1. Министерство науки и высшего образования Российской Федерации
2. Санкт-Петербургский политехнический университет Петра Великого
3. Институт компьютерных наук и кибербезопасности
4. Высшая школа кибербезопасности

**ЛАБОРАТОРНАЯ РАБОТА № 2**

1. по дисциплине «Основы построения стойких криптопримитивов и псевдослучайных генераторов»
2. Выполнил
3. студент гр. 5151001/00201 Устюгов А.А.

<*подпись*>

1. Преподаватель д.ф.-м.н. Шенец Н.Н.

<*подпись*>

1. Санкт-Петербург
2. 2024

# Цель работы

Изучение разностного метода криптоанализа, способов его оптимизации и способа оценки стойкости шифра.

# Задание

1. В качестве анализируемой блочной криптосистемы взять свой вариант криптосистемы из курса КМЗИ.
2. Изучить метод оценки стойкости шифра к разностному криптоанализу
3. Составить таблицу разностей подстановки
4. Найти наиболее вероятную характеристику, ее вероятность и оценить стойкость шифра к разностному методу

# Ход работы

В заданной криптосистеме есть 4 раунда: SP-сеть, подстановка Фейстеля, SP-сеть, подстановка Лай-Месси. Подстановка представлена вектором {11, 7, 14, 3, 9, 15, 0, 6, 13, 1, 10, 12, 8, 2, 4, 5}, Перестановка задана функцией f(x) = 21\*x+23(mod 32), в качестве функции для подстановок Фейстеля и Лай-Месси выступает 16-битная SP-сеть.

В основу разностного криптоанализа положена неравномерность распределения поразрядных разностей по модулю 2 (в общем случае по модулю степени 2) пар открытых и соответствующих зашифрованных текстов. Необходимым условием того, что разностный криптоанализ r-тактового шифра будем успешным, является существование (r-1)-тактовых дифференциалов, вероятность которых значительно больше, чем , n – длина блока.

Дифференциал для *i* тактов шифрования (*i*-тактовый дифференциал) определяется как пара векторов такая, что пара открытых текстов с разностью может перейти после i-го такта в пару выходных текстов с разностью .

Вероятность *i*-тактового дифференциала – это условная вероятность того, что разность пары шифртекстов после *i*-го такта равна при условии, что пара соответствующих открытых текстов имеет разность , когда открытый текст и ключи, используемые на тактах шифрования, независимы и равновероятны.

Дифференциальная характеристика – последовательность однотактовых дифференциалов, при этом выходная разность текстов для предыдущего такта совпадает с входной разностью текстов последующего такта. S-блок называется активным, если он входит в характеристику. Для того, чтобы характеристика, составленная из наиболее вероятных однотактовых дифференциалов, имела большую вероятность, она должна содержать минимальное число активных s-блоков.

Обычно наилучшая характеристика, составленная из S-блоков для соответствующих тактов шифрования, имеет вид «песочных часов»: на первых тактах число активных s-блоков велико, с ростом номера такта их число сначала сокращается, а потом увеличивается.

В данной работе необходимо найти высоковероятный 3-тактовый дифференциал.

В предыдущей работе была получена таблица разностей для заданной подстановки (рисунок 1).

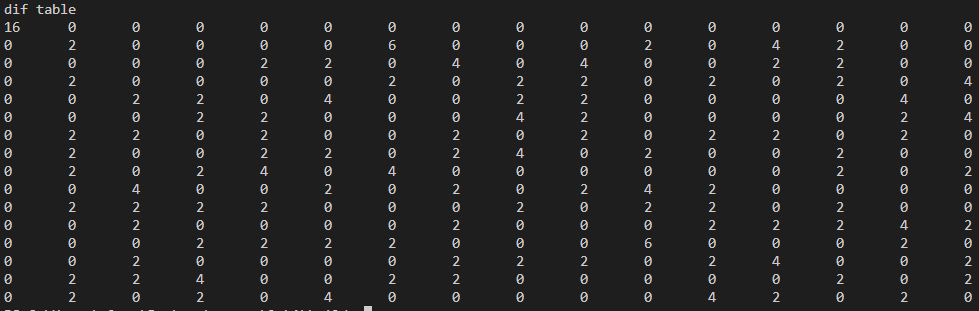


Рисунок 1 – таблица разностей подстановки

Начнем анализ с подстановки Фейстеля. Структура подстановки представлена на рисунке 2.

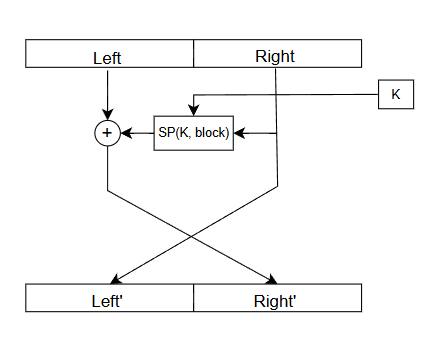


Рисунок 2 – структурная схема подстановки Фейстеля

Перейдем сразу к тому, что будем анализировать разности текстов, приходящих на вход подстановки. Если , то тоже равна 0. Кроме этого, выход SP-сети тоже равен 0 и поэтому с вероятностью 1.

Вход 3 раунда связан с выходом 1 раунда, так как подстановка Фейстеля для заданной входной разности лишь меняет полублоки местами, поэтому, можно взять тот, который соответствует максимальному значению в таблице разности подстановки. В таблице разности подстановки максимальное значение 6 соответствует и .

Пусть . Тогда выход после 1 такта зашифрования равен . На рисунке 3 изображена SP-сеть, где прерывистой линией проведен путь к выходу s-блока, откуда должна выйти 1. Из рисунка понятно, что необходимо найти максимальный элемент в таблице разностей в 8 столбце. Максимальное значение равно 4 и оно соответствует двум . Соответственно, на вход 1 раунду зашифрования можно подать два текста со следующими разностями: 0 || 0101 || 0 || 0 || 0 || 0 || 0 || 0 или = 0 || 0111 || 0 || 0 || 0 || 0 || 0 || 0 и с вероятностью 0,25 на выходе будет .

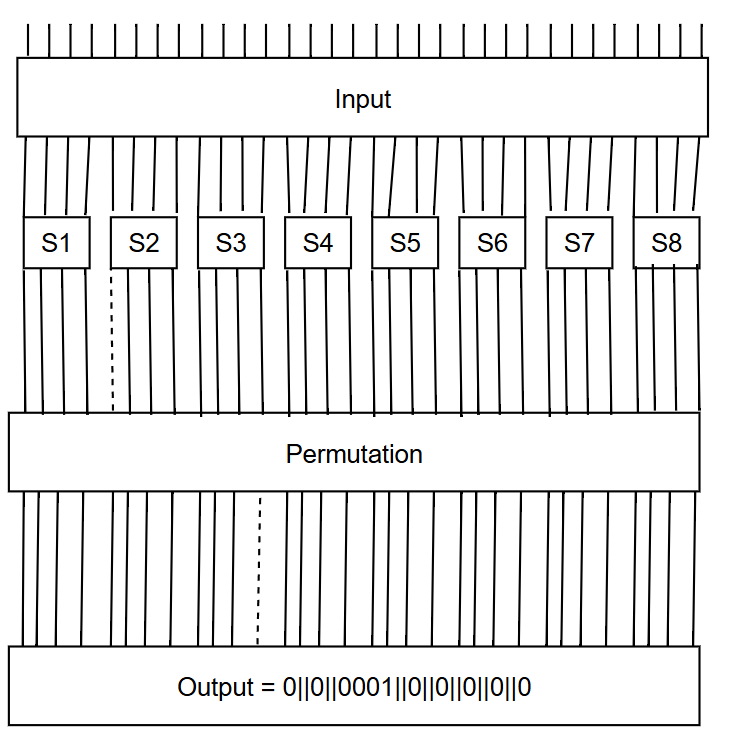


Рисунок 3 – SP-сеть 1 раунда

Перейдем к 3 раунду зашифрования. Так как изначально подбирали вход, для которого существует максимальное значение из таблицы разности, то мы знаем выход s-блока с вероятностью 0,375. Тогда легко построить выход , который и будет подаваться на вход 4 раунду. На рисунке 4 представлена SP – сеть с заданным входом 0 || 0 || 0 || 0 || 0 || 0 || 0001 || 0. По рисунку видно, что 0 || 1000 || 0 || 0 || 0 || 0 || 0100 || 0. Тогда, активными S-блоками являются и . Они же и входят в характеристику. Вероятность характеристики равна 0,375 \* 0,25 = 0,09375. Для взлома последнего тактового ключа достаточно примерно 11 пар открытый текст – шифртекст.

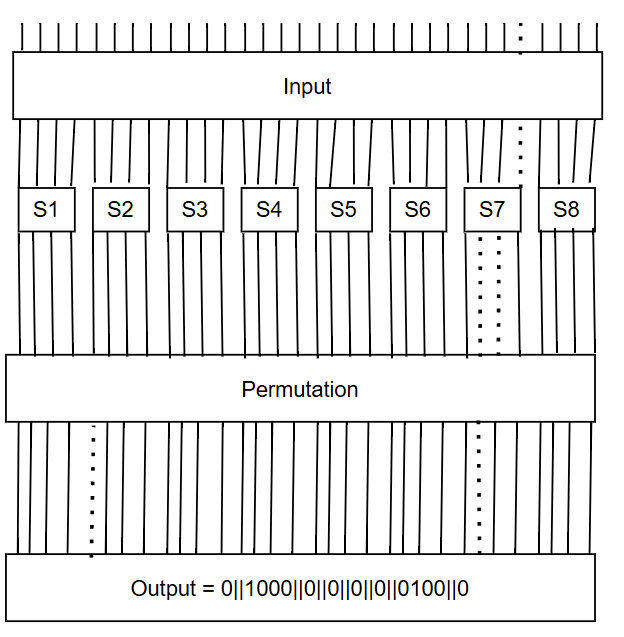


Рисунок 4 – SP – сеть 3 раунда

Если при первом предположении использовать , то вероятность характеристики точно не увеличится, а скорее всего даже уменьшится, поскольку тогда на первом раунде будет участвовать не 1 s-блок, а 2, поэтому данный вариант подробно не рассматривался.

# Контрольные вопросы

1. *Что такое характеристика?*

Дифференциальная характеристика – последовательность однотактовых дифференциалов, при этом выходная разность текстов для предыдущего такта совпадает с входной разностью текстов последующего такта

1. *Как можно найти распределение вероятностей дифференциалов подстановки?*

По таблице разностей подстановки.

1. *Как влияет вес дифференциалов на стойкость шифра?*

Одним из вариантов построения высоковероятностной характеристики является построение, составленное из дифференциалов веса 2, которые обладают ненулевой вероятностью, поскольку число активных дифференциалов в такой характеристике минимально. Поэтому желательно, чтобы подстановка имела минимально возможную вероятность дифференциалов веса 2.

1. *Почему сложность атаки практически не зависит от того, одинаковы или попарно различны тактовые ключи подстановки?*

Потому что атака проводится в предположении, что все ключи распределены равновероятно.

# Вывод

В результате данной работы была найдена высоковероятностная 3-х тактовая характеристика для заданной криптосистемы. В нее вошло 2 s-блока, вероятность характеристика равна 0,09375, что явно больше чем , поэтому, скорее всего, разностная атака пройдет успешно. Для атаки достаточно около 11 пар открытый текст – шифртекст.