БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ

КАФЕДРА ИНФОРМАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

**Практическое занятие №7**

Тема «Криптографическая защита информации»

**Выполнил:**

студент 2 курса 4 группы

Карленок Юрий Андреевич

**Проверил:**

Берников Владислав Олегович

Минск 2019

Цель: Овладение основными криптографическими алгоритмами 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.

Задание к выполнению:

1. Реализовать пример генерации секретного ключа методом Диффи-Хелмана
   1. В качестве p и g взять два любых простых числа.
   2. Секретный ключ 1-го человека должен быть: номер варианта + 8.

|  |  |
| --- | --- |
| Человек 1 | Человек 2 |
| Открытое простое число p=7 | Открытое простое число p=7 |
| Открытое простое число g=11 | Открытое простое число g=11 |
| Секретный ключ а=8+8=16 | Секретный ключ b=9 |
| Открытый ключ A=mod 7 =4 | Открытый ключ B=mod 7 =1 |
| Секретный ключ S= mod 7=1 | Секретный ключ S= mod 7=1 |
| S=1 | S=1 |

1. Зашифровать сообщение «хочузачетавтоматом» с использованием шифра Цезаря и полученного секретного ключа.

Пусть ключом k будет номер моего варианта, т.е. k=8.

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



Из этого следует, что в результате побуквенного шифрования фразы «хочузачетавтоматом» получаем шифртекст «эцяыпзямьзйьцфзьцф».

**Вывод:** я овладел основными криптографическими алгоритмами шифрования.