УВАЖАЕМЫЕ СТУДЕНТЫ! Изучите теоретические сведения к лабораторной работе, выполните практическое задание, дайте ответы на контрольные вопросы.

Результаты работы, фотоотчет, предоставить преподавателю на e-mail: r.bigangel@gmail.com до 06.03.2023.

Требования к отчету:

Отчет предоставляется преподавателю в электронном варианте и должен содержать:

- **название работы, постановку цели, вывод;**
- **ответы на контрольные вопросы, указанные преподавателем.**

При возникновении вопросов по приведенному материалу обращаться по следующему номеру телефона: (072)111-37-59, (Viber, WhatsApp), vk.com: https://vk.com/daykini

ВНИМАНИЕ!!! При отправке работы, не забывайте указывать ФИО студента, наименование дисциплины, дата проведения занятия (по расписанию).

Лабораторная работа №32
Тема: Криптография. Защита от несанкционированного доступа.
Введение

Появление новых информационных технологий и развитие мощных компьютерных систем хранения и обработки информации повысили уровни защиты информации и вызвали необходимость того, чтобы эффективность защиты информации росла вместе со сложностью архитектуры хранения данных. Постепенно защита информации становится обязательной: разрабатываются всевозможные документы по защите информации; формируются рекомендации; даже проводится ФЗ о защите информации, который рассматривает проблемы и задачи защиты информации, а также решает некоторые уникальные вопросы защиты информации.

Таким образом, угроза защиты информации сделала средства обеспечения информационной безопасности одной из обязательных характеристик информационной системы.

Под информационной безопасностью Российской Федерации (информационной системы) подразумевается техника защиты информации от преднамеренного или случайного несанкционированного доступа и нанесения тем

самым вреда нормальному процессу документооборота и обмена данными в системе, а также хищения, модификации и уничтожения информации.

Другими словами вопросы защиты информации решаются для того, чтобы изолировать нормально функционирующую информационную систему от несанкционированных управляющих воздействий и доступа посторонних лиц или программ к данным с целью хищения.

Под фразой «угрозы безопасности информационных систем» понимаются реальные или потенциально возможные действия или события, которые способны исказить хранящиеся в информационной системе данные, уничтожить их или использовать в каких-либо целях, не предусмотренных регламентом заранее.

Для обеспечения защиты информации в настоящее время не существует единого технического приема или средства, однако общим в решении многих проблем безопасности является использование криптографии и криптоподобных преобразований информации. Защита конфиденциальной информации, основанная на криптографической защите информации, шифрует данные при помощи семейства обратимых преобразований, каждое из которых описывается параметром, именуемым «ключом» и порядком, определяющим очередность применения каждого преобразования.

Защита информации в БД также является актуальной задачей как при единоличном использовании БД, так и при совместной работе пользователей с ней. Защита должна обеспечивать неизменность и целостность БД и содержащейся в ней информации, а также регламентировать права доступа к ней.

При корпоративной работе группы пользователей с одной базой данных необходимо выбрать администратора, обслуживающего БД и обладающего соответствующими правами доступа. Права доступа пользователей устанавливаются администратором, который может включать и исключать пользователей, разбивать их на группы. Пользователи, входящие в состав определенной группы, обладают всеми предоставленными ей правами. Если личные права пользователя выше прав доступа группы, то личные права за ним сохраняются.

Для организации эффективных мероприятий по защите информации требуется не только разработка модели механизмов защиты информации и средства защиты информации в сети, но также и реализация системного подхода по обеспечению безопасности информационных систем – использование комплекса взаимосвязанных мер по защите информации, включающих в себя специальные технические и программные средства.

1. Цель работы

Исследование основных методов криптографической зашиты информации.

2. Краткие сведения из теории

Криптография – обеспечивает сокрытие смысла сообщения с помощью шифрования и открытия его расшифрованием, которые выполняются по специальным алгоритмам с помощью ключей.

Ключ – конкретное секретное состояние некоторых параметров алгоритма криптографического преобразования данных, обеспечивающее выбор только одного варианта из всех возможных для данного алгоритма.

Криптоанализ – занимается вскрытием шифра без знания ключа (проверка устойчивости шифра).

Кодирование – (не относится к криптографии) – система условных обозначений, применяемых при передаче информации. Применяется для увеличения качества передачи информации, сжатия информации и для уменьшения стоимости хранения и передачи.

Криптографические преобразования имеют цель обеспечить недоступность информации для лиц, не имеющих ключа, и поддержание с требуемой надежностью обнаружения несанкционированных искажений.

Большинство средств защиты информации базируется на использовании криптографических шифров и процедур шифрования - расшифрования. В соответствии со стандартом ГОСТ 28147-89 под *шифром* понимают совокупность обратимых преобразований множества открытых данных на множество зашифрованных данных, задаваемых ключом и алгоритмом преобразования.

В криптографии используются следующие основные алгоритмы шифрования:

- алгоритм замены (подстановки) – символы шифруемого текста заменяются символами того же или другого алфавита в соответствии с заранее обусловленной схемой замены;
- алгоритм перестановки – символы шифруемого текста переставляются по определенному правилу в пределах некоторого блока этого текста;
- гаммирование – символы шифруемого текста складываются с символами некоторой случайной последовательности;
- аналитическое преобразование – преобразование шифруемого текста по некоторому аналитическому правилу (формуле).

Процессы шифрования и расшифрования осуществляются в рамках некоторой криптосистемы. Для **симметричной** криптосистемы характерно применение одного и того же ключа как при шифровании, так и при расшифровании сообщений. В **асимметричных** криптосистемах для зашифрования данных используется один (общедоступный) ключ, а для расшифрования – другой (секретный) ключ.

2.1. Симметричные криптосистемы

2.1.1.Шифры перестановки

В шифрах средних веков часто использовались таблицы, с помощью которых выполнялись простые процедуры шифрования, основанные на перестановке букв в сообщении. Ключом в данном случае является размеры таблицы. Например, сообщение “Неясное становится еще более непонятным” записывается в таблицу из 5 строк и 7 столбцов по столбцам.

Таблица 1

Н	О	Н	С	Б	Н	Я
Е	Е	О	Я	О	Е	Т
Я	С	В	Е	Л	П	Н
С	Т	И	Щ	Е	О	Ы
Н	А	Т	Е	Е	Н	М

Для получения шифрованного сообщения текст считывается по строкам и группируется по 5 букв:

НОНСБ НЯЕЕО ЯОЕТЯ СВЕЛП НСТИЩ ЕОЫНА ТЕЕНМ

Несколько большей стойкостью к раскрытию обладает *метод одиночной перестановки* по ключу. Он отличается от предыдущего тем, что столбцы таблицы переставляются по ключевому слову, фразе или набору чисел длиной в строку таблицы. Используя в качестве ключа слово - ЛУНАТИК, получим следующую таблицу

Таблица 2

Л	У	Н	А	Т	И	К			А	И	К	Л	Н	Т	У
4	7	5	1	6	2	3			1	2	3	4	5	6	7
Н	О	Н	С	Б	Н	Я			С	Н	Я	Н	Н	Б	О
Е	Е	О	Я	О	Е	Т			Я	Е	Т	Е	О	О	Е
Я	С	В	Е	Л	П	Н			Е	П	Н	Я	В	Л	С
С	Т	И	Щ	Е	О	Ы			Щ	О	Ы	С	И	Е	Т
Н	А	Т	Е	Е	Н	М			Е	Н	М	Н	Т	Е	А

До перестановки После перестановки

В верхней строке левой таблицы записан ключ, а номера под буквами ключа определены в соответствии с естественным порядком соответствующих букв ключа в алфавите. Если в ключе встретились бы одинаковые буквы, они бы нумеровались слева направо. Получается шифровка: СНЯНН БОЯЕТ ЕООЕЕ ПНЯВЛ СЩОЫС ИЕТЕН МНТЕА. Для обеспечения дополнительной скрытности можно повторно шифровать сообщение, которое уже было зашифровано. Для этого размер второй таблицы подбирают так, чтобы длины ее строк и столбцов отличались от длин строк и столбцов первой таблицы. Лучше всего, если они будут взаимно простыми.

Кроме алгоритмов одиночных перестановок применяются *алгоритмы двойных перестановок*. Сначала в таблицу записывается текст сообщения, а потом поочередно переставляются столбцы, а затем строки. При расшифровке порядок перестановок был обратный. Пример данного метода шифрования показан в следующих таблицах:

Двойная перестановка столбцов и строк

Таблица 3

	2	4	1	3		1	2	3	4		1	2	3	4
4	П	Р	И	Е	4	И	П	Е	Р	1	А	З	Ю	Ж
1	З	Ж	А	Ю	1	А	З	Ю	Ж	2	Е	-	С	Ш
2	-	Ш	Е	С	2	Е	-	С	Ш	З	Г	Т	О	О
3	Т	О	Г	О	3	Г	Т	О	О	4	И	П	Е	Р

В результате перестановки получена шифровка АЗЮЖЕ_СШГТООИПЕР. Ключом к шифру служат номера столбцов 2413 и номера строк 4123 исходной таблицы.

Число вариантов двойной перестановки достаточно быстро возрастает с увеличением размера таблицы: для таблицы 3 х 3 их 36, для 4 х 4 их 576, а для 5*5 их 14400.

В средние века для шифрования применялись и *магические квадраты*. Магическими квадратами называются квадратные таблицы с вписанными в их клетки последовательными натуральными числами, начиная с единицы, которые дают в сумме по каждому столбцу, каждой строке и каждой диагонали одно и то же число. Для шифрования необходимо вписать исходный текст по приведенной в квадрате нумерации и затем переписать содержимое таблицы по строкам. В результате получается шифротекст, сформированный благодаря перестановке букв исходного сообщения.

Таблица 4

П	Р	И	Е	З	Ж	А	Ю	_	Ш	Е	С	Т	О	Г	О
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16

16	3	2	13			О	И	Р	Т
5	10	11	8			З	Ш	Е	Ю
9	6	7	12			-	Ж	А	С
4	15	14	1			Е	Г	О	П

Число магических квадратов очень резко возрастает с увеличением размера его сторон: для таблицы 3*3 таких квадратов -1; для таблицы 4*4 – 880; а для таблицы 5*5-250000.

2.2. Шифры простой замены

Система шифрования Цезаря - частный случай шифра простой замены. Метод основан на замене каждой буквы сообщения на другую букву того же алфавита, путем смещения от исходной буквы на К букв.

Известная фраза Юлия Цезаря VENI VINI VICI – пришел, увидел, победил, зашифрованная с помощью данного метода, преобразуется в SBKF SFAF SFZF (при смещении на 4 символа).

Греческим писателем Полибием за 100 лет до н.э. был изобретен так называемый *полибианский квадрат* размером 5*5, заполненный алфавитом в случайном порядке. Греческий алфавит имеет 24 буквы, а 25-м символом является пробел. Для шифрования на квадрате находили букву текста и записывали в шифротекст букву, расположенную ниже ее в том же столбце. Если буква оказывалась в нижней строке таблицы, то брали верхнюю букву из того же столбца.

2.3. Шифры сложной замены

Шифр Гронсфельда состоит в модификации шифра Цезаря числовым ключом. Для этого под буквами сообщения записывают цифры числового ключа. Если ключ короче сообщения, то его запись циклически повторяют. Шифротекст получают примерно так же, как в шифре Цезаря, но отсчитывают не третью букву по алфавиту (как в шифре Цезаря), а ту, которая смещена по алфавиту на соответствующую цифру ключа.

Пусть в качестве ключа используется группа из трех цифр – 314, тогда

Сообщение СОВЕРШЕННО СЕКРЕТНО

Ключ 3143143143143143143

Шифровка ФПЖИСЬИОССАХИЛФИУСС

В *шифрах многоалфавитной замены* для шифрования каждого символа исходного сообщения применяется свой шифр простой замены (свой алфавит).

Таблица 5

	АБВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭЮЯ_
А	АБВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭЮЯ_
Б	_АБВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭЮЯ
В	Я_АБВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭЮ
Г	ЮЯ_АБВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭ
.	……
Я	ВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭЮЯ_АБ
_	БВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭЮЯ_А

Каждая строка в этой таблице соответствует одному шифру замены аналогично шифру Цезаря для алфавита, дополненного пробелом. При шифровании сообщения его выписывают в строку, а под ним ключ. Если ключ оказался короче сообщения, то его циклически повторяют. Шифротекст получают, находя символ в колонке таблицы по букве текста и строке, соответствующей букве ключа. Например, используя ключ АГАВА, из сообщения ПРИЕЗЖАЮ ШЕСТОГО получаем следующую шифровку:

Таблица 6

Сообщение	ПРИЕЗЖАЮ_ШЕСТОГО
Ключ	АГАВААГАВААГАВАА
Шифровка	ПНИГЗЖЮЮЮШЕОТМГО

В компьютере такая операция соответствует сложению кодов ASCII символов сообщения и ключа по модулю 256.

2.4. Гаммирование

Процесс зашифрования заключается в генерации гаммы шифра и наложении этой гаммы на исходный открытый текст. Перед шифрованием открытые данные разбиваются на блоки $Т(0)_i$ одинаковой длины (по 64 бита). Гамма шифра вырабатывается в виде последовательности блоков $Г(ш)_i$ аналогичной длины ($Т(ш)_i=Г(ш)_i+Т(0)_i$, где + - побитовое сложение, i =1-m).

Процесс расшифрования сводится к повторной генерации шифра текста и наложение этой гаммы на зашифрованные данные $Т(0)_i$=$Г(ш)_i$+$Т(ш)_i$.

Исходное сообщение из букв русского алфавита преобразуется в числовое сообщение заменой каждой его буквы числом по следующей таблице:

Таблица 7

Числовая замена букв														
А	Б	В	Г	Д	Е	Ж	З	И	К	Л	М	Н	О	П
00	01	02	03	04	05	06	07	08	09	10	11	12	13	14
Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Э	Ю	Я
15	16	17	18	19	20	21	22	23	24	25	26	27	28	29

$$\Omega_{i+1}= [(A_i + C_1 – 1) \bmod 30] + 1$$

Исходное сообщение ОТДУШКА. Для шифрования числового сообщения используется шифрующий отрезок последовательности A_1, A_2, ... подходящей длины, начинающийся с A_{100}:

Таблица 8

Остатки при делении на 30						
A_{100}	A_{101}	A_{102}	A_{103}	A_{104}	A_{105}	A_{106}
1	5	6	17	18	19	3

При шифровании каждое число числового сообщения складывается с соответствующим числом шифрующего отрезка. Затем вычисляется остаток от деления полученной суммы на 30, который по данной таблице заменяется буквой.

Таблица 9

Исходное сообщение	О	Т	Д	У	Ш	К	А
Числовое исходное сообщение	13	17	4	18	23	9	0
Шифрующий отрезок	1	5	6	17	8	19	3
Числовое шифрованное сообщение	14	23	10	5	1	28	3
Шифрованное сообщение	П	Ш	Л	Е	Б	Ю	Г

2.5. Асимметричные криптосистемы

2.5.1. Схема шифрования Эль Гамаля

Алгоритм шифрования Эль Гамаля основан на применении больших чисел для генерации открытого и закрытого ключа, криптостойкость же обусловлена сложностью вычисления дискретных логарифмов.

Последовательность действий пользователя:

1. Получатель сообщения выбирает большое, простое число P и большое целое число G, причем $P > G$.
2. Получатель выбирает секретный ключ - случайное целое число $X < P$.
3. Вычисляется открытый ключ $Y = G^X \bmod P$.
4. Получатель выбирает случайное целое число K, $1 < K < P-1$, такое, что числа K и (P-1) являются взаимно простыми.
5. Шифрование сообщения (M): $a = G^K \bmod P$, $b = Y^K M \bmod P$, где пара чисел (a,b) является шифротекстом.
6. Надо придумать сообщение M, зашифровать его, а потом с помощью секретного ключа X расшифровать сообщение.

Шифрование

1. Допустим что нужно зашифровать сообщение $M = 5$.
2. Произведем генерацию ключей :
    1. пусть $p = 11, g = 2$. Выберем $x = 8$- случайное целое число x такое,что $1 < x < p$.
    2. Вычислим $y = g^x \bmod p = 2^8 \bmod 11 = 3$.
    3. Итак , открытым является тройка $(p, g, y) = (11, 2, 3)$,а закрытым ключом является число $x = 8$.
3. Выбираем случайное целое число kтакое, что 1 < k < (p − 1). Пусть $k = 9$.
4. Вычисляем число $a = g^k \bmod p = 2^9 \bmod 11 = 512 \bmod 11 = 6$.
5. Вычисляем число $b = y^k M \bmod p = 3^9 5 \bmod 11 = 19683 \cdot 5 \bmod 11 = 9$.

6. Полученная пара $(a,b) = (6,9)$является шифротекстом.

Расшифрование

1. Необходимо получить сообщение $M = 5$по известному шифротексту $(a,b) = (6,9)$и закрытому ключу $x = 8$.
2. Вычисляем M по формуле :

$$M = b(a^x)^{-1} \mathrm{mod} p = 9(6^8)^{-1} \mod 11 = 5$$

3. Получили исходное сообщение $M = 5$.

2.5.2. Криптосистема шифрования данных RSA

Предложена в 1978 году авторами Rivest, Shamir и Aldeman и основана на трудности разложения больших целых чисел на простые сомножители.

Последовательность действий пользователя:

1. Получатель выбирает 2 больших простых целых числа *p* и *q*, на основе которых вычисляет *N*=*pq*; *M*=(*p*-1)(*q*-1).

2. Получатель выбирает целое случайное число *d*, которое является взаимопростым со значением *M*, и вычисляет значение *e* из условия *ed*=1/(mod *M*).

3. *d* и *N* публикуются как открытый ключ, *e* и *M* являются закрытым ключом.

4. Если *S* –сообщение и его длина: 1<Len(*S*)<*N*, то зашифровать этот текст можно как *S*'=S^d(mod *N*), то есть шифруется открытым ключом.

5. Получатель расшифровывает с помощью закрытого ключа: *S*=*S*'^{e}(mod *N*).

6. Представить шифруемое сообщение как последовательность целых чисел в диапазоне 0…32. Пусть буква А изображается числом 1, буква Б- числом 2, буква В- числом 3 и т.д. Тогда сообщение будет принимать вид числовой последовательности, которое зашифровывается с помощью открытого ключа. Надо расшифровать его с помощью закрытого ключа.

Зашифруем сообщение «САВ». Для простоты будем использовать маленькие числа (на практике применяются гораздо большие).

1. Выберем *p=3* и *q=11*.
2. Определим *n*=3*11=33.

3. Найдем *(p-1)(q-1)*=20. Следовательно, в качестве *d,* взаимнопростое с 20, например, *d*=3.
4. Выберем число *e*. В качестве такого числа может быть взято любое число, для которого удовлетворяет соотношение *(e*3)(mod20)=1*, например 7.
5. Представим шифруемое сообщение как последовательность целых чисел с помощью отображения: A1, B2, C3. Тогда сообщение принимает вид (3,1,2). Зашифруем сообщение с помощью ключа {7,33}.
   ШТ1 = (3^7) (mod 33) = 2187 (mod 33) = 9,
   ШТ2 = (1^7) (mod 33) = 1 (mod 33) = 1,
   ШТ3 = (2^7) (mod 33) = 128 (mod 33) = 29.
6. Расшифруем полученное зашифрованное сообщение (9,1,29) на основе закрытого ключа {3,33}:
   ИТ1 = (9^3) (mod 33) = 729 (mod 33) = 3,
   ИТ2 = (1^3) (mod 33) = 1 (mod 33) = 1,
   ИТ3 = (29^3) (mod 33) = 24389 (mod 33) = 2.

Итак в реальных системах алгоритм RSA реализуется следующим образом: каждый пользователь выбирает два больших числа, и в соответствии с описанным выше алгоритмом выбирает два простых числа *e* и *d*. Как результат умножения первых двух чисел (*p* и *q*) устанавливается *n*.
{e,n} образует открытый ключ, а *{d,n}* – закрытый (хотя можно взять и наоборот). Открытый ключ публикуется и доступен каждому, кто желает послать владельцу ключа сообщение, которое зашифровывается указанным алгоритмом. После шифрования, сообщение невозможно раскрыть с помощью открытого ключа. Владелец же закрытого ключа без труда может расшифровать принятое сообщение.

3. Задание к работе

Зашифровать любыми пятью методами свои данные: Фамилию, Имя, Отчество, любимую фразу.

Контрольные вопросы

1. Объяснить цель и задачи криптографии.

2. Шифры одиночной перестановки и перестановки по ключевому слову. Шифр Гронфельда.

3. Шифры двойной перестановки. Шифрование с помощью магического квадрата.

4. Шифр многоалфавитной замены и алгоритм его реализации.

5. Пояснить алгоритм шифрации двойным квадратом. Шифр Enigma.

6. Пояснить алгоритм шифрования DES.

7. Пояснить алгоритм шифрования ГОСТ 28147-89.

8. Пояснить алгоритм шифрования RSA.

9. Пояснить алгоритм шифрования Эль Гамаля.

10. Каковы задачи и алгоритмы электронной подписи?

11. Какие задачи распределения ключей?