МИНИСТЕРСТВО ПО РАЗВИТИЮ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
И КОММУНИКАЦИЙ РЕСПУБЛИКИ УЗБЕКИСТАН

ТАШКЕНТСКИЙ УНИВЕРСИТЕТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
ИМЕНИ МУХАММАДА АЛ-ХОРАЗМИЙ

ФАКУЛЬТЕТ ТЕЛЕКОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ

КАФЕДРА «СЕТИ И СИСТЕМЫ ПЕРЕДАЧИ ДАННЫХ»

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ТЕЛЕКОММУНИКАЦИЙ

Методические указания по выполнению практических работ
для направления бакалавриата 5350100- Телекоммуникационные технологии
(Телекоммуникации, Телерадиовещание, Мобильные системы)

Ташкент 2021

Авторы: Джураев Р.Х., Джаббаров Ш.Ю., Маткурбонов Д.М., Лазарев А.П., «Информационная безопасность телекоммуникаций. Методические указания по выполнению практических работ» / ТУИТ имени Мухаммада ал-Хоразмий, 61 с. Ташкент, 2021

Цель данных методических указаний – эффективно организовать процесс проведения практических работ по дисциплине «Информационная безопасность телекоммуникаций».

Рассматривая арифметику криптографических алгоритмов, в частности модульную арифметику, вычислении при подборе паролей и зашумленных кодов используемые при передаче данных по сетям студенты освоят теоретические и практические навыки.

Методические указания рассчитаны на использование в учебном процессе при подготовке бакалавров по направлению «Телекоммуникационные технологии». Продолжительность работ, приведенных в данных методических указаниях, составляет 24 академических часов.

Рецензент: PhD. доцент кафедры
«Обеспечение информационной безопасности» Насруллаев Н. Б

Введение

Сетевая безопасность охватывает множество мер и должна рассматриваться как часть общей политики, проводимой организацией (предприятием, компанией, фирмой) по информационной безопасности. В обеспечении безопасности сети занято много служб и используются различные средства. Эффективность компьютерной сети во многом зависит от степени защищенности обрабатываемой и передаваемой информации. Степень защищенности информации от различного вида угроз при ее получении, обработке, хранении, передаче и использовании называют безопасностью информации. Актуальность проблеме сетевой безопасности придает широкое использование компьютерных технологий во всех сферах жизни современного общества, а также переход от использования выделенных каналов к публичным сетям.

В разных программных и аппаратных продуктах, предназначенных для защиты данных, часто используются одинаковые подходы, приемы и технические решения, которые в совокупности образуют технологию безопасности. Одним из важных технологий при защите информаций является технология криптография, которая занимается методами преобразования информации в целях ее защиты.

В данных методических указаниях описаны открытые криптотехнологии обеспечивающие целостность, доступность и конфиденциалность информации в телекоммуникациях. Открытые криптотехнологии – ЭЦП, идентификация и аутентификация и т.п.. А также указаны математические основы криптографии и соответствующие методы защиты.

Практическая работа №1

ИССЛЕДОВАНИЕ АРИФМЕТИЧЕСКИХ ВЫЧИСЛЕНИЙ ПРИ РЕШЕНИИ КРИПТОГРАФИЧЕСКИХ ЗАДАЧ

Цель работы: Закрепление практических навыков математических преобразования, используемые в криптографии.

Краткие теоретические сведения

Где – любая из следующих операций: «+» сложение, «—» вычитание, «·» умножение.

1. Наибольший общий делитель

Наибольшим общим делителем (НОД, или англ. - *Greatest Common Divider - GCD*) целых чисел a_1, a_2, ..., a_n называется такой положительный общий делитель этих чисел, который делится на любой другой общий делитель этих чисел.

Пример:

НОД(21,15)=3;

НОД(27,44)=1;

НОД(120,66)=6.

2. Алгоритм Евклида

Используется для нахождения наибольшего общего делителя (НОД) двух чисел. Идея:

НОД(a, *б*) = НОД(b, *r*), где

$$a = b \cdot q + r$$

Пример: НОД(22, 8) = ?

22 = 8·2+6

(22, 8) = (8, 6)

8 = 6·1 +2 (8,

6) = (6, 2)

$6 = 2 \cdot 2 + 2$

(6, 2) = (2, 2)

$2 = 2 \cdot 1 + 0$

Получили: НОД(22, 8) = 2.

3. Бинарный алгоритм

Данный алгоритм также используется для нахождения наибольшего общего делителя 2-х чисел и базируется на следующих четырёх утверждениях:

1) если оба числа *a* и *b* - четные, то: НОД (a, *b*) = 2·НОД(a/2, b/2);

2) если *a* - четное, *b* - нечетное, то НОД *(a, b)* = НОД(a/2, *b*);

3) НОД(a, b) = НОД(b, a-b);

4) если a и b -нечетны, то (a-b)- четно.

Пример: НОД(1173, 323) = ?

(1173, 323) = (323, 850) = (323, 425) = (323, 102) = (323, 51) = (51, 272) = (51, 136) = (51, 68) = (51, 34) = (51, 17) = (17, 34) = (17, 17) = 17

Получили: НОД(1173, 323) = 17.

4. Простые числа

Положительное целое не равное нулю число называется простым, если оно делится только на самого себя и на единицу.

Примеры: 11 - простое; 29 - простое; 56 - составное ($56 = 7 \cdot 4 \cdot 2$).

Два числа *m* и *n* называются взаимно простыми, если они не имеют общих делителей кроме единицы, то есть наибольший общий делитель НОД(*m*, *n*) = 1.

5. Функция Эйлера

Функцией Эйлера $\varphi(n)$ $(n > 1)$ называют число положительных целых чисел меньших n и взаимно простых с *n*.

Примеры: $\varphi(1) = 0$; $\varphi(2) = 1$; $\varphi(3) = 2$; $\varphi(4) = 2$; $\varphi(5) = 4$; $\varphi(6) = 2$; $\varphi(7) =$

6; φ(8) = 4; φ(9) = 6; φ(10) = 4; φ(11) = 10.

Если n - простое число, то $\varphi(n) = n - 1$.

Пример: φ(31) =30.

Если $n=p*q$, где p и q - простые числа, то φ(n)=(p-1) · (q-1)

Пример: φ(35) = φ(5) · φ(7) = 4 · 6 = 24.

Обобщенный алгоритм вычисления функции Эйлера для произвольного числа n.

Если n представить как произведение простых чисел в соответствующих степенях:

$n = p_1^{a_1} \cdot p_2^{a_2} \cdot p_3^{a_3} \cdot \ldots \cdot p_r^{a_r}$ ($p_1, p_2, p_3, \ldots, p_r$ - простые),

то

$$\varphi(n) = n \cdot \left(1 - \frac{1}{p_1}\right) \cdot \left(1 - \frac{1}{p_2}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_r}\right).$$

Пример:

φ (2700) = ?

2700 но представить как $2^2 \cdot 3^3 \cdot 5^2$.

Тогда $\varphi(2700) = 2700 \cdot \left(1 - \frac{1}{2}\right) \cdot \left(1 - \frac{1}{3}\right) \cdot \left(1 - \frac{1}{5}\right) = 720$

6. Теорема Эйлера

Если $n > 0$ - положительное целое число и $(a, n) = 1$, где a - целое, то справедливо:

$$a^{\varphi(n)} = 1 \bmod n$$

Пример: 41^{126} = ? mod 127.

НОД(41,127) = 1.

φ (127) = 126. поэтому $41^{126} = 1$ mod 127.

Пример: 4^{336} = ? mod 377.

НОД(336,377) = 1.

377 13·29. 13 и 29 - простые числа, поэтому

$\varphi(377) = \varphi(13) \cdot \varphi(29) = 12 \cdot 28 = 336$. поэтому $4^{336} = 1$ mod 377.

7. Взаимообратные числа

Для числа n взаимообратным по модулю r называется такое число m, для которого выполняется:

$$(n \cdot m) mod\ r = 1$$

или

$$n \cdot m = 1\ mod\ r \qquad (1)$$

Доказательство: по теореме Эйлера: $n^{\varphi(n)} = 1\ mod\ r$ или

$$1 = n^{\varphi(n)} mod\ r \qquad (2)$$

Перемножив (1) и (2) получим: $n \cdot m = n^{\varphi(n)} mod\ r$, разделив обе части на n , получим: $m = n^{\varphi(n)-1} mod\ r$.

Пример:

Найти взаимообратное по модулю 7 для числа 4.

$$4 \cdot m = 1\ mod\ 7, m = 4^{\varphi(7)-1} mod\ 7 = 4^5 mod\ 7 = 2.$$

Проверка: $4 \cdot 2\ mod\ 7 = 8\ mod\ 7 = 1$.

8. Принципы модулярной арифметики

Модулярная арифметика основывается на следующем равенстве:

$$(a \cdot b) mod\ m = [(a\ mod\ m) \cdot (b\ mod\ m)] mod\ m, \qquad (3)$$

Данное равенство говорит о том, что вычисление $(a \cdot b)$ mod m в модулярной арифметике даёт тот же результат что и вычисление $(a \cdot b)$ в обычной целочисленной арифметике с последующим взятием остатка от деления полученного результата на m $(mod\ n)$.

Пример: $7 \cdot 9\ mod\ 5 = [(7\ mod\ 5) \cdot (9\ mod\ 5)] mod\ 5$.

Принципы модулярной арифметики также применимы к операции возведения в степень, поскольку возведение в степень эквивалентно многократному умножению.

Пример: Рассмотрим выражение 3^5 mod 7. Возведение 3 в степень 5 и затем взятие результата по модулю 7 может быть произведено следующим образом:

Поскольку $5 = 2 \cdot 2 + 1$, то $3^5 = 3^{2 \cdot 2 + 1} = (3^2)^2 \cdot 3^1$.

1) Возводим число 3 в квадрат: $3 \cdot 3 = 9$ (3^2)

2) Возводим результат в квадрат: $9 \cdot 9 = 81$ ($(3^2)^2$)

3) Умножаем на 3: $81 \cdot 3 = 243$ ($(3^2)^2 \cdot 3$)

4) Берём по модулю 7: $243 \bmod 7 = 5$.

Каждый из полученных промежуточных результатов может быть взят по модулю 7.

1) Возводим число 3 в квадрат: $3 \cdot 3 \bmod 7 = 2$

2) Возводим результат в квадрат: $2 \cdot 2 \bmod 7 = 4$

3) Умножаем на 3: $4 \cdot 3 \bmod 7 = 5$.

Задание

1. Вычислите НОД *(m, n)* по алгоритму Евклида.
2. Вычислите НОД *(m, n)* используя бинарный алгоритм.
3. Вычислите функцию Эйлера для n=... (произвольное число)
4. Покажите, что $a^b = 1 \bmod n$
5. Вычислите взаимообратное число для m по модулю r.
6. Покажите, что $m^n \bmod r = k$.

Контрольные вопросы

1. Что такое НОД?
2. Что представляет собой функция Эйлера?
3. Результат операции mod?
4. Как вычисляется взаимообратное число?

Варианты

Вариант 1
1. m=347, n=723;
2. m=112, n=679;
3. n=324;
4. a=4, b=336, n=377;
5. r=29, n=5;
6. n=8, m=7, r=13, k=3.

Вариант 2
1. m=552, n=874;
2. m=1934, n=725;
3. n=863;
4. a=6, b=480, n=527;
5. r=23, n=3;
6. n=8, m=5, r=19, k=4.

Вариант 3
1. m=1236, n=935;
2. m=1778, n=994;
3. n=632;
4. a=10, b=220, n=253;
5. r=26, n=5;
6. n=9, m=7, r=17, k=10.

Вариант 4
1. m=845, n=652;
2. m=964, n=1277;
3. n=953;
4. a=14, b=448, n=493;
5. r=55, n=6;
6. n=8, m=9, r=13, k=3.

Вариант 5
1. m=1974, n=528;
2. m=998, n=1285;
3. n=746;
4. a=13, b=504, n=551;
5. r=91, n=8;
6. n=9, m=7, r=19, k=4.

Вариант 6
1. m=1532, n=643;
2. m=994, n=778;
3. n=488;
4. a=13, b=672, n=731;
5. r=13, n=5;
6. n=4, m=11, r=7, k=4.

Вариант 7
1. m=2674, n=1699;
2. m=2674, n=1118;
3. n=886;
4. a=7, b=264, n=299;
5. r=18, n=7;
6. n=7, m=9, r=17, k=2.

Вариант 8
1. m=933, n=525;
2. m=525, n=1385;
3. n=724;
4. a=12, b=648, n=703;
5. r=26, n=11;
6. n=6, m=12, r=13, k=1.

Вариант 9
1. m=835, n=1562;
2. m=838, n=1200;
3. n=678;
4. a=8, b=360, n=407;
5. r=33, n=5;
6. n=9, m=8, r=19, k=18.

Вариант 10
1. m=2525, n=1186;
2. m=745, n=1375;
3. n=884;
4. a=15, b=756, n=817;
5. r=44, n=7;
6. n=9, m=5, r=17, k=12.

Вариант 11
1. m=472, n=844;
2. m=844, n=1483;
3. n=625;
4. a=24, b=936, n=1007;
5. r=28, n=7;
6. n=8, m=5, r=19, k=4.

Вариант 12
1. m=552, n=938;
2. m=938, n=1366;
3. n=728;
4. a=9, b=832, n=901;
5. r=32, n=9;
6. n=6, m=9, r=23, k=3.

Вариант 13
1. m=702, n=1157;
2. m=774, n=1266;
3. n=872;
4. a=8, b=624, n=689;
5. r=18, n=5;
6. n=9, m=8, r=17, k=8.

Вариант 14
1. m=1045, n=836;
2. m=686, n=1078;
3. n=842;
4. a=5, b=520, n=583;
5. r=25, n=6;
6. n=7, m=5, r=11, k=3.

Вариант 15
1. m=1265, n=2024;
2. m=1092, n=689;
3. n=634;
4. a=6, b=312, n=371;
5. r=16, n=3;
6. n=9, m=5, r=11, k=9.

Вариант 16
1. m=686, n=1078;
2. m=1045, n=836;
3. n=556;
4. a=8, b=624, n=689;
5. r=32, n=9;
6. n=9, m=8, r=19, k=18.

Вариант 17
1. m=1092, n=689;
2. m=1265, n=2024;
3. n=734;
4. a=14, b=448, n=493;
5. r=29, n=5;
6. n=8, m=5, r=19, k=4.

Вариант 18
1. m=938, n=1366;
2. m=552, n=938;
3. n=867;
4. a=7, b=264, n=299;
5. r=91, n=8;
6. n=8, m=9, r=13, k=3.

Вариант 19
1. m=994, n=778;
2. m=1532, n=643;
3. n=462;
4. a=10, b=220, n=253;
5. r=44, n=7;
6. n=11, m=4, r=17, k=13

Вариант 20
1. m=112, n=679;
2. m=347, n=723;
3. n=532;
4. a=15, b=756, n=817;
5. r=18, n=7;
6. n=9, m=5, r=11, k=9.

Вариант 21
1. m=998, n=1285;
2. m=1974, n=528;
3. n=474;
4. a=8, b=624, n=689;
5. r=33, n=5;
6. n=9, m=6, r=23, k=16.

Вариант 22
1. m=1934, n=725;
2. m=552, n=874;
3. n=375;
4. a=8, b=624, n=689;
5. r=25, n=6;
6. n=9, m=5, r=11, k=9.

Вариант 23
1. m=1778, n=994;
2. m=1236, n=935;
3. n=552;
4. a=5, b=520, n=583;
5. r=18, n=5;
6. n=6, m=9, r=23, k=3

Вариант 24
1. m=844, n=1483;
2. m=472, n=844;
3. n=423;
4. a=24, b=936, n=1007;
5. r=44, n=7;
6. n=8, m=9, r=19, k=17.

Вариант 25
1. m=1379, n=254;
2. m=1116, n=975;
3. n=752;
4. a=5, b=520, n=583;
5. r=17, n=14;
6. n=9, m=6, r=22, k=2.

Вариант 26
1. m=844, n=1483;
2. m=472, n=844;
3. n=493;
4. a=24, b=936, n=907;
5. r=31, n=9;
6. n=8, m=9, r=19, k=17.

Вариант 27
1. m=2778, n=1194;
2. m=2236, n=1135;
3. n=374;
4. a=5, b=510, n=511;
5. r=19, n=11;
6. n=9, m=5, r=23, k=11.

Вариант 28
1. m=2844, n=1483;
2. m=3472, n=1844;
3. n=925;
4. a=24, b=936, n=807;
5. r=47, n=7;
6. n=8, m=7, r=17, k=16.

Вариант 29
1. m=2778, n=1994;
2. m=2236, n=335;
3. n=472;
4. a=5, b=520, n=583;
5. r=19, n=7;
6. n=6, m=9, r=23, k=6.

Вариант 30
1. m=844, n=2483;
2. m=2472, n=544;
3. n=583;
4. a=7, b=936, n=1007
5. r=43, n=11;
6. n=8, m=5, r=17, k=16.

Практическая работа №2

ПАРОЛЬНЫЕ МЕТОДЫ В СИСТЕМЕ ЗАЩИТЫ ДАННЫХ

Цель работы: Целью работы является исследование структуры, характеристик, сильных и слабых сторон парольных систем защиты, закрепление на практике навыков по определению стойкости парольных систем, а также получение практических навыков по работе с парольными системами.

Краткие теоретические сведения

Характеристики парольных систем защиты

Парольная система защиты является «первым рубежом» на пути злоумышленника к защищаемой информации. Поэтому во многом от стойкости парольной системы защиты зависит успешность реализации злоумышленником своих замыслов. Существует множество реализаций парольных систем, в структуре которых можно выделить несколько наиболее важных компонентов:

- интерфейс пользователя;
- интерфейс администратора;
- база учетных записей пользователей;
- модуль сопряжения с другими подсистемами безопасности.

Несмотря на то, что существуют характерные угрозы, направленные на каждый из элементов парольной системы защиты, основные злоумышленные действия направлены на базу учетных записей, т.к. завладев и раскрыв эту базу, злоумышленник может зарегистрироваться в системе от имени любого санкционированного пользователя и скрытно выполнить любые действия. Поэтому информация, хранимая в базе учетных записей, должна быть надежно защищена.

В большинстве систем пользователи имеют возможность самостоятельно выбирать пароли или получают их от системных

администраторов. При этом для уменьшения деструктивного влияния описанного выше человеческого фактора необходимо реализовать ряд требований к выбору и использованию паролей:

- установление минимальной длины пароля.
- использование в пароле различных групп символов.
- проверка и отбраковка пароля по словарю.
- установление максимального срока действия пароля.
- ведение журнала истории паролей. Применение эвристического алгоритма, бракующего пароли на основании данных журнала истории.
- ограничение числа попыток ввода пароля.
- поддержка режима принудительной смены пароля пользователя.
- использование задержки при вводе неправильного пароля.
- запрет на выбор пароля самими пользователями и автоматическая генерация паролей.
- принудительная смена пароля при первой регистрации пользователя в системе.

Злоумышленник может реализовывать угрозы парольной системы защиты в двух режимах - интерактивном, т.е. с применением штатных средств парольной системы (интерфейса пользователя), и неинтерактивном (например, он может завладеть базой учетных записей и применить программу для определения паролей в этой базе). Наиболее опасным является неинтерактивный вариант, т.к. злоумышленник может скрытно и с большой скоростью «подбирать» пароли.

Для численной оценки параметров парольной системы защиты используются следующие показатели:

A — мощность алфавита паролей, т. е. то множество знаков, которое может применяться при вводе пароля.

L — длина пароля (в знаках). Может изменяться для обеспечения заданной стойкости парольной системы.

S — мощность пространства паролей, т. е. множество всех возможных паролей в системе.

Мощность пространства паролей связана с мощностью алфавита паролей и длиной паролей следующим выражением:

$$S=A^L.$$

V —скорость подбора пароля (соответственно различают скорость подбора пароля для интерактивного (1-2 паролей / минуту) и неинтерактивного (10 и более паролей / секунду) подбора паролей).

T — срок действия (жизни) пароля (обычно задается в днях).

P — вероятность подбора пароля в течение срока его действия.

Вероятность подбора пароля можно определить следующим образом:

$$P=V\cdot T/S.$$

В конкретной ситуации задают некоторые желательные значения для одних параметров (например, очень маленькое значение вероятности подбора пароля) и высчитывают остальные параметры.

Очевидно, что с увеличением длины пароля и/или мощности алфавита паролей вероятность подбора пароля уменьшается. А при увеличении срока жизни пароля, вероятность его подбора увеличивается.

Пример 1.

Задание: определить время перебора всех паролей, состоящих из 6 цифр.

Решение: алфавит составляют цифры (A=10). Длина пароля 6 символов (L=6). Таким образом, получаем количество вариантов: $S=A^L=10^6$ (паролей).

Примем скорость перебора паролей *V=10* Длина пароля 6 символов (L=6). Таким образом, получаем количество вариантов: $S=A^L=10^6$ (паролей).

Примем скорость перебора паролей *V=10* паролей/секунду. Получаем время перебора всех паролей

$$T = S / V = 10^5 \text{ секунд} \approx 1667 \text{ минут} \approx 28 \text{часов} \approx 1{,}2 \text{ дня}.$$

Примем, что после каждого из $m = 3$ неправильно введенных паролей идет пауза в $v = 5$ секунд. Получаем продолжительность всех пауз при переборе всех паролей

$T_{пауза}=(S\cdot v)/m = (10^6\cdot 5)/3 \approx 1666667$ секунд ≈ 27778 минут ≈ 463 часа ≈ 19.3 дня.

$T_{итог} = T + T_{пауза} = 1{,}2 + 19{,}3 \approx 20{,}5$ дня

Таким образом, за счет введения пауз при неправильном вводе пароля мы можем существенно увеличить время интерактивного подбора пароля.

Пример 2.

Определить минимальную длину пароля, алфавит которого состоит из 10 символов, время перебора которого было не меньше 10 лет.

Алфавит составляют символы A = 10.

Длина пароля рассчитывается: $L = \log_A S = \lg S$.

Определим количество вариантов $S = T \cdot V = 10$лет $\cdot$ 10паролей/сек. $= 10 \cdot 365 \cdot 24 \cdot 60 \cdot 60 \cdot 10 \approx 3{,}15 \cdot 10^9$ вариантов

Таким образом, получаем длину пароля: $L=\lg (3{,}15 \cdot 10^9) \approx 9{,}5$

Очевидно, что длина пароля должна быть не менее 10 символов.

Задание

1. Определить время перебора всех паролей со следующими параметрами (*См. Пример 1*):

- алфавит состоит из *A* символов;
- длина пароля символов *L;*
- скорость перебора *V* паролей в секунду.

После каждого из *m* неправильно введенных паролей идет пауза в *v* секунд

Таблица 2.1. Варианты к первой задаче

Вариант	*A*	*L*	*V*	*m*	*v*
1	10	4	2	1	2
2	8	2	3	2	2
3	5	6	3	5	6
4	6	7	2	1	3
5	10	5	2	3	2
6	10	3	5	7	2

продолжение таблицы 2.1.

7	12	4	5	2	1
8	15	3	2	5	3
9	20	2	6	7	3
10	8	5	5	1	2
11	8	3	2	4	3
12	9	5	3	0	7
13	6	5	5	5	2
14	12	4	3	5	3
15	4	7	4	7	2
16	10	7	3	5	2
17	8	6	8	4	8
18	7	5	4	5	1
19	9	4	5	3	6
20	5	6	10	3	5
21	10	4	5	4	4
22	8	5	2	5	1
23	9	6	4	4	3
24	8	7	5	3	5
25	7	5	3	5	7

2. Определить минимальную длину пароля, алфавит которого состоит из A символов, время перебора которого было не меньше T лет.

Скорость перебора V паролей в секунду (*См. Пример 2*).

Таблица 2.2. Варианты к второй задаче

Вариант	A	T	V
1	10	2	10
2	8	2	13
3	5	6	30
4	6	7	20
5	10	5	200
6	10	9	50
7	12	10	500

продолжение таблицы 2.2

Вариант	A	T	V
8	15	3	200
9	20	2	600
10	8	3	10
11	8	4	100
12	9	4	20
13	6	2	300
14	12	2	15
15	4	3	500
16	10	1	400
17	8	7	35
18	7	6	28
19	9	7	40
20	5	8	50
21	10	8	10
22	8	7	5
23	9	5	20
24	8	6	10
25	7	8	3

Контрольные вопросы

1. Перечислите основные компоненты парольных систем защиты;
2. Перечислите основные численные характеристики парольных систем защиты и их взаимосвязь между собой;
3. Какова зависимость между вероятностью подбора пароля и мощностью алфавита паролей при прочих равных характеристиках:
4. Перечислите особенности реализации парольных систем защиты, которые позволяют увеличить время подбора пароля методом тотального перебора;

Практическая работа №3

СИММЕТРИЧНЫЕ АЛГОРИТМЫ ШИФРОВАНИЯ ДАННЫХ

Цель работы: Получение теоретических и практических знаний связанные симметричными алгоритмами шифрования.

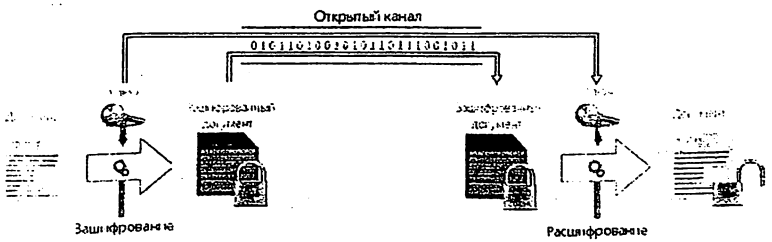
Краткие теоретические сведения

Шифрование — обратимое преобразование информации в целях скрытия от неавторизованных лиц, с предоставлением, в это же время, авторизованным пользователям доступа к ней. Главным образом, шифрование служит задачей соблюдения конфиденциальности передаваемой информации. Важной особенностью любого алгоритма шифрования является использование ключа, который утверждает выбор конкретного преобразования из совокупности возможных для данного алгоритма.

Не вдаваясь в технические подробности, можно сказать что шифрование — это преобразование данных для сокрытия информации.
Есть различные алгоритмы шифрования, мы же поверхностно познакомимся с основными актуальными алгоритмами шифрования.

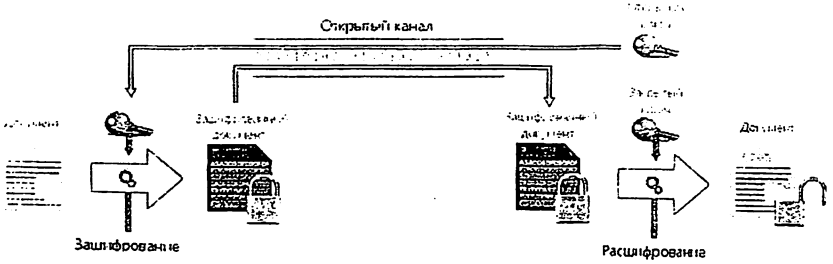
Алгоритмы шифрования делятся на симметричные алгоритмы и ассиметричные алгоритмы:

– Симметричное шифрование использует один и тот же ключ и для зашифровывания, и для расшифровывания (3.1. рис.).



3.1. рис. Симметричное шифрование.

– Асимметричное шифрование использует два разных ключа: один для зашифровывания (который также называется открытым), другой для расшифровывания (называется закрытым) (3.2. рис.).



3.2. рис. Асимметричное шифрование.

Шифр DES. DES (алгоритм шифрования данных) был выпущен в 1977 году и до сих пор является широко используемым симметричным алгоритмом, используемым в коммерческих системах защиты данных. Алгоритм DES шифрует 64-битные блоки. В основе алгоритма лежит сеть Фейстеля с 16 циклами (раундами) и ключом, имеющим длину 56 бит.

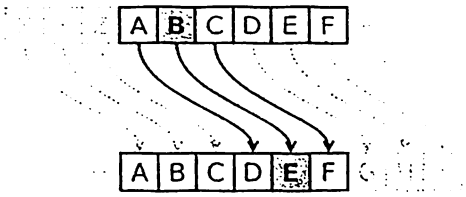
Прямым развитием DES в настоящее время является алгоритм Triple DES (3DES). В 3DES шифрование/расшифровка выполняются путём троекратного выполнения алгоритма DES.

Шифр AES — также известный как Rijndael (произносится [rɛinda:l] (Рэндал)) — симметричный алгоритм блочного шифрования (размер блока 128 бит, ключ 128/192/256 бит), принятый в качестве стандарта шифрования правительством США по результатам конкурса AES. Этот алгоритм хорошо проанализирован и сейчас широко используется, как это было с его предшественником DES.

Blowfish (произносится [блóуфиш]) — криптографический алгоритм, реализующий блочное симметричное шифрование с переменной длиной ключа. Разработан Брюсом Шнайером в 1993 году.

Шифр Цезаря. Метод Цезаря можно назвать методом перестановки. В методе Цезаря заменяемые буквы определяются переходом на число k. Юлий Цезарь использовал этот метод напрямую, когда k = 3.

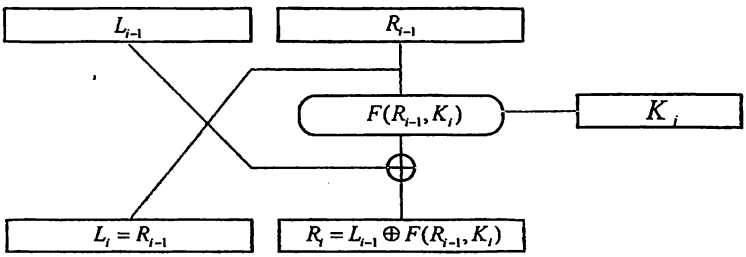
Когда k = 3 и буквы алфавита m = 26, формируется ситуация, показанная на следующем рисунке:



3.1-рис. шифр Цезаря.

Сеть Фейстелья. Использование сети Фейстелья распространено во многих алгоритмах симметричного блочного шифрования. Примерами этих криптоалгоритмов являются стандартные алгоритмы, такие как FEAL, LOCI, Lucifer, CAST, а также DES, ГОСТ 28147-89.

Идея сети Фейстелья выражается следующим образом. Зашифрованный блок разделен на две части L_0, R_0. Замена Фейстельского i – раунда итеративным блочным шифрованием определяется по следующей схеме:



3.2-расм. i – раунд сети Фейстелья

Пример: Необходимо шифровать следующий текст:

Кафедры Ташкентского университета информационных технологий

Шифрование приведенной выше текста выполняется в несколько шагов:

Шаг 1. Определяется количество букв (знаков) в заданном тексте. При подсчете количества символов каждый пробел - это один символ. В данном тексте 59 символов.

Шаг 2. Поместите этот текст в таблицу следующим образом. (Таблица выбрана так, чтобы уместить все символы. Например: 8x8 = 64, 10x6 = 60. Для повышения эффективности шифрования количество строк и столбцов выбирается из чисел, максимально приближенных друг к другу.

Ячейка, которая остается открытой, заполняется необязательным символом.

Таблица 3.1. Размещение информации в таблице

	1	2	3	4	5	6	7	8
1	К	а	ф	е	д	р	ы	—
2	Т	а	ш	к	е	н	т	с
3	к	о	г	о	у	н	и	в
4	е	р	с	и	т	е	т	а
5	—	и	н	ф	о	р	м	а
6	ц	и	о	н	н	ы	х	—
7	т	е	х	н	о	л	о	г
8	и	й	*	*	*	*	*	*

Шаг 3. Выбирается ключ шифрования. Ключ состоит из двух частей **Ключ – А** и **Ключ – Б.**

Ключ – А: может состоять из произвольной комбинаций порядквых номеров столбец . (7.1.2.5.3.4.6.8)

Ключ – Б: может состоять из произвольной комбинаций порядквых номеров строк (3.2.8.5.1.6.4.7)

Будем считать что эти ключи известны обеим сторонам обмена.

Шаг 4. Порядковые номера столбца заменяются ключом. По Ключу А заменяются столбцы.

Таблица 3.2. Замена столбцов по ключу А

Ключ – А								
	7	1	2	5	3	4	6	8
1	ы	К	а	д	ф	е	р	—
2	т	Т	а	е	ш	к	н	с
3	и	к	о	у	г	о	н	в
4	т	е	р	т	с	и	е	а
5	м	—	и	о	н	ф	р	а
6	х	ц	и	н	о	н	ы	—
7	о	т	е	о	х	н	л	г
8	*	и	й	*	*	*	*	*

Шаг 5. Создается таблица с номером столбец в возрастающем порядке с порядковыми номерами

Таблица 3.3. Замена строк по ключу Б

Ключ – Б									
	7	1	2	5	3	4	6	8
3	и	к	о	у	г	о	н	в
2	т	Т	а	е	ш	к	н	с
8	*	и	й	*	*	*	*	*
5	м	—	и	о	н	ф	р	а
1	ы	К	а	д	ф	е	р	—
6	х	ц	и	н	о	н	ы	—
4	т	е	р	т	с	и	е	а
7	о	т	е	о	х	н	л	г

Шаг 6. Создается таблица с номером строк в возрастающем порядке с порядковыми номерами

Таблица 3.4. Конечный результат

ы	К	а	д	ф	е	р	—
т	Т	а	е	ш	к	н	с
и	к	о	у	г	о	н	в
т	е	р	т	с	и	е	а
м	—	и	о	н	ф	р	а
х	ц	и	н	о	н	ы	—
о	т	е	о	х	н	л	г
*	и	й	*	*	*	*	*

В итоге получится шифр текст:

ыКадфер—тТаешкнсикоугонвтертсиеам—ионфрахциноны—отеохнлг*ий***

Процесс дешифрования выполняется в обратном порядке

Шаг 1: Принимающей стороне известны размер таблицы и ключи А и Б. Принимающая сторона с перва вставляет строки по **Ключу Б**:

Таблица 3.5. Обратный процесс по ключу Б

Ключ – Б		7	1	2	5	3	4	6	8
	3	и	к	о	у	г	о	н	в
	2	т	Т	а	е	ш	к	н	с
	8	*	и	й	*	*	*	*	*
	5	м	—	и	о	н	ф	р	а
	1	ы	К	а	д	ф	е	р	—
	6	х	ц	и	н	о	н	ы	—
	4	т	е	р	т	с	и	е	а
	7	о	т	е	о	х	н	л	г

Шаг 2: Принимающая сторона заменяет столбы по **Ключу А:**

Таблица 3.6. Обратный процесс по ключу А

Ключ А								
	7	1	2	5	3	4	6	8
3	К	а	ф	е	д	р	ы	—
2	Т	а	ш	к	е	н	т	с
8	к	о	г	о	у	н	и	в
5	е	р	с	и	т	е	т	а
1	—	и	н	ф	о	р	м	а
6	ц	и	о	н	н	ы	х	—
4	т	е	х	н	о	л	о	г
7	и	й	*	*	*	*	*	*

В итоге получит открытый текст:

Кафедры Ташкентского университета информационных технологий

Задание

1. По приведенному примеру студент шифрует/дешифрует свою Ф.И.О.

Контрольные вопросы

1) Что такое шифрование?

2) Принцип работы алгоритма шифрования DES.

3) Виды алгоритмов симметричного шифрования.

4) Основная разница симметричных и асимметричных алгоритмов шифрования.

5) Что такое открытый ключ?

Практическая работа №4

АЛГОРИТМЫ АСИММЕТРИЧНОГО ШИФРОВАНИЯ ДАННЫХ (АЛГОРИТМ RSA, DIFFIE-HELLMAN)

Цель работы: Данная практическая работа предназначена для получения базовых практических навыков по асимметричным алгоритмам шифрования информации; ознакомления такими алгоритмами как RSA и Diffie-Hellman.

Краткие теоретические сведения

В асимметричных криптосистемах процедуры прямого и обратного преобразования (шифрования и дешифрования) выполняются с использованием различных ключей и не имеют между собой очевидных и легко прослеживаемых связей, позволяющих по одному ключу определить другой (4.1. рис.). В такой системе знание ключа, с помощью которого производилось шифрование, не позволяет расшифровать исходное сообщение. Поэтому ключ шифрования не является секретным и, как правило, публикуется участником обмена для того, чтобы любой желающий мог послать ему зашифрованное сообщение.

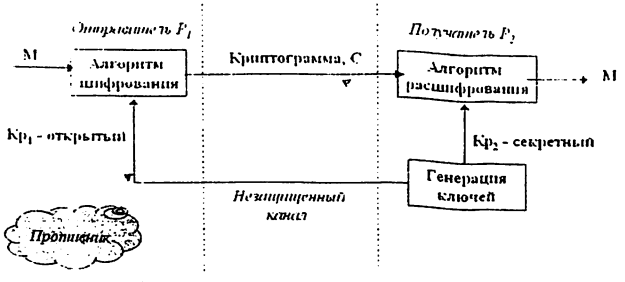


Рис. 4.1. Обобщенная схема асимметричной криптосистемы

Принцип функционирования асимметричной криптосистемы заключается в следующем:

- получатель генерирует два ключа (открытый и закрытый), и передает открытый ключ по незащищенному каналу отправителю;

- отправитель шифрует исходное сообщение, используя принятый открытый ключ;

- отправитель отправляет зашифрованное сообщение получателю по незащищенному каналу;

- получатель принимает зашифрованное сообщение и дешифрует его, используя закрытый ключ.

Одной из реализаций асимметричного шифрования является алгоритм RSA, предложенный в 1977 г. группой ученных, в которую входили Р. Ривест, А. Шамир и А. Аделман. Алгоритм RSA состоит из двух частей - генерация ключей и шифрование/дешифрование сообщения:

1. Генерация ключей:

1.1. Выбрать два различных случайных простых числа p и q заданного размера;

1.2. Вычислить их произведение $n = pq$, которое называется модулем;

1.3. Вычислить значение функции Эйлера $\phi(n) = (p - 1)(q - 1)$;

1.4. Выбрать целое число e взаимно простое со значением функции $\phi(n)$ и удовлетворяющее условию $e < \phi(n)$;

1.5. Выбрать число d такое, что $1 < d < \phi(n)$, а остаток от деления произведения de на значение функции $\phi(n)$ равен единице;

1.6. В качестве открытого ключа будет использоваться пара $\{e, n\}$, а в качестве закрытого - $\{d, n\}$.

2. Шифрование и дешифрование:

2.1. Разбить исходное сообщение на блоки m_i одинаковой длины. Каждый блок представляется в виде десятичного числа, меньшего n;

2.2. Шифр каждого блока m определяется по следующей формуле:

$c = mod(m^e, n)$;

2.3. Дешифрование каждого зашифрованного блока производится по следующей формуле:

$m = mod(c^d, n)$.

Выполнение практического задания.

Действия пользователя Б:

1. Выбираю два различных случайных простых числа p и q:

$p = 5, q = 7;$

2. Вычисляю их произведение n:

$n = pq = 5 \cdot 7 = 35;$

3. Вычисляю значение функции Эйлера от числа n:

$\Phi(n) = (p - 1)(q - 1) = (5 - 1)(7 - 1) = 4 \cdot 6 = 24;$

4. Выбираю целое число e взаимно простое со значением функции $\phi(n)$ и удовлетворяющее условию $e < \phi(n)$:

$e = 7;$

5. Выбирает число e такое, что $1 < d < \phi(n)$, а остаток от деления произведения de на значение функции $\phi(n)$ равен единице:

$$d = 7;$$

6. Открытым ключом будет $\{7, 35\}$, а закрытым - $\{7, 35\}$.

7. Пользователь Б передает открытый ключ $\{7, 35\}$ пользователю А.

Действия пользователя А:

Представляю сообщение в виде последовательности целых чисел $m1$-$m26$:

$m1 = 11; m2 = 11; m3 = 12; m4 = 13; m5 = 15; m6 = 11; m7 = 6; m8 = 9; m9 = 14;$
$m10 = 16; m11 = 3; m12 = 9; m13 = 14; m14 = 17; m15 = 6; m16 = 9; m17 = 16;$
$m18 = 4; m19 = 5; m20 = 8; m21 = 14; m22 = 13; m23 = 12; m24 = 5; m25 = 11;$
$m26 = 13$

1. Вычисляю зашифрованное значение каждого символа сообщения по

формуле $c = mod(m^e, n)$:

$c1 = mod(11^7, 35) = mod(19487171, 35) = 11$

$c2 = mod(11^7, 35) = mod(19487171, 35) = 11$

$c3 = mod(12^7, 35) = mod(35831808, 35) = 33$

$c4 = mod(13^7, 35) = mod(62748517, 35) = 27$

$c5 = mod(15^7, 35) = mod(170859375, 35) = 15$

$c6 = mod(11^7, 35) = mod(19487171, 35) = 11$

$c7 = mod(6^7, 35) = mod(279936, 35) = 6$

$c8 = mod(9^7, 35) = mod(4782969, 35) = 9$

$c9 = mod(14^7, 35) = mod(105413504, 35) = 14$

$c10 = mod(16^7, 35) = mod(268435456, 35) = 16$

$c11 = mod(3^7, 35) = mod(2187, 35) = 17$

$c12 = mod(9^7, 35) = mod(4782969, 35) = 9$

$c13 = mod(14^7, 35) = mod(105413504, 35) = 14$

$c14 = mod(17^7, 35) = mod(410338673, 35) = 3$

$c15 = mod(6^7, 35) = mod(279936, 35) = 6$

$c16 = mod(9^7, 35) = mod(4782969, 35) = 9$

$c17 = mod(16^7, 35) = mod(268435456, 35) = 16$

$c18 = mod(4^7, 35) = mod(16384, 35) = 4$

$c19 = mod(5^7, 35) = mod(78125, 35) = 5$

$c20 = mod(8^7, 35) = mod(2097152, 35) = 22$

$c21 = mod(14^7, 35) = mod(105413504, 35) = 14$

$c22 = mod(13^7, 35) = mod(62748517, 35) = 27$

$c23 = mod(12^7, 35) = mod(35831808, 35) = 33$

$c24 = mod(5^7, 35) = mod(78125, 35) = 5$

$c25 = mod(11^7, 35) = mod(19487171, 35) = 11$

$c26 = mod(13^7, 35) = mod(62748517, 35) = 27$

2. Передаю пользователю Б зашифрованное сообщение *{11 11 33 27 15 11 6 9 14 16 17 9 14 3 6 9 16 4 5 22 14 27 33 5 11 27}*.

Действия пользователя Б:

1. Вычисляю исходное значение каждого символа по следующей формуле $m = mod(d^{l}, n)$:

$m1 = mod(11^{7}, 35) = mod(19487171,35) = 11$

$m2 = mod(11^{7}, 35) = mod(19487171,35) = 11$

$m3 = mod(33^{7}, 35) = mod(42618442977,35) = 12$

$m4 = mod(27^{7}, 35) = mod(10460353203,35) = 13$

$m5 = mod(15^{7}, 35) = mod(170859375,35) = 15$

$m6 = mod(11^{7}, 35) = mod(19487171,35) = 11$

$m7 = mod(6^{7}, 35) = mod(279936,35) = 6$

$m8 = mod(9^{7}, 35) = mod(4782969,35) = 9$

$m9 = mod(14^{7}, 35) = mod(105413504,35) = 14$

$m10 = mod(16^{7}, 35) = mod(268435456,35) = 16$

$m11 = mod(17^{7}, 35) = mod(410338673,35) = 3$

$m12 = mod(9^{7}, 35) = mod(4782969,35) = 9$

$m13 = mod(14^{7}, 35) = mod(105413504,35) = 14$

$m14 = mod(3^{7}, 35) = mod(2187,35) = 17$

$m15 = mod(6^{7}, 35) = mod(279936,35) = 6$

$m16 = mod(9^{7}, 35) = mod(4782969,35) = 9$

$m17 = mod(16^{7}, 35) = mod(268435456,35) = 16$

$m18 = mod(4^{7}, 35) = mod(16384,35) = 4$

$m19 = mod(5^{7}, 35) = mod(78125,35) = 5$

$m20 = mod(22^{7}, 35) = mod(2494357888,35) = 8$

$m21 = mod(14^{7}, 35) = mod(105413504,35) = 14$

$m22 = mod(27^{7}, 35) = mod(10460353203,35) = 13$

$m23 = mod(33^{7}, 35) = mod(42618442977,35) = 12$

$m24 = mod(5^{7}, 35) = mod(78125,35) = 5$

$m25 = mod(11^{7}, 35) = mod(19487171,35) = 11$

$m26 = mod(27^{7}, 35) = mod(10460353203,35) = 13$

В результате он получает дешифрованное сообщение *{11 11 12 13 15 11 6 9 14 16 3 9 14 17 6 9 16 4 5 8 14 13 12 5 11 13}*

Таким образом, исходное сообщение будет восстановлено.

Алгоритм Диффи-Хеллмана

Алгоритм Диффи-Хеллмана (Diffie-Hellman) использует функцию дискретного возведения в степень. Сначала генерируются два больших простых числа n и q. Эти два числа не обязательно хранить в секрете. Далее один из партнеров P_1 генерирует случайное число x и посылает другому участнику будущих обменов P_2 значение

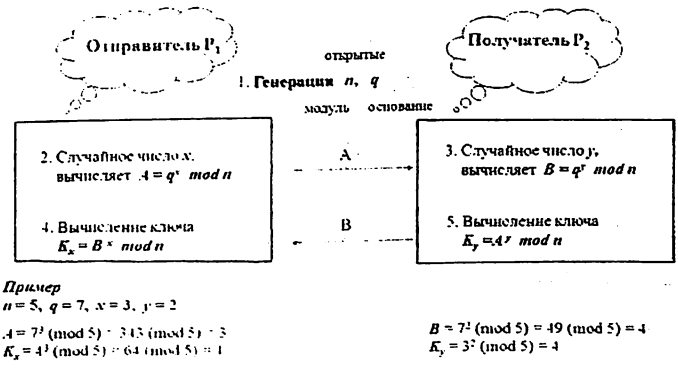
$$A=q^x \bmod n$$

По получении A партнер P_2 генерирует случайное число y и посылает участнику обмена P_1 вычисленное значение

$$B=q^y \bmod n$$

Партнер P 1 , получив B, вычисляет $K_x = B^x \bmod n$, а партнер P_2 вычисляет $K_y = A^y \bmod n$. Алгоритм гарантирует, что числа K_y и K_x равны и могут быть использованы в качестве секретного ключа для шифрования.

Ведь даже перехватив числа A и B, трудно вычислить K_x или K_y. Схематично, работа алгоритма Диффи-Хеллмана представлена на 4.2. рис.



4.2. рис. Алгоритм Диффи-Хеллмана

3. Задание

Используя алгоритм шифрования RSA зашифровать, а потом дешифровать сообщение в соответствии с вариантом.

Варианты

Таблица 4.1. варианты.

Вариант	Исходное сообщение
1	12 9 14 12 11 15 12 10 12 7 4 8 14 2 14 11 6 15 15 4 8 4 13 17 6 6
2	4 12 15 5 3 11 11 16 9 17 7 4 3 3 6 10 4 12 11 2 6 11 3 2 2 17
3	15 8 6 5 12 5 11 17 15 5 11 12 5 14 7 14 6 6 14 13 9 12 12 5 2 10
4	9 14 7 11 7 8 9 11 8 14 11 3 2 12 10 4 2 5 14 8 6 17 14 17 3 5
5	13 5 14 8 9 14 12 11 13 17 4 5 9 5 14 2 15 3 4 4 17 3 9 17 15 9
6	13 10 16 14 12 15 14 11 15 4 16 17 8 2 6 15 7 11 16 4 5 11 7 2 15 17
7	11 11 12 13 15 11 6 9 14 16 3 9 14 17 6 9 16 4 5 8 14 13 12 5 11 13
8	14 9 5 6 4 8 14 6 6 9 15 2 6 5 4 11 7 15 2 14 2 11 17 8 12 16
9	11 7 12 14 15 3 14 11 16 9 15 2 8 14 2 11 17 11 15 10 6 5 2 11 14 10
10	3 14 15 10 10 9 14 13 3 15 15 12 17 15 17 13 10 3 6 11 13 7 6 6 2 7
11	7 10 6 5 13 11 5 15 6 3 15 10 5 7 6 7 14 14 3 10 2 3 9 14 11 15
12	5 5 14 8 7 11 10 3 2 13 2 7 12 11 5 16 3 10 7 11 4 8 2 3 2 4
13	3 13 15 15 4 10 15 16 4 8 16 4 12 2 9 7 8 3 4 13 6 4 14 12 6 2
14	6 2 14 14 14 3 11 13 10 12 7 14 11 4 15 8 6 15 12 16 3 8 4 10 17 3
15	13 2 4 3 2 16 14 11 16 13 12 17 15 15 5 15 8 17 3 11 15 12 3 7 12 14
16	6 5 6 12 12 4 5 4 5 16 4 4 7 11 7 7 15 16 8 14 9 17 10 16 9 14
17	3 2 14 8 14 5 13 9 15 16 14 3 11 10 15 6 11 6 4 11 14 10 16 15 6 4
18	2 11 7 12 9 12 13 15 3 13 9 8 15 6 13 3 6 3 6 17 6 16 11 7 10 15
19	3 9 14 6 16 8 4 13 3 16 16 14 14 16 10 14 14 11 10 17 5 10 11 14 16 6
20	16 16 10 13 3 4 9 17 2 10 8 11 17 6 14 9 2 5 16 16 11 17 10 8 11 11

Контрольные вопросы

1. Что такое шифрования?
2. Принцип работы алгоритм шифровании RSA?
3. Принцип работы алгоритм шифровании Диффи-Хеллмана
4. Что такое дешифрования?
5. Основные отличий ассиметричного шифрования от симметричного шифрования?
6. Что такое открытый ключ?
7. Что такое закрытый ключ?
8. В чём заключаются достоинства и недостатки асимметричных алгоритмов?
9. В чём заключаются достоинства и недостатки симметричных алгоритмов?

Практическая работа №5

ШИФРОВАНИЕ И ДЕШИФРОВАНИЕ ДАННЫХ ПО АЛГОРИТМУ ЭЛЬ-ГАМАЛЯ

Цель работы: Данная практическая работа предназначена для получения базовых практических навыков по асимметричным алгоритмам шифрования данных, ознакомления с алгоритмом Эль-Гамаля.

Краткие теоретические сведения

Еще одной из реализаций асимметричного шифрования является алгоритм, разработанный Эль-Гамалем в 1985 г.

1. Генерация ключей:

1.1. Выбрать случайное простое число p;

1.2. Выбрать наименьшее целое положительное число $g < p$, такое, что $mod(g^{p-1}, p) = 1$ и $mod(g^i, p) \neq 1$ для любого целого числа $i < p-1$;

1.3. Выбрать случайное число x, такое, что $1 < x < p-1$;

1.4. Вычислить число y по следующей формуле:

$$y = mod(g^x, p);$$

1.5. В качестве открытого ключа выбирается набор чисел $\{y, g, p\}$, а в качестве закрытого – число x.

2. Шифрование и дешифрование:

2.1. Разбить исходное сообщение на блоки m_i одинаковой длины. Каждый блок представляется в виде десятичного числа;

2.2. Выбирать случайное число k, такое, что выполняется условие $1 < k < p-1$;

2.3. Вычисляется число a:

$$a = mod(g^k, p);$$

2.4. Вычисляется число b:

$$b = mod(y^k \cdot m, p);$$

2.5. Дешифрование производится по следующей формуле:

$$m = mod(b \cdot a^{p-1-x}, p).$$

Рассмотрим следующий пример. Пользователь А хочет передать пользователю Б сообщение «10 2 5 7» в зашифрованном виде, используя алгоритм Эль-Гамаля. Для представления передаваемого сообщения используются целые числа в диапазоне от 1 до 33,причем букве «А» соответствует число 1, букве «Б» – 2 и т.д.

Действия пользователя Б:

1. Выбирает случайное простое число p:

$$p = 23;$$

2. Выбирает наименьшее целое положительное число g, такое, что $mod(g^{p-1}, p)=1$ и $mod(g^i, p) \neq 1$ для любого целого числа $i < p-1$:

$$g = 2;$$

3. Выбирает случайное число x, такое, что $1 < x < p$:

$$x = 8;$$

4. Вычисляет число y по формуле $y = mod(g^x, p)$:

$$y = mod(2^8, 23) = 3;$$

5. Открытым ключом будет набор чисел $\{3, 2, 23\}$, а закрытым – число 8. Пользователь Б передает открытый ключ $\{3, 2, 13\}$ пользователю А.

Действия пользователя А:

1. Представляет сообщение «10 2 5 7» в виде последовательности целых чисел $m1$-$m4$:

$$m1 = 10, m2 = 2, m3 = 5, m4 = 7;$$

2. Выбирает случайное число k, такое, что выполняется условие $1 < k < p-1$:

$$k = 8;$$

3. Вычисляет значение числа a:

$$a = mod(g^k, p) = mod(2^8, 23) = 3;$$

4. Вычисляет значения числа b:

$$b_1 = mod(y^k \cdot m_1, p) = mod(3^8 \cdot 10, 23) = 14,$$

$$b_2 = mod(y^k \cdot m_2, p) = mod(3^8 \cdot 2, 23) = 12,$$

$$b_3 = mod(y^k \cdot m_3, p) = mod(3^8 \cdot 5, 23) = 7,$$

$$b_4 = mod(y^k \cdot m_4, p) = mod(3^8 \cdot 7, 23) = 19;$$

5. Передает пользователю Б зашифрованное сообщение {3 14 3 12 3 7 3 19}.

Действия пользователя Б:

1. Вычисляет исходное значение каждого символа по формуле

$$m=mod(b*a^{p-1-x},p):$$

$$m_1 = mod(b_1 \cdot a^{p-1-x}, p) = mod(14 \cdot 3^{14}, 23) = 10,$$

$$m_2 = mod(b_2 \cdot a^{p-1-x}, p) = mod(12 \cdot 3^{14}, 23) = 2,$$

$$m_3 = mod(b_3 \cdot a^{p-1-x}, p) = mod(7 \cdot 3^{14}, 23) = 5,$$

$$m_4 = mod(b_4 \cdot a^{p-1-x}, p) = mod(19 \cdot 3^{14}, 23) = 7.$$

Таким образом, исходное сообщение будет восстановлено.

3. Задание

Используя алгоритм шифрования Эль-Гамаля зашифровать, а потом дешифровать сообщение в соответствии с вариантом.

Варианты

Таблица 5.1. варианты

Вариант	Исходное сообщение
1	12 9 14 12 11 15 12 10 12 7 4 8 14 2 14 11 6 15 15 4 8 4 13 17 6 6
2	4 12 15 5 3 11 11 16 9 17 7 4 3 3 6 10 4 12 11 2 6 11 3 2 2 17
3	15 8 6 5 12 5 11 17 15 5 11 12 5 14 7 14 6 6 14 13 9 12 12 5 2 10
4	9 14 7 11 7 8 9 11 8 14 11 3 2 12 10 4 2 5 14 8 6 17 14 17 3 5
5	13 5 14 8 9 14 12 11 13 17 4 5 9 5 14 2 15 3 4 4 17 3 9 17 15 9
6	13 10 16 14 12 15 14 11 15 4 16 17 8 2 6 15 7 11 16 4 5 11 7 2 15 1
7	11 11 12 13 15 11 6 9 14 16 3 9 14 17 6 9 16 4 5 8 14 13 12 5 11 13
8	14 9 5 6 4 8 14 6 6 9 15 2 6 5 4 11 7 15 2 14 2 11 17 8 12 16
9	11 7 12 14 15 3 14 11 16 9 15 2 8 14 2 11 17 11 15 10 6 5 2 11 14 1
10	3 14 15 10 10 9 14 13 3 15 15 12 17 15 17 13 10 3 6 11 13 7 6 6 2 7
11	7 10 6 5 13 11 5 15 6 3 15 10 5 7 6 7 14 14 3 10 2 3 9 14 11 15

Продолжение таблицы 5.1.

12	5 5 14 8 7 11 10 3 2 13 2 7 12 11 5 16 3 10 7 11 4 8 2 3 2 4
13	3 13 15 15 4 10 15 16 4 8 16 4 12 2 9 7 8 3 4 13 6 4 14 12 6 2
14	6 2 14 14 14 3 11 13 10 12 7 14 11 4 15 8 6 15 12 16 3 8 4 10 17 3
15	13 2 4 3 2 16 14 11 16 13 12 17 15 15 5 15 8 17 3 11 15 12 3 7 12 1
16	6 5 6 12 12 4 5 4 5 16 4 4 7 11 7 7 15 16 8 14 9 17 10 16 9 14
17	3 2 14 8 14 5 13 9 15 16 14 3 11 10 15 6 11 6 4 11 14 10 16 15 6 4
18	2 11 7 12 9 12 13 15 3 13 9 8 15 6 13 3 6 3 6 17 6 16 11 7 10 15
19	3 9 14 6 16 8 4 13 3 16 16 14 14 16 10 14 14 11 10 17 5 10 11 14 16
20	16 16 10 13 3 4 9 17 2 10 8 11 17 6 14 9 2 5 16 16 11 17 10 8 11 11
21	15 2 6 5 4 11 7 15 2 14 15 7 10 5 7 6 7 14 14 3 10 6 11 6 8 11 13
22	7 10 5 7 6 7 14 14 3 2 11 7 12 9 12 13 15 3 13 9 9 8 15 6 7 6 7 14
23	13 15 11 6 9 14 16 3 9 14 17 6 9 16 14 5 13 9 15 16 14 8 9 10 7 6
24	11 7 12 9 12 13 15 3 13 9 8 15 6 13 3 9 8 15 6 13 3 6 3 6 17 6 8 7 9
25	8 2 6 15 7 10 5 7 6 7 14 14 3 10 14 8 14 5 13 9 15 16 14 3 8 7 11 8
26	15 14 11 15 4 16 17 8 2 6 15 7 11 16 4 11 13 10 12 7 14 11 4 15 7

Контрольные вопросы

1) Что такое шифрования?

2) Что такое дешифрования?

3) Основные отличий ассиметричного шифрования от симметричного шифрования?

4) Какие виды асимметричные алгоритмы шифрования информации?

5) Принцип работы ассиметричного шифрования?

6) Принцип работы алгоритм шифровании Эл-Гамалья?

Практическая работа №6

СОЗДАНИЕ И ПРОВЕРКА ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ

Цель работы: Данная практическая работа предназначена для получения базовых практических навыков по асимметричным алгоритмам шифрования данных.

Краткие теоретические сведения

Электронная цифровая подпись (ЭЦП) – средство, позволяющее на основе криптографических методов надежно установить авторство и подлинность документа. Важнейшей задачей является создание таких условий для использования ЭЦП, которые обеспечили бы ее надежность и позволили бы с высокой степенью уверенности определять подделки как самой ЭЦП, так и заверенных ею документов.

ЭЦП позволяет заменить при электронном (безбумажном) документообороте традиционную печать и подпись. При построении ЭЦП вместо обычной связи между печатью или рукописной подписью и листом бумаги выступает сложная математическая зависимость между документом, секретным и общедоступным ключом, а также цифровой подписью. Каждый абонент, обладающий правом подписи, самостоятельно формирует два ключа подписи – секретный и открытый.

Наличие секретного ключа гарантирует невозможность подделки злоумышленником документа и цифровой подписи от имени заверяющего. Каждый пользователь системы ЭЦП должен обеспечить сохранение в тайне своего секретного ключа.

Открытый ключ вычисляется как значение некоторой функции от секретного, но знание открытого ключа не дает возможности определить секретный ключ. Открытый ключ может быть опубликован и использоваться для проверки подлинности документа и цифровой подписи, а также для

предупреждения мошенничества со стороны, заверяющего в виде отказа его от подписи документа.

Для выработки ЭЦП подписываемый документ подвергается хешированию, а полученный хеш-документ (дайджест) зашифровывается закрытым ключом. Хеширование применяется для сокращения объема шифруемой информации и повышению производительности системы. Хеш-функция, не будучи взаимно-однозначным отображением, подбирается таким образом, чтобы было практически невозможно изменить документ, сохранить результат хешированием. По дайджесту невозможно установить исходный документ.

Хеш-функцией называется преобразование данных, переводящее последовательность символов M произвольной длины в последовательность символов $H(M)$ заданной длины.

Хеш-функция $H(M)$ должна удовлетворять следующим требованиям:

- хеш-функция $H(M)$ должна 1094 _uc2bq

- по известному значению хеш-функции $H(M)$ должно быть невозможно найти исходное сообщение M;

- для известного значения хеш-функции $H(M_1)$ должно быть невозможно найти такое отличное от исходного сообщение M_2 (т.е. $M_2 \neq M_1$), что $H(M_1) = H(M_2)$.

При нахождении хеш-образа исходное сообщение разбивается на отдельные блоки (символы), к которым применяется функция вида $Hi = f(Hi-1, Mi)$.

Значение, полученное после обработки последнего блока (символа), будет являться хеш-образом всего сообщения.

Рассмотрим один их простейших алгоритмов вычисления хеш-функции сообщения:

1. Выбрать два простых числа p и q;

2. Вычислить их произведение $n = p \cdot q$;

3. Выбрать произвольное число H_0;

4. Хеш-функция H_i сообщения M будет определяться следующим образом:

$$Hi = \mathrm{mod}((H_{i-1} + M_i)^2, n)$$

где M_i – i-ый символ сообщения.

При этом количество итераций при вычислении хеш-функции будет равно количеству символов в исходном сообщении.

Рассмотрим следующий пример. Пусть требуется определить значение хеш-функции сообщения [10 08 17 02 04 15 12 02].

1. Выбираем два простых числа p и q:

$$p = 13, q = 19;$$

2. Вычисляем произведение n:

$$n = p \cdot q = 13 \cdot 19 = 247;$$

3. Выбираем случайное число H_0:

$$H_0 = 8$$

4. Итеративно вычисляем значение хеш-функции сообщения:

$H_1 = \mathrm{mod}((H_0 + M_1)^2, n) = \mathrm{mod}((8 + 10)^2, 247) = \mathrm{mod}\ (324, 247) = 77$

$H_2 = \mathrm{mod}((H_1 + M_2)^2, n) = \mathrm{mod}((77 + 8)^2, 247) = \mathrm{mod}\ (7225, 247) = 62$

$H_3 = \mathrm{mod}((H_2 + M_3)^2, n) = \mathrm{mod}((62 + 17)^2, 247) = \mathrm{mod}\ (6241, 247) = 66$

$H_4 = \mathrm{mod}((H_3 + M_4)^2, n) = \mathrm{mod}((66 + 2)^2, 247) = \mathrm{mod}\ (4624, 247) = 178$

$H_5 = \mathrm{mod}((H_4 + M_5)^2, n) = \mathrm{mod}((178 + 4)^2, 247) = \mathrm{mod}\ (33124, 247) = 26$

$H_6 = \mathrm{mod}((H_5 + M_6)^2, n) = \mathrm{mod}((26 + 15)^2, 247) = \mathrm{mod}\ (1681, 247) = 199$

$H_7 = \mathrm{mod}((H_6 + M_7)^2, n) = \mathrm{mod}((199 + 12)^2, 247) = \mathrm{mod}\ (44521, 247) = 61$

$H_8 = \mathrm{mod}((H_7 + M_8)^2, n) = \mathrm{mod}((61 + 2)^2, 247) = \mathrm{mod}\ (3969, 247) = 17$

Таким образом, значение хеш-функции исходного сообщения $H(M) = 17$.

Значение хеш-функции исходного сообщения $H(M)=17$ шифруется согласно алгоритму RSA [практическая работа №4]:

p=13, q=19

n=p*q=247

$$\varphi(247)= \varphi(19)*\varphi(13)=18*12=216$$

$$e=7,\ d=31$$

{e,n}– {7, 247} = открытый; {d,n} – {31, 247} = закрытый.

шифрование:

$$c_1=\mathrm{mod}1^7,247=1$$

$$c_2=\mathrm{mod}7^7,247=45$$

дешифрование:

$$m_1=\mathrm{mod}1^{31},247=1$$

$$m_2=\mathrm{mod}45^{31},247=7$$

Задание

Используя рассмотренный в данной работе алгоритм вычисления хеш-функции и алгоритм ассиметричного шифрования RSA, сформировать цифровую подпись для сообщения в соответствии с вариантом.

Варианты

Таблица 6.1. варианты

Вариант	Сообщение
1	12 9 14 12 11 15 12 10 12 7 4 8 14 2 14 11 6 15 15 4 8 4 13 17 6 6
2	4 12 15 5 3 11 11 16 9 17 7 4 3 3 6 10 4 12 11 2 6 11 3 2 2 17
3	15 8 6 5 12 5 11 17 15 5 11 12 5 14 7 14 6 6 14 13 9 12 12 5 2 10
4	9 14 7 11 7 8 9 11 8 14 11 3 2 12 10 4 2 5 14 8 6 17 14 17 3 5
5	13 5 14 8 9 14 12 11 13 17 4 5 9 5 14 2 15 3 4 4 17 3 9 17 15 9
6	13 10 16 14 12 15 14 11 15 4 16 17 8 2 6 15 7 11 16 4 5 11 7 2 15 17
7	11 11 12 13 15 11 6 9 14 16 3 9 14 17 6 9 16 4 5 8 14 13 12 5 11 13
8	14 9 5 6 4 8 14 6 6 9 15 2 6 5 4 11 7 15 2 14 2 11 17 8 12 16
9	11 7 12 14 15 3 14 11 16 9 15 2 8 14 2 11 17 11 15 10 6 5 2 11 14 10
10	3 14 15 10 10 9 14 13 3 15 15 12 17 15 17 13 10 3 6 11 13 7 6 6 2 7
11	7 10 6 5 13 11 5 15 6 3 15 10 5 7 6 7 14 14 3 10 2 3 9 14 11 15
12	5 5 14 8 7 11 10 3 2 13 2 7 12 11 5 16 3 10 7 11 4 8 2 3 2 4
13	3 13 15 15 4 10 15 16 4 8 16 4 12 2 9 7 8 3 4 13 6 4 14 12 6 2

продолжение таблицы 6.1.

14	6 2 14 14 14 3 11 13 10 12 7 14 11 4 15 8 6 15 12 16 3 8 4 10 17 3
15	13 2 4 3 2 16 14 11 16 13 12 17 15 15 5 15 8 17 3 11 15 12 3 7 12 14
16	6 5 6 12 12 4 5 4 5 16 4 4 7 11 7 7 15 16 8 14 9 17 10 16 9 14
17	3 2 14 8 14 5 13 9 15 16 14 3 11 10 15 6 11 6 4 11 14 10 16 15 6 4
18	2 11 7 12 9 12 13 15 3 13 9 8 15 6 13 3 6 3 6 17 6 16 11 7 10 15
19	3 9 14 6 16 8 4 13 3 16 16 14 14 16 10 14 14 11 10 17 5 10 11 14 16 6
20	16 16 10 13 3 4 9 17 2 10 8 11 17 6 14 9 2 5 16 16 11 17 10 8 11 11
21	14 15 10 10 9 14 13 3 15 15 12 17 15 6 13 3 6 3 6 17 6 16 11 7 10 15
22	14 5 13 9 15 16 14 3 11 10 15 6 11 6 3 9 14 6 16 8 4 13 3 16 16 14
23	3 14 11 16 9 15 2 8 14 2 11 17 11 15 3 11 13 10 12 7 14 11 4 15 8 6 15
24	4 8 14 6 6 9 15 2 6 5 4 14 8 7 11 10 3 2 13 2 7 12 11 5 16 4 13 6
25	13 15 15 4 10 15 16 4 8 16 4 12 2 9 7 8 3 4 13 16 4 4 7 11 7 9 8
26	14 15 3 14 11 16 9 15 2 8 14 2 11 17 11 15 10 12 11 13 17 4 5 9 5
27	9 14 12 11 13 17 4 5 9 5 14 2 15 3 4 4 17 7 4 3 3 6 10 4 12 11 2 6 11
28	16 14 12 15 14 11 15 4 16 17 8 2 6 15 7 11 16 4 13 15 3 13 9 8 15 6 13
29	17 15 5 11 12 5 14 7 14 6 6 14 13 9 12 12 12 9 14 12 11 15 12 10
30	13 5 14 8 9 14 12 11 13 17 4 5 9 5 14 25 15 6 3 15 10 5 7 6 7 14 14 3

Контрольные вопросы

1) Что такое ЭЦП?

2) Что такое открытый ключ ЭЦП?

3) Что такое закрытый ключ ЭЦП?

4) Для чего нужно ЭЦП?

5) Что такое хеш-функция?

Практическая работа №7

ПРОВЕРКА ЦЕЛОСТНОСТИ ИНФОРМАЦИИ С ПОМОЩЬЮ ЗАШУМЛЕННЫХ КОДОВ

Цель работы: получение базовых практических навыков по использованию помехоустойчивого кода.

Краткие теоретические сведения

Под кодированием понимается процесс преобразования дискретного сообщения в сигнал. Тогда кодом будет называться соответствие между алфавитом сообщения, т.е. набором символов, и значениями информационного параметра сигнала, формируемыми в процессе передачи.

Код, способный обнаружить или исправить ошибки, называют помехоустойчивым или корректирующим.

Помехоустойчивые коды строятся так, что для передачи сообщения используются не все кодовые комбинации, а лишь некоторая их часть (разрешенные кодовые комбинации). Тем самым создается возможность обнаружения и исправления ошибки при неправильном воспроизведении некоторого числа символов. Корректирующие свойства кодов достигаются введением в кодовые комбинации дополнительных (избыточных) символов.

Линейным кодом называется код, в котором любая разрешенная кодовая комбинация может быть получена в результате линейной операции над набором линейно-независимых кодовых комбинаций.

Циклический код – это линейный код, обладающий свойством цикличности, то есть каждая циклическая перестановка кодового слова также является кодовым словом. Такой код используется для преобразования информации с целью защиты ей от ошибок. При использовании циклических кодов в кодовом слове длинной n принято выделять k информационных символов и r проверочных.

Слова циклического кода удобно представлять в виде многочленов. Так кодовое слово { $a^7\ a^6\ a^5\ a^4\ a^3\ a^2\ a^1\ a^0$} можно записать в виде следующего многочлена:

$$P(x) = a^7x^7 + a^6x^6 + a^5x^5 + a^4x^4 + a^3x^3 + a^2x^2 + a^1x + a^0.$$

Все кодовые слова конкретного циклического кода кратны определённому образующему полиному. С помощью образующего полинома осуществляется кодирование циклическим кодом. В качестве порождающих полиномов используются неприводимые полиномы.

Введем следующие обозначения:

- F(x) – информационный полином, соответствующий исходному сообщению;
- R(x) – проверочный полином, соответствующий проверочным разрядам;
- G(x) – полином после кодирования, соответствующий кодовому слову;
- P(x) – образующий полином.

Кодовое слово может быть получено из исходного сообщения в соответствии со следующим выражением:

$$G(x) = F(x)\cdot x^r + R(x).$$

Проверочный полином $R(x)$ определяется как остаток от деления $F(x)\cdot xr$ на образующий полином $P(x)$, где r – количество проверочных разрядов.

Рассмотрим следующий пример. Пусть необходимо закодировать исходное сообщение 1011. Так как количество информационных разрядов в сообщении равно 4, то для обнаружения и исправления однократных ошибок количество проверочных разрядов должно быть не меньше трех (т.е. достаточно взять $r = 3$). Следовательно, можно использовать образующий полином третьей степени $x^3 + x^2 + 1$.

Информационный полином соответствующий заданному сообщению имеет следующий вид:

$$F(x) = x^3 + x + 1.$$

Тогда

$$F(x)\cdot x^r = (x^3 + x + 1)\, x^3 = x^6 + x^4 + x^3.$$

Разделив $F(x)\cdot x^r$ на $P(x)$ найдем остаток $R(x)$:

$$\begin{array}{l} x^6 + 0 + x^4 + x^3 \; x^3 + x^2 + 1 \\ \qquad\qquad x^6 + x^5 + 0 + x^3 \; x^3 + x^2 \\ \qquad\qquad\quad\; x^5 + x^4 \\ \qquad\qquad\quad\; x^5 + x^4 + x^2 \\ \qquad\qquad\qquad\; x^2 = R(x) \end{array}$$

Тогда кодовое слово будет иметь следующий вид:

$$G(x) = F(x)\cdot x^r + R(x) = x^6 + x^4 + x^3 + x^2.$$

В двоичном представлении кодовое слово будет иметь следующий вид:

1011100,

где старшие четыре символа представляют собой информационные разряды, а три младших – проверочные.

В процессе передачи передаваемое кодовое слово $G(x)$ в результате воздействия внешних факторов на сигнал может измениться на кодовое слово $G'(x)$. Проверка наличия ошибок в принятом кодовом слове $G'(x)$ осуществляется делением $G'(x)$ на образующий полином $P(x)$.

Если остаток (синдром ошибки $S(x)$), полученный в результате деления, равен нулю, принимается решение об отсутствии ошибок, в противном случае – об их наличии.

Как правило, циклические коды (как и другие помехоустойчивые коды) применяются для обнаружения и исправления ошибок в сообщениях, возникающих вследствие помех. Однако они также могут применяться для

контроля целостности передаваемой информации, т.е. для обнаружения попыток искажения передаваемой информации со стороны злоумышленника.

Принятое кодовое слово $G'(x)$ можно представить в виде следующего выражения:

$$G'(x) = G(x) + E(x),$$

где $E(x)$ – вектор ошибки. Вектор ошибки представляется в виде последовательности единиц и нулей, в которой позиции, занимаемые единицами, соответствуют позициям ошибок в кодовом слове.

Чтобы найти синдром ошибки в n-ом разряде кодового слова, можно воспользоваться следующим методом:

1. Выбрать вектор ошибки $En(x) = xn$.

2. Определить остаток $Sn(x)$ от деления $En(x)$ на образующий полином $P(x)$. Этот остаток соответствует синдрому ошибки в n-ом разряде принятого сообщения.

Таким образом, чтобы найти разряд кодового слова $G'(x)$, в котором произошла ошибка, можно сравнить остаток, полученный от деления кодового слова $G'(x)$ на образующий полином $P(x)$, с синдромами ошибки.

Задание

1. Используя циклический код (7, 4), закодировать исходные сообщения в соответствии с вариантом.
2. Найти все возможные синдромы ошибки для данного кода.
3. Изменить в соответствии с вариантом один символ в закодированном сообщении.
4. Определить ошибочный разряд, сравнив остаток от деления измененного кодового слова на образующий полином, с синдромами ошибки.
5. Изменить в соответствии с вариантом два символа в закодированном сообщении.

6. Определить ошибочный разряд. сравнив остаток от деления измененного кодового слова на образующий полином, с синдромами ошибки.

Таблица 7.1. пример варианта

Вариант	Исходное сообщение	Образующий полином	Ошибочный разряд	Ошибочные разряды
11	1101	1101	5	0, 2

Информационный полином, соответствующий заданному сообщению, имеет следующий вид:

$$F(x) = x^3 + x^2 + 1$$

$$r \geq \log_2(r + k + 1) \Rightarrow 2^r - r \geq 5 \Rightarrow r \geq 3$$

$$P(x) = x^3 + x^2 + 1$$

Тогда

$$F(x) \cdot x^r = (x^3 + x^2 + 1)x^3 = x^6 + x^5 + x^3$$

Циклический код

$F(x) \cdot x^r = x^6 + x^5 + x^3$ $\qquad$ $P(x) = x^3 + x^2 + 1.$

Разделив $F(x) \cdot x^r$ на P(x) найдем остаток R(x):

$$\begin{array}{llll} x^6 + x^5 + \ldots + x^3 & | & x^3 + x^2 + 1 \\ \hline x^6 + x^5 + \ldots + x^3 & | & x^3 \\ \hline 0 \end{array}$$

R(x)=0

Тогда кодовое слово будет иметь следующий вид:

$$G(x) = F(x) \cdot x^r + R(x) = x^6 + x^5 + x^3 + 0$$

В двоичном представлении кодовое слово будет иметь следующий вид:

1101000

Проверка наличия ошибок в принятом кодовом слове $G(x)$ осуществляется делением $G'(x)$ на образующий полином $P(x)$.

$$\begin{array}{l|l} x^6+x^5+\ldots+x^3 & x^3+x^2+1 \\ \hline x^6+x^5+\ldots+x^3 & x^3 \\ \hline 0 & \end{array}$$

Циклический код –ошибка в 5-м разряде

1001000

$G(x) = x^6 + x^3$ $\qquad$ $P(x) = x^3 + x^2 + 1.$

$$\begin{array}{l|l} x^6+\ldots+\ldots+x^3 & x^3+x^2+1 \\ \hline x^6+x^5+\ldots+x^3 & x^3+x^2+x \\ \hline x^5 & \end{array}$$

$$\begin{array}{l} x^5+x^4+x^2 \\ \hline x^4+x^2 \\ x^4+x^3+x \\ \hline x^3+x^2+x \\ x^3+x^2+1 \\ \hline x+1 \end{array}$$

Ошибка в 0,2-х разрядах:

1101101

$$\begin{array}{l|l} x^6+x^5+x^3+x^2+1 & x^3+x^2+1 \\ \hline x^6+x^5+x^3 & x^3 \\ \hline x^2+1 & \end{array}$$

Синдром ошибки:

E(x)=x^6 {1000000}

$$
\begin{array}{llll|l}
x^6 & & & & x^3+x^2+1 \\
\hline
x^6+x^5+x^3 & & & & x^3+x^2+x \\
\hline
x^5+x^3 & & & & \\
x^5+x^4+x^2 & & & & \\
\hline
x^4+x^3+x^2 & & & & \\
x^4+x^3+x & & & & \\
\hline
x^2+x & & & &
\end{array}
$$

S6(x)= x^2+x

E(x)=x^5 {0100000}

$$
\begin{array}{llll|l}
x^5 & & & & x^3+x^2+1 \\
\hline
x^5+x^4+x^2 & & & & x^2+x+1 \\
\hline
x^4+x^2 & & & & \\
x^4+x^3+x & & & & \\
\hline
x^3+x^2+x & & & & \\
\underline{x^3+x^2+1} & & & & \\
x+1 & & & &
\end{array}
$$

S5(x)= x+1

E(x)=x^4 {0010000}

$$
\begin{array}{llll|l}
x^4 & & & & x^3+x^2+1 \\
\hline
x^4+x^3+x & & & & x+1 \\
\hline
x^3+x & & & & \\
\underline{x^3+x^2+1} & & & & \\
x^2+x+1 & & & &
\end{array}
$$

$S4(x) = x^2 + x + 1$

E(x)=x^3{0001000}

x^3 | $x^3 + x^2 + 1$

$x^3 + x^2 + 1$ | 1

$x^2 + 1$

$S3(x)= x^2+1$

E(x)=x^2{0000100}

x^2 | $x^3 + x^1 + 1$

x^2 $\quad S2(x) = x^2$

E(x)=x{0000010}

x | $x^3 + x^2 + 1$

x $\quad$ S1(x)= x

E(x)=1{0000001}

1 | $x^3 + x^2 + 1$

1 $\quad S0(x) = 1$

Контрольные вопросы

1) Что такое код?

2) Что такое помехоустойчивый код?

3) Основная функция помехоустойчивая кода?

4) Что обозначает полином?

Варианты

Таблица 7.2. варианты

Вариант	Исходное сообщение	Образующий полином	Ошибочный разряд	Ошибочные разряды
1	0011	1101	3	3,5
2	0100	1011	4	3,6
3	0101	1101	5	3,6
4	0110	1011	6	4,5
5	0111	1101	6	4,6
6	1000	1011	0	4,6
7	1001	1101	1	5,6
8	1010	1011	2	5,6
9	1011	1101	3	1,6
10	1100	1011	4	0,1
11	1101	1101	5	0,2
12	1110	1011	6	0,3
13	1111	1101	6	0,4
14	0000	1011	0	0,5
15	0001	1101	1	0,6
16	0010	1011	2	2,6
17	0011	1101	3	1,2
18	0100	1011	4	1,3
19	0101	1101	5	1,4
20	0110	1011	6	1,5

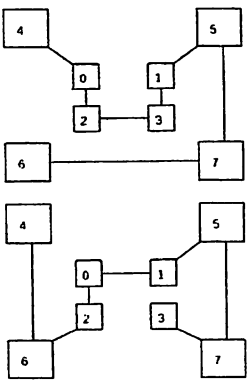
Практическая работа №8

МЕТОД ГАМИЛЬТОНА В ШИФРОВАНИИ ДАННЫХ

Цель работы: Данная практическая работа предназначена для исследования метода перестановки на основе маршрутов Гамильтона.

Краткие теоретические сведения

Весьма высокую стойкость шифрования можно обеспечить усложнением перестановок по *маршрутам типа гамильтоновских*. При этом, для записи символов шифруемого текста используются вершины некоторого гиперкуба, а знаки зашифрованного текста считываются по маршрутам Гамильтона, причём используется восемь различных маршрутов. Размер ключа перестановки в данном случае равен восьми по числу вершин куба. Для примера, два маршрута Гамильтона представлено на 8.1.рис. Первому маршруту соответствует перестановка 4-0-2-3-1-5-7-6, второму 4-6-2-0-1-5-7-3 (нумерация символов в блоке осуществляется с нуля).



8.1. рис. Пример маршрутов Гамильтона

Зашифруем открытый текст «ВОСЕМЬ МАРШРУТОВ» с помощью перестановок Гамильтона при использовании в качестве ключа двух перестановок, представленных на 8.1.рис.

Таблица 8.1. Шифрование открытого текста

0	1	2	3	4	5	6	7	0	1	2	3	4	5	6	7
В	О	С	Е	М	Ь		М	А	Р	Ш	Р	У	Т	О	В
4	**0**	**2**	**3**	**1**	**5**	**7**	**6**	**4**	**6**	**2**	**0**	**1**	**5**	**7**	**3**
М	В	С	Е	О	Ь	М		У	О	Ш	А	Р	Т	В	Р

Этот метод реализуется путем выполнения следующих шагов.

Шаг 1. Исходный текст разбивается на блоки. Если длина шифруемого текста не кратна длине блока, то на свободные места последнего блока помещаются служебные символы- заполнители(например,*)

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

Шаг 3. Считывание символов из таблицы осуществляется по одному из маршрутов. Увеличение числа маршрутов повышает крипто стойкость шифра. Маршруты выбирают либо последовательно, либо их очередность задается ключом К.

Шаг 4. Зашифрованная последовательность символов разбивается на блоки Фиксированной длины L. Величина L может отличаться от длины блоков. на которые разбивается исходный текст на шаге 1.

Расшифрование производится в обратном порядке.

Пример . Требуется зашифровать текст T_o = <Экономическая теория> . Ключ и длины зашифрованных блоков равны: K =< 2,1,1 > , L = 4 . Для шифрования использовать таблицу и два маршрута, представленные на рис.2.1.

Решение: Воспользуемся вышеизложенной методикой построения шифра по шагам.

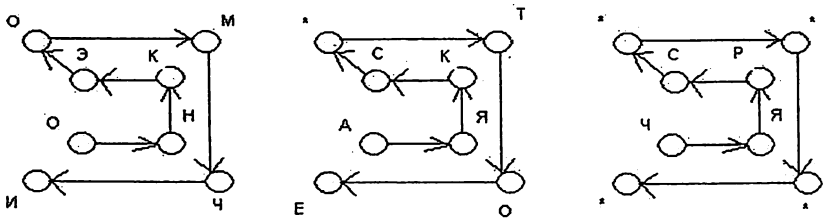
Шаг 1. Исходный текст разбивается на 3 блока:

Блок Б1= <Экономич>

Блок Б2= <Ская*тео>

Блок Б3=<рия*****>

Шаг 2. Заполняется 3 матрицы с маршрутами 1(8.2.рис.).



8.2.рис. – Шифрование с помощью маршрутов Гамильтона

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

Т1 =<ОНКЭОМИЧАЯКС*ТОЕИЯРС***** >

Шаг 4. Разбиение на блоки шифртекста

Т1 =<ОНКЭ ОМИЧ АЯКС *ТОЕ ИЯРС ****>

Возможно применение и других маршрутов.

Задание

Студент шифрует и дешифрует свою Ф.И.О по маршруту Гамильтона

Контрольные вопросы

1. К какому типу шифрования относится маршрут Гамильтона?
2. Каков размер ключа?
3. Сколько маршрутов можно использовать?

Практическая работа №9

ИССЛЕДОВАНИЕ ПРОТОКОЛОВ АУТЕНТИФИКАЦИИ, АВТОРИЗАЦИИ И УЧЕТА В СЕТЯХ ПЕРЕДАЧИ ДАННЫХ

Цель работы: Освоение теоретических знаний и практических навыков по протоколам аутентификации, авторизации и учета в сетях передачи данных.

Краткие теоретические сведения

Механизм AAA (Authentication, Authorization, Accounting) используется для описания процесса предоставления доступа и контроля над ним.

Аутентификация – сопоставление персоны (запроса) существующей учётной записи в системе безопасности. Осуществляется по логину, паролю, сертификату, смарт-карте и т.д.

Авторизация (проверка полномочий, уровня доступа) – сопоставление учётной записи в системе (и персоны, прошедшей аутентификацию) и определённых полномочий (или запрета на доступ).

Учёт – сбор данных об использовании пользователем ресурсов системы.

Одним из протоколов, реализующих AAA является, RADIUS (Remote Authentication Dial-In User Service).

Протокол RADIUS используется для осуществления проверки подлинности, авторизации и учета. RADIUS-клиент (обычно сервер удаленного доступа. VPN-сервер, точка доступа к беспроводной сети и т.п.) посылает учетные данные пользователя и параметры подключения в форме сообщения RADIUS на RADIUS-сервер. Сервер проверяет подлинность и авторизует запрос клиента, а затем посылает обратно ответное сообщение. Клиенты посылают на серверы также сообщения учета. Кроме того стандарт RADIUS поддерживает использование прокси-серверов. Прокси-сервер

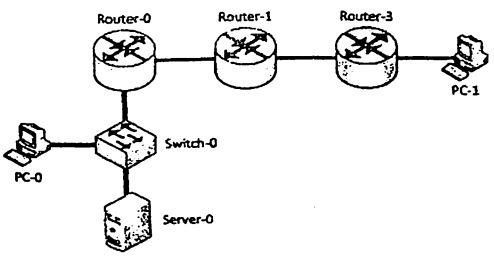
RADIUS – это компьютер, пересылающий RADIUS-сообщения между узлами, поддерживающими протокол RADIUS.

Для передачи сообщений RADIUS используется протокол UDP. Для сообщений проверки подлинности RADIUS используется UDP-порт 1812, а для сообщений учета – UDP-порт 1813. Некоторые серверы доступа к сети могут использовать UDP-порт 1645 для сообщений проверки подлинности RADIUS и UDP-порт 1646 для сообщений учета RADIUS.

Задание

В данной работе необходимо:

- построить модель сети в соответствии со схемой, приведенной на 9.1.рис.;
- настроить AAA-сервер таким образом, чтобы обеспечить доступ к маршрутизаторам с PC-0 и PC-1. На сервере должно быть зарегистрировано не менее двух учетных записей;
- настроить AAA-клиент на маршрутизаторах;
- попытаться получить доступ к маршрутизатору посредством Telnet, используя неправильный пароль или имя пользования;
- попытаться получить доступ к маршрутизатору посредством Telnet, используя правильные имя пользователя и пароль.



9.1.рис. Схема сети

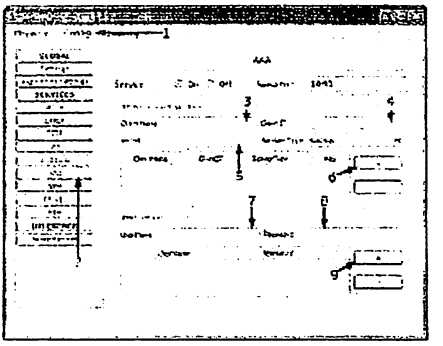
Методика выполнения

Для настройки AAA-сервера следует щелчком левой кнопки мыши по модели сервера открыть окно конфигурирования, перейти на вкладку «Config» (9.2.рис., маркер 1) и нажать на кнопку «AAA» (9.2.рис, маркер 2).

В результате должно отобразиться окно настройки AAA-сервера. В этом окне нужно указать следующие параметры:

- Client Name (9.2.рис, маркер 3) – имя сетевого элемента, являющегося клиентом AAA-сервера;
- Client IP (9.2.рис, маркер 4) – IP-адрес сетевого элемента, являющегося клиентом AAA-сервера;
- Secret (9.2.рис, маркер 5) – ключ шифрования, используемый протоколом RADIUS;
- User Name (9.2.рис, маркер 7) – имя пользователя (логин) для доступа к сетевому элементу;
- Password (9.2.рис, маркер 8) – пароль для доступа к сетевому элементу.

После указания значений всех вышеперечисленных параметров следует нажать кнопки «+» (9.2.рис, маркеры 6 и 9) для добавления соответствующих записей на AAA-сервер.



9.2.рис. Окно конфигурирования AAA-сервера

Теперь нужно настроить маршрутизаторы Cisco. После активации интерфейсов маршрутизаторов следует настроить ААА-клиент на маршрутизаторе. Для этого нужно выполнить приведенную ниже последовательность команд:

4.1. Указать IP-адрес ААА-сервера:

```
Router(config)#radius-server host <IP-адрес>
```

где <IP-адрес> – IP-адрес ААА-сервера.

4.2. Указать ключ шифрования для протокола RADIUS:

```
Router(config)#radius-server key <ключ>
```

где <ключ> – ключ шифрования.

4.3. Активировать все ААА-службы на маршрутизаторе:

```
Router(config)#aaa new-model
```

4.4. Настроить процесс аутентификации на маршрутизаторе:

```
Router(config)#aaa authentication login default <метод1>
                [<метод2> ...]
```

где <метод> – метод аутентификации. Методу аутентификации по протоколу RADIUS соответствует значение данного параметра «group radius».

4.5. Настроить процесс авторизации на маршрутизаторе:

- авторизация для начала сеанса управления:

```
Router(config)#aaa authorization exec default <метод1>
                [<метод2> ...]
```

- авторизация для сетевых сеансов:

```
aaa authorization network default <метод1>
                [<метод2> ...]
```

где <метод> – метод авторизации. Методу аутентификации по протоколу RADIUS соответствует значение данного параметра «group radius».

Функции учета (accounting) в Cisco Packet Tracer не доступны.

Задание

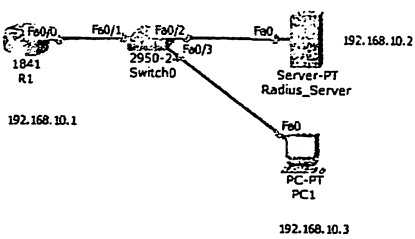
Подготовить отчет по теме практической работы. Содержание отчета:

- номер и тему работы;
- задание;
- изображение модели сети из Cisco PacketTracer;
- описание модели, включающее распределение IP-адресов в сети, схему подключения (номера интерфейсов);
- использованные в работе имена пользователей и пароли;
- листинг конфигурирования сетевых элементов;
- результаты попыток получения доступа к сетевым элементам.

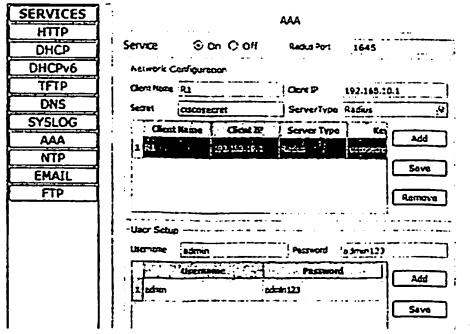
Контрольные вопросы

1) Что такое аутентификация?
2) Что такое авторизация?
3) Что такое идентификация?
4) Как расшифруется RADIUS?
5) Что такое учёт?
6) Какой протокол используется для передачи сообщений RADIUS ?
7) Какая функция у протокола UDP?
8) Что такое Telnet?

Пример: (9.2.рис.)



а)



б)

9.2.рис. а) схема сети б) окно конфигурирования AAA-сервера

Листинг команд маршрутизатора

hostname **R1**

enable secret **123456**

aaa new-model

aaa authentication login default group radius none

radius-server host **192.168.10.2** auth-port 1645 key **ciscosecret**

СПИСОК ЛИТЕРАТУРЫ

1. Джураев Р.Х.. Джаббаров Ш.Ю.. Умирзаков Б.М. Сетевая безопасность. Учебник – Т. "Алокачи", 2019, 308 с.
2. W. Stallings. Network security essentials, Applications and Standards. Fourth Edition. Upper Saddle River, NJ: Prentice Hall, 2011-417p.
3. С.К. Ганиев, М.М. Каримов, К.А. Ташев. Ахборот хавфсизлиги. – Т.: "Фан технология", 2016, 372 бет.
4. Устинов Г.Н. Основы информационной безопасности систем и сетей передачи данных. Учебное пособие. Серия «Безопасность». – М.: СИНТЕГ, 2000. 248с.
5. Jerome F. DiMarzio "Cisco ® Routers in 21 Days" Санкт Петербург – Москва 2003
6. O'z DSt ISO/IEC 2382-8.2007 Ўзбекистон Давлат Стандарти. Ахборот хавфсизлиги. Атамалар ва таърифлар.
7. TSt 45-010:2010. Алока ва ахборотлаштириш соҳасида ахборот хавфсизлиги. Атамалар ва таърифлар.
8. Д.Е. Акбаров. Ахборот хавфсизлигини таъминлашнинг криптографик усуллари ва уларнинг қўлланилиши. Тошкент. "Ўзбекистон маркаси" нашриёти 2009.
9. Новиков А.А. Уязвимость и информационная безопасность телекоммуникационных технологий: учеб. Пособие для студ./ Под ред. Г.Н. Устинова. – М.: Радио и связь, 2003. -296с.
10. Конахович Г.Ф.. Климчук В.П. Паук С.М., Патапов В.Г. Защита информации в телекоммуникационных системах. К.: МК-Пресс. 2005

Содержание

Введение..... 3

1. Исследование арифметических вычислений при решении криптографических задач 4
2. Парольные методы в системе защиты данных 11
3. Симметричные алгоритмы шифрования данных 17
4. Алгоритмы асимметричного шифрования данных (алгоритм RSA, Diffie-Hellman)..... 24
5. Шифрование и дешифрование данных по алгоритму Эль-Гамаля 32
6. Создание и проверка электронной цифровой подписи 36
7. Проверка целостности информации с помощью зашумленных кодов..... 41
8 Метод Гамильтона в шифровании данных 50
9 Исследование протоколов аутентификации, авторизации и учета в сетях передачи данных..... 53

Список литературы 59

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ТЕЛЕКОММУНИКАЦИЙ

Методические указания к выполнению практических работ по курсу «Информационная безопасность телекоммуникаций». Для направления бакалавриата 5350100-Телекоммуникационные технологии (Телекоммуникации, Телерадиовещание, Мобильные системы).

Рассмотрены на заседании кафедры С и СПД протокол №___ от_____ 20__ и рекомендовано к печати.

Рассмотрены и рекомендованы к печати научно-методическим советом ТФ ТУИТ имени Мухаммада ал-Хоразмий (Протокол № ____ от _____ 20__ г

Составители: Джураев Р.Х.
Джаббаров Ш.Ю.
Маткурбонов Д.М.
Лазарев А.П.

Рецензент: д.т.н., доцент _____

Ответственный редактор: Лазарев А.П.

Корректор: Абдуллаева С.Х

Формат 60x84 1/16. Печ.лист 4.
Заказ №40. Тираж 10.
Отпечатано в «Редакционно издательском» отделе при ТУИТ.
Ташкент ул. Амир Темур, 108.