Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**Основы Защиты Информации**

**Практическое занятие №7**

**Тема «Криптографическая защита информации»**

Студент: Городилов М. П.

ФИТ 2 курс 4 группа

Преподаватель: Буснюк Н. Н.

Минск 2020

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

**Теоретические сведения**

***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, 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).

**Алгоритм Диффи-Хелмана**

Сначала генерируются два больших простых числа *n* и *q*. Эти два числа не обязательно хранить в секрете. Далее один из партнеров *P*1 генерирует случайное число x и посылает другому участнику будущих обменов *P*2 значение *A* = *qx mod n*

По получении *А* партнер *P*2 генерирует случайное число у и посылает *P2* вычисленное значение *B = qy mod n*

Партнер *P*1, получив *В*, вычисляет *Kx* = *Bx mod n*, а партнер *P*2 вычисляет *Ky* = *Ay mod n*. Алгоритм гарантирует, что числа *Ky* и *Kx* равны и могут быть использованы в качестве секретного ключа для шифрования. Ведь даже перехватив числа *А* и *В*, трудно вычислить *Kx* или *Ky*.

*g* = открытое простое число. *g* = 19

*p* = открытое простое число. *p* = 61

*a* = секретный ключ 1-го человека. *a* = 16

*A* = открытый ключ 1-го человека. *A* = *ga* mod *p* = 42

*b* = секретный ключ 2-го человека. *b* = 33

*B* = открытый ключ 2-го человека. *B* = *gb* mod *p* = 27

*Kа*=*Ba* mod *p* = 34

*Kb*=*Ab* mod *p* = 34

Полученный секретный ключ s = 34.

**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. | 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 | а | б | в |  |

“хочузачетавтоматом” = “шсъцкгъзхгехспгхсп”

**Вывод:** в ходе проведения данной лабораторной работы я ознакомился с различными методами криптографической защиты информации. На практике применил алгоритм Диффи-Хелмана и по полученному ключу использовал шифр Цезаря.