Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации
Федеральное государственное образовательное бюджетное учреждение высшего профессионального образования
Поволжский государственный университет телекоммуникаций и информатики
Кафедра ИБ

«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ИНФОКОММУНИКАЦИОННЫХ СЕТЕЙ И СИСТЕМ»

1 часть

Задания и методические указания для контрольной работы

Самара, 2021

Содержание:

1 Симметричные криптосистемы	3
1.1 Шифры перестановки	3
1.2 Шифры простой замены	9
1.3 Аналитические методы шифрования	15
2 Асимметричная криптосистема RSA	17
3 Симметричная криптосистема DES	21
4 Политика безопасности	22
Задачи для самопроверки и контрольной работы	26

Необходимо решить задачи в конце методических указаний.
Решение предоставляется полностью!

1 Симметричные криптосистемы

Исторически первыми появились симметричные криптографические системы. В симметричной криптосистеме шифрования используется один и тот же ключ для зашифровывания и расшифровывания информации. Это означает, что любой, кто имеет доступ к ключу шифрования, может расшифровать сообщение.

В рамках симметричного шифрования будут рассмотрены следующие шифры:

- шифры перестановок;
- шифры замены;
- шифры, основанные на аналитических преобразованиях шифруемых данных.

Шифрование перестановкой заключается в том, что символы шифруемого текста переставляются по определенному правилу в пределах некоторого блока этого текста. При достаточной длине блока, в пределах которого осуществляется перестановка, и сложном неповторяющемся порядке перестановки можно достигнуть приемлемой для простых практических приложений стойкости шифра.

Шифрование заменой (подстановкой) заключается в том, что символы шифруемого текста заменяются символами того же или другого алфавита в соответствии с заранее обусловленной схемой замены.

Шифрование аналитическим преобразованием заключается в том, что шифруемый текст преобразуется по некоторому аналитическому правилу (формуле).

1.1 Шифры перестановки

В шифрах перестановки все символы открытого текста переносятся в шифрограмму в неизменном виде, но меняют своё местоположение. Шифры перестановки применялись с V в. до н.э. – например, жезл сцитала, затем использовались блочная перестановка, простая табличная перестановка, маршрутная перестановка, вертикальная перестановка, поворотные решётки, двойная табличная перестановка, множественные перестановки. В современных стандартах шифрования применяются блочные одинарные перестановки.

1.1.1 Шифрующие таблицы

С начала эпохи Возрождения (конец XIV столетия) начала возрождаться и криптография. Наряду с традиционными применениями криптографии в политике, дипломатии и военном деле появляются и другие задачи - защита интеллектуальной собственности от преследований инквизиции или заимствований злоумышленников. В разработанных шифрах перестановки того времени применяются

шифрующие таблицы, которые в сущности задают правила перестановки букв в сообщении.

В качестве ключа в шифрующих таблицах используются:

- размер таблицы;
- слово или фраза, задающие перестановку;
- особенности структуры таблицы.

Одним из самых примитивных табличных шифров перестановки является простая перестановка, для которой ключом служит размер таблицы

Задача 1.1. Зашифровать методами простой перестановки сообщение: *ЗАПУСК РАКЕТЫ НАЗНАЧЕН УТРОМ В ПЯТЬ*.

Решение:

Необходимо подобрать такой размер таблицы, чтобы все буквы сообщения вписались в нее. Количество ячеек таблицы совпадает с количеством символов в тексте без учета пробелов.

Сообщение записывается в таблицу поочерёдно по столбцам. Считывание производится по строкам.

З	К	Т	Н	У	В
А	Р	Ы	А	Т	П
П	А	Н	Ч	Р	Я
У	К	А	Е	О	Т
С	Е	З	Н	М	Ь

Шифртекст записывается блоками для удобства, например по шесть букв:

ЗКТНУВ АРЫАТП ПАНЧРЯ УКАЕОТ СЕЗНМЬ.

Отравитель и получатель сообщения должны заранее условиться об общем ключе в виде размера таблицы. При расшифровании действия выполняют в обратном порядке.

Несколько большей стойкостью к раскрытию обладает метод шифрования, называемый одиночной перестановкой по ключу. Этот метод отличается от предыдущего тем, что столбцы таблицы переставляются по ключевому слову, фразе или набору чисел длиной в

строку таблицы.

Задача 1.2. Зашифровать сообщение задачи 1.1. методом одиночной перестановки по ключу. В качестве ключа использовать слово ОСАДКИ.

Решение: Составим две таблицы, заполненные текстом сообщения и ключевым словом. Ниже представлены таблица до перестановки (с ключевым словом и порядком следования букв в нем) и после перестановки.

В верхней таблице в нижних строках записан ключ, а номера под буквами ключа определены в соответствии с естественным порядком соответствующих букв ключа в алфавите. Если бы в ключе встретились одинаковые буквы, они бы были пронумерованы слева направо. В нижней таблице столбцы переставлены в соответствии с упорядоченными номерами букв ключа.

Таблица до перестановки

З	К	Т	Н	У	В
А	Р	Ы	А	Т	П
П	А	Н	Ч	Р	Я
У	К	А	Е	О	Т
С	Е	З	Н	М	Ь
О	**С**	**А**	**Д**	**К**	**И**
5	**6**	**1**	**2**	**4**	**3**

Таблица после перестановки

1	**2**	**3**	**4**	**5**	**6**
Т	Н	В	У	З	К
Ы	А	П	Т	А	Р
Н	Ч	Я	Р	П	А
А	Е	Т	О	У	К
З	Н	Ь	М	С	Е

При считывании содержимого нижней таблицы по строкам и записи шифртекста блоками получим шифрованное сообщение:

ТНВУЗК ЫАПТАР НЧЯРПА АЕТОУК ЗНЬМСЕ.

Задача 1.3. Расшифровать сообщение *ТНВУЗК ЫАПТАР НЧЯРПА АЕТОУК ЗНЬМСЕ*, используя ключевое слово ОСАДКИ.

Решение: При расшифровании действия производятся в обратном порядке.

Построчно заполняется таблица шифртекстом и проставляются по прядку номера столбцов.

1	**2**	**3**	**4**	**5**	**6**
Т	Н	В	У	З	К
Ы	А	П	Т	А	Р
Н	Ч	Я	Р	П	А
А	Е	Т	О	У	К
З	Н	Ь	М	С	Е

В следующей таблице записывается ключевое слово и порядок следования букв в нем. В соответствие с этим порядком меняются местами столбцы.

О	**С**	**А**	**Д**	**К**	**И**
5	**6**	**1**	**2**	**4**	**3**
З	К	Т	Н	У	В
А	Р	Ы	А	Т	П
П	А	Н	Ч	Р	Я
У	К	А	Е	О	Т
С	Е	З	Н	М	Ь

Считывание производится по столбцам:
ЗАПУСК РАКЕТЫ НАЗНАЧЕН УТРОМ В ПЯТЬ

Для обеспечения дополнительной скрытности можно повторно зашифровать сообщение, которое уже прошло шифрование. Такой метод шифрования называется двойной перестановкой. В случае двойной перестановки столбцов и строки таблицы перестановки определяются отдельно для столбцов и отдельно для строк. Сначала в таблицу записывается текст сообщения, потом поочередно переставляются столбцы, а затем строки. При расшифровании порядок перестановок должен быть обратным.

Задача 1.4. Зашифровать методом *двойной перестановки* сообщение: *ПРИЛЕТАЮ ВОСЬМОГО*.

Для шифрования использовать ключи:
по столбцам - *4 1 3 2*, по строкам - *3 1 4 2*.

Решение: текст исходного сообщения записывается в таблицу 4х4, т.к. сообщение содержит 16 символов. Затем поочередно переставляются столбцы, а затем строки.

Исходная таблица

	4	**1**	**3**	**2**
3	П	Е	В	М
1	Р	Т	О	О
4	И	А	С	Г
2	Л	Ю	Ь	О

Перестановка столбцов

	1	**2**	**3**	**4**
3	Е	М	В	П
1	Т	О	О	Р
4	А	Г	С	И
2	Ю	О	Ь	Л

Перестановка строк

	1	**2**	**3**	**4**
1	Т	О	О	Р
2	Ю	О	Ь	Л
3	Е	М	В	П
4	А	Г	С	И

Если считывать шифртекст из правой таблицы построчно блоками по четыре буквы, то получится следующее:

ТООР ЮОЬЛ ЕМВП АГСИ

Число вариантов двойной перестановки быстро возрастает при увеличении размера таблицы:

- Для таблицы 3х3 – 36 вариантов;
- Для таблицы 4х4 – 576 вариантов;
- Для таблицы 5х5 – 14400 вариантов.

1.1.2 Шифрование магическими квадратами

Магическими квадратами называют квадратные таблицы с вписанными в их клетки последовательными натуральными числами, начиная от 1, которые дают в сумме по каждому столбцу, каждой строке и каждой диагонали одно и то же число.

Шифруемый текст вписывали в магические квадраты в соответствии с нумерацией их клеток. Если затем выписать содержимое такой таблицы по строкам, то получится шифртекст, сформированный благодаря перестановке букв исходного сообщения. Считалось, что созданные с помощью магических квадратов шифртексты охраняет не только ключ, но и магическая сила.

Задача 1.5. Зашифровать сообщение задачи 1.4 с помощью магического квадрата

Решение: буквы в сообщении нумеруются подряд с первой до последней и затем вписываются в магический квадрат.

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

О	И	Р	М
Е	О	С	Ю
В	Т	А	Ь
Л	Г	О	П

Шифртекст, получаемый при считывании содержимого правой таблицы по строкам, имеет вид:

ОИРМ ЕОСЮ ВТАЬ ЛГОП

Число магических квадратов быстро возрастает с увеличением размера квадрата. Существует только один магический квадрат размером 3x3. Количество магических квадратов 4x4 - 880, а 5x5 - 250000.

1.1.3 Метод перестановок на основе маршрутов Гамильтона

Этот метод реализуется путем выполнения следующих шагов.

Шаг 1. Исходный текст разбивается на блоки по *n* символов (включая пробелы). Если длина последнего шифруемого блока не кратна длине блока, то на свободные места блока помещают служебные символы-заполнители (например,*)

Шаг 2. Символами блока заполняется таблица (маршрут), в которой для каждого порядкового номера символа в блоке отводится вполне определенное место (рис. 1.1).

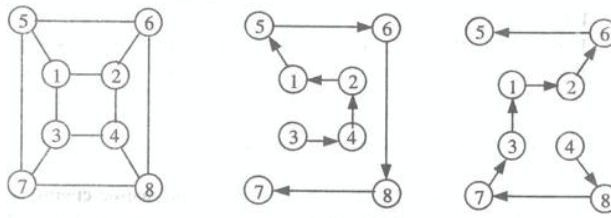


Рис. 1.1 – Вариант таблицы и маршрутов Гамильтона

Шаг 3. Считывание символов из таблицы осуществляется по одному из маршрутов. Увеличение числа маршрутов повышает криптостойкость шифра. Маршруты выбирают либо последовательно, либо их очерёдность задаётся ключом К.

Шаг 4. Зашифрованная последовательность символов разбивается на блоки фиксированной длины L (необходимо для передачи по каналам связи). Величина L может отличаться от длины блоков, на которые разбивается исходный текст на шаге 1.

Расшифрование производится в обратном порядке.

Задача 1.6. Требуется зашифровать текст *МЕТОДЫ ПЕРЕСТАНОВКИ*. Ключ и длины зашифрованных блоков равны: K=211, L=4.

Для шифрования использовать таблицу и два маршрута, представленные на

рис.1.1.

Решение:

Воспользуемся вышеизложенной методикой построения шифра по шагам.
Шаг 1. Исходный текст разбивается на 3 блока:

Блок Б1=<МЕТОДЫ_П>

Блок Б2=<ЕРЕС_ТАНО>

Блок Б3=<ВКИ*****>

Шаг 2. Заполняется 3 матрицы с маршрутами 2,1,1 (рис.1.2.)

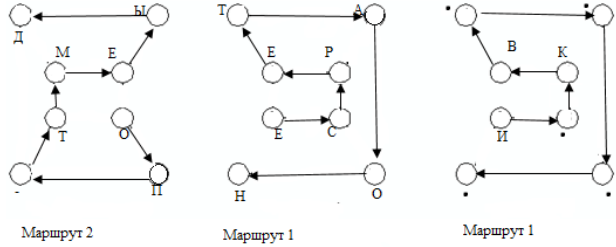


Рис.2.1 - Шифрование с помощью маршрутов Гамильтона

Шаг 3. Получение шифртекста путем расстановки символов в соответствии с маршрутами.

*ОП_ТМЕЫДЕСРЕТАОНИ*КВ*****

Шаг 4._Разбиение на блоки шифртекста

*ОП_ТМЕЫД ЕСРЕТАОН И*КВ*****

Возможно применение и других маршрутов.

1.2 Шифры простой замены

При шифровании заменой (подстановкой) символы шифруемого текста заменяются символами того же или другого алфавита по заранее установленным правилам замены. В шифре простой замены каждый символ исходного текста заменяется символами того же алфавита одинаково на всем протяжении текста. Часто шифры простой замены называют шифрами одноалфавитной подстановки.

1.2.1 Система шифрования Цезаря

Шифр Цезаря является частным случаем шифра простой замены (одноалфавитной подстановки). При шифровании исходного текста каждая буква заменялась на другую букву того же алфавита по следующему правилу. Заменяющая буква определялась путём смещения по алфавиту от исходной буквы на К букв. При достижении конца алфавита выполнялся циклический переход ков началу. Цезарь использовал шифр замены при смещении ***К=3.*** Такой шифр замены можно задать таблицей подстановок, содержащей соответствующие пары букв открытого текста и шифртекста.

Задача 1.7. Зашифровать послание Цезаря: *VENI VID1 VICI*

Решение:

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

Таблица подстановок Цезаря К=3

Используя таблицу подстановок получаем шифртекст: *YHQL YLGL YLFL.*

Задача 1.8. Зашифровать слово «*ЦЕЗАРЬ*» с помощью системы Цезаря при смещении К=5.

Решение:

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

Таблица подстановок Цезаря К=5

В результате получаем шифртекст: *ЫКМЕХБ*.

1.2.2 Система Цезари с ключевым словом

Система шифрования Цезаря с ключевым словом является одноалфавитной системой подстановок. Особенностью этой системы является использование ключевого слова для смещения и изменения порядка символов в алфавите подстановок. Ключевое слово записывается под буквами алфавита, начиная с буквы, числовой код которой равен числу k+1. Оставшиеся буквы алфавита подстановки записываются после ключевого слова в алфавитном порядке. Расшифровка происходит в обратном порядке.

Задача 1.9. Зашифровать сообщение «*ТЕРПЕНИЕ И ТРУД ВСЕ ПЕРЕТРУТ*» по системе Цезаря с ключевым словом «Тюльпан», k=7.

Решение:

Мы имеем подстановку для каждой буквы произвольного сообщения.

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

Исходное сообщение шифруется как *ЕЭГВЭНЮЭ Ю ЕГЖЫ ЩДЭ ВЭГЭЕГЖЕ*.

Задача 1.10. Сформировать таблицу подстановок в системе с ключевой фразой *КАК ДЫМ ОТЕЧЕСТВА НАМ СЛАДОК И ПРИЯТЕН*, полагая k = 3

Решение:

Записать ключевое слово (или фразу) без повторения одинаковых букв.

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

Несомненным достоинством системы Цезаря с ключевым словом является то, что количество возможных ключевых слов практически неисчерпаемо. Недостатком этой системы является возможность взлома шифртекста на основе анализа частот появления букв.

1.2.3 Шифрующие таблицы Трисемуса

В 1508 г. аббат из Германии Иоганн Трисемус написал печатную работу по криптологии под названием "Полиграфия". В этой книге он впервые систематически описал применение шифрующих таблиц, заполненных алфавитом в случайном порядке.

Для получения такого шифра замены обычно использовались таблица для записи букв алфавита и ключевое слово (или фраза). В таблицу сначала вписывалось по строкам ключевое слово, причем

повторяющиеся буквы отбрасывались. Затем эта таблица дополнялась не вошедшими в нее буквами алфавита по порядку. Поскольку ключевое слово или фразу легко хранить в памяти, то такой подход упрощал процессы шифрования и расшифрования.

При шифровании находят в этой таблице очередную букву открытого текста и записывают в шифртекст букву, расположенную ниже неё в том же столбце. Если буква текста оказывается в нижней строке таблицы, тогда для шифртекста берут самая верхнюю букву из того же столбца.

Такие табличные шифры называются монограммными, так как шифрование выполняется по одной букве. Трисемус первым заметил, что шифрующие таблицы позволяют шифровать сразу по две буквы. Такие шифры называются биграммными.

Задача 1.11. Зашифровать сообщение *ЗНАНИЕ-СИЛА*. В качестве ключа взять слово БАНДЕРОЛЬ.

Решение:

Для русского алфавита шифрующая таблица может иметь размер 4x8. Шифрующая таблица с ключевым словом выглядит следующим образом:

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

Получаем шифртекст: *УГВГФЗ-ЩФКВ*

Задача 1.12. Расшифровать сообщение *ПЕКЗЪВЗЧШЛЪЙСЙ* с помощью таблицы Трисемуса с ключевым словом БАНДЕРОЛЬ

Решение: *ВЫЛЕТАЕМ ПЯТОГО.*

1.2.4 Биграммный шифр Плейфейра

Шифр Плейфейра, изобретенный в 1854 г., является наиболее известным биграммным шифром замены. Он применялся Великобританией во время первой мировой войны. Основой шифра Плейфейра является шифрующая таблица со случайно расположенными буквами алфавита исходных сообщений.

Для удобства запоминания шифрующей таблицы отправителем и получателем сообщений можно использовать ключевое слово (или фразу) при заполнении начальных строк таблицы. В целом структура шифрующей таблицы системы Плейфейра полностью аналогична структуре шифрующей таблицы Трисемуса. Поэтому для пояснения процедур шифрования и расшифрования в системе Плейфейра воспользуемся шифрующей таблицей Трисемуса из предыдущей задачи.

Процедура шифрования включает следующие шаги.

1. Открытый текст исходного сообщения разбивается на пары букв (биграммы). Текст должен иметь четное количество букв и в нем не должно быть биграмм, содержащих две одинаковые буквы. Если эти требования не выполнены, то текст модифицируется даже из-за незначительных орфографических ошибок.

2. Последовательность биграмм открытого текста преобразуется с помощью шифрующей таблицы в последовательность биграмм шифртекста по следующим правилам:

2.1. Если обе буквы биграммы открытого текста не попадают на одну строку или столбец (как, например, буквы А и Й), тогда находят буквы в углах прямоугольника, определяемого данной парой букв (в нашем примере это - буквы АЙОВ. Пара букв АЙ отображается в пару ОВ. Последовательность букв в биграмме шифртекста должна быть зеркально расположенной по отношению к последовательности букв в биграмме открытого текста)

2.2. Если обе буквы биграммы открытого текста принадлежат одному столбцу таблицы, то буквами шифртекста считаются буквы, которые лежат под ними (например, биграмма НС дает биграмму шифртекста ГЩ). Если при этом буква открытого текста находится в нижней строке, то для шифртекста берется соответствующая буква из верхней строки того же столбца (например, биграмма ВШ дает биграмму шифртекста ПА.)

2.3. Если обе буквы биграммы открытого текста принадлежат одной строке таблицы, то буквами шифртекста считаются буквы, которые лежат справа от них (например, биграмма НО дает биграмму шифртекста ДЛ.) Если при этом буква открытого текста находится в крайнем правом столбце, то для шифра берут соответствующую букву из левого столбца в той же строке (например, биграмма ФЦ дает биграмму шифртекста ХМ.)

Задача 1.13. Зашифровать биграммным шифром Плейфейра текст «*ВЕЛОСИПЕДИСТ*». Ключевое слово «Карусель».

Решение: Разобьём этот текст на биграммы (блоки по два символа)

ВЕ ЛО СИ ПЕ ДИ СТ

Данная последовательность биграмм открытого текста преобразуется с помощью шифрующей таблицы в последовательность биграмм шифртекста. Для этого составим таблицу:

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

При шифровании биграмм получим следующий текст:

ЗАРХЛЖФУЖЙЖЫ

Задача 1.14. Расшифровать текст, полученный в предыдущей задаче.

Решение: для расшифровки необходимо выполнить действия в обратном порядке после того, как текст будет разбит на биграммы.

1.3 Аналитические методы шифрования

Среди аналитических методов наибольшее распространение получили методы, основанные на использовании матриц. Зашифрование *К*-го блока исходной информации, представленного в виде вектора $B_k = ||b_j||$, осуществляется путём перемножения матрицы ключа $A = \|a_{ij}\|$ и вектора B_k. В результате перемножения получается блок шифртекста в виде вектора $C_k = ||c_i||$, где элементы вектора C_k определяются по формуле:

$$C_i = \sum_{j=1} a_{ij} * b_j \qquad (2.1)$$

Расшифрование информации осуществляется путём последовательного перемножения векторов $C_к$ и обратной матрицы A^{-1}.

Последовательность действий при расшифровке:

1. Вычисляется определитель $|A|$

2. Определяется присоединенная матрица A^*, каждый элемент которой является алгебраическим дополнением элемента a_{ij} матрицы A:

3. Определяется транспонированная матрица A^T

4. Вычисляется обратная матрица $A^{-1} = \dfrac{A^T}{|A|}$

5. Определяются векторы B_1 и B_2: $B_1 = A^{-1}C_1$; $B_2 = A^{-1}C_2$

Задача 1.15. Зашифровать слово T_0 =<КНИЖКА> с помощью матрицы-ключа А.

$$A=\begin{vmatrix}1 & 4 & 8\\ 3 & 7 & 2\\ 6 & 9 & 5\end{vmatrix}$$

Решение.

1.Определяется числовой эквивалент исходного слова как последовательность соответствующих порядковых номеров букв слов: *T*=<11 14 9 7 11 1>.

2. Затем *T* разбивается на два вектора B_1 и B_2.

3. Матрица *A* умножается на векторы B_1 = {11,14, 9} и B_2 = {7, 11, 1}.

$$C_1=\begin{vmatrix}1 & 4 & 8\\ 3 & 7 & 2\\ 6 & 9 & 5\end{vmatrix}\times\begin{vmatrix}11\\ 14\\ 9\end{vmatrix}=\begin{vmatrix}11+56+72\\ 33+98+18\\ 66+126+45\end{vmatrix}=\begin{vmatrix}139\\ 149\\ 237\end{vmatrix}$$

$$C_2=\begin{vmatrix}1 & 4 & 8\\ 3 & 7 & 2\\ 6 & 9 & 5\end{vmatrix}\times\begin{vmatrix}7\\ 11\\ 1\end{vmatrix}=\begin{vmatrix}7+44+8\\ 21+77+2\\ 42+99+5\end{vmatrix}=\begin{vmatrix}59\\ 100\\ 146\end{vmatrix}$$

4.Зашифрованное слово записывается в виде последовательности чисел *C*=<139 149 237 59 100 146>.

Задача 1.16. Расшифровать *C*=<139 149 237 59 100 146> с помощью матрицы-ключа A.

$$A=\begin{vmatrix}1 & 4 & 8\\ 3 & 7 & 2\\ 6 & 9 & 5\end{vmatrix}$$

Решение.

1. Вычисляется определитель $|A|$

$$A=\begin{vmatrix}1 & 4 & 8\\ 3 & 7 & 2\\ 6 & 9 & 5\end{vmatrix}=(35+48+216)-(336+18+60)=299-414=-115$$

2. Определяется присоединенная матрица *A**.

$A_{ij}=(-1)^{i+j}M_{ij}$

$$A^*=\begin{vmatrix}17 & -3 & -15\\ 52 & -43 & 15\\ -48 & 22 & -5\end{vmatrix}$$

3. Вычисляется траспонированная матрица

$$A^T=\begin{vmatrix}17 & 52 & -48\\ -3 & -15 & 22\\ -15 & 15 & -5\end{vmatrix}$$

4. Вычисляется обратная матрица

$$A^{-1}=\begin{vmatrix} -\frac{17}{115} & -\frac{52}{115} & \frac{48}{115} \\ \frac{3}{115} & \frac{43}{115} & -\frac{22}{115} \\ \frac{15}{115} & -\frac{15}{115} & \frac{5}{115} \end{vmatrix}$$

5. Определяются векторы B_1 *и* B_2.

где C_1=<139 149 237>, C_2=<59 100 146>.

$$B_1=\begin{vmatrix} -\frac{17}{115} & -\frac{52}{115} & \frac{48}{115} \\ \frac{3}{115} & \frac{43}{115} & -\frac{22}{115} \\ \frac{15}{115} & -\frac{15}{115} & \frac{5}{115} \end{vmatrix} \times \begin{vmatrix} 139 \\ 149 \\ 237 \end{vmatrix} = \begin{vmatrix} 11 \\ 14 \\ 9 \end{vmatrix}$$

$$B_2=\begin{vmatrix} -\frac{17}{115} & -\frac{52}{115} & \frac{48}{115} \\ \frac{3}{115} & \frac{43}{115} & -\frac{22}{115} \\ \frac{15}{115} & -\frac{15}{115} & \frac{5}{115} \end{vmatrix} \times \begin{vmatrix} 59 \\ 100 \\ 146 \end{vmatrix} = \begin{vmatrix} 7 \\ 11 \\ 1 \end{vmatrix}$$

6.Получаем числовой эквивалент расшифрованного слова:

T=<11 14 9 7 11 1>, который заменяется символами, в результате получается исходное слово *КНИЖКА*.

2 Асимметричная криптосистема RSA
Расширенный алгоритм Евклида

1. Выбирают два больших простых числа p и q. Для большей криптостойкости p и q выбирают равной длины.
2. Вычисляют произведение: $n=pq$
3. Вычисляют $z=(p-1)(q-1)$ и выбирают число e взаимно простое с z, т.е. НОД $(e,z)=1$.
4. Для вычисления закрытого (секретного) ключа d решается сравнение

$$ed \equiv 1 \bmod z \qquad (1)$$

Решение (1) имеет вид $d=(-1)^{k-1}Q_{k-1}$

Для вычисления ключа d воспользуемся расширенным алгоритмом Евклида.

Для этого число $\frac{e}{z}$ обращается в конечную цепную дробь:

$$e = zq_0 + e_1$$
$$z = e_1q_1 + e_2$$

$$e_1 = e_2q_2 + e_3$$
$$e_2 = e_3q_3 + e_4$$
$$\ldots\ldots\ldots\ldots\ldots$$
$$e_{k-1} = e_{k-1}q_{k-1} + e_k$$
$$e_{k-1} = e_kq_k + 0$$

Цепная дробь имеет вид: $\frac{e}{z} = [q_0, q_1, q_2 \ldots q_k]$, а последовательности $\{P_n\}$ и$\{Q_n\}$ числителей и знаменателей подходящих дробей к цепной дроби определяются рекуррентно:

$$P_{-2}=0, \quad P_{-1}=1,$$
$$Q_{-2}=1, \quad Q_{-1}=0.$$
$$P_n = q_n \cdot P_{n-1} + P_{n-2} : n \geq 0$$

$$Q_n = q_n \cdot Q_{n-1} + Q_{n-2} : n \geq 0$$

Их вычисления удобно оформить в виде таблицы:

n	-2	-1	0	1	2	...	k-1	k
q_n			q_0	q_1	q_2		q_{k-1}	q_k
P_n	0	1	P_0	P_1	P_2		P_{k-1}	P_k
Q_n	1	0	Q_0	Q_1	Q_2		Q_{k-1}	Q_k

Параметры криптосистемы RSA

Открытый ключ:	n – произведение двух простых чисел p и q (p и q должны храниться в секрете); e – число, взаимно простое с z
Секретный ключ:	$d = e^{-1} \bmod z$ $\quad (d \cdot e = 1 \bmod z)$
Шифрование:	$C = m^e \bmod n$
Дешифрование:	$m = C^d \bmod n$

Задача 2.1. Решить уравнение $1181 \cdot x = 1 \bmod 1290816$

Решение: для нахождения x воспользуемся расширенным алгоритмом Евклида

$1181 = 1290816 \cdot 0 + 1181$ $\quad e = zq_0 + e_1$
$1290816 = 1181 \cdot 1092 + 1164$ $\quad z = e_1q_1 + e_2$
$1181 = 1164 \cdot 1 + 17$ $\quad e_1 = e_2q_2 + e_3$

$1164 = 17 \cdot 68 + 8$ $\quad e_2 = e_3 q_3 + e_4$

$17 = 8 \cdot 2 + 1$ $\quad e_3 = e_4 q_4 + e_5$

$8 = 1 \cdot 8 + 0$ $\quad e_4 = e_5 q_5 + e_6$

n	-2	-1	0	1	2	3	4	5
q_n			0	1092	1	68	2	8
P_n	0	1	0	1	1	69	139	1181
Q_n	1	0	1	1092	1093	75416	151925	1290816

$k = 5;\ \ x = (-1)^4 \cdot 151925 = 151925 \bmod (1290816)$

В самом деле, $1181 \cdot 151925 = 1290816 \cdot 139 + 1 = 1 \bmod 1290816$.

Задача 2.2. Абоненты А и В решили установить секретную переписку. А сгенерировал простые числа *p1* = 7 и *q1* = 23. В сгенерировал простые числа *p2* = 11 и *q2* = 17. А выбрал простое число *e1* = 7. В выбрал простое число *e2* = 9. Абонент А отсылает сообщение m = 3 абоненту В. Каковы секретные ключи абонентов? Как выглядит зашифрованное сообщение? Выполните шифрование и дешифрование.

Решение:

1. $161 = 7 \cdot 23 = n1$ $\qquad 187 = 11 \cdot 17 = n2$
2. $(7-1)(23-1) = 132 = z1$ $\qquad (11-1)(17-1) = 160 = z2$
3. $\begin{cases} 7 \cdot d_1 = 1 \bmod 132 \\ 9 \cdot d_2 = 1 \bmod 160 \end{cases} \rightarrow \begin{cases} d_1 = 19 \\ d_2 = 89 \end{cases}$
4. Шифрование: $\begin{cases} C = 3^9 \bmod (187) = 19683 \bmod (187) \\ C < 187 \end{cases} \rightarrow c = 48$
5. Расшифровка: $m = c^{89} \bmod 187 = 3$.

Задача 2.3. Пусть выбраны простые числа p = 47, q = 71 и случайное число (открытый ключ) e = 79.

Выполните шифрование и дешифрование в асимметричной криптосистеме для сообщения 6882326879666683.

Решение:

1. Открытый ключ *e* не имеет сомножителей с $Z = (p-1)(q-1) = 46 \cdot 2 = 3220$
2. Найдём секретный ключ *d* из условия

$$d \cdot e \bmod z = 1; \quad d \cdot 79 \bmod 3220 = 1 \to d = 1019$$

3. Разобьём сообщение на блоки:

Так как $n = p \cdot q = 47 \cdot 71 = 3337$, то блоки должны иметь длину меньшую, чем длина *n*. В данном случае ограничимся блоками по 3 разряда.

$$m_1 = 688$$
$$m_2 = 232$$
$$m_3 = 687$$
$$m_4 = 966$$
$$m_5 = 668$$
$$m_6 = 003$$

4. Теперь шифруем блоки

$$C_1 = 688^{79} \bmod 3337 = 1570$$

и так далее. Получим сообщение:

$$C = (C_1 C_2 C_3 C_4 C_5 C_6) = 1570\ \ 2756\ \ 2091\ 2276\ \ 2423\ \ 0158$$

C1 C2 C3 C4 C5 C6.

5. Для зашифрования используем ключ d = 1019

$m_1 = (1570)^{1019} \bmod 3337 = 688 m_1$ и т.д.

Задача 2.4 Зашифровать и расшифровать сообщение CAB. Для простоты вычислений использовать небольшие числа*:* $p=3$, $q=11$, открытый ключ $e=7$. Для вычисления секретного ключа d воспользоваться расширенным алгоритмом Евклида.

Решение

Действия пользователя В - получателя сообщения.

1. Выбирает p =3 и q =11.

2. Вычисляет модуль $n=p*q=3*11=33$.

3. Вычисляет значение функции Эйлера для n =33

$$z(33) = (p-1)(q - 1) = 2*10 = 20.$$

4. Выбирает в качестве открытого ключа e произвольное число с учетом выполнения условий:

$$1<e\leq 20, \ \text{НОД}\ (e, 20) = 1.$$

Пусть e = 7.

5. Вычисляет значение секретного ключа d, используя расширенный алгоритм Евклида при решении сравнения

$$d \equiv 7^{-1} \ (\text{mod}20).$$

Решение дает d = 3.

6. Пересылает пользователю А (отправителю) пару чисел (n = 33, e = 7).

Действия пользователя А-отправителя сообщения.

7. Представляет шифруемое сообщение как последовательность целых чисел в диапазоне 0 ... 32. Пусть буква А представляется как число 1, буква В – как число 2, буква С — как число 3. Тогда сообщение САВ можно представить как последовательность чисел 312, т.е. m_1, = 3, $m_2 = 1$, $m_3 = 2$.

8. Шифрует текст, представленный в виде последовательности чисел m_1,m_2 и m_3, используя ключ $e = 7$ и $n = 33$, по формуле

$m_i^e(modn) = m_i^7(mod33)$

Получает криптограмму:

$C_1 = 3^7(mod33) = 2187 (mod33) = 9$,

$C_2=1^7(mod\ 33) =1 (mod\ 33) =1$,

$C_3 = 2^7 (mod\ 33) =128 (mod\ 33) = 29$.

Отправляет пользователю В криптограмму: C_1,C_2, C_3 = 9,1,29.

Действия пользователя В.

9. Расшифровывает принятую криптограмму C_1, C_2, C_3, используя секретный ключ d=3, по формуле

$m_i= C_i^d(modn)$

Получает:

$m_i = 9^3(mod\ 33) = 729 (mod33) = 3$,

$m_2=l^3(mod\ 33) =1 (mod\ 33) =1$,

$m_3= 29^3 (mod\ 33)=24389 (mod\ 33)=2$.

Таким образом, восстановлено исходное сообщение: САВ

3 1 2

3 Симметричная криптосистема DES

Стандарт шифрования DES используется как официальный стандарт шифрования для несекретной информации правительства США. В России используется улучшенная модификация DES – стандарт ГОСТ28147-89.

DES представляет собой блочный шифр. Шифруются данные 64-битовыми блоками. DES является симметричным алгоритмом. Для шифрования и дешифрования используются одинаковые алгоритм и ключ. Длина ключа равна 56 битам. (Ключ обычно представляется 64-битным ключом, но каждый восьмой бит используется для проверки на чётность и игнорируется). Ключ, который может быть любым 56 битовым ключом, можно изменить в любой момент времени.

DES состоит из 16 циклов, в каждом из которых выполняется комбинация перестановок и подстановок. Криптостойкость системы полностью определяется ключом.

Задача 3.1. Предположим, что при известном ключе К для расшифровки сообщения, зашифрованного по стандарту DES,

требуется 100 мс. Допустим, атакующий, пытаясь расшифровать сообщение, перебирает ключи случайным образом. Какое время в среднем потребуется ему для взлома шифра?

Решение:

Длина ключа DES равна 56 бит.

Всего возможных комбинаций - 2^{56}.

В среднем потребуется время $\frac{1}{2}\cdot 100\cdot 2^{56} = 100\cdot 2^{55}$ (мс)

Задача 3.2. Обозначим через C,P,K шифротекст, открытый текст и ключ соответственно. Для процедуры шифрования и дешифрования на ключ K примем обозначения E_k и D_k.

$$C = E_k(P)$$

$$P = D_k(C)$$

Чтобы повысить криптостойкость блочного шифра предложите варианты двоичного шифрования на двух и трех разных ключах.

Решение:

Двойное шифрование

$$C = E_{k2}\left(E_{k1},(P)\right)$$

$$P = D_{k2}\left(D_{k1},(C)\right)$$

Тройное шифрование

$$C = E_{k1}\left(D_{k2},\left(E_{k1}(P)\right)\right)$$

На 2^x ключах

$$P = D_{k1}\left(E_{k2},\left(D_{k1}(C)\right)\right)$$

На 3^x ключах

$$C = E_{k3}\left(D_{k2},\left(E_{k1}(P)\right)\right)$$

$$P = D_{k3}\left(E_{k2}\left(D_{k1}(C)\right)\right)$$

4 Политика безопасности

Политика безопасности - это набор правил, которые регулируют управление, защиту и распределение ценной информации**.**

Политика безопасности включает:

1. Множество возможных операций над объектами.
2. Множество разрешенных операций для каждой пары «субьект-объект»

Существует два типа *политики безопасности:*

1. дискреционная;
2. мандатная.

Дискреционная политика определяет следующие правила.

1. Все субъекты (S) и объекты (O) должны быть идентифицированы.
2. Права доступа субъекта к объекту определяются на основе некоторого внешнего по отношению к системе правила.

Дискреционная политика задается матрицей доступа:

O / S	O_1	O_2	…	O_n
S_1	own, r, w			
S_2				
…				
S_n				

Множество прав доступа R=(own, r, w) включает права:
own - владение, *r* - чтение, w- запись.

Собственник (*own*) может определять права доступа других субъектов к данному объекту.

Мандатная политика определяет следующие правила.

1. Все субъекты и объекты должны быть идентифицированы.
2. Задан линейно упорядоченный набор меток секретности (решетка секретности).
3. Каждому объекту присваивается метка секретности, определяющая ценность содержащейся в нем информации.
4. Каждому субъекту присваивается метка секретности, определяющая уровень доверия к нему.

В мандатной политике вводится понятие информационного потока.

Информационный поток X→Y (X –источник, Y – получатель) разрешен тогда и только тогда, когда c (Y)≥c(X) по решетке секретности.

В системе с двумя доступами *r* и *w* мандатная политика определяет следующие правила доступа:

$$X \xrightarrow{R} Y \Leftrightarrow c(X) \geq c(Y)$$

$$X \xrightarrow{W} Y \Leftrightarrow c(X) \leq c(Y)$$

Мандатная политика устойчива к атакам «Троянским конём» в отличие от дискреционной политики.

Задача 4.1. В сети применяется дискреционная политика безопасности и матрица доступа имеет вид:

	O_1	O_2
U_1	own r w	w
U_2		own r w

Обозначения:

U_1 – законный пользователь;

U_2 - злоумышленник;

O_1- объект, содержащий ценную информацию;

O_2 - объект, содержащий программу «Троянский конь».

Показать, что злоумышленник U_2 может считать ценную информацию объекта O_1.

Решение:

1. Злоумышленник U_2 является собственником (own) программы O_2.
2. Злоумышленник U_2 заставляет U_1 каким-либо образом запустить программу «Троянский конь». Для этого O_2 может, например**,** выглядеть интересной компьютерной игрой.
3. Если пользователь U_1 обратится к O_2, то он запустит скрытую программу T («Троянский конь»). Эта программа завладеет правами доступа пользователя U_1, поскольку была им запущена.
4. Программа T, обладая правами доступа пользователя U_1, списывает (w) в объект O_2 информацию, содержащуюся в объекте O_1.
5. Злоумышленник U_2 владеет (own) объектом O_2 и, пользуясь своими правами, имеет возможность считать из объекта O_2 ценную информацию объекта O_1.

Задача 4.2. Покажите, что мандатная политика устойчива к атакам «Троянским конём».

Решение:

Пусть пользователи U_1 и U_2 находятся на разных уровнях доступа, т.е. $c(U_1)>c(U_2)$.

1. U_1 помещает в объект O_1 ценную информацию.
2. U_1 может записывать в объект O_1

$$U_1 \xrightarrow{w} O_1 \Leftrightarrow c(U_1) \le c(O_1).$$

3. Троянский конь T, содержащийся в объекте O_2, который может считать информацию из O_1, должен отражать соотношение:

$$O_1 \xrightarrow{w} O_2 \Leftrightarrow c(O_2) \geq c(O_1).$$

4. $\begin{cases} c(U_2) < c(U_1) \leq c(O_1) \\ c(O_2) \geq c(O_1) \end{cases} \rightarrow c(O_2) > c(U_2)$,

И тогда пользователь U_2 не имеет право прочитать из O_2 ($c(O_2) > c(U_2)$), что делает съём из O_1 и запись в O_2 бессмысленным.

Задачи для самопроверки и контрольной работы (шифрование и расшифрование)

1. Зашифровать методом простой перестановки сообщение: «Самолет привезет груз намного быстрее, чем машина». (СТЗЗГРМ АПЕНОЕВ МРТАБЕШ ОИГМЫЧИ ЛВРНСЕН ЕЕУОТМА).

2. Зашифровать методом простой перестановки сообщение: «Малыш научился выговаривать слова». Ключевое слово: «Осадки». (ЛГСИМИ СОЛВАА ЯВОАЛУ ВАВТЫЧ ЫРАЬШИ).

3. Зашифровать методом простой перестановки сообщение: «Караван верблюдов бредет в пустыне». Ключевое слово: «Осадки». (БВСЕКА ЛБТТАН ЮРЫВРВ ДЕНПАЕ ОДЕУВР).

4. Зашифровать методом простой перестановки сообщение: «Я оказалась в пробке по дороге домой». Ключевое слово: «Выступ». (ЯДВКОА ООПЕРЛ КМРПОА АОООГС ЗЙБДЕЬ).

5. Зашифровать сообщение «Тише едешь дальше будешь» по системе Цезаря с ключевым словом «Платон», k=5. (ИТУП ПЯПУЧ ЯЫБЧУП ЬЙЯПУЧ).

6. Зашифровать сообщение «Учение свет, а неучение тьма» по системе Цезаря с ключевым словом «Тюльпан», k=7. (ЖКЭНЮЭ ДЩЭЕ Ч НЭЖКЭНЮЭ ЕУАЧ).

7. Зашифровать сообщение «Знание-сила» по системе Цезаря с ключевым словом «Тюльпан», k=7. (ТНЧНЮЭ ДЮПЧ).

8. Зашифровать сообщение «Encryption passphrase» по системе Цезаря с ключевым словом «This», k=5. (ZEXKRGMSFE GVLLGIKVLZ).

9. Зашифровать сообщение «Right you are» по системе Цезаря с ключевым словом «This», k=5. (KSHIM RFN VKZ).

10. Зашифровать сообщение «To be or not to be» по системе Цезаря с ключевым словом «This», k=5. (MFWZFKEFMMFWZ).

11. Зашифровать сообщение «Speak English» по системе Цезаря с ключевым словом «This», k=5. (LGTVB ZEHCLI).

12. Зашифровать биграммным шифром Плейфейра текст «Средства». Ключевое слово «Карусель». (ЕУУЗЖЫНВ).

13. Зашифровать биграммным шифром Плейфейра текст «Птицефабрика». Ключевое слово «Карусель». (ТОЙХЗЭКВЛГАР).

14. Зашифровать биграммным шифром Плейфейра текст «Тиранозавр». Ключевое слово «Бумажный». (ФЗ СМ БФ ЕЖ ДО).

15. Зашифровать биграммным шифром Плейфейра текст «Булочник». Ключевое слово «Бумажный». (УМВЦЭБКЛ).

16. Зашифровать биграммным шифром Плейфейра текст «Шифрование». Ключевое слово «Бумажный». (ЭГХСЧОЖЫКЗ).

17. Зашифровать биграммным шифром Плейфейра текст «Информация». Ключевое слово «Бумажный». (ФИХПЩДЙСЛЭ).

18. Зашифровать биграммным шифром Плейфейра текст «Вылетаем седьмого». Ключевое слово «Бандероль». (ЗШБРПДБУ УНБЖХБЙН).

19. Зашифровать биграммным шифром Плейфейра текст «Все тайное станет явным». Ключевое слово «Бандероль». (ГП ДУ ОВ ДЛ НУ ПД ДР ЦЪ ГА ЧУ).

20. Зашифровать слово T_0 =<КНИЖКА> с помощью матрицы-ключа А.

$$A=\begin{vmatrix}1 & 5 & 2\\ 6 & 9 & 3\\ 4 & 7 & 8\end{vmatrix}$$

(Ответ: 99_219_214_64_144_113).