ФЕДЕРАЛЬНОЕ АГЕНТСТВО ВОЗДУШНОГО ТРАНСПОРТА

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
«МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ ГРАЖДАНСКОЙ АВИАЦИИ»

Кафедра основ радиотехники и защиты информации

Э. А. Болелов

ПОСОБИЕ

к выполнению практических занятий
по дисциплине

«КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ»

для студентов 4 курса
специальности 090106
дневной формы обучения

Москва – 2010

Данное учебно-методическое пособие издается в соответствии с рабочей программой учебной дисциплины «Криптографические методы защиты информации» по Учебному плану специальности 090106 для студентов дневного обучения.

Учебно-методическое пособие способствует реализации квалификационных требований к студентам по обеспечению знаний в области криптографических методов защиты информации.

В учебно-методическом пособии приведены организационно-методические указания по проведению практических занятий и задания на их проведение.

Рассмотрено и одобрено на заседаниях кафедры 26 января 2010 г. и методического совета 26 января 2010 г.

СОДЕРЖАНИЕ

Общие организационно-методические указания по подготовке и проведению практических занятий

При подготовке к занятию студенты должны:

- уяснить цель и порядок проведения практического занятия;
- изучить учебные материалы, изложенные в рекомендуемой к практическому занятию литературе, а также лекционный материал.

В результате самостоятельной подготовки студенты должны уметь ответить вопросы самоконтроля. На занятии каждый студент должен иметь конспект лекций, данные организационно-методические указания и отдельную тетрадь для оформления отчетов по практическим занятиям.

Практическое занятие начинается с контроля готовности студентов к занятию. Контроль готовности к практическому занятию начинается с проверки присутствия студентов на занятии, наличия у каждого студента организационно-методических указаний, тетради для оформления отчетов по практическим занятиям, конспекта лекций и заканчивается контрольным опросом студентов по знанию основных теоретических положений практического занятия.

Затем студенты самостоятельно решают задачи, полученные решения обсуждаются в группе. Условия задач и их решения оформляются студентами в отчетах.

Заканчивается занятие подведением итогов с оценкой работы студентов, оформлением и защитой отчета по практическому занятию.

Практическое занятие №1
Свойства простейших шифров. Освоение процессов зашифрования и расшифрования для простейших шифров

Цель занятия – закрепление теоретических знаний и практическое освоение процессов зашифрования и расшифрования для простейших шифров.

1. Учебные вопросы

1. Освоение процессов зашифрования и расшифрования для шифров перестановки.
2. Освоение процессов зашифрования и расшифрования для шифров замены (подстановки).

2. Литература

1. Баричев С.Г.и др. Основы современной криптографии: Учебный курс. – 2-е изд., испр.доп. – М.: Горячая линия – Телеком, 2002.
2. Осипян В.О, Осипян К.В. Криптография в задачах и упражнениях. – М.: Гелиос АРВ, 2004.
3. Нечаев В.И. Элементы криптографии (Основы защиты информации): Учеб.пособие для ун-тов и пед.вузов/ Под ред. В.А. Садовничего – М.: Высш. шк., 1999.

3. Задание на практическое занятие

При подготовке к занятию студенты должны изучить учебные материалы темы №2 «Основные классы симметричных криптосистем и их свойства», используя литературу [1], с.7-15, [2], с.22-33, [3], с.9-22, а также конспект лекций.

3.1 Освоение процессов зашифрования и расшифрования для шифров перестановки

Задача 1. Пусть дан открытый текст X =КРИПТОГРАФИЯ. Требуется получить криптограмму, используя шифр простой перестановки при заданном ключе $K = (10,2,3,7,5,8,9,11,12,1,4,6)$.

Задача 2. Пусть дан открытый текст: X =ИСТОРИЯ_КРИПТОГРАФИИ. Требуется получить криптограмму, используя шифр простой перестановки при заданном ключе $K = (5,3,4,1,2)$.

Задача 3. Дано открытое сообщение

X =ЭТО_ШИФР_ВЕРТИКАЛЬНОЙ_ПЕРЕСТАНОВКИ.

Требуется зашифровать данное сообщение шифром вертикальной перестановки используя ключ К= $(5,2,3,4,1)$.

Задача 4. Дан открытый текст X =ДОЛГ – ЭТО ТО, ЧТО ОЖИДАЕШЬ ОТ ДРУГИХ, НО НЕ ОТ СЕБЯ. ОСКАР УАЙЛЬД. Требуется зашифровать открытый текст.

Задан «магический квадрат»:

2	7	6
9	5	1
4	3	8

Задача 5. Зашифровать шифром маршрутной перестановки сообщение $X =$ФЕДЕРАЛЬНОЕ_АГЕНСТВО_ВОЗДУШНОГО_ТРАНСПОРТА.

Задача 6. Зашифровать сообщение $X =$ЛЕГКО КРИТИКОВАТЬ ДРУГИХ – СЛОЖНЕЕ ИЗМЕНИТЬСЯ САМОМУ, с помощью «магического квадрата»:

16	2	3	13
5	11	10	8
9	7	6	12
4	14	15	1

Задача 7. С помощью шифра маршрутной перестановки зашифровать открытое сообщение $X =$СМИРНОВ ПРИЕЗЖАЕТ ПЯТОГО, ОРГАНИЗУЙТЕ ВСТРЕЧУ. Запись текста в таблицу осуществлять в обычном порядке. Размер таблицы и порядок считывания криптограммы определить самостоятельно.

Задача 8. Дана криптограмма, полученная шифром перестановки с фиксированным периодом

$Y =$ЯИРЕДОЖМРОДОПЗЕСМЕИНОУОТСЕЩВВНИИНАИОЯОПОГРДЕЕВАКЩЙТЕЛОБЕАЕТСНИВНМОГОНИЕСПЕЕНОТГЬИЖИОООЛУХ.ИКАА ТРОСРОЛУШФЗ.

Расшифровать криптограмму при известном ключе $K = 1$7,5,4,3,2,6 .

3.2 Освоение процессов зашифрования и расшифрования для шифров замены (подстановки)

Задача 9.

Дан «квадрат Полибия»

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

Зашифровать открытое сообщение $X =$МАТЕМАТИКА - ЦАРИЦА НАУК.

Задача 10. Имеется криптограмма $Y =$ПШХБЙХФХОЁАИЕЙЧФЙХУЗУ, полученная применением шифра Цезаря с ключом $K = 5$. Расшифровать криптограмму.

Задача 11. Зашифровать сообщение $X =$ИМПЕРАТОР ЦЕЗАРЬ аффинным шифром Цезаря с ключами: $K_1 = 2$, $K_2 = 3$.

Задача 12. Зашифровать, используя шифр Виженера, открытое сообщение $X =$ШИФР СКРЫВАЕТ СОДЕРЖАНИЕ ТЕКСТА. Ключ шифра – $K =$МГТУГА.

Задача 13. Зашифровать сообщение $X =$КРИПТОГРАФИЯ НАИБОЛЕЕ ВАЖНАЯ ФОРМА РАЗВЕДКИ В СОВРЕМЕННОМ МИРЕ шифром Плейфера с ключом $K =$ГРОЗА.

Задача 14. Используя шифр простой литореи, зашифровать сообщение $X =$ВСТРЕЧА ОТМЕНЯЕТСЯ.

Задача 15. Шифром гаммирования зашифровать сообщение $X =$ШИФР ВЕРНАМА – СОВЕРШЕННО СТОЙКИЙ ШИФР, при заданной гамма-последовательности $\gamma =$ТРВЛСТТВНЕДИТЫЗЗЭКЙКЁТМАОВТЕНГЫБ.

Задача 16. Имеется открытый текст $X =$В ЧУЖОЙ МОНАСТЫРЬ СО СВОИМ УСТАВОМ НЕ ХОДЯТ. Зашифровать текст шифром Плейфера на ключе $K =$КРИПТОГРАФИЯ.

Задача 17. Зашифровать сообщение $X =$ПРИШЕЛ УВИДЕЛ ПОБЕДИЛ шифром Виженера с автоключом. В качестве ключа использовать первое слово открытого сообщения.

Задача 18. Шифром Виженера зашифровать открытый текст $X =$ЧТОБЫ УЗНАТЬ МЫСЛИ ЧЕЛОВЕКА, ЕМУ ВЛЕЗАЮТ В СЕРДЦЕ, А В ПИСЬМА – ТЕМ БОЛЕЕ. ВИЛЬЯМ ШЕКСПИР. При зашифровании использовать ключ $K =$ПОЭМА и лозунг – АЛФАВИТ.

Задача 19. Зашифровать текст $X =$ЛЮБОЙ ШИФР МОЖЕТ БЫТЬ ВСКРЫТ, ЕСЛИ ТОЛЬКО В ЭТОМ ЕСТЬ НАСТОЯТЕЛЬНАЯ НЕОБХОДИМОСТЬ. НОРБЕРТ ВИНЕР с помощью «доски Полибия» используя ключ $K =$ПОЛИБИЙ.

Задача 20. Криптограмма, полученная при зашифровании сообщения шифром Цезаря, имеет вид

$Y =$ХПНЬЪШЧЭХЫИМШЫЩШНЙЩЪТЫИРЧЕОСЙЫОНЙЬОХТ.

Расшифровать сообщение при известном ключе К=10.

Задача 21. Криптограмма, полученная при зашифровании сообщения шифром Виженера, имеет вид $Y =$ТХТЩНТУТФЦЧТВ. Расшифровать сообщение при известном ключе $K =$РИМ.

Задача 22. Получена криптограмма, зашифрованная шифром Плейфера $Y =$ТПФРХИМОШЙГОЫЙЭШТГНЗЖНКДЙЦЛЙНГМОЙ АБОВЗКДЖОМГ. Расшифровать криптограмму, используя исходные данные задачи 13.

Вопросы для самоконтроля:

1. Дате определение шифра перестановки.
2. Приведите примеры шифров перестановки. В чем их суть?
3. Поясните процесс зашифрования сообщений шифром маршрутной перестановки.
4. Поясните, в чем различия между шифрами маршрутной перестановки и вертикальной перестановки.
5. Поясните процесс зашифрования (расшифрования) текстов шифром «магический квадрат».
6. В чем заключаются особенности зашифрования (расшифрования) сообщений «решеткой Кордано»?
7. Дайте определение шифра замены (подстановки).
8. Приведите примеры шифров замены. В чем их суть?
9. Что называется моноалфавитной и многоалфавитной заменой?
10. Поясните связь между шифром Цезаря и шифром Виженера.
11. Поясните процесс зашифрования (расшифрования) сообщений шифром Плейфера.

4. Ответы к задачам

Задача 1. $Y =$ ФРИГТРАИЯКПО.

Задача 2. $Y =$ РТОИСР_КИЯГТОИПИФИРА.

Задача 3. $Y =$ ШВКОРНЯТФРЛ_СВОРТЬПТК_ _ИНЕАИЭИЕАЙЕО.

Задача 4. $Y =$ ОТЭТ-ДГЛО,ЖОДООТЧИАТОРЬДШЕДГННЕ,УХИ НТ.ЯСБОЕСОАЛЙДАКУРЬ.

Задача 5. $Y =$ НОВЕЬФСГОННЕПОЗСОДО_ДТЕЕРТУВ_РТРШО ААААН_ГЛ.

Задача 8. $X =$ Я ОДЕРЖИМ ПОДОЗРЕНИЕМ О СУЩЕСТВОВАНИИ ИНОГО ПОРЯДКА ВЕЩЕЙ БОЛЕЕ ТАИНСТВЕННОГО И МЕНЕЕ ПОСТИЖИМОГО. ХУЛИО КОРТАСАР.

Задача 9. $Y =$ ВБААГБАЕВБААГББГБЕАААЕЕГЕААВЕБГГЕААВВА АГВББЕ.

Задача 10. $X =$ КУРЬЕР ПРИБЫВАЕТ ПЕРВОГО.

Задача 11. $Y =$ ХЭГНЕВИБЕРНУВЕЬ.

Задача 12. $Y =$ ЁМЗУХЛЮЯХФИУЯТЧЩФЗНСЬЩЦЁШХЁФ.

Задача 13. $Y =$ ЖАЕТЪИРОКЬНЪКДЛОБИМГРККДЬЧЗОКВОБАДНГ ЛЙРЦЗДГЖНЖИДНЙГЖ.

Задача 14. $Y =$ ШЛКМЕГА ОКРЕПЯЕКЛЯ.

Задача 20. $X =$ ЛЕД ТРОНУЛСЯ ГОСПОДА ПРИСЯЖНЫЕ ЗАСЕДАТЕЛИ.

Задача 21. $X =$ БЛЕЗ ДЕ ВИЖЕНЕР.

Задача 22. $X =$ СЧАСТЛИВЫЕ ДРУЗЬЯ ПОЙДЕМ НА МУКИ. ДЕВИЗ КАРБОНАРИЕВ.

Практическое занятие №2
Освоение процессов зашифрования и расшифрования блочными симметричными криптосистемами

Цель занятия – закрепление теоретических знаний и практическое освоение процессов зашифрования и расшифрования сообщений для блочных симметричных криптосистем.

1. Учебные вопросы

1. Зашифрование сообщений блочными симметричными криптосистемами.
2. Расшифрование криптограмм, полученных блочными симметричными криптосистемами.

2. Литература

1. Рябко Б.Я., Фионов А.Н. Криптографические методы защиты информации. Учебное пособие для вузов. М.: Горячая линия – Телеком, 2005.

2. Баричев С.Г., Гончаров В.В., Серов Р.Е. Основы современной криптографии: Учебный курс. – 2-е изд., испр. и доп. – М.: Горячая линия – Телеком, 2002.

3. Задание на практическое занятие

При подготовке к занятию студенты должны изучить учебные материалы темы №2 «Основные классы симметричных криптосистем и их свойства», используя учебник [1], с.156-177, [2], с.14-46, а также конспект лекций.

3.1 Освоение процессов зашифрования сообщений блочными симметричными криптосистемами

Задача 1. Блочная криптосистема представлена структурной схемой (рис. 1). Исходный текст разбивается на блоки по два символа, причем x_i нечетный символ, а x_{i+1} - четный. Все операции сложения вычисляются по модулю $m = |A|$. Требуется зашифровать сообщение: $X =$АВСТРАЛИЯ. Ключ шифра - $K = k_1 = 3; k_2 = 7$.

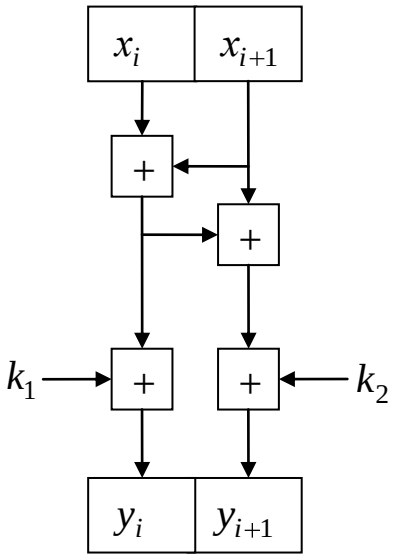

Рисунок 1.

Постройте алгоритм расшифрования.

Задача 2. Блок замены (S-блок) осуществляет замену входного 4-х битового сообщения на выходное 3-х битовое сообщение в соответствии с табл.1.

Таблица 1.

a2a3a4 / A1	**000**	**001**	**010**	**011**	**100**	**101**	**110**	**111**
0	4	6	1	3	5	7	2	5
1	5	7	2	4	6	1	3	6

Для следующих входных сообщений X={1101, 0010, 1010, 0101} найти сообщения на выходе S-блока.

Задача 3. Блок замены (S-блок) осуществляет замену входного 4-х битового сообщения на выходное 2-х битовое сообщение в соответствии с табл.2. Для следующих входных сообщений X={1001, 0011, 1110, 0101} найти сообщения на выходе S-блока.

Таблица 2

a2a3 a1a4	**00**	**01**	**10**	**11**
00	3	3	1	1
01	2	1	3	3
10	3	2	1	3
11	1	3	2	1

Задача 4. Блочная криптосистема имеет в своем составе РЕ-блок, осуществляющий перестановку с расширением в соответствии с табл. 3.

Таблица 3

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

Для следующих входных сообщений X={11111001, 11000011, 00011110, 00000101} найти сообщения на выходе РЕ-блока.

Задача 5. Имеется открытый текст $X =$БЛОЧНЫЙ ШИФР. Получить криптограмму, если матрица шифрования имеет вид:

$$F = \begin{bmatrix} 2 & 3 \\ 7 & 8 \end{bmatrix}.$$

3.2 Освоение процессов расшифрования криптограмм, полученных блочными симметричными криптосистемами

Задача 6. Криптограмма, имеющая вид

$$Y =$$ХЖТЫЦАЗВЙНИТАЮБЦЗВШТДЭШО,

получена линейным шифрующим преобразованием триграмм 33 буквенного русского алфавита с числовыми эквивалентами 1-33. Известно, что последние три триграммы составляют часть открытого сообщения КРЕТНОСТЬ. Найти шифрующую матрицу F и прочитать сообщение.

Задача 7. На выходе блочной симметричной криптосистемы с криптографическим преобразованием

$$y_i = (x_i + k_1) \bmod 33,$$
$$y_{i+1} = (x_{i+1} + k_2) \bmod 33,\ i = 1,3,5,...$$

получена криптограмма $Y =$ГМЁЁДСГЙЪЁФЛГАГУГЛГ. Расшифровать криптограмму при $K = (3,1)$.

Вопросы для самоконтроля:

1. Какие криптосистемы называются блочными?
2. Перечислите блочные криптосистемы, основанные на схеме Фейстеля.
3. Поясните принцип функционирования криптосистемы AES.
4. Какие криптосистемы называются поточными.
5. Поясните принцип функционирования криптосистемы RC4

4. Ответы к задачам

Задача 1. $Y =$ЁМЗЯФЩШЁГЖ, буква «пустышка» - А.

Задача 2. $Y = \{001, 001, 010, 111\}$.

Задача 3. $Y = \{01, 01, 10, 11\}$.

Задача 4. $Y = \{111100111111, 001101010111, 010011100000, 000010010100\}$.

Задача 5. $Y =$ИСЖНРЁАУТНЕБ.

Задача 6.

$$F = \begin{bmatrix} 5 & 4 & 4 \\ 4 & 5 & 6 \\ 3 & 2 & 5 \end{bmatrix},\ X =$$ТЕОРЕТИЧЕСКАЯ СЕКРЕТНОСТЬ.

Задача 7. $X =$АЛГЕБРАИЧЕСКАЯ АТАКА.

Практическое занятие №3
Комбинирование криптосистем

Цель занятия – закрепление теоретических знаний по комбинированию криптосистем и практическое освоение процессов шифрования и расшифрования для комбинированных криптосистем.

1. Учебные вопросы

1. Взвешенная сумма криптосистем.
2. Произведение криптосистем.

2. Литература

1.Осипян В.О, Осипян К.В. Криптография в задачах и упражнениях. – М.: Гелиос АРВ, 2004.

2.Математические и компьютерные основы криптологии: Учеб. пособие/ Ю.С. Харин, В.И. Берник, Г.В. Матвеев, С.В. Агиевич. – Мн.: Новое знание, 2003.

3. Задание на практическое занятие

В процессе подготовки к занятию студенты должны изучить учебные материалы темы №2 «Основные классы шифров и их свойства», используя литературу [1], с.42-44, [2], с.140-145, а также конспект лекций.

3.1 Взвешенная сумма криптосистем

Задача 1. Криптосистема S представляет собой взвешенную сумму шифра Цезаря и шифра перестановки с фиксированным периодом.

Ключ криптосистемы имеет вид $K = (k_1, k_2)$, где $k_1 = 20$, $k_2 = (4,3,2,1)$.

Построить структурную схему криптосистемы S и зашифровать сообщение $X =$АТАКА В ПОЛДЕНЬ. Вероятности выбора криптосистем $p_1 = 0{,}8$ и $p_2 = 0{,}2$, соответственно.

3.2 Произведение криптосистем

Задача 2. Криптосистема является произведением шифра Виженера и шифра вертикальной перестановки. Зашифровать текст:

$X =$НЕВОЗМОЖНО ОБЪЯТЬ НЕОБЪЯТНОЕ

на ключе $K = \{$АМУР;3,5,2,1,4$\}$.

Задача 3. Расшифровать сообщение $Y =$РУЩХЧРЧРУЩВЁЧАК, полученное двукратным применением шифра Цезаря с ключом $K = 3$.

Задача 4. Зашифровать сообщение $X =$ВРАГИ - ЭТО БЫВШИЕ ДРУЗЬЯ используя двукратное применение шифра «магический квадрат».

Магический квадрат:

2	7	6
9	5	1
4	3	8

Задача 5. Зашифровать сообщение $X =$ТИШЕ ЕДЕШЬ ДАЛЬШЕ БУДЕШЬ используя следующее преобразование:

$$V = CZR_{k_1} CZR_{k_2}^{-1} CZR_{k_3},$$

где CZR - шифр Цезаря. Ключ шифра - $K = \{10;5;2\}$.

Построить структурную схему алгоритма шифрования.

Задача 6. Зашифровать сообщение $X =$ПОСПЕШИШЬ ЛЮДЕЙ НАСМЕШИШЬ, используя следующее преобразование

$$V = VIG_{k_1} VIG_{k_2}^{-1} VIG_{k_1},$$

где VIG - шифр Виженера. Ключ шифра - $K =$ {МОСКВА; ЗРИ В КОРЕНЬ}.

Построить структурную схему алгоритма шифрования.

Вопросы для самоконтроля:

1. Какие существую модели криптосистем?
2. Дайте определение взвешенной суммы криптосистем.
3. Дате определение произведения криптосистем.
4. Дайте определение эндоморфной криптосистемы.
5. Какая криптосистема называется идемпотентной?
6. Назовите основные свойства произведения криптосистем.
7. Какие криптосистемы называются эквивалентными.

4. Ответы к задачам

Задача 1.

$Y_1 =$УЁУЮУФГВЯЧШБП, $p_1 = 0{,}8$;

$Y_2 =$АКАТАДЛОПВХХЬНЕ, $p_2 = 0{,}2$.

На рис. 1 представлена схема комбинированной криптосистемы.

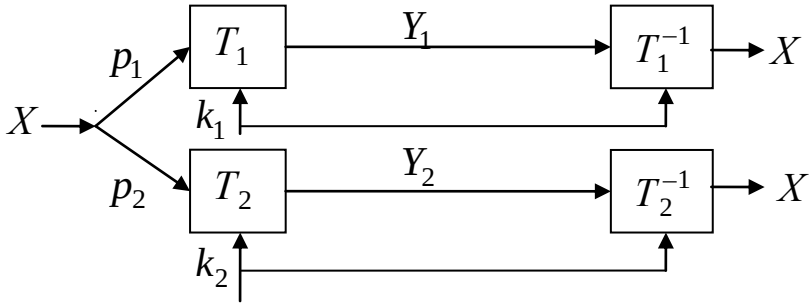

Рисунок 1.

Задача 2.

Y_1 =ОТЦАИЪГШОЬГТЫМЖНОТГТЫМЖЮПТ.

Y =ЦШЫТЖРИЬЖТПВТГТОМНОЪГНЫТАОМГЮА.

Задача 3. X =ВЕК ЖИВИ - ВЕК УЧИСЬ.

Практическое занятие №4
Криптоанализ простейших шифров

Цель занятия – закрепление теоретических знаний и выработка практических умений по применению методов криптоанализа простейших шифров.

1. Учебные вопросы

1. Метод полного перебора (метод «грубой силы».
2. Бесключевые методы криптоанализа простейших шифров.

2. Литература

1. Рябко Б.Я., Фионов А.Н. Криптографические методы защиты информации. Учебное пособие для вузов. М.: Горячая линия – Телеком, 2005.

2. Математические и компьютерные основы криптологии: Учеб. пособие/ Ю.С. Харин, В.И. Берник, Г.В. Матвеев, С.В. Агиевич. – Мн.: Новое знание, 2003.

3. Фомичев В.М. Дискретная математика и криптология. Курс лекций/ Под ред. Н.Д. Подуфалова. – М.: ДИАЛОГ-МИФИ, 2003.

3. Задание на практическое занятие

В процессе подготовки к занятию студенты должны изучить учебные материалы темы №3 «Методы криптоанализа симметричных криптосистем», используя учебник [1], с.5-11, [2], с.245-272, [3], с.283-287, а также конспект лекций.

3.1 Метод полного перебора (метод «грубой силы»)

Задача 1. Имеется криптограмма:

Y =СХТХУЦЖ,

полученная шифром Цезаря. Требуется методом полного перебора (brute-force attack) определить ключ шифра и прочесть сообщение.

Задача 2. Определить ключ шифра Цезаря, если известна пара «открытый текст-криптограмма»:

X =КРИПТОЛОГИЯ – Y =ПХНФЧУРУЗНД.

Задача 3. Определить ключ шифра Цезаря, если даны пары «открытый текст-криптограмма»:

1) X =АПЕЛЬСИН – Y =САЦЬНВЩЮ;

2) X =АБРИКОС – Y =ЫЬЛГЕЙМ.

Задача 4. Дешифровать сообщения, зашифрованные шифром Цезаря:

Y =ГРХГРГРГУЛЕЦ.

3.2 Бесключевые методы криптоанализа простейших шифров

Задача 5. Методом чтения в колонках дешифровать криптограмму:

Y =СШЫУЙА,

если известно, что при шифровании использована не равновероятная гамма, у которой все символы, кроме А, Б, И имеют нулевую вероятность.

Априорно известно, что криптограмма представляет собой зашифрованное название одной из стран мира.

Задача 6. Даны две криптограммы:

Y =ВЖТЕЛД;

Y' =ВЕЖСИЛБ.

Известно, что при зашифровании текстов использовалась одна и та же γ-последовательность, причем вторая криптограмма Y' есть результат зашифрования текста, полученного за счет видоизменения первого текста, а именно, за счет вставки после первой буквы произвольной буквы Г.

Требуется определить γ-последовательность и прочитать текст.

Задача 7. Методом чтения в колонках дешифровать криптограмму:

Y =ГЪЩРТДМББ,

полученную применением не равновероятной γ-последовательности, у которой все символы, кроме А, К, О, Ф имеют нулевую вероятность.

Задача 8. Даны две криптограммы:

Y =ЛЭМЭВЮУБЛНЯХ;

Y' =ЛЭМВЯВЯУЬБЯВБ.

Известно, что при зашифровании текстов использовалась одна и та же γ-последовательность, причем вторая криптограмма Y' есть результат зашифрования видоизмененного первого текста, полученного за счет вставки после третьей буквы произвольной буквы Ф.

Требуется определить γ-последовательность и прочитать текст.

Вопросы для самоконтроля:

1. Что такое криптоатака?
2. Назовите основные принципы криптографии.
3. В чем заключается метод полного перебора?
4. Поясните метод чтения в колонках.
5. Поясните метод восстановления текстов, основанный на атаке с помощью вставки символа.

6. Оцените вычислительную сложность метода прямого перебора для шифров: простой замены, простой перестановки, шифра Виженера, шифра Вернама, криптосистемы DES.

4. Ответы к задачам

Задача 1. $X =$КОЛОМНА, $K = 7$.
Задача 2. $K = 5$.
Задача 4. $X =$АНТАНАНАРИВУ, $K = 3$.
Задача 5. $X =$РОССИЯ, $\gamma =$АИИБАА.
Задача 6. $X =$БЕРЕЗА, $\gamma =$АББАГГ.
Задача 7. $X =$ВЕНЕСУЭЛА, $K =$АФККАООФА.
Задача 8. $X =$КРИПТОГРАММА, $K =$АЛГМООППКАСФ.

Практическое занятие №5
Расстояние единственности шифра

Цель занятия – закрепление теоретических знаний по вопросам стойкости криптосистем и выработка практических умений по оценке расстояния единственности шифра.

1. Учебные вопросы

1. Оценка апостериорной вероятности ключа.
2. Расчет расстояния единственности шифра.

2. Литература

1. Рябко Б.Я., Фионов А.Н. Криптографические методы защиты информации. Учебное пособие для вузов. М.: Горячая линия – Телеком, 2005.
2. Математические и компьютерные основы криптологии: Учеб. пособие/ Ю.С. Харин, В.И. Берник, Г.В. Матвеев, С.В. Агиевич. – Мн.: Новое знание, 2003.

3. Задание на практическое занятие

В процессе подготовки к занятию студенты должны изучить учебные материалы темы №4 «Теория стойкости криптосистем», используя литературу [1], с.132-148, [2], с.145-150, а также конспект лекций.

3.1 Оценка апостериорной вероятности ключа

Задача 1. Источник открытых сообщений без памяти характеризуется следующими параметрами: алфавит $A = \{a, b, c\}$ вероятности символов алфавита - $P(a) = 0{,}8,\ P(b) = 0{,}15,\ P(c) = 0{,}05$.

Используется шифр простой перестановки, причем все ключи равновероятные и имеют вид:

$k = 1$: (a, b, c);
$k = 2$: (a, c, b);
$k = 3$: (b, a, c);

$k=4$: (c,c,a);

$k=5$: (c,a,b);

$k=6$: (c,b,a).

Перехвачена криптограмма: $Y=cccbc$. Требуется определить ключ.

Задача 2. Пусть источник без памяти порождает буквы из алфавита A= (a,b,c) с вероятностями $P(a)$, $P(b)$ и $P(c)$. Шифратор реализует замену букв, используя одну из шести возможных перестановок (см. задачу 1). Определить апостериорные вероятности использованных ключей для заданной криптограммы:

1) $P(a)=0{,}1, P(b)=0{,}7,\ P(c)=0{,}2;\ Y=abaacac$;

2) $P(a)=0{,}9, P(b)=0{,}09,\ P(c)=0{,}01;\ Y=cbaccca$;

3) $P(a)=0{,}1, P(b)=0{,}7,\ P(c)=0{,}2;\ Y=abbbbab$;

4) $P(a)=0{,}14, P(b)=0{,}06,\ P(c)=0{,}8;\ Y=bbabbcab$.

Задача 3.

По имеющейся криптограмме найти апостериорные вероятности использованных ключей и соответствующие им сообщения, если известно, что используется шифр замены (см. задачу 1), а сообщения порождаются марковским источником с матрицей вероятностей переходов

$$\Pi = \begin{array}{c|ccc} & a & b & c \\ a & 0 & 0{,}9 & 0{,}1 \\ b & 0 & 0{,}1 & 0{,}9 \\ c & 0{,}4 & 0{,}3 & 0{,}3 \end{array}$$

и начальными вероятностями $P(a)=0{,}19, P(b)=0{,}34,\ P(c)=0{,}47$:

1) $Y=bcacbcacc$;

2) $Y=caaabaaba$;

3) $Y=aaacaaaca$.

3.2 Расчет расстояния единственности шифра

Задача 4. Оценить расстояние единственности криптосистемы. Криптосистема представляет собой шифр простой перестановки. В качестве исходных данных использовать данные из задачи 1.

Задача 5. Используя исходные данные из условия задачи 2 вычислить расстояние единственности криптосистемы.

Вопросы для самоконтроля:

1. Дайте определение совершенно стойкой криптосистемы.
2. Сформулируете и докажите теорему Шеннона.
3. Докажите утверждение о совершенной стойкости шифра Вернама.
4. Дате определения понятиям идеальной и практической стойкой криптосистемы.
5. Что такое расстояние избыточности шифра?
6. Дайте определение избыточности шифруемого сообщения.
7. Поясните методику расчета расстояния единственности шифра.

4. Ответы к задачам

Задача 1. $P(k_5 \mid Y) \approx 0{,}25$, $P(k_6 \mid Y) \approx 0{,}75$.

Задача 2.

1) $P_1 \approx 0{,}002$, $P_2 \approx 0{,}006$, $P_3 \approx 0{,}623$, $P_4 \approx 0{,}051$, $P_5 \approx 0{,}002$, $P_6 \approx 0{,}311$;

2) $P_1 \approx 0{,}000$, $P_2 \approx 0{,}009$, $P_3 \approx 0{,}000$, $P_4 \approx 0{,}000$, $P_5 \approx 0{,}892$, $P_6 \approx 0{,}099$;

3) $P_1 \approx 0{,}196$, $P_2 \approx 0{,}000$, $P_3 \approx 0{,}001$, $P_4 \approx 0{,}000$, $P_5 \approx 0{,}018$, $P_6 \approx 0{,}785$;

4) $P_1 \approx 0{,}000$, $P_2 \approx 0{,}697$, $P_3 \approx 0{,}000$, $P_4 \approx 0{,}004$, $P_5 \approx 0{,}299$, $P_6 \approx 0{,}000$.

Задача 3.

1) $P_1 \approx 0{,}7$ ($X = bcacbcacc$), $P_2 = 0$, $P_3 \approx 0{,}3$ ($X = acbcacbcc$), $P_4 = 0$, $P_5 = 0$, $P_6 = 0$;

2) $P_1 = 0$, $P_2 = 0$, $P_3 = 0$, $P_4 \approx 0{,}21$ ($X = bcccaccac$), $P_5 \approx 0{,}2$ ($X = abbbcbbcb$), $P_6 \approx 0{,}59$ ($X = acccbccbc$);

3) $P_1 = 0$, $P_2 = 0$, $P_3 \approx 0{,}009$ ($X = bbbcbbbcb$), $P_4 \approx 0{,}970$ ($X = cccbcccbc$), $P_5 = 0$, $P_6 \approx 0{,}021$ ($X = cccacccac$).

Задача 4. $n \geq \dfrac{2{,}58}{\log 3 - 0{,}88} \approx 3{,}7$.

Задача 5.

1) $n \approx 6{,}04$; 2) $n \approx 2{,}42$; 3) $n \approx 6{,}04$; 4) $n \approx 3{,}76$.

Практическое занятие №6
Теоретические основы криптосистем с открытым ключом

Цель занятия – закрепление знаний по теоретическим основам криптосистем с открытым ключом.

1. Учебные вопросы

1. Основные понятия теории чисел. Функция Эйлера.
2. Теорема Ферма.
3. Теорема Эйлера.

2. Литература

1. Рябко Б.Я., Фионов А.Н. Криптографические методы защиты информации. Учебное пособие для вузов. М.: Горячая линия – Телеком, 2005.

2. Баричев С.Г., Гончаров В.В., Серов Р.Е. Основы современной криптографии: Учебный курс. – 2-е изд., испр. и доп. – М.: Горячая линия – Телеком, 2002.

3. Задание на практическое занятие

В процессе подготовки к практическому занятию студенты должны изучить учебные материалы темы №5 «Криптосистемы с открытым ключом», используя учебник [1], с.12-28, [2], с.61-66, а также конспект лекций.

3.1 Основные понятия теории чисел. Функция Эйлера

Задача 1. Разложить числа 108, 77, 65, 30, 159 на простые множители.

Задача 2. Определить, какие из пар чисел (25,12), (25,15), (13,39), (40,27) взаимно просты.

Задача 3. Найти значение функции Эйлера: а) $\varphi(10)$; б) $\varphi(14)$, в) $\varphi(20)$.

3.2 Теорема Ферма

Задача 4. Используя теорему Ферма вычислить: а) $2^{12} \bmod 13$; б) $3^{13} \bmod 13$, в) $5^{22} \bmod 11$, г) $3^{17} \bmod 5$.

3.3 Теорема Эйлера

Задача 5. Используя теорему Эйлера вычислить: а) $5^4 \bmod 12$, б) $3^9 \bmod 20$, в) $2^{14} \bmod 21$, г) $2^{107} \bmod 159$.

Задача 6. С помощью обобщенного алгоритма Евклида найти значения x и y в уравнениях:

а) $21x + 12y = НОД(21,12)$;

б) $30x + 12y = НОД(30,12)$.

Вопросы для самоконтроля:

1. Дате определения простого числа..
2. Какие числа называются взаимно простыми?.
3. Сформулируйте основную теорему арифметики.
4. Дайте определение функции Эйлера.
5. Сформулируйте и докажите теорему Ферма.
6. Сформулируйте и докажите теорему Эйлера.
7. Поясните суть алгоритм Евклида.
8. Поясните суть обобщенного алгоритма Евклида.
9. Что называется инверсией числа по некоторому модулю?

4. Ответы к задачам

Задача 1. 108=2·2·3·3·3, 77=7·11, 65=5·13, 30=3·3·5, 159=3·53.

Задача 2. Взаимно просты пары (25,12), (40,27).

Задача 3.

а) $\varphi(10)$=4; 1,~~2~~,3,~~4,5,6~~,7,~~8~~,9;

б) $\varphi(14) = 6$;

в) $\varphi(20) = 8$.

Задача 4.

а) $2^{12} \bmod 13 = (2^2)^2 \cdot (2^2)^2 \bmod 13 = 3 \cdot 9 \bmod 13 = 1$;

б) $3^9 \bmod 13 = 3 \cdot 3^{12} \bmod 13 = 3$;

в) $5^{22} \bmod 11 = 25$;

г) $3^{17} \bmod 5 = 3$.

Задача 5.

а) $5^4 \bmod 12 = |\varphi(12) = 4| = (5^2)^2 \bmod 12 = 1$;

б) $3^9 \bmod 20 = 3 \cdot 3^8 \bmod 20 = 3$;

в) $2^{14} \bmod 21 = 4$;

г) $2^{107} \bmod 159 = 8$.

Задача 6.

а) $x = -1, y = 2$;

б) $x = 1, y = -2$.

Практическое занятие №7
Криптосистемы с открытым ключом

Цель занятия – закрепление теоретических знаний и практическое освоение процессов шифрования и расшифрования сообщений криптосистемами с открытым ключом.

1. Учебные вопросы

1. Криптосистема Эль-Гамаля.
2. Криптосистема RSA.

2. Литература

1. Рябко Б.Я., Фионов А.Н. Криптографические методы защиты информации. Учебное пособие для вузов. М.: Горячая линия – Телеком, 2005.

2. Баричев С.Г., Гончаров В.В., Серов Р.Е. Основы современной криптографии: Учебный курс. – 2-е изд., испр. и доп. – М.: Горячая линия – Телеком, 2002.

3. Задание на практическое занятие

В процессе подготовки к практическому занятию студенты должны изучить учебные материалы темы №5 «Криптосистемы с открытым ключом», используя учебник [1], с.12-38, [2], с.69-87, а также конспект лекций.

3.1 Криптосистема Эль-Гамаля

Задач 1. Передаваемое сообщение $x = 15$. Параметры криптосистемы Эль-Гамаля: $p = 23$, $g = 5$, $c_B = 13$. Сформировать криптограмму и восстановить открытый текст.

Задача 2. Для криптосистемы Эль-Гамаля с заданными параметрами p, g, c_B и k найти недостающие параметры и описать процесс передачи сообщения x:

а) $p = 19$, $g = 2$, $c_B = 5$, $k = 7$, $x = 5$;

б) $p = 23$, $g = 5$, $c_B = 8$, $k = 10$, $x = 10$;

в) $p = 17$, $g = 3$, $c_B = 10$, $k = 5$, $x = 10$.

3.2 Криптосистема RSA

Задача 3. Сформировать криптограмму и восстановить открытое сообщение, если криптосистема RSA имеет следующие параметры: $p_B = 3$,

$q_B = 11$, $n_B = 33$ и открытый ключ - $d_B = 3$. Исходное сообщение необходимо взять из условия задачи 1.

Задача 4.

В криптосистеме RSA с заданными параметрами p_B, q_B, d_B найти недостающие параметры и описать процесс передачи сообщения x:

а) p_B=5, q_B=11, d_B=3, $x = 12$;

б) p_B=7, q_B=13, d_B=5, $x = 30$;

в) p_B=3, q_B=11, d_B=3, $x = 15$.

Вопросы для самоконтроля:

1. Дайте определение односторонней функции.
2. Дайте определение односторонней функции с «лазейкой».
3. Поясните алгоритм криптосистемы Шамира.
4. Поясните алгоритм криптосистемы Эль-Гамаля.
5. Назовите основные отличия алгоритмов Шамира и Эль-Гамаля.
6. Поясните алгоритм криптосистемы RSA.
7. В чем заключаются особенности алгоритмов криптосистем RSA и Эль-Гамаля, основанных на эллиптических кривых.

4. Ответы к задачам

Задача 1. $y = \langle 17,12 \rangle$, $x = e \cdot r^{p-1-c_B} \bmod p = 12 \cdot 17^{23-1-13} \bmod 23 = 15$.

Задача 2. а) $d_B = 13$, r=14, y=12; б) $d_B = 16$, r=9, y=15; в) $d_B = 8$, r=5, y=5.

Задача 3. $y = 9$, $x = y^{c_B} \bmod n_B = 9^7 \bmod 33 = 15$.

Задача 4. а) $n_B = 55$, $\varphi(n_B) = 40$, $c_B = 27$, y=23; б) $n_B = 91$, $\varphi(n_B) = 72$, $c_B = 29$, y=88; в) $n_B = 33$, $\varphi(n_B) = 20$, $c_B = 7$, y=9.

Практическое занятие №8
Методы криптоанализа криптосистем с открытым ключом

Цель занятия – закрепление теоретических знаний и выработка практических умений по применению методов криптоанализа криптосистем с открытым ключом.

1. Учебные вопросы

1. Метод «шаг младенца, шаг великана».
2. Алгоритм исчисления порядка.

2. Литература

1. Рябко Б.Я., Фионов А.Н. Криптографические методы защиты информации. Учебное пособие для вузов. М.: Горячая линия – Телеком, 2005.

3. Организационно-методические указания по подготовке к занятию

При подготовке к занятию студенты должны изучить учебные материалы темы №5 «Криптосистемы с открытым ключом», используя учебник [1], с.41-50, а также учебные материалы к практическому занятию №8.

3.1 Метод «шаг младенца, шаг великана»

Задача 1. Найти решение уравнений:

а) $2^x \bmod 23 = 9$;

б) $2^x \bmod 29 = 21$;

в) $3^x \bmod 31 = 25$;

г) $6^x \bmod 41 = 21$,

используя метод «шаг младенца, шаг великана».

3.2 Алгоритм исчисления порядка

Задача 8.2.

Найти решение уравнений:

а) $10^x \bmod 47 = 37$;

б) $2^x \bmod 53 = 24$;

в) $7^x \bmod 71 = 41$;

г) $2^x \bmod 61 = 45$,

используя алгоритм исчисления порядка.

Вопросы для самоконтроля:

1. Сформулируйте возможные атаки на криптосистему Эль-Гамаля.
2. Поясните метод криптоанализа «шаг младенца, шаг великана».
3. Поясните алгоритм исчисления порядка.
4. Оцените вычислительную сложность метода «шаг младенца, шаг великана» и алгоритма исчисления порядка.
5. Сформулируйте возможные атаки на криптосистему RSA.
6. Поясните метод факторизации Ферма.

4. Ответы к задачам

Задача 1. а) $x = 5$, б) $x = 17$; в) $x = 10$; г) $x = 14$.

Задача 2. а) $x = 24$, б) $x = 20$; в) $x = 25$; г) $x = 34$.

Практическое занятие №9
Электронная цифровая подпись

Цель занятия – закрепление теоретических знаний и практическое освоение алгоритмов формирования электронной цифровой подписи.

1. Учебные вопросы

1. Электронная цифровая подпись на основе криптосистемы RSA.
2. Электронная цифровая подпись на базе криптосистемы Эль-Гамаля.

2. Литература

1. Рябко Б.Я., Фионов А.Н. Криптографические методы защиты информации. Учебное пособие для вузов. М.: Горячая линия – Телеком, 2005.

2. Баричев С.Г., Гончаров В.В., Серов Р.Е. Основы современной криптографии: Учебный курс. – 2-е изд., испр. и доп. – М.: Горячая линия – Телеком, 2002.

3. Задание на практическое занятие

В процессе подготовки к занятию студенты должны изучить учебные материалы темы №6 «Электронная цифровая подпись», используя учебник [1], с.52-62, [2], с.87-113, а также конспект лекций.

3.1 Электронная цифровая подпись на основе криптосистемы RSA

Задача 1. Построить электронную подпись RSA для заданного сообщения x и известного значения его хэш-функции при следующих параметрах пользователя:

а) $p=5,\ q=11,\ c=27,\ h_X=13$;

б) $p=5,\ q=11,\ c=27,\ h_X=7$;

в) $p=5,\ q=13,\ c=29,\ h_X=10$;

г) $p=7,\ q=13,\ c=29,\ h_X=15$.

При формировании подписи считать, что $x=h_X$.

Задача 2. Для указанных параметров пользователей RSA проверить подлинность подписанных сообщений:

а) $n=55,\ d=3;\ \langle 7,28\rangle,\ \langle 22,15\rangle,\ \langle 16,36\rangle$;

б) $n=65,\ d=5;\ \langle 6,42\rangle,\ \langle 10,30\rangle,\ \langle 6,41\rangle$;

в) $n=91,\ d=5\ \langle 15,71\rangle,\ \langle 11,46\rangle,\ \langle 16,74\rangle$.

3.2 Электронная цифровая подпись на базе криптосистемы Эль-Гамаля

Задача 3. Для сети, абоненты которой применяют подпись Эль-Гамаля с общими параметрами $p=23,\ g=5$, построить подпись:

а) $c=7,\ k=5,\ h_X=3$;

б) $c=11,\ k=3,\ h_X=15$;

в) $c=10,\ k=15,\ h_X=5$;

с) $c=3,\ k=13,\ h_X=8$.

При формировании подписи считать, что $x=h_X$.

Задача 4. Для указанных открытых ключей d пользователей системы Эль-Гамаля с общими параметрами $p=23,\ g=5$ проверить подлинность подписанных сообщений:

а) $d=22$: $\langle 15,20,3\rangle,\ \langle 15,10,5\rangle,\ \langle 15,19,3\rangle$;

б) $d=9$: $\langle 5,19,17\rangle,\ \langle 7,17,8\rangle,\ \langle 6,17,8\rangle$;

в) $d=11$: $\langle 15,7,1\rangle,\ \langle 10,15,3\rangle,\ \langle 15,7,16\rangle$.

Вопросы для самоконтроля:

1. Дайте определение электронной цифровой подписи.
2. Сформулируете основные требования к электронной цифровой подписи.
3. Поясните методику формирования подписи, основанную на криптосистеме RSA.
4. Поясните методику формирования подписи, основанную на криптосистеме Эль-Гамаля.
5. Дайте сравнительную характеристику электронным цифровым подписям, полученным с помощью криптосистем RSA и Эль-Гамаля.
6. Какие стандарты на электронную цифровую подпись существуют в настоящее время?
7. Сформулируйте основные подходы к уменьшению размера подписи.
8. Дайте определение хэш-функции.
9. Сформулируйте основные требования к хэш-функции.
10. Какие стандарты на хэш-функцию существуют в настоящее время?

4. Ответы к задачам

Задача 1. а) $\langle 13,7 \rangle$, б) $\langle 28,7 \rangle$; в) $\langle 30,10 \rangle$; г) $\langle 71,15 \rangle$.

Задача 2. а) подлинны - $\langle 7,28 \rangle$, $\langle 16,36 \rangle$; б) подлинна - $\langle 10,30 \rangle$; в) подлинны - $\langle 15,71 \rangle$, $\langle 16,74 \rangle$.

Задача 3. а) $\langle 3,20,21 \rangle$, б) $\langle 15,10,5 \rangle$; в) $\langle 5,19,17 \rangle$; г) $\langle 8,21,11 \rangle$.

Задача 4. а) подлинны - $\langle 15,20,3 \rangle$, $\langle 15,10,5 \rangle$; б) подлинны - $\langle 5,19,17 \rangle$, $\langle 6,17,8 \rangle$; в) подлинны - $\langle 10,15,3 \rangle$, $\langle 15,7,16 \rangle$.

Практическое занятие №10
Криптографические генераторы

Цель занятия – закрепление теоретических знаний и выработка практических умений по применению алгоритмов генерации псевдослучайных последовательностей.

1. Учебные вопросы

1. Конгруэнтные криптографические генераторы.
2. LFSR – генераторы.
3. Криптографические генераторы Фибоначчи.
4. Комбинированные криптографические генераторы.

2. Литература

1. Рябко Б.Я., Фионов А.Н. Криптографические методы защиты информации. Учебное пособие для вузов. М.: Горячая линия – Телеком, 2005.

2. Математические и компьютерные основы криптологии: Учеб. пособие / Ю.С. Харин, В.И. Берник, Г.В. Матвеев, С.В. Агиевич. – Мн.: Новое знание, 2003.

3. Фомичев В.М. Дискретная математика и криптология. Курс лекций / Под ред. Н.Д. Подуфалова. – М.: ДИАЛОГ-МИФИ, 2003.

3. Задание на практическое занятие

В процессе подготовки к практическому занятию студенты должны изучить учебные материалы темы №8 «Криптографические генераторы», используя литературу [1], с.192-195, [2], с.193-210, [2], с.318-339, а также конспект лекций.

3.1 Конгруэнтные криптографические генераторы

Задача 1. Линейный конгруэнтный генератор с параметрами $a=5,\ c=10,$ $n=23$ порождает псевдослучайную последовательность $x_i,\ i=\overline{1,N}$. Найти значение первых пяти членов последовательности при начальном значении $x_0=3.$

Задача 2. Для условий задачи 1 определить значение двадцатого члена псевдослучайной последовательности.

Задача.3. Дан квадратичный конгруэнтный генератор с параметрами $a=3,$ $c=11,\ d=6,\ n=16$ и начальным состоянием $x_0=10.$ Определить значения первых шести членов псевдослучайной последовательности и найти значение наибольшего периода этой последовательности $T_{\max}$.

Задача 4. Выполнить программную реализацию генератора Эйхенауэра-Лена с параметрами $a=3,\ c=9,\ n=20$ и начальным состоянием $x_0=5.$ Определить период псевдослучайной последовательности.

Задача 5. Выполнить программную реализацию конгруэнтного генератора с переносом с параметрами $a=7,\ n=19$ и начальным состоянием $x_0=1,$ $c_0=5,.$ Сформировать первых пятнадцать значений псевдослучайной последовательности и определить период псевдослучайной последовательности.

3.2 LFSR - генераторы

Задача 6. Генератор LFSR состоит из $N=5$ ячеек памяти. Начальные состояния ячеек памяти определяются вектором $S_0=(1011)$, а вектор коэффициентов передачи имеет вид $a=(1100)$.

Построить структурную схему генератора LFSR и определить первых десять членов псевдослучайной последовательности.

3.3 Криптографические генераторы Фибоначчи

Задача 7. выполнить программную реализацию генератора Фибоначчи, при $\Diamond\in$ [illegible] и $k=3$. Параметры генератора: $r=3,\ s=2,$ начальные значения $x_0=(7)$.

Определить значение периода каждой псевдослучайной последовательности.

3.4 Комбинированные криптографические генераторы

Задача 8. Выполнить программную реализацию комбинированного LFSR генератора, включающего в себя $i = 3$ однотипных генератора. Параметры i-го LFSR генератора взять из условий задачи 6 за исключением вектора начального состояния, который требуется задать самостоятельно.

Выходная функцию комбинированного LFSR генератора имеет вид:

$$F(x) = (x_1 + x_2 + x_3 + x_1 \oplus x_2 + x_1 \oplus x_3) \bmod 2.$$

Вопросы для самоконтроля:

1. Что такое криптографический генератор?
2. Дайте классификацию криптографических генераторов.
3. Сформулируйте основные свойства линейных конгруэнтных генераторов.
4. Поясните алгоритм генерации псевдослучайной последовательности нелинейными конгруэнтными генераторами.
5. Дайте определение криптографических генераторов Фибоначчи.
6. Дайте определение элементарной псевдослучайной последовательности.
7. Сформулируйте основные подходы к «улучшению» элементарных псевдослучайных последовательностей.
8. Сформулируйте основные методы комбинирования криптографических генераторов.
9. Поясните суть метода Маклорена-Марсальи для комбинирования криптографических генераторов.

4. Ответы к задачам

Задача 1. $x = (2,20,18,8,4)$.

Задача 2. $x_{20} = 6$.

Задача 6.

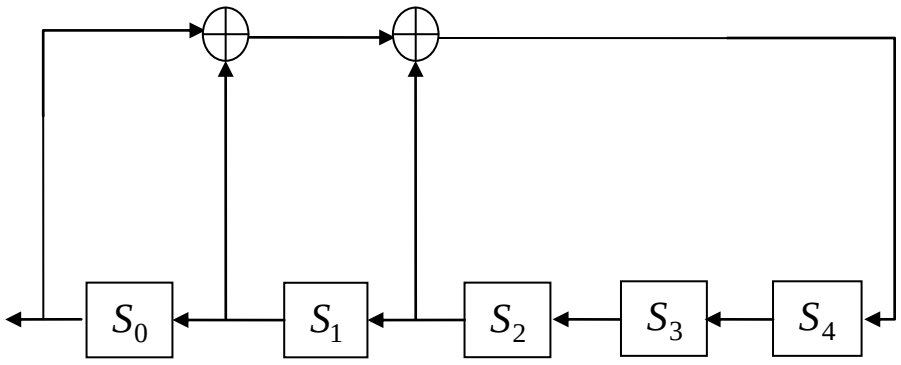

Рисунок 1.

Русский алфавит

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н
16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь
31	32	33												
Э	Ю	Я												

Основные формулы и расчетные соотношения

Криптосистема Цезаря:

$$y_i = (x_i + K) \bmod M,$$

где y_i и x_i - i-е буквы криптограммы и открытого сообщения, соответственно; K - ключ; M - мощность алфавита.

Аффинная криптосистема Цезаря:

$$y_i = (K_1 x_i + K_2) \bmod M,$$

где K_1 и K_2 - некоторые натуральные числа, являющиеся ключам шифра.

Криптосистема Виженера:

$$y_i = (x_i + k_i^d) \bmod M,$$

где k^d - ключевая последовательность.

Криптосистема гаммирования

$$y_i = (x_i + \gamma_i) \bmod M.$$

где γ - ключевая гамма-последовательность.

Взвешенная сумма криптосистем - это такая криптосистема, которая образована «взвешенным» суммирование нескольких криптосистем:

$$S = p_1 T_1 + p_2 T_2 + ... + p_m T_m = \sum_{m=1}^{M} p_m T_m, \ \sum_{m=1}^{M} p_m = 1,$$

где T_m - криптографическое преобразование m-й криптосистемы; p_m - вероятность выбора m-й криптосистемы.

Произведение криптосистем - это такая криптосистема V, для которой выполняется равенство:

$$V = T_1 T_2 ... T_m = \prod_{m=1}^{M} T_m.$$

Расстояние единственности – такая минимальная длина криптограммы n, при которой исчезает неопределенность в исходном тексте и ключ восстанавливается с высокой вероятностью.

$$n \geq \frac{H(K)}{R},$$

где $H(K)$ - энтропия ключа; R - избыточность шифруемого сообщения.

Формула Байеса для расчета значений апостериорных вероятностей ключей:

$$P(k_i \mid Y) = \frac{P(k_i) P(Y \mid k_i)}{\sum_{j=1}^{I} P(k_j) P(Y \mid k_j)}, \ i = \overline{1, I}.$$

Линейный конгруэнтный генератор:

$$x_{i+1} = (a x_i + c) \bmod N, \ i = \overline{0, \infty},$$

где $x_0 \in A$ - стартовое (начальное) значение; $a \in A \setminus \{0\}$ - ненулевой множитель; $c \in A$ - приращение; N - модуль, равный мощности алфавита A.

Если приращение $c = 0$, то генератор называется *мультипликативным конгруэнтным генератором*.

Выражение для общего члена последовательности $\{x_i\} \subset A$:

$$x_i = \left(a^i x_0 + \frac{a^i - 1}{a - 1} c \right) \bmod N,\ i \geq 1.$$

Квадратичный конгруэнтный генератор определяется квадратичным рекуррентным соотношением:

$$x_{i+1} = (dx_i^2 + ax_i + c) \bmod N,\ i = \overline{0, \infty},$$

где $a, c, d, x_0 \in A$ - параметры генератора.

Конгруэнтный генератор, использующий умножение с переносом определяется рекуррентным соотношением:

$$x_i = (ax_i + c_i) \bmod N,\ i = \overline{0, \infty},$$

где $c_i = \left\lfloor \frac{ax_{i-1} + c_{i-1}}{N} \right\rfloor$.

Генератор Фибоначчи:

$$x_t = x_{t-r} \lozenge x_{t-s},\ t = r, r+1, r+2, \ldots$$

где $r, s\ (r > s)$ - параметры генератора; $\lozenge$ - символ бинарного отношения: $\lozenge \in \{+, -, \times, \oplus\}$.