Министерство образования Республики Беларусь

Учреждение образования «Белорусский государственный технологический университет»

Факультет информационных технологий

Отчет

К практической работе №5:

Основы защиты информации

«Криптографическая защита информации»

Выполнил:

Студент 2 курса 2 группы ФИТ

Радивил Данила Юрьевич

**Минск, 2022**

**Практическое занятие №5**

**«Криптографическая защита информации»**

Цель: Овладение навыками работы с компьютерными программами для криптографической защиты информации при передаче и хранении.

**Выполнение**

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

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

Классификация алгоритмов шифрования:

– симметричные (с секретным, единым ключом, одноключевые, single-key).

а) потоковые:

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

2) с конечным ключом;

3) на основе генератора псевдослучайных чисел;

б) блочные:

1) шифры перестановки (permutation, P-блоки);

2) шифры замены (substitution, S-блоки):

2.1) моноалфавитные;

2.2) полиалфавитные;

– асимметричные (с открытым ключом, public-key):

а) Диффи-Хеллман DH (Diffie, Hellman);

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

в) 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.

**Шифр 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.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Исх.алфавит | А | Б | В | Г | Д | Е | Ё | Ж | З | И | Й | К | Л | М | Н | О | П |
|  | Р | С | Т | У | Ф | Х | Ц | Ч | Ш | Щ | Ъ | Ы | Ь | Э | Ю | Я |  |
| Шифр. алф. | x | ц | Ч | ш | щ | ъ | ы | ь | э | ю | я | а | б | в | г | д | е |
|  | ё | ж | З | и | й | к | л | м | н | о | п | р | с | т | у | ф |  |

**Задания для выполнения**

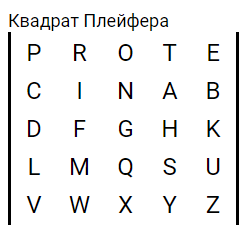
1. Изучить теоретические сведения по данной теме.
2. Зашифровать сообщение с использованием шифра Цезаря, Трисемуса, Плейфейра и Вижинера и полученного секретного ключа (по номеру варианта и ключевому слову «Защита»). В качестве сообщения использовать свою Фамилию Имя Отчество.

Сообщение (ФИО) Радивил Данила Юрьевич (Radzivil Danila Yuirvich)

Ключ = 20

Дучьхья Чубьяу Сдпшхьк

-шифр Плейфейра XPOTBGTPMCYBZPAHZSIFPZAB



TIKVCWCM HCAISC ZSRFWCAD

шифр Трисемуса : Vptrrpu Ltrjlhrhp Oljbyqjx

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

шифр Вижинера (ключ Защита): шаэсфиу дщцылз юйезеврч



|  |  |
| --- | --- |
| **иецеж пецен, пй ыд зещеъез** | Расшифровать с помощью шифра Трисемуса  **Ключ МОСКВА** |

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

гкпка жкпкё, жд хс бкукцкб