**Лабораторная работа 3**

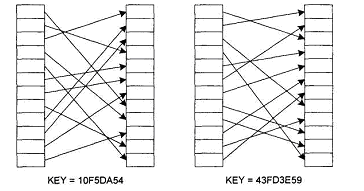
**Блочные алгоритмы шифрования**

**Цель работы:** освоить навыки применения классических блочных методов шифрования данных.

**Краткие теоретические сведения.**

Отличительной чертой *блочных* шифров является обработка исходного тек­ста по несколько (десятки, сотни) бит, т. е. поблочно. Блочные шифры яв­ляются логичным продолжением идеи алфавитных замен, перенесенной в новый цифровой век.

Любой блочный шифр в общем виде представляет собой закон отображения множества входных блоков исходного текста на множество блоков зашиф­рованного текста (рисунок 1). Кроме того, этот закон очень сильно зависит от секретного ключа шифрования.



***Рисунок 1*** *Блочный шифр как закон отображения (на примере двух ключей)*

В принципе, блочный шифр — это шифр замены над очень большим алфа­витом (из десятков и сотен бит). Потенциально любой шифр замены можно описать полной таблицей соответствий между входными и выходными дан­ными. Современный блочный шифр — это закон, описывающий данное отображение *алгоритмически.*

Количество бит в обрабатываемом блоке называется *разрядностью блока,* количество бит в ключе — *размером ключа* алгоритма. Наиболее популярная на сегодняшний день разрядность блока — 64 и 128 бит, о размере ключа уже шел разговор (это 128, 192 или 256 бит). В общем виде про­цесс блочного шифрования описывается формулой:

Z= *En Crypt (X, Key),*

где *X —* блок исходного текста, *Z—* зашифрованный блок, *Key*— ключ шифрования. Разрядность зашифрованного блока в классических блоч­ных шифрах в точности совпадает с разрядностью исходного блока, по­этому за этап собственно шифрования поток данных не уменьшается и не увеличивается в размерах. Дешифрование описывается соответственно формулой

*Х= DeCrypt (Z, Key).*

В тех случаях, когда и для шифрования и для дешифрования используется одна и та же последовательность действий, т. е. *EnCrypt = DeCrypt = Crypt* и, соответственно, *Crypt (Crypt (X, Key), Key) = X* блочный шифр называется *абсолютно симметричным.* Подобные шифры обладают преимуществами и недостатками, а их построение на самом деле не такая сложная задача, как может показаться на первый взгляд.

Одной из наиболее распространенных схем блочных шифров являются *сети* (англ. *network).* Блочный шифр, построенный по такой схеме, состоит из многократных повторений, называемых *циклами,* или *раундами* (англ. *round),* нескольких видов операций, называемых *слоями.* Разбиение всего процесса шифрования на несколько однотипных слоев позволяет:

* сократить размер программного кода использованием цикла;
* унифицировать "алгоритмическую формулу" шифрования и, как следствие, упростить проверку стойкости шифра к известным видам криптоатак;
* сделать шифр легко усложняемым при необходимости (путем увеличе­ния числа раундов);
* ввести понятие *ключей раунда,* на которые разбивается весь материал ключа.

Независимые потоки информации, порожденные из исходного блока, назы­ваются ветвями сети. Операции над вервями определяет функция F(Vi) на­зывается образующей. Величины Vi именуются параметрами сети, обычно их роль играет материал ключа.

**Задание.**

Разработать приложение, выполняющее шифрование и дешифрование текста в соответствии с заданным алгоритмом (табл.1).

Ключ выбрать самостоятельно.

Протестировать работу приложения на не менее чем трех текстах от 10 до 20 символов.

Таблица 1

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Вариант | Вид сети | Образующая функция | Размер входного блока, бит | Число раундов | Расчет параметров сети |
| 1 | Классическая сеть Файстеля | X’=S-box(X) | 64 | 32 | Vi для четных раундов определяет использование первой строки таблицы, для нечетных - второй |
| 2 | Абсолютно симметричная сеть Файстеля | X’=P-box(X) | 64 | 32 |
| 3 | Сеть Файстеля с четырьмя ветвями тип 1 | X’=X ROR Vi | 128 | 16 | Vi определяется i-й парой бит ключа |
| 4 | Классическая сеть Файстеля с предварительным перемешиванием | X’=X ROR Vi | 64 | 16 | Vi определяется i-й парой бит ключа |
| 5 | Классическая сеть Файстеля с предварительным перемешиванием | X’=X ROL Vi | 64 | 16 | Vi определяется i-й парой бит ключа |
| 6 | Сеть Файстеля с четырьмя ветвями тип 2 | X’=X1 + X2 + X3 + Vi | 128 | 16 | Vi для четных раундов определяет первой половиной бит ключа, для нечетных – второй |
| 7 | Сеть Файстеля с четырьмя ветвями тип 3 | X’=X ROL Vi | 128 | 16 | Vi определяется i-й парой бит ключа |
| 8 | Классическая сеть Файстеля | X’=P-box(X) | 64 | 32 | Vi для четных раундов определяет использование первой строки таблицы, для нечетных - второй |
| 9 | Абсолютно симметричная сеть Файстеля | X’=S-box(X) | 64 | 32 |

**Электронный отчет должен содержать**

Титульный лист

Название работы

Цель

Задание

Описание алгоритма

Текст программы с комментариями

Тесты, выполненные вручную

Иллюстрации правильности выполнения тестов программой

Содержательный вывод (копия цели выводом не является).

**Контрольные вопросы и задания.**

1. Кратко охарактеризовать сущность методов изученных при лабораторной выполнении работы.
2. Описать алгоритм одной из криптосистем, представленных в таблице 1.