МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ
ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ ГРАЖДАНСКОЙ АВИАЦИИ

А.А. Антонов

ИСТОРИЯ КРИПТОГРАФИИ

Учебно-методическое пособие
по проведению практических занятий

для студентов III курса
специальности 10.05.02
очной формы обучения

Москва · 2022

ФЕДЕРАЛЬНОЕ АГЕНТСТВО ВОЗДУШНОГО ТРАНСПОРТА
(РОСАВИАЦИЯ)

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ
УНИВЕРСИТЕТ ГРАЖДАНСКОЙ АВИАЦИИ» (МГТУ ГА)

Кафедра основ радиотехники и защиты информации

А.А. Антонов

ИСТОРИЯ КРИПТОГРАФИИ

Учебно-методическое пособие
по проведению практических занятий

для студентов III курса
специальности 10.05.02
очной формы обучения

Москва
ИД Академии Жуковского
2022

УДК 519.7+003.26.09
ББК 6Ф7.3
А72

Рецензент:
Петров В.И. – канд. техн. наук, доцент

Антонов А.А.
А72 История криптографии [Текст] : учебно-методическое пособие по проведению практических занятий / А.А. Антонов. – М.: ИД Академии Жуковского, 2022. – 24 с.

Данное учебно-методическое пособие соответствует рабочей программе учебной дисциплины «История криптографии» по специальности 10.05.02 для студентов III курса очной формы обучения.

В учебно-методическом пособии рассматриваются свойства простейших шифров, основные понятия и определения криптографии, освоение процессов шифрования и расшифрования простейших шифров, блочных криптосистем, комбинирование криптосистем.

Рассмотрено и одобрено на заседаниях кафедры 19.04.2022 г. и методического совета 21.04.2022 г.

УДК 519.7+003.26.09
ББК 6Ф7.3

В авторской редакции

Подписано в печать 12.07.2022 г.
Формат 60x84/16 Печ. л. 1,5 Усл. печ. л. 1,395
Заказ № 902/0603-УМП13 Тираж 30 экз.

Московский государственный технический университет ГА
125993, Москва, Кронштадтский бульвар, д. 20

Издательский дом Академии имени Н. Е. Жуковского
125167, Москва, 8-го Марта 4-я ул., д. 6А
Тел.: (495) 973-45-68
E-mail: zakaz@itsbook.ru

ОБЩИЕ МЕТОДИЧЕСКИЕ УКАЗАНИЯ

При подготовке к практическому занятию студенты должны:

уяснить цель и порядок проведения занятия;

изучить материалы, изложенные на лекциях и в рекомендуемой литературе.

На занятии студент должен иметь конспект лекций и данное пособие.

Практическое занятие начинается с опроса студентов по знанию теоретических положений изучаемого практического занятия, проверяются знания по представленным контрольным вопросам.

Далее студенты решают приведенные в пособии задания с последующим обсуждением полученных результатов. В случае дистанционного обучения оформляется отчет.

РЕКОМЕНДУЕМАЯ ЛИТЕРАТУРА

а) основной литературой по дисциплине является:

1. История криптографии автор Болелов Э.А. М.: МГТУ ГА, Учебное пособие, 2016.

Работу с литературой целесообразно начать с изучения данного учебного пособия. Следующим этапом работы с литературными источниками является создание конспектов, фиксирующих основные тезисы и аргументы.

б) дополнительная литература включает в себя:

1. Криптография: страницы истории тайных операций Гольев Ю.И., Ларин Д.А., Тришин А.Е., Шанкин Г.П. . – М.: Гелиос АРВ, 2008.

2. Книга шифров: тайная история шифров и их расшифровки Саймон Сингк. . – М.: АСТ: Астрель, 2007.

3. Криптография Бабаш А.В., Шанкин Г.П. – Москва: СОЛОН-Р, 2002,

4. Пять столетий тайной войны Черняк Е. – М., 1991.

5. Секретная дипломатия Великобритании Черняк Е. – М., 1975.

6. История криптографии ч.1. Бабаш А.В., Шанкин Г.П.– М.: Гелиос АРВ, 2012.

7. Криптография от папируса до компьютера Жельников В. – М.: Отдел Исследования Программ, 1996.

8. История шифровального дела в России Соболева Т. А. – М.: «ОЛМА-ПРЕСС», 2012.

9. Коды и шифры, Юлий Цезарь, «Энигма» и Интернет Черчхауз Р. / Пер. с англ. – М.: Издательство «Весь Мир», 2005.

10. Взломщики кодов Дэвид Кан. – М.: Центрполиграф, 2000.

Практическое занятие № 1

Шифры Древней Греции и Древнего Рима

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

2. Теоретические сведения

Шифр простой перестановки заключается в следующем. В соответствии с заданным правилом осуществляется перестановка букв открытого текста. Правило перестановки является ключом шифра. Как правило, длина ключа соответствует длине открытого сообщения.

Шифр вертикальной перестановки. Шифрование заключается в записи по строкам открытого текста в таблицу, а считывание криптограммы осуществляется по столбцам.

Шифры маршрутной перестановки используют прямоугольную таблицу, в которую текст записывается, например, по строкам, а криптограмма считывается по определенному маршруту (по столбцам, по диагонали и т.п.). Расшифрование состоит в обратной действии, сначала по заданному маршруту заполняется таблица, а затем, например, по строкам, считывается исходный текст. Ключом таких шифров являются размеры таблицы и маршрут записи и считывания символов.

Квадрат Полибия появился в древней Греции во втором веке до нашей эры. Этот метод шифрования представляет собой квадрат, разделённый на 5*5 клеток (применительно к латинскому алфавиту), в каждую клетку вписываются все буквы алфавита, при этом буквы I, J не различаются (J=I):

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

Рис 1.1 Квадрат Полибия

Каждая шифруемая буква заменялась на координаты квадрата, в котором она записана. Так, A заменялась на AA, Q на AD и т.д.

Такой квадрат уже не нужно иметь при себе, достаточно запомнить ключ – пароль.

Шифр Цезаря. С математической точки зрения шифр Цезаря, точнее, процесс шифрования исходного текста определяется выражением:

$$y_i = (x_i + k) \bmod m,\ i = \overline{1,n},$$

где y_i - буква криптограммы, x_i - буква открытого сообщения, k - ключ шифра, n - длина криптограммы (открытого текста), $m = |A_X|$ - мощность алфавита A_X.

Очевидно, что выражение:

$x_j = (y_j - k) \bmod m$, $j = \overline{1,n}$, определяет процесс расшифрования криптограммы.

Аффинный шифр Цезаря. Обобщением шифра Цезаря является аффинный шифр Цезаря, он определяется выражением:

$$y_i = (ax_i + k) \bmod m,\ i = \overline{1,n}.$$

Он определяется двумя целыми числами a и k, где $0 \le a, k \le m - 1$.

Числа a и n должны быть взаимно простыми. Взаимная простота a и n необходима, т.к. в противном случае возможны отображения различных символов в один и, как следствие, неоднозначность расшифрования.

Процесс расшифрования аффинного шифра Цезаря определяется выражением $x_j = (y_j - k)a^{-1} \bmod m$, где число a^{-1} является инверсией числа a по модулю m.

Вычисление инверсии. С помощью теории чисел разберем нахождение инверсии числа по модулю целого числа.

Во многих задачах криптографии для заданных чисел c, m требуется находить такое число d < m , что:

$$cd \bmod m = 1$$

Число d, удовлетворяющее данному равенству называется *инверсией c по модулю m и часто обозначается c в минус первой степени по mod m.*

Данное обозначение для инверсии довольно естественно, так как мы можем теперь переписать cd mod m = 1 в виде:

$$cc^{-1} \bmod m = 1$$

Таким образом, умножение на c в минус первой степени соответствует делению на c при вычислениях по модулю m, а также числу d .

По аналогии можно ввести произвольные отрицательные степени при вычислениях по модулю m:

$$c^{-e} = c^{e^{-1}} = {c^{-1}}^{e} \bmod m$$

Здесь e - просто число, степень, не экспонента.

3. Контрольные вопросы

1. Понятие криптосистемы. Классификация криптосистем. Основные требования к криптосистеме.
2. Шифры перестановки: определение, разновидности шифров перестановки.
3. Шифр Цезаря: определение, модификации.
4. Суть обобщенного алгоритма Евклида.

4. Задание на практическое занятие

При подготовке к занятию необходимо изучить материалы лекций, и ответить на контрольные вопросы, используя рекомендованную литературу.

Цель занятия достигается путем получения навыков при решении представленных задач:

Задача № 1

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

Задача № 2

Задан 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 K=(5, 2, 3, 4, 1).

Задача № 4

Зашифровать шифром маршрутной перестановки сообщение X=ФЕДЕРАЛЬНОЕ_АГЕНСТВО.

Задача № 5

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	,	.	-

Рис 1.2 Квадрат Полибия для задачи № 5

Необходимо зашифровать открытое сообщение X= МАТЕМАТИКА - ЦАРИЦА НАУК.

Задача № 6

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

Задача № 7

Зашифровать сообщение X=ИМПЕРАТОР ЦЕЗАРЬ аффинным шифром Цезаря с ключами: K1=2, K2=3.

Задача № 8

Вычислить инверсию числа с помощью обобщенного алгоритма Евклида и вычислить выражение: $\frac{48}{5}\mathrm{mod}49$

5. Содержание отчета о практическом занятии

1. Титульный лист
2. Ответы на контрольные вопросы
3. Задачи
4. Решение
5. Вывод

Практическое занятие № 2

Шифры криптографии средних веков и эпохи возрождения

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

2. Теоретические сведения

Шифр «магический квадрат».

«Магическим квадратом» является таблица размером $m \times m$, в которую вписываются числа от 1 до m^2 так, чтобы сумма чисел по строкам, столбцам и полным диагоналям равнялась одному и тому же числу. Процесс шифрования сводился к тому, что символы открытого текста в соответствии с их порядковым номером вписывались с соответствующую этому номеру ячейку квадрата, а считывание криптограммы осуществлялось по строкам. Если в квадрате оставались пустые ячейки, то их заполняли произвольными символами. Ключом данного шифра является «магический квадрат».

Шифр Виженера. В шифре Виженера ключ $k^{(d)}$ задается набором из d символов. Такие наборы подписываются под буквами открытого текста $X = x_1, x_2,..., x_n$, $x_i \in A_X$, до получения периодической ключевой последовательности $\bar{k} = k_1, k_2,..., k_n$, $n = \mathrm{sd} + r$, где s - число полных периодов $k^{(d)}$, $r = n \bmod d$, а значение d определяет период ключевой последовательности. Процесс шифрования определяется выражением:

$$y_i = (x_i + \bar{k}_i) \bmod m,\ i = \overline{1, n}.$$

Шифр Плейфера предусматривает шифрование пар символов (биграмм). Для шифрования сообщения необходимо разбить его на биграммы (группы из

двух символов), при этом, если в биграмме встретятся два одинаковых символа, то между ними добавляется заранее оговоренный вспомогательный символ (в оригинале – X, для русского алфавита — Я). Затем, руководствуясь следующими правилами, выполняется зашифровывание пар символов исходного текста:

1. Если символы биграммы исходного текста встречаются в одной строке, то эти символы замещаются на символы, расположенные в ближайших столбцах справа от соответствующих символов. Если символ является последним в строке, то он заменяется на первый символ этой же строки.

2. Если символы биграммы исходного текста встречаются в одном столбце, то они преобразуются в символы того же столбца, находящимися непосредственно под ними. Если символ является нижним в столбце, то он заменяется на первый символ этого же столбца.

3. Если символы биграммы исходного текста находятся в разных столбцах и разных строках, то они заменяются на символы, находящиеся в тех же строках, но соответствующие другим углам прямоугольника.

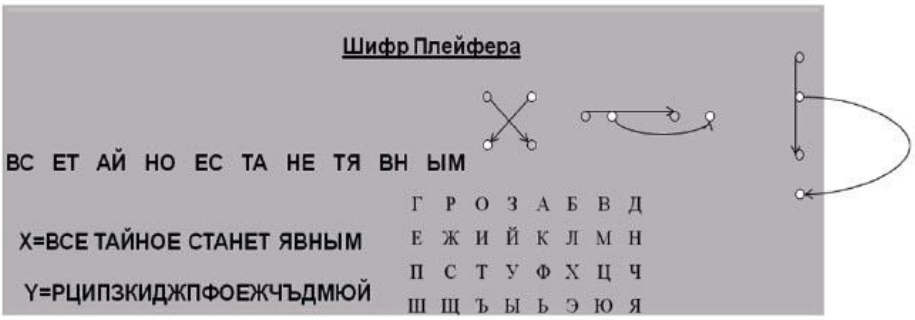

Рис 2.1 Принцип шифра Плейфера

Литорея (от лат. littera - буква) тайнописание, род шифрованного письма, которое употреблялось в древнерусской рукописной литературе.

Простая, иначе называемая тарабарской грамотой, — это замена одних согласных букв на другие. Самый простой способ заключается следующем: поставив согласные буквы в два ряда, употребляют в письме верхние буквы вместо нижних и наоборот, причём гласные остаются без перемены.

Рис 2.2 Принцип простой литореи

3. Контрольные вопросы

1. Шифр «магический квадрат». Принцип, алгоритм, особенности.
2. Шифр Виженера. Принцип, алгоритм, особенности.
3. Шифр Плейфера. Принцип, алгоритм, особенности.
4. Шифр простой литореи. Принцип, алгоритм, особенности.

4. Задание на практическое занятие

При подготовке к занятию необходимо изучить материалы лекций, и ответить на контрольные вопросы, используя рекомендованную литературу.

Цель занятия достигается путем получения навыков при решении представленных задач:

Задача № 1

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 № 2

Зашифровать сообщение X=ЛЕГКОКРИТИКОВАТЬ, с помощью «магического квадрата»:

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

Задача № 3

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

Задача № 4

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

Задача № 5

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

Задача № 6

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

Задача № 7

Зашифровать сообщение X=ПРИШЕЛ УВИДЕЛ ПОБЕДИЛ шифром Виженера. В качестве ключа использовать первое слово открытого сообщения.

5. Содержание отчета о практическом занятии

1. Титульный лист
2. Ответы на контрольные вопросы
3. Задачи
4. Решение
5. Вывод

Практическое занятие № 3

Комбинированные криптосистемы на основе шифров древнего времени, средних веков и эпохи возрождения

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

2. Контрольные вопросы

1. Особенности шифрования комбинированными криптосистемами.
2. Особенности расшифрования комбинированных криптосистем.
3. Поясните принцип шифра Цезаря.
4. Поясните принцип шифра «магический квадрат».

3. Задание на практическое занятие

При подготовке к занятию необходимо изучить материалы лекций, и ответить на контрольные вопросы, используя рекомендованную литературу.

Цель занятия достигается путем получения навыков при решении представленных задач:

Задача № 1

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

X =НЕВОЗМОЖНО ОБЪЯТЬ НЕОБЪЯТНОЕ

на ключе K ={АМУР;3,5,2,1,4}.

Рисунок 2.2 – Исходные данные

Рассмотрим коммерческую страховую компанию, занимающуюся урегулированием убытков. Информационная система обрабатывает персональные данные.

На ИС используется средства защиты, представленные на рисунке 2.2. СКЗИ, межсетевой экран, антивирусные средства защиты, внедрены меры по безопасные разработки программного обеспечения и другие.

Далее идет определение негативных последствий – рисунок 2.3.

У1 в части персональных данных. Возможные ущербы персональным данным.

У2 относится к организации. Может быть простой информационной системы, утрата доверия и потеря клиентов, поставщиков, которые оказывают какие-то услуги.

У3 соответственно возникновение ущерба.

Рисунок 2.3 – Определение негативных последствий

Другие виды последствий также могут быть, но как правило они несут на несколько порядков меньший ущерб

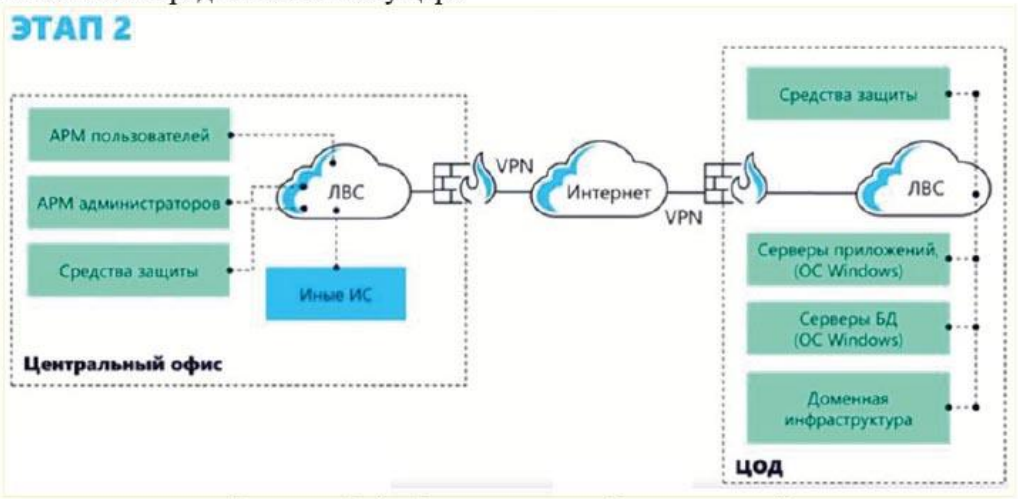

Рисунок 2.4 – Определение объектов воздействия

Следующий шаг определяем объекты воздействия, как представлено на рисунке 2.4. В рамках ЦОД есть наша система с серверами приложений и баз данных, а также всякие вспомогательные элементы.

(2/3) ЭТАП 2

Негативные последствия	Объекты воздействия	Виды воздействия
Утечка персональных данных	Серверы БД	• Модификация данных • Несанкционированный доступ
Простой информационной системы или сети	• Серверы инфраструктуры • Серверы БД • Серверы приложений	Отказ в обслуживании

Рисунок 2.5 – Определение видов воздействия на объекты

Далее определяем виды воздействия на объекты, как представлено на рисунке 2.5. Здесь рассматриваем объекты прямого воздействия.

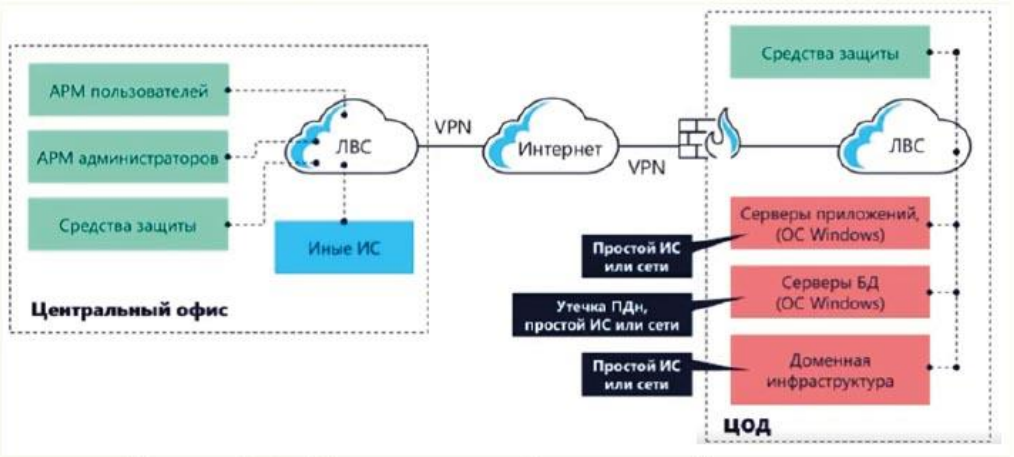

Рисунок 2.6 – Сопоставление объектов воздействия и негативных последствий

На рисунке 2.6 таблицу рисунка 2.5 перевели в схему о сопоставлении последствий и объектов воздействия. Если нарушитель достигнет своих целей организация получит данные негативные последствия.

Тип нарушителя	У1	У2	У3	Оценка актуальности
Специальные службы иностранных государств	–	–	–	Неактуальный
Преступные группы (криминальные структуры)	+	+	–	Актуальный
Отдельные физические лица (хакеры)	+	+	–	Актуальный
Конкурирующие компании	–	+	–	Актуальный

Рисунок 2.7 – Моделирование возможных нарушителей

Следующий шаг представлен на рисунке 2.7 - это моделирование нарушителей. Здесь использованы цели по аналогии с мотивацией. Т.к. информационная система не представляет интерес для специальных служб, то данный нарушитель неактуален. Остальные нарушители могут иметь какой-то интерес, с точки зрения обрабатываемых данных. Исключить больше нарушителей по данной методике не представляется возможным.

Также актуальны разработчики, администраторы, бывшие работники и сами пользователи.

Какие выводы, можно сделать из условий задачи для ускорения процесса подбора пароля?

4. Содержание отчета о практическом занятии

1. Титульный лист
2. Ответы на контрольные вопросы
3. Задачи
4. Решение
5. Вывод

Практическое занятие № 4

Шифры криптографии нового времени

1. Цель занятия - закрепление теоретических знаний по шифрованию и дешифрованию криптосистем на основе шифров нового времени.

2. Контрольные вопросы

1. Перечислите основные шифры криптографии нового времени.

3. Задание на практическое занятие

При подготовке к занятию необходимо изучить материалы лекций, и ответить на контрольные вопросы, используя рекомендованную литературу.

Цель занятия достигается путем получения навыков при решении представленных задач:

Задача № 1

Приведенный ниже шифр построен на тех же принципах, которые можно заметить на картинке "двоичных часов". Расшифруйте сообщение:

000011010011000110001111000001001001000001
011011001010010100010101001010001111010110
010000010010001110000001011000001010001010

Каждая буква криптограммы закодирована шестью символами двоичного кода.

Рис 4.1 Часы с двоичными отметками

Задача № 2

Студент Василий очень любит посещать лекции по криптографии. А еще Василий очень бережно относится к своим ботинкам, поэтому каждый вечер ставит их в пуленепробиваемый сейф с кодовым замком. На замке имеется 13 переключателей, каждый из которых может быть установлен в 2 положения - "1" или "0". В понедельник утром Василий по какой-то причине забыл комбинацию, который поставил накануне вечером на кодовом замке. Ему смутно помнится только, что число переключателей, установленных в положение "1", было нечетным.

Василий очень хочет попасть на любимую лекцию. Но босиком ему идти совсем не хочется. А времени - мало ... Если начать перебирать все комбинации - можно и не успеть ...

Помогите хорошему студенту. Подскажите, сколько различных вариантов комбинаций переключателей с нечетным количеством "1" может быть в замке его сейфа?

Ответ выведите в виде целого числа.

Задача № 3

Однажды младший брат Василия Петр, ученик 1 класса, попросил Васю помочь с его домашним заданием. Петру было даны две фразы. Первая из них была зашифрована шифром простой замены 1 раз, вторая – 2 раза. Первая фраза **ТАЦРЖ ИЦВЗДБПСЖ**, вторая - **АЫИЮШЧНЛКГТ З СЗАГХЫТ.** Расшифруйте фразы.

Ответ выведите в следующем виде: запишите прописными (большими) буквами расшифровку первой фразы и за ней, через пробел, расшифровку второй фразы. Внутри фраз слова разделяются одним пробелом.

Задача № 4

Студент Василий решил развить теорию Эйлера и предложить свое решение для обхода шахматным конем фигурных досок определенного класса - ступенчатых квадратов. Порядок или размер таких квадратов определяется по числу ступенек на каждой стороне.

Если бы все свободное время у Василия не занимало изучение дисциплин по компьютерной безопасности - он продвинулся бы очень далеко. И, возможно, изобрел бы собственную криптосистему, основанную на обходе конем ступенчатых квадратов большой размерности.

Пока же Василию удалось зашифровать свои сообщения в ступенчатых квадратах 2-го и 3-го порядка.

Ответ - расшифровку обоих сообщений - запишите прописными (большими) буквами, разделив расшифрованные сообщения символом @, с сохранением пробелов, которые были в исходных сообщениях.

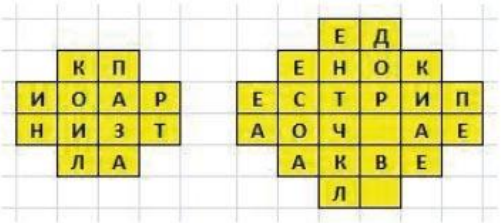

Рис 4.2 Шифрограммы Василия, построенные путем обхода ходом шахматного коня доски в форме ступенчатых квадратов 2-го и 3-го порядков.

4. Содержание отчета о практическом занятии

1. Титульный лист
2. Ответы на контрольные вопросы
3. Задачи
4. Решение
5. Вывод

Практическое занятие № 5

Избыточное кодирование и декодирование цифровых сообщений

1. Цель занятия - закрепление теоретических знаний по кодированию и декодированию сообщений.

2. Теоретические сведения

Сообщения в автоматизированных системах управления воздушным движением передаются двоичной кодировкой. Каждому символу соответствует свой код. Необходимо предусмотреть возможность обнаруживать и исправлять ошибки. Чтобы такая возможность появилась, надо добавить несколько дополнительных двоичных символов на букву, т.е. умышленно ввести некоторую избыточность, которая смогла бы помочь нам обнаружить или исправить ошибки.

Пример алгоритма кодирования сообщения из четырех информационных разрядов и трех контрольных разрядов:

1. Формирование кода символа.

Пусть $m=4$ – число информационных разрядов. Число контрольных символов должно быть не менее трех, т.е. $x=3$. (вычисление происходит по следующей зависимости: $2^X - X - 1 \geq m$.)

2. Выбор контрольных разрядов.

Контрольные символы назначаются так: индексы равны целым степеням двойки, т.е. 1, 2, 4, 8, 16,.... Вычисление происходит по следующей зависимости:2^{X-1}. При *x=3*, числа: 1, 2, 4.

B3-B5-B6-B7 B1-B2-B4
(информационные символы) (контрольные символы)

Пусть информационные символы имеют вид: 0111. Следовательно, сообщение будет иметь вид: B1-B2-0-B4-1-1-1, теперь необходимо вычислить контрольные символы.

3. Вычисление контрольных разрядов.

В случае же, когда ошибка в кодирование символа не имела места, набор $e_2e_1e_0$ должен указать на нулевую позицию, т.е. на несуществующий символ B0, в противном случае на разряд, где произошла ошибка: $e_2e_1e_0$

0 0 0 (B0)
0 0 1 (B1)
0 1 0 (B2)
0 1 1 (B3)
1 0 0 (B4)
1 0 1 (B5)
1 1 0 (B6)
1 1 1 (B7)

Легко уследить, что значение e_0 "несет ответственность" за позиции B1, B3, B5 и B7. Аналогично, обращая внимание на то, что значения e_1 и e_2 отвечают за соответственно B2 B3 B6 B7, B4 B5 B6 B7. Поэтому в качестве функции берется зависимость:

$$e_0 = (B1+B3+B5+B7) \bmod 2,$$
$$e_1 = (B2+B3+B6+B7) \bmod 2,$$
$$e_2 = (B4+B5+B6+B7) \bmod 2.$$

Подставляя в систему уравнений $e_0=e_1=e_2=0$, получим систему из трех уравнений:

$$B1=(B3+B5+B7) \bmod 2,$$
$$B2=(B3+B6+B7) \bmod 2,$$
$$B4=(B5+B6+B7) \bmod 2.$$

B3-B5-B6-B7 - информационные символы известны.

4. Определение ошибочного разряда.

Пусть набор информационных символов B3-B5-B6-B7=1011. Следовательно, контрольные разряды равны:

$$B1=(1+0+1)\bmod 2=0,$$
$$B2=(1+1+1)\bmod 2=1,$$
$$B4=(0+1+1)\bmod 2=0.$$

Сообщение будет иметь вид: 0110011.

Пусть ошибка произошла на уровне символа B5 т.е. вместо истинного расширенного кодового набора 0110(0)11 получен код 0110(1)11. Проверим в каком разряде ошибка:

$$e_0 = (B1+B3+B5+B7)\bmod 2=(0+1+1+1)\bmod 2=1,$$
$$e_1= (B2+B3+B6+B7)\bmod 2=(1+1+1+1)\bmod 2=0,$$
$$e_2= (B4+B5+B6+B7)\bmod 2=(0+1+1+1)\bmod 2=1.$$

3. Контрольные вопросы

1. Опишите алгоритм кодирования сообщений, приведенный в теоретических сведениях к данному практическому занятию.
2. Поясните суть алгоритма архивации из задачи №2.

4. Задание на практическое занятие

При подготовке к занятию необходимо изучить материалы лекций, и ответить на контрольные вопросы, используя рекомендованную литературу.

Цель занятия достигается путем получения навыков при решении представленных задач:

Задача № 1

Составить алгоритм кодирования сообщения в соответствии с приведенным описанием теоретической части из пяти информационных разрядов и четырех контрольных разрядов (m=5, x=4). Закодировать по разработанному алгоритму сообщения: 00001, 11111, 10000.

Задача № 2

Алгоритм архивации текстовых данных имеет вид:

- выписывают символы вертикально в ряд в виде ячеек будущего графа по правому краю листа;
- выбирают два символа с наименьшим количеством повторений в тексте;

- проводят от них линии влево к новой вершине графа и записывают в нее значение, равное сумме частот повторения каждого из объединяемых символов;
- рассматривают новую вершину как полноценную ячейку с частотой появления, равной сумме частот появления двух соединившихся вершин;
- повторяют операцию объединения вершин до тех пор, пока не придут к одной вершине с числом.
- затем расставляют на двух ребрах графа, исходящих из каждой вершины, биты 0 и 1, на каждом верхнем ребре 0, а на каждом нижнем – 1;
- для определения кода каждой конкретной буквы необходимо просто пройти от вершины дерева до нее, выписывая нули и единицы по маршруту следования. При расшифровке отделяется первый символ, затем снова начиная с вершины дерева, затем аналогично декодируется вся запись;
- для рисунка символ "А" получает код "100", символ "Б" – код "0", символ "К" – код "101", а символ "О" – код "11".

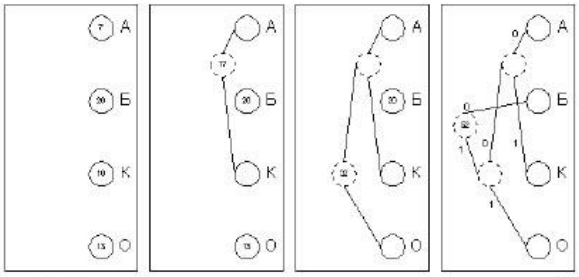

Рис 5.1 Визуализация алгоритма архивации задания №2

Восстановить по заданному дереву фразу: 0100101101110100.

Задача № 3

Исследовать вероятность пропуска ошибки *i*-й кратности от длительности одной операции одной операции при выбранном методе аппаратного контроля. Общая вероятность пропуска ошибки имеет вид: $Pnp = \sum_{t=0}^{n}(Pi(t) \cdot Pmnpi)$, где $Pmnpi = 4$ - выбранный метод контроля, *Pi(t)* - вероятности появления ошибки *i-й* кратности, n – количество ошибок. Вычислить значение общей вероятности пропуска ошибки, используя значения *Pi(t),* вычисленное в третьем пункте второго задания.

5. Содержание отчета о практическом занятии

1. Титульный лист
2. Ответы на контрольные вопросы
3. Задачи
4. Решение
5. Вывод

Практическое занятие № 6

Шифр Вернама

1. Цель занятия - закрепление теоретических знаний по кодированию и декодированию сообщений.

2. Теоретические сведения

В начале XX века значительный вклад в развитие криптографии внес американец Г. Вернам.

В 1917 году он, будучи сотрудником телеграфной компании, предложил идею автоматического шифрования телеграфных сообщений, суть которой заключается в следующем.

Открытый текст представляется в коде Бодо (в виде пятизначных "импульсных комбинаций").

В этом коде, например, буква "А" имела вид (+ + — — —).

На бумаге знак "+" означал отверстие, а знак "-" - его отсутствие.

При считывании с ленты пятерка металлических щупов "опознавала" отверстия (при наличии отверстия щуп замыкал электрическую цепь). В линию связи посылались импульсы тока.

Вернам предложил электромеханически, покоординатно складировать импульсы знаков секретного текста с импульсами секретного ключа, представляющего из себя хаотический набор букв того же самого алфавита. Сложение, по современной терминологии, осуществлялось по модулю 2.

Г. Вернам создал устройство, производящее операции шифрования автоматически, без участия шифровальщика, тем самым было положено начало так называемому "линейному шифрованию", когда процессы шифрования и передачи сообщения происходят одновременно.

До той поры шифрование было предварительным, поэтому линейное шифрование существенно повышало оперативность связи. Шифр Вернама обладает исключительной криптографической стойкостью.

В то же время очевиден и недостаток этой системы шифрования - ключ должна иметь ту же длину, что и открытый текст. Для расшифрования на приемном конце связи туда нужно передать (по тайным, защищенным каналам) ключ достаточной длины.

Для того, чтобы разобрать **шифр Вернама** с математической точки зрения, вспомним шифр Виженера, где ключ $k^{(d)}$ задается набором из d символов.

Такие наборы подписываются под буквами открытого текста $X = x_1, x_2, \ldots, x_n$, $x_i \in A_X$, до получения периодической ключевой последовательности $\overline{k} = k_1, k_2, \ldots, k_n$, $n = \mathrm{sd} + r$, где s - число полных периодов $k^{(d)}$, $r = n \bmod d$, а значение d определяет период ключевой последовательности.

Процесс шифрования определяется выражением:

$$y_i = (x_i + k_i) \bmod m,\ i = \overline{1,n}.$$

При повторных операциях шифрования открытого теста шифром Виженера получаем **составной шифр Виженера**, который описывается выражением:

$$y_i = (x_i + k_i + v_i + \ldots + w_i) \bmod m,\ i = \overline{1,n},$$

где $k_i, v_i, \ldots, w_i$ - ключевые последовательности, имеющие, как правило, различные периоды. Период суммы этих ключевых последовательностей равен наименьшему общему кратному отдельных периодов.

Иногда используется **усложненный шифр Виженера**. Усложнение заключается в «перемешивании» исходного алфавита и получении нового алфавита A'_X, причем $|A_X| = |A'_X| = m$. Перемешивание обычно проводится при помощи **лозунга (ключа)**, который представляет собой слово или фразу, неповторяющиеся символы которого образуют начало алфавита.

Заметим, что шифр Виженера с периодом d равным единице представляет собой шифр Цезаря.

Если же криптосистема Виженера имеет период $d = n$, то получаем **шифр гаммирования**:

$y_i = (x_i + \gamma_i) \bmod m,\quad i = \overline{1,n}$. В шифре гаммирования ключевая последовательность носит название гамма-последовательности γ.

3. Контрольные вопросы

1. Понятие совершенно стойкой криптосистемы.
2. Поясните суть шифра Вернама.
3. Теорема о совершенной стойкости шифра Вернама.

4. Задание на практическое занятие

При подготовке к занятию необходимо изучить материалы лекций, и ответить на контрольные вопросы, используя рекомендованную литературу.

Цель занятия достигается путем получения навыков при решении представленных задач:

Задача № 1

Декодировать сообщение X=esnq^uix^qhqd^uix^i`qqx при *ключе равном: 00000001*, восстановить текст сообщения в символах алфавита.

Задача № 2

Зашифровать сообщение X=sing_thy_songs_of_happy при помощи двух *ключей: K1=11110001* и *K2=11110001*.

Задача № 3

Зашифровать сообщение при*: K1=00000001 и K2=01010001* в символах алфавита (*слова разделены нижнем подчеркиванием)*

my mother bore me in the southern wild
and i am black but o my soul is white
white as an angel is the english child
but i am black as if bereav'd of light

Таблица символов алфавита имеет следующий вид:

Таблица 6.1 Коды символов алфавита

a	01100001	i	01101001	q	01110001	y	01111001	,	00101100
b	01100010	j	01101010	r	01110010	z	01111010	;	00111011
c	01100011	k	01101011	s	01110011	_	01011111		
d	01100100	l	01101100	t	01110100	`	01100000		
e	01100101	m	01101101	u	01110101	^	01011110		
f	01100110	n	01101110	v	01110110	{	01111011		
g	01100111	o	01101111	w	01110111	.	00101110		
h	01101000	p	01110000	x	01111000	:	00111010		

5. Содержание отчета о практическом занятии

1. Титульный лист
2. Ответы на контрольные вопросы
3. Задачи
4. Решение
5. Вывод

Практическое занятие № 7

Волновой метод криптографии

1. Цель занятия - закрепление теоретических знаний по кодированию и декодированию сообщений.

2. Теоретические сведения

Шифрование данным методом достигается тем, что изменяем стандартный способ шифрования, путем использования периодических функций типа y=cos(x) и уравнения тригонометрических функций «волны» типа y=cos(x+dx).

Существует огромное количество периодических функций, имеющих постоянную амплитуду, которые определены и непрерывны на всем промежутке x (“-“ бесконечность; “+” бесконечность).

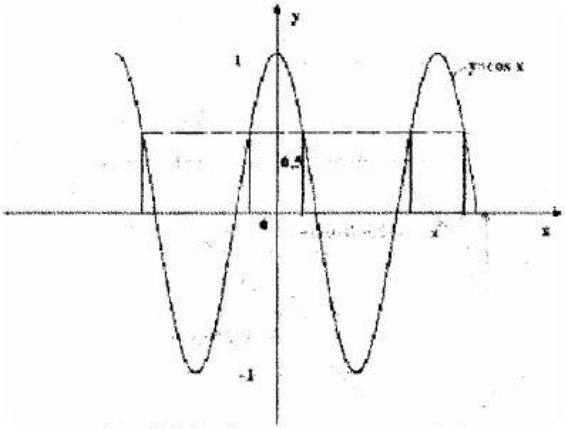

Рис 7.1 График функции y=cos(x)

На графике представлена функция y=cos(x). Особенность периодической функции в том, что, к максимальному значению y = 0,5 соответствует бесконечное количество значений x.

Применяя уравнение волны y=cos(x+N*dx), где N - любое целое число, а dx->0, получаем, что при y=0,5x может принимать любые значения от"-"бесконечности до "+" бесконечности.

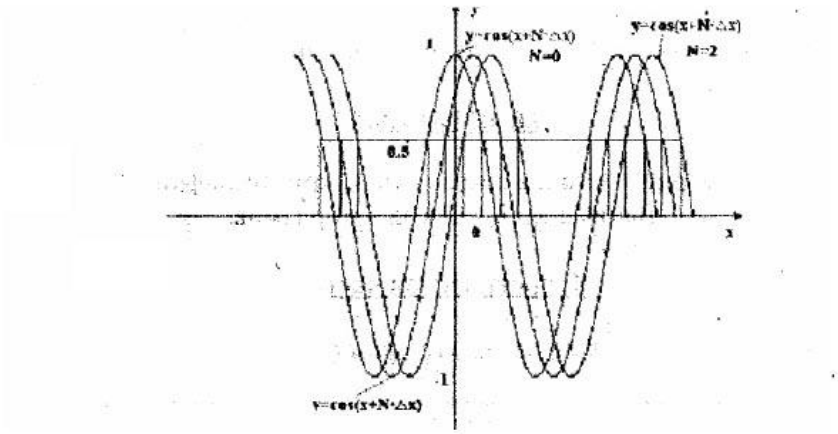

Рис 7.2 Визуализация y=cos(x+N*dx) при y=0.5x

По оси X расставляют и номеруют те символы, которые нужно зашифровать, а по оси Y т.е., которые будут использованы в шифровке. Шифрование идет по линейной функции Y = X, которая перемещается по осям координат. Перемещение линейной функции y=x происходит по уравнению волны. По координатным осям X и Y расставляются компьютерные символы в

любом порядке. Всего используется в компьютере 255 символов. Они все расставляются по оси X в любом порядке, по оси Y расставляем те же самые символы в любом порядке. Три линейные функции 1,2,3 описываются как: Y1, Y2, Y3:

$$Y1=X + 255\cdot[\cos(z + N\cdot dx)] + 255$$
$$Y2 =X + 255 \cdot [\cos (z + N\cdot dx)]$$
$$Y3 =X + 255 \cdot [\cos (z + N \cdot dx)] -255$$

где: X - тот байт (знак), который нужно зашифровать; Z - любое число; N-номер по счету шифруемого знака в исходном тексте; dx- любое число.

Пример реализации волнового метода:

Для примера зашифруем исходный текст, состоящий из пяти букв А. **АААА**А - исходный текст. Порядок расстановки знаков по осям **X** и **Y** одинаковый. Например, знак А занимает промежуток (191-192) по оси **X,** знак Б-(192-193); В-(193-194); …; Я-(250-251). То же_самое по оси **Y**. Имея три формулы, подставляем значение 191,5 - середину промежутка (191-192) - буква А.

Пусть: Z = 0 (для удобства); N = 1 (т.к. шифруется первый по счету знак из исходного текста, потом 2,3,4,5); dx = 32. Подставляем эти цифры в формулу:

$$Y1 = 191,5 + 255\cdot [\cos(z + 1 \cdot 32)] + 255=659,227;$$
$$Y2 =191,5 + 255 \cdot [\cos(z + 1 \cdot 32)] =404,227;$$
$$Y3 =191,5 + 255 \cdot [\cos(z+ 1\cdot32)] -255 = 149,227.$$

Из трех значений Y I, Y2, Y3 выбираем Y3, так как оно попало в промежуток то 0 до 255 и округляем значение Y3 до большего целого Y=150. Шифруем второй знак исходного текста:

$$Y1 =191,5 + 255\cdot [\cos(z + 2 \cdot 32)] + 255=546,42;$$
$$Y2 =191,5 + 255\cdot [\cos(z + 2 \cdot 32)] =291,42;$$
$$Y3 =191,5 + 255 \cdot [\cos(z+ 2\cdot32)] -255 = 36,42.$$

В шифровку, соответственно, записываем Y3=37.Соответственно получаем третий, четвертый и пятый знаки шифровки:

Третий знак – 146, Четвертый знак- 15, Пятый знак- 198.

В итоге получили числовой ряд 150; 37; 146; 15; 198 – шифровка, т.е.:

– **%** ’ □ **Ж**

Для расшифровки применяют те же самые формулы:

$$X1 = Y - 255 \cdot [\cos (z + N \cdot dx)]- 255;$$

$$X2=Y-255 \cdot [\cos(z + N \cdot dx)];$$
$$X3=Y-255 \cdot [\cos(z + N \cdot dx)]+255.$$

Подставляя уже известные значения получаем:

$$XI = 191{,}5 - 255 \cdot [COS (0 + 1 \cdot 32)] - 255 = -318{,}23$$
$$X2 = 191{,}5 - 255 \cdot [COS (0 + 1 \cdot 32)] = -63{,}22$$
$$X3 = 191{,}5 - 255 \cdot [COS (0 + 1 \cdot 32)] + 255 = 191{,}73$$
$$X=191{,}73$$

Подставляя следующие значения символов получаем ряд: 191,73; 191,58; 191,51; 191,19; 191,28 все эти значения попали в промежуток (191-192), соответственно получили текст: **А А А А А**.

3. Контрольные вопросы

1. Поясните суть волнового метода криптографии.
2. Какие особенности возникают при использовании волнового метода.

4. Задание на практическое занятие

При подготовке к занятию необходимо изучить материалы лекций, и ответить на контрольные вопросы, используя рекомендованную литературу.

Цель занятия достигается путем получения навыков при решении представленных задач:

Задача № 1

Декодировать сообщение при *Z=45*, восстановить текст сообщения в символах алфавита.

\ Ю Ъ v ¬ D K M _ G П D µ f „ P m б N _ 1 ґ * — q Є ч } я S

Рис 7.3 Закодированное сообщение для задачи №1

Задача № 2

Декодировать сообщение при *Z=33* восстановить текст сообщения в символах алфавита.

г | s ° * T : у 8 Э Н Б о Ґ Д ^ д С f % ё % i ` Ъ л х э d W

Рис 7.4 Закодированное сообщение для задачи №2

Задача № 3

Зашифровать сообщение при *Z=12* в символах алфавита.

my mother taught me underneath a tree
and sitting down before the heat of day,
she took me on her lap and kissed me,
and pointing to the east began to say.

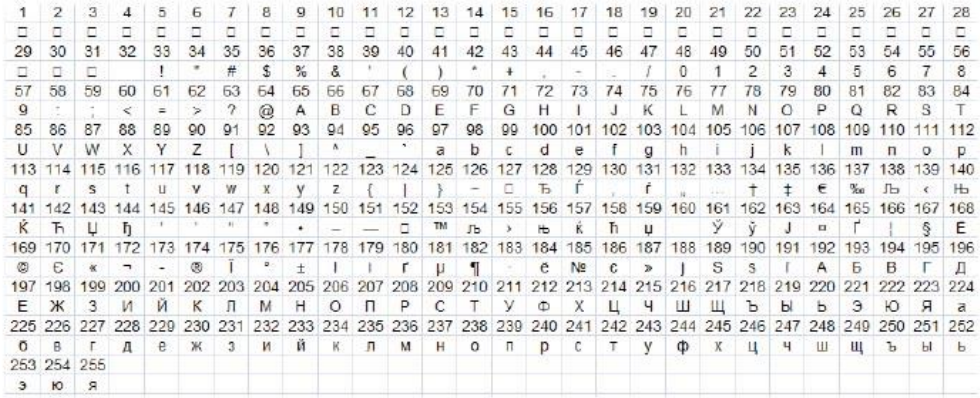

Рис 7.5 Кодовое представление символов алфавита

5. Содержание отчета о практическом занятии

1. Титульный лист
2. Ответы на контрольные вопросы
3. Задачи
4. Решение
5. Вывод