Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Основы защиты информации

Студент: Круглик А.В.

ФИТ 2 курс 5 группа

Преподаватель: Берников В.О.

Минск 2022

**Практическое занятие №5**

**Тема «**Криптографическая защита информации**»**

**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 eпользователей сети, публикует);

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

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

**Задание**

Круглик Алексей Викторович – исходная сообщение

**Шифр Цезаря**



Рисунок 5.2 – Алфавит

Таблица 5.1 Шифр Цезаря

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Сообщение** | **К** | **Р** | **У** | **Г** | **Л** | **И** | **К** | **А** | **Л** | **Е** | **К** | **С** | **Е** | **Й** |  |  |  |  |
| **Номер** | 12 | 18 | 21 | 4 | 13 | 10 | 12 | 1 | 13 | 6 | 12 | 19 | 6 | 11 |  |  |  |  |
| **Номер + 15** | 27 | 33 | 36 | 22 | 28 | 25 | 27 | 16 | 28 | 21 | 27 | 34 | 21 | 26 |  |  |  |  |

Щявсъчщ ОЬущауш– шифр Цезаря

## **Система Трисемуса**

Шифрующая система Трисемуса (Тритемия). В 1508 г. аббат из Германии Иоганн Трисемус написал печатную работу по криптологии под названием «Полиграфия». В этой книге он впервые систематически описал применение модифицированного шифра Цезаря.

Здесь шаг смещения делается переменным, то есть зависящим от каких-либо дополнительных факторов. Например, можно задать закон смещения в виде линейной функции (уравнения зашифрования) позиции шифруемой буквы.

Сама функция должна гарантировать целочисленное значение. Прямая функция шифрования должна иметь обратную функцию шифрования, тоже целочисленную.



Оригинальный текст:

КругликАлексей

Шифрованный текст:

НЪЕЁЯРКюжетвёю

## **Система Вижинера**

В [шифре Цезаря](https://ru.wikipedia.org/wiki/%D0%A8%D0%B8%D1%84%D1%80_%D0%A6%D0%B5%D0%B7%D0%B0%D1%80%D1%8F) каждая буква алфавита сдвигается на несколько строк; например в шифре Цезаря при сдвиге +3, A стало бы D, B стало бы E и так далее. Шифр Виженера состоит из последовательности нескольких шифров Цезаря с различными значениями сдвига. Применительно к латинскому алфавиту таблица Виженера составляется из строк по 26 символов, причём каждая следующая строка сдвигается на несколько позиций. Таким образом, в таблице получается 26 различных шифров Цезаря. На каждом этапе шифрования используются различные алфавиты, выбираемые в зависимости от символа ключевого слова. Например, предположим, что исходный текст имеет вид:

**Круглик Алексей**– исходное сообщение

*ЗащитаЗащитаЗа*– ключ

трмлюитаенэсмй– зашифрованное сообщение

Шифруется с помощью специальной таблицы

**Задание**

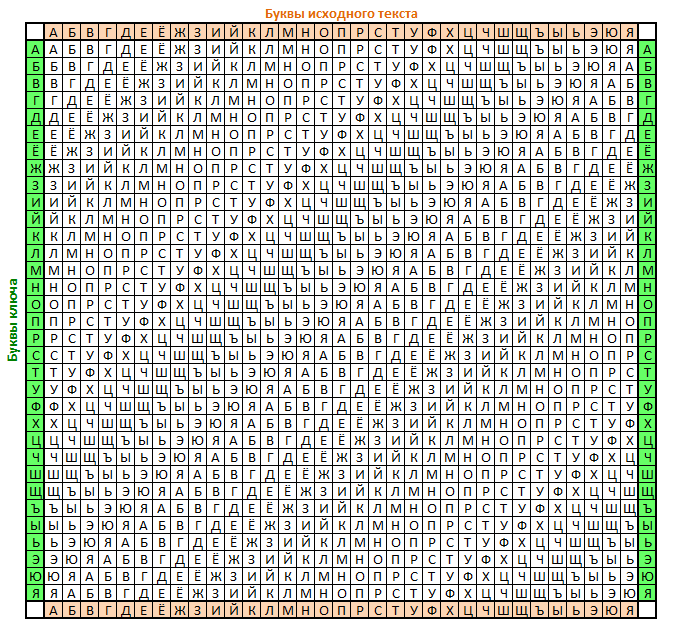


Рисунок 5.3 – Таблица Виженера для русского алфавита

Вы там, где вы есть, и тот, кто вы есть потому что вы решили тут быть

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Ф | Е | В | Р | А | Л | Ь |
| 6 | 3 | 2 | 5 | 1 | 4 | 7 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| \_ | \_ | е | о | о | в | и |
| п | и | \_ | \_ | \_ | ы | \_ |
| о | \_ | в | в | в | \_ | т |
| т | т | ы | ы | ы | т | у |
| о | о | \_ | \_ | \_ | а | т |
| м | т | е | р | е | м | \_ |
| у | , | с | е | с | , | б |
| \_ | \_ | т | ш | т | \_ | ы |
| ч | к | ь | и | ь | г | т |
| т | т | , | л | , | д | ь |

**Вывод:** Овладел основными криптографическими алгоритмами симметричного шифрования.

|  |  |
| --- | --- |
| Ф | 6 |
| Е | 3 |
| В | 2 |
| Р | 5 |
| А | 1 |
| Л | 4 |
| Ь | 7 |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| \_ | П | О | Т | О | М | У | - | Ч | Т |
| \_ | И | - | Т | О | Т | , | - | К | Т |
| Е | - | В | Ы | - | Е | С | Т | Ь | , |
| О | - | В | Ы | - | Р | У | Ш | И | Л |
| О | - | В | Ы | - | Е | С | Т | Ь | , |
| В | Ы | - | Т | А | М | , | - | Г | Д |
| и | - | Т | У | Т | - | Б | Ы | т | ь |

|  |  |
| --- | --- |
| А | 1 |
| В | 2 |
| Е | 3 |
| Л | 4 |
| Р | 5 |
| Ф | 6 |
| Ь | 7 |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| О | - | В | Ы | - | Е | С | Т | Ь | , |
| Е | - | В | Ы | - | Е | С | Т | Ь | , |
| \_ | И | - | Т | О | Т | , | - | К | Т |
| В | Ы | - | Т | А | М | , | - | Г | Д |
| О | - | В | Ы | - | Р | У | Ш | И | Л |
| \_ | П | О | Т | О | М | У | - | Ч | Т |
| и | - | Т | У | Т | - | Б | Ы | т | ь |