Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Основы защиты информации

Студентка: Коржова В.С.

ФИТ 2 курс 4 группа

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 пользователей сети, публикует);

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

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

**Практическая часть**

*Коржова Валерия Сергеевна*

2) Шифр Цезаря: Щвдювшц Шциьдзх Еьдъььшбц

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Буква** | **а** | **б** | **в** | **г** | **д** | **е** | **ё** | **ж** | **з** | **и** | **й** |
| **Шифр** | **ц** | **ч** | **ш** | **ъ** | **ы** | **ь** | **э** | **ю** | **я** | **з** | **а** |
| Номер | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 |
| **Буква** | **к** | **л** | **м** | **н** | **о** | **п** | **р** | **с** | **т** | **у** | **ф** |
| **Шифр** | **щ** | **и** | **т** | **б** | **в** | **г** | **д** | **е** | **ё** | **ж** | **й** |
| Номер | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 |
| **Буква** | **х** | **ц** | **ч** | **ш** | **щ** | **ь** | **ы** | **ъ** | **э** | **ю** | **я** |
| **Шифр** | **к** | **л** | **м** | **н** | **о** | **п** | **р** | **с** | **у** | **ф** | **х** |
| Номер | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 | 32 | 33 |

Шифр Трисемуса: Учърчмш Мефпъйг Ыпънппмце

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| з | а | щ | и | т | б | в | г |
| д | е | ж | й | к | л | м | н |
| о | п | р | с | у | ф | х | ц |
| ч | ш | ъ | ы | ь | э | ю | я |

Шифр Плейфейра: цыкухзуйгшжлщбжпгйзейвщуайгмв

ся тк ов ск ая ек ат ер ин ад ми тр ие вн а

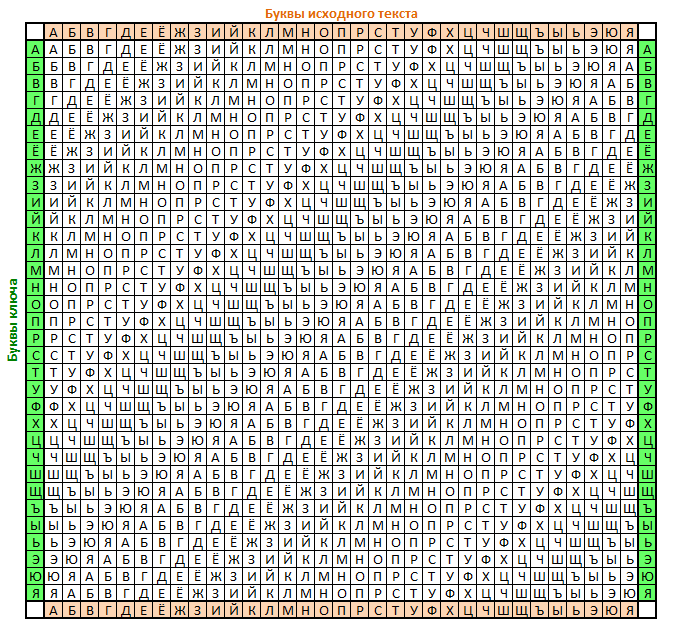
ко рж ов ав ал ер ия се рг ех ев на

ду ър хз щг бе жп гы пй цщ мп ма ег

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| з | а | щ | и | т | б | в | г |
| д | е | ж | й | к | л | м | н |
| о | п | р | с | у | ф | х | ц |
| ч | ш | ъ | ы | ь | э | ю | я |

Шифр Вижинера: тойпбвз вщфчрря кнггмеыцт

з а щ и т а з а щ и т а з а щ и т а з а щ и т

 к о р ж о в а в а л е р и я с е р г е е в н а

3)жъйтаьъщ ёьръ клъюё жёйлал

**Расшифровать с помощью шифра Цезаря.**

**Ключ 6.**

**Ключевое слово ЗИМА**

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Буква** | **а** | **б** | **в** | **г** | **д** | **е** | **ё** | **ж** | **з** | **и** | **й** |
| **Шифр** | **ъ** | **ы** | **ь** | **э** | **ю** | **я** | **з** | **и** | **м** | **а** | **б** |
| Номер | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 |
| **Буква** | **к** | **л** | **м** | **н** | **о** | **п** | **р** | **с** | **т** | **у** | **ф** |
| **Шифр** | **в** | **г** | **д** | **е** | **ё** | **ж** | **й** | **к** | **л** | **н** | **о** |
| Номер | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 |
| **Буква** | **х** | **ц** | **ч** | **ш** | **щ** | **ь** | **ы** | **ъ** | **э** | **ю** | **я** |
| **Шифр** | **п** | **р** | **с** | **т** | **у** | **ф** | **х** | **ц** | **ч** | **ш** | **щ** |
| Номер | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 | 32 | 33 |

**Паршивая овца стадо портит**

**Вывод:** Овладела основными криптографическими алгоритмами шифрования.