**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ**

**«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО»**

**Факультет безопасности информационных технологий**

**Дисциплина:**

**«**Разработка систем аутентификации и криптографии**»**

**Лабораторная работа 1** на тему

«Алгоритм шифрования IDEA»

**Выполнил:**

магистрант гр. N42514c

Самоследов Г.А.

**Проверил:**

Федоров И. Р.

Санкт-Петербург

2020

**Цель работы:** приобрести навыки реализации криптографических алгоритмов.

**Задача:** программно реализовать алгоритм шифрования IDEA.

**Средства реализации:**

Язык программирования: C. Выбран как один из наиболее производительных, а также удобный для работы на низком уровне с битами и байтами.

IDE: MS Visual Studio 2017, выбрана как специализированная IDE для программирования на языке C. Также в ней имеется компилятор, что позволяет не устанавливать компилятор отдельно.

**Алгоритм:**

IDEA (англ. International Data Encryption Algorithm, международный алгоритм шифрования данных) — симметричный блочный алгоритм шифрования данных.

Размер ключа: 128 бит (16 байт).

Размер блока: 64 бит (8 байт).

Количество раундов: 8 раундов плюс выходное преобразование.

Количество подключей: по 6 на раунд плюс 4 на выходное преобразование (всего 8\*6 + 4 = 52).

Размер подключа: 16 бит (2 байта).

Количество подблоков: 4.

Размер подблоков: 16 бит (2 байта).

Для шифрования и расшифрования IDEA использует один и тот же алгоритм. Изменяются только подключи: при дешифрации они потребуют дополнительного преобразования.

Каждый исходный незашифрованный 64-битный блок делится на четыре подблока по 16 бит каждый, так как все алгебраические операции, использующиеся в процессе шифрования, совершаются над 16-битными числами.

Применяемый математический аппарат:

* сложение по модулю 216;
* умножение по модулю 216 + 1;
* побитовое исключающее ИЛИ (XOR);
* аддитивная инверсия по модулю 216;
* мультипликативная инверсия по модулю 216 + 1;

Для вычисления мультипликативной инверсии по модулю используются:

* нахождение наименьшего общего делителя;
* малая теорема Ферма;

Также используется циклический битовый сдвиг.

Указанный выше матаппарат реализован без использования сторонних библиотек.

На рисунке 1 изображена схема алгоритма.

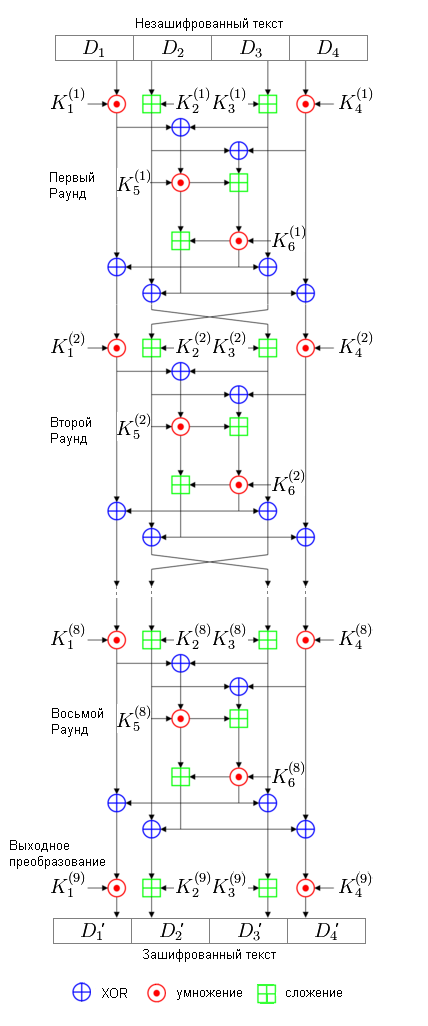


Рисунок 1 – Схема алгоритма IDEA

**Исходный код:**

https://github.com/4444gleb/Cryptography/tree/main/1

**Выводы:**

В ходе проделанной работы был реализован алгоритм шифрования IDEA, были получены навыки реализации криптографических алгоритмов.