МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждения образования «БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ

ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**Практическая работа №4**

по дисциплине «Основы информационной безопасности»

на тему: Криптографическая защита информации

Выполнил студент 2 курса 7 группы специальность ПОИБМС Володькин Никифор Дмитриевич

(Ф.И.О.)

Преподаватель Ржеутская Надежда Викентьевна

(Ф.И.О.)

**Цель: Овладение основными криптографическими алгоритмами симметричного шифрования .**

**Теоретическое введение**

Криптография - наука о методах обеспечения конфиденциальности (невозможности прочтения информации посторонним) и аутентичности (целостности и подлинности авторства) информации.

Изначально криптография изучала методы шифрования информации – обратимого преобразования открытого (исходного) текста на основе секретного алгоритма и/или ключа в шифрованный текст (шифротекст). Традиционная криптография образует раздел симметричных криптосистем, в которых зашифрование и расшифрование проводится с использованием одного и того же секретного ключа.

Помимо этого современная криптография включает в себя асимметричные криптосистемы, системы электронной цифровой подписи, хеш-функции, управление ключами, получение скрытой информации, квантовую криптографию.

Шифрованием (encryption) называют процесс преобразования открытых данных (plaintext) в зашифрованные (шифртекст, ciphertext) или зашифрованных данных в открытые по определенным правилам с применением ключей.

В англоязычной литературе зашифрование / расшифрование – enciphering / deciphering.

Классификация алгоритмов шифрования

1. Симметричные (с секретным, единым ключом, одноключевые, single-key).

1.1. Потоковые:

· с одноразовым или бесконечным ключом (infinite-key cipher);

· с конечным ключом;

· на основе генератора псевдослучайных чисел.

1.2. Блочные:

1.2.1. Шифры перестановки (permutation, P-блоки);

1.2.2. Шифры замены (substitution, S-блоки):

· моноалфавитные;

· полиалфавитные;

2. Асимметричные (с открытым ключом, public-key):

· Диффи-Хеллман DH (Diffie, Hellman);

· Райвест-Шамир-Адлeман RSA (Rivest, Shamir, Adleman);

· Эль-Гамаль (ElGamal).

Симметричные алгоритмы шифрования (или криптография с секретными ключами) основаны на том, что отправитель и получатель информации используют один и тот же ключ. Этот ключ должен храниться в тайне и передаваться способом, исключающим его перехват.

Обмен информацией осуществляется в 3 этапа:

* отправитель передает получателю ключ (в случае сети с несколькими абонентами у каждой пары абонентов должен быть свой ключ, отличный от ключей других пар);
* отправитель, используя ключ, зашифровывает сообщение, которое пересылается получателю;
* получатель получает сообщение и расшифровывает его.

Если для каждого дня и для каждого сеанса связи будет использоваться уникальный ключ, это повысит защищенность системы.

При блочном шифровании информация разбивается на блоки фиксированной длины и шифруется поблочно. Блочные шифры бывают двух основных видов:

· шифры перестановки (transposition, permutation, P-блоки);

· шифры замены (подстановки, substitution, S-блоки).

Шифры перестановок переставляют элементы открытых данных (биты, буквы, символы) в некотором новом порядке. Различают шифры горизонтальной, вертикальной, двойной перестановки, решетки, лабиринты, лозунговые и др.

Шифры замены заменяют элементы открытых данных на другие элементы по определенному правилу. Paзличают шифры простой, сложной, парной замены, буквенно-слоговое шифрование и шифры колонной замены. Шифры замены делятся на две группы:

· моноалфавитные (код Цезаря);

· полиалфавитные (шифр Видженера, цилиндр Джефферсона, диск Уэтстоуна, Enigma).

В моноалфавитных шифрах замены буква исходного текста заменяется на другую, заранее определенную букву. Например в коде Цезаря буква заменяется на букву, отстоящую от нее в латинском алфавите на некоторое число позиций.



Очевидно, что такой шифр взламывается совсем просто. Нужно подсчитать, как часто встречаются буквы в зашифрованном тексте, и сопоставить результат с известной для каждого языка частотой встречаемости букв.

В полиалфавитных подстановках для замены некоторого символа исходного сообщения в каждом случае его появления последовательно используются различные символы из некоторого набора. Понятно, что этот набор не бесконечен, через какое-то количество символов его нужно использовать снова. В этом слабость чисто полиалфавитных шифров.

В современных криптографических системах, как правило, используют оба способа шифрования (замены и перестановки). Такой шифратор называют составным (product cipher). Oн более стойкий, чем шифратор, использующий только замены или перестановки.

В асимметричных алгоритмах шифрования (или криптографии с открытым ключом) для зашифровывания информации используют один ключ (открытый), а для расшифровывания - другой (секретный). Эти ключи различны и не могут быть получены один из другого.

Схема обмена информацией такова:

· получатель вычисляет открытый и секретный ключи, секретный ключ хранит в тайне, открытый же делает доступным (сообщает отправителю, группе пользователей сети, публикует);

· отправитель, используя открытый ключ получателя, зашифровывает сообщение, которое пересылается получателю;

· получатель получает сообщение и расшифровывает его, используя свой секретный ключ.

**Выполнение работы**

**Шифрование с помощью шифра Цезаря**

Шифр Цезаря — это вид шифра подстановки, в котором каждый символ в открытом тексте заменяется символом, находящимся на некотором постоянном числе позиций левее или правее него в алфавите.

Для построения таблицы смещения достаточно сместить все буквы алфавита на фиксированное число, равное числовому ключу.

Для ключа **7** таблица смещения будет выглядеть так:



Сопоставив символы с таблицей смещения, сообщение **володькин никифор дмитриевич** шифруется как **ызезэхдвж жвдвнзй эёвлйвюывр**.

**Шифрование шифром Трисемуса**

Шифр Трисемуса по принципу шифрования аналогичен полибианскому квадрату. Различия между ними заключаются лишь в принципе заполнения таблиц буквами алфавита.

Таблица Трисемуса заполняется с помощью ключевого слова, повторяющиеся буквы которого отбрасываются. Затем таблица дополняется не вошедшими в нее буквами алфавита по порядку как в системе Цезаря с ключевым словом. Таким образом, ключом в таблицах Трисемуса является ключевое слово и размер таблицы.

При шифровании буква открытого текста заменяется буквой, расположенной ниже нее в том же столбце.

Таблица **5x7** с ключевым словом **ЗАЩИТА** будет выглядеть так:



Сопоставив символы с таблицей смещения, сообщение **володькин никифор дмитриевич** шифруется как **кцуцмщсех хесеьцш мфеёшенкея**.

**Шифрование шифром Плейфера**

Шифр плейфера также использует прямоугольник (квадрат), который представляет собой таблицу смещения. Сообщение разбивается на биграммы, после чего шифруется по следующим правилам:

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

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

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

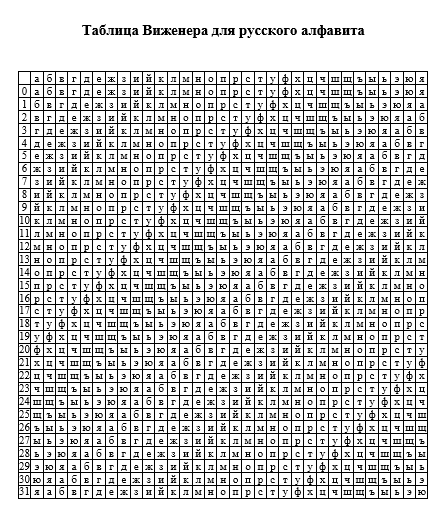
Таблица **5x7** с ключевым словом **ЗАЩИТА** будет выглядеть так:



Сообщение **володькин никифор дмитриевич** было разбито на биграммы **во ло дь ки нн ик иф ор дм ит ри ев ич**. Сопоставив биграммы с таблицей смещения по правилам сообщение шифруется как **ёк мп из нз оо зн щх пк мф та нб ёг ах**.

**Шифрование шифром Виженера**

Шифр Виженера состоит из последовательности нескольких шифров Цезаря с различными значениями сдвига. Для зашифровывания может использоваться таблица алфавитов, называемая квадрат (таблица) Виженера:



На каждом этапе шифрования используются различные алфавиты, выбираемые в зависимости от символа ключевого слова.

Человек, посылающий сообщение, записывает ключевое слово циклически до тех пор, пока его длина не будет соответствовать длине исходного текста, а код каждого символа полученного ключевого слова является кодом алфавита, который следует использовать для шифрования символа сообщения.

Пользуясь квадратом Виженера при ключевом слове **ЗАЩИТА**, сообщение **володькин никифор дмитриевич** шифруется как **йоечцьтиж цыкрфзщ цмртйсчврч**.

**Расшифровка сообщения**

В системе Цезаря с ключевым словом наряду с числовым ключом, задающим смещение, используется ключевое слово для изменения порядка символов в заменяющем алфавите.

Для создания таблицы замены ключевое слово записывается под буквами алфавита, начиная с буквы, числовой код которой совпадает с выбранным числовым ключом. Оставшиеся буквы алфавита замены записываются в алфавитном порядке (избегая повтора букв) после ключевого слова. При достижении конца таблицы циклически переходим на ее начало и дописываем последние буквы алфавита, не встречавшиеся ранее.

Таким образом при ключе **8** и ключевом слове **ВЕСНА** была построена следующая таблица смещения:



Сопоставив символы с таблицей смещения, сообщение **гэ ишн зижшпэг оюжи** расшифровывается как **не так страшен чёрт**.

**Вывод: изучены основные криптографические алгоритмамы симметричного шифрования.**