**Тема: Основные методы шифрование**

**Цель работы:** Изучить основные методы шифрование и дешифрование данных.

Задание:

***Задание к лабораторной работе***

* Реализовать функции шифрации и дешифрации текстового файла Методом Виженера.

**Функция шифрации на С#:**

private string Encode(string input, string keyword)

{

input = input.ToUpper();

keyword = keyword.ToUpper();

string result = "";

int keyword\_index = 0;

foreach (char symbol in input)

{

int c = (Array.IndexOf(characters, symbol) +

Array.IndexOf(characters, keyword[keyword\_index])) % N;

result += characters[c];

keyword\_index++;

if ((keyword\_index + 1) == keyword.Length)

keyword\_index = 0;

}

return result;

}

**Функция дешифрации на C#:**

private string Decode(string input, string keyword)

{

input = input.ToUpper();

keyword = keyword.ToUpper();

string result = "";

int keyword\_index = 0;

foreach (char symbol in input)

{

int p = (Array.IndexOf(characters, symbol) + N -

Array.IndexOf(characters, keyword[keyword\_index])) % N;

result += characters[p];

keyword\_index++;

if ((keyword\_index + 1) == keyword.Length)

keyword\_index = 0;

}

return result;

}

**Контрольные вопросы**

*1. Что такое криптографическое преобразование информации?*

Криптографическое преобразование - это преобразование информации, основанное на некотором алгоритме, зависящем от изменяемого параметра (обычно называемого секретным ключом), и обладающее свойством невозможности восстановления исходной информации по преобразованной, без знания действующего ключа, с трудоемкостью меньше заранее заданной.

*2. Что понимается под шифрованием, расшифрованием и дешифрованием данных?*

Шифрование (зашифрование) — процесс применения шифра к защищаемой информации, т.е. преобразование исходного сообщения в зашифрованное.

Дешифрование (расшифрование) — процесс, обратный шифрованию, т. е. преобразование шифрованного сообщения в исходное.

Расшифрование — процесс преобразования зашифрованных данных в открытые данные при помощи шифра.

*3. Дайте определения ключа и алгоритма шифрования?*

Ключ – переменный параметр шифра, обеспечивающий выбор одного преобразования из совокупности всевозможных для данного алгоритма и сообщения. В общем случае, ключ – это минимально необходимая информация (за исключением сообщения, алфавитов и алгоритма), необходимая для шифрования и дешифрования сообщений.

Алгоритм криптографического преобразования — набор правил (инструкций), определяющих содержание и порядок операций по шифрованию и дешифрованию информации.

*4. Расскажите о криптографическом методе перестановки?*

Шифр перестано́вки — это метод симметричного шифрования, в котором элементы исходного открытого текста меняют местами. Элементами текста могут быть отдельные символы (самый распространённый случай), пары букв, тройки букв, комбинирование этих случаев и так далее. Типичными примерами перестановки являются анаграммы. В классической криптографии шифры перестановки можно разделить на два класса:

* Шифры одинарной (простой) перестановки — при шифровании символы открытого текста перемещаются с исходных позиций в новые один раз.
* Шифры множественной (сложной) перестановки — при шифровании символы открытого текста перемещаются с исходных позиций в новые несколько раз.

*5. В чем суть криптографического метода замены?*

Шифр подстано́вки — это метод шифрования, в котором элементы исходного открытого текста заменяются зашифрованным текстом в соответствии с некоторым правилом. Элементами текста могут быть отдельные символы (самый распространённый случай), пары букв, тройки букв, комбинирование этих случаев и так далее. В классической криптографии различают четыре типа шифра подстановки:

* Одноалфавитный шифр подстановки (шифр простой замены) — шифр, при котором каждый символ открытого текста заменяется на некоторый, фиксированный при данном ключе символ того же алфавита.
* Однозвучный шифр подстановки похож на одноалфавитный за исключением того, что символ открытого текста может быть заменен одним из нескольких возможных символов.
* Полиграммный шифр подстановки заменяет не один символ, а целую группу.
* Полиалфавитный шифр подстановки состоит из нескольких шифров простой замены.

*6. Какие методы шифрования Вы знаете? Назовите их достоинства и недостатки.*

Симметричное шифрование использует один и тот же ключ и для зашифровывания, и для расшифровывания.

Сохранение ключа в секретности является важной задачей для установления и поддержки защищённого канала связи. В связи с этим, возникает проблема начальной передачи ключа (синхронизации ключей). Кроме того, существуют методы криптоатак, позволяющие так или иначе дешифровать информацию не имея ключа или же с помощью его перехвата на этапе согласования.

Асимметричное шифрование использует два разных ключа: один для зашифровывания (который также называется открытым), другой для расшифровывания (называется закрытым).

Открытый ключ передаётся по открытому каналу и используется для шифрования сообщения и для проверки ЭЦП. Данная схема решает проблему симметричных схем, связанную с начальной передачей ключа другой стороне. Если в симметричных схемах злоумышленник перехватит ключ, то он сможет как «слушать», так и вносить правки в передаваемую информацию. В асимметричных системах другой стороне передается открытый ключ, который позволяет шифровать, но не расшифровывать информацию. Таким образом решается проблема симметричных систем, связанная с синхронизацией ключей.