1967.
37. Matsumoto T., Takashima Y., Imai H. On seeking smart public- key- distribution system // Trans. of the IECE of Japan. – 1986. –E 69. – p. 99-106.
38. Menezes A.J., van Oorschot P.C., Vanstone S.A. Hand book of applied cryptography. – CRC Press, Boca Raton, New York, London, Tokyo, 1997.
39. Needham R.M., Schroeder M.D. Using encryption for authentication in large networks of computers // Communications of the ACM. – 1978.- Vol. 21. –pp. 993-999.
40. Yardley H.O. The american black chamber. – Bobbs Merrill, Indianapolis, IN, 1931.
41. Shamir A. How to share a secret // Commun. ACM. – 1979. - V. 22. – № 11. – pp. 612-613.
42. Rivest R.L., Shamir A., Adleman L. A Method for obtaining didital signatures and public key cryptosystems // Commun. ACM. – 1978. – V. 21. - № 2
43. Stinson D.R. Cryptography: Theory and practice. – CRC Press, N.Y., 1995.

Программное обеспечение

№ п/п	Наименование	Условия доступа
1.	Microsoft Windows 10 Microsoft Windows 8.1 Professional RUS	*Из внутренней сети университета (договор)*
2.	Microsoft Office Professional Plus 2010	*Из внутренней сети университета (договор)*

Профессиональные базы данных, информационные справочные системы, интернет-ресурсы (электронные образовательные ресурсы)

№ п/п	Наименование	Условия доступа
	Профессиональные базы данных, информационно-справочные системы	
1.	Консультант Плюс	*Из внутренней сети университета (договор)*
2.	Электронно-библиотечная система Юрайт	URL: https://biblio-online.ru/
	Интернет-ресурсы (электронные образовательные ресурсы)	
1.	Открытое образование	URL: https://openedu.ru/

Материально-техническое обеспечение дисциплины

Учебные аудитории для лекционных занятий по дисциплине обеспечивают использование и демонстрацию тематических иллюстраций, соответствующих программе дисциплины в составе:

– персональные компьютеры с доступом в Интернет (операционная система, офисные программы, антивирусные программы);

– мультимедийный проектор с дистанционным управлением.

Учебные аудитории для лабораторных и самостоятельных занятий по дисциплине оснащены перечисленным выше ПО, с возможностью подключения к сети Интернет и доступом к электронной информационно-образовательной среде НИУ ВШЭ.