Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

ИССЛЕДОВАНИЕ БЛОЧНЫХ ШИФРОВ

Студент: Точило О. В.

ФИТ 3 курс 4 группа

Преподаватель: Сазонова Д. В.

Минск 2024

# **Алгоритм DES**

Алгоритм строится на основе сети Фейстеля. Входной блок данных, состоящий из 64 битов, преобразуется в выходной блок идентичной длины. В алгоритме широко используются рассеивания (подстановки) и перестановки битов текста, о которых мы упоминали выше. Комбинация двух указанных методов преобразования образует фундаментальный строительный блок DES, называемый раундом или циклом. Один блок данных подвергается преобразованию (и при зашифровании, и при расшифровании) в течение 16 раундов. После первоначальной перестановки и разделения 64-битного блока данных на правую и левую половины длиной по 32 бита выполняются 16 раундов одинаковых действий.

Вначале правая часть блока *Ri* расширяется до 48 битов с использованием таблицы, которая определяет перестановку плюс расширение на 16 битов. Эта операция приводит размер правой половины в соответствие с размером ключа для выполнения операции XOR.

После выполнения перестановки с расширением для полученного 48-битного значения выполняется операция XOR с 48-битным подключом *Ki*. Затем полученное 48-битное значение подается на вход блока подстановки *S*, результатом которой является 32-битное значение. Подстановка выполняется в восьми блоках подстановки или восьми *S*-блоках.

При выполнении этой операции 48 битов данных делятся на восемь 6-битных подблоков, каждый из которых по соответствующей таблице замен замещается четырьмя битами. Подстановка с помощью *S*-блоков является одним из важнейших этапов DES. Таблицы замен для этой операции специально спроектированы так, чтобы обеспечивать максимальную криптостойкость. В результате выполнения этого этапа получаются восемь 4-битных блоков, которые вновь объединяются в единое 32-битное значение.

Далее полученное 32-битное значение обрабатывается с помощью перестановки *Р*, которая не зависит от используемого ключа. Целью перестановки является такое максимальное переупорядочивание битов, чтобы в следующем раунде шифрования каждый бит с большой вероятностью обрабатывался другим *S*-блоком.

И наконец, результат перестановки объединяется с помощью операции XOR с левой половиной первоначального 64-битного блока данных. Затем левая и правая половины меняются местами, и начинается следующий раунд.

# **Зашифрование**

Для начала, нам необходимо убедиться, что ключ, подаваемый на вход функции зашифрования, будет иметь размерность 64 бита. Для этого реализована функция, представленная на рисунке 1.1.

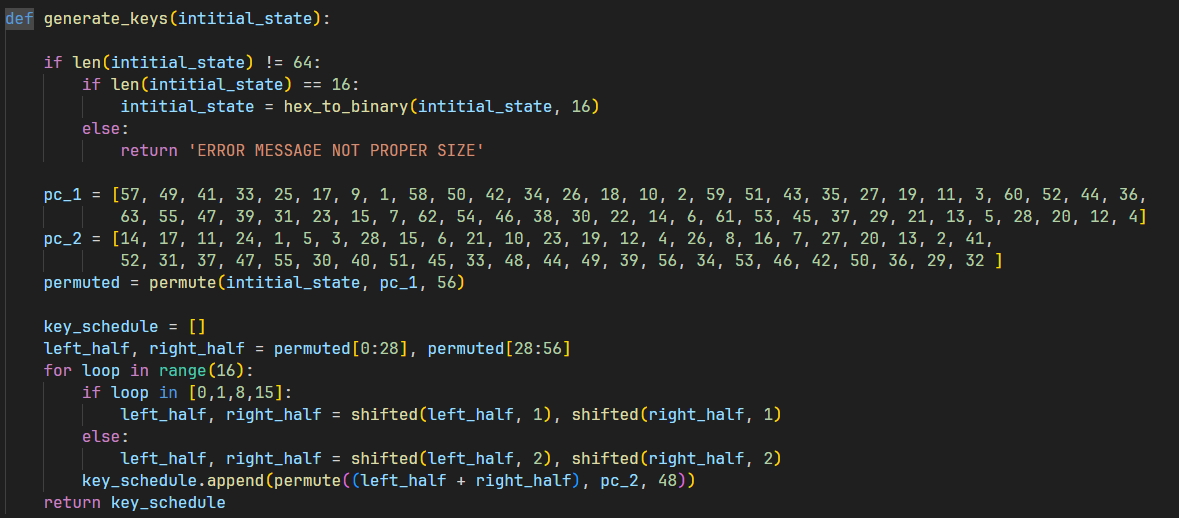


Рисунок 1.1 – Функция для создания 64-битного ключа

Для зашифрования необходимо убедиться, что блоки исходного текста будут иметь размерность 64 бита и при необходимости дополняться до данного размера. Блоки будут дополняться байтами, равными длине дополнения. Например, если размер блока 8 байт, то для дополнения блока длиной 6 байт будет добавлено 2 байта со значением 0x02. Функция зашифрования представлена на рисунке 1.2.

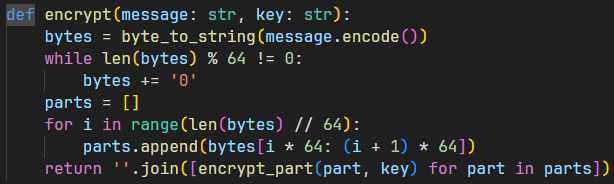


Рисунок 1.2 – Функция зашифрования алгоритмом DES

# **Расшифрование**

Для расшифрования необходимо повторить тот же самый алгоритм с обратным порядком ключей. Если использовались раундовые ключи с 1-го по 16-ый, то при расшифровании они будут применять в обратном порядке – с 16-го по 1-ый. Функция расшифрования представлена на рисунке 1.3.

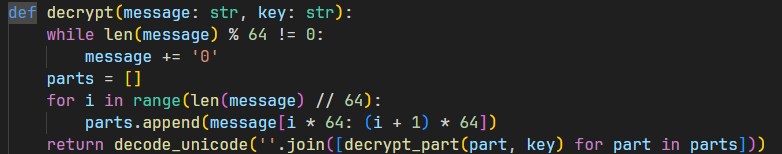


Рисунок 1.3 – Функция расшифрования алгоритмом DES

# **Лавинный эффект**

Алгоритму DES присуще такое свойство, как «лавинный» эффект. Оно заключается в том, что изменение значения малого количества битов во входном тексте или в ключе ведет к «лавинному» изменению значений выходных битов шифротекста.

Для оценки «лавинного» эффекта можно побитово сравнить исходный текст и шифротекст и посчитать количество изменённых битов. Функция, высчитывающая «лавинный» эффект, представлена на рисунке 1.4.

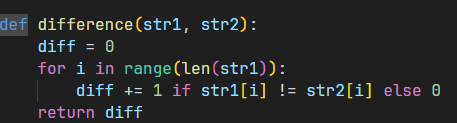


Рисунок 1.4 – Функция оценки «лавинного» эффекта

# **Вывод**

В данный лабораторной работе были изучены и приобретены практические навыки разработки и использования приложений для реализации блочного шифра DES.