Контрольная работа
Вариант №4.

Роман Астраханцев, СКБ-171

15 февраля 2022 г.

Задача 1

Дана сеть Фейстеля, состоящая из 8 итераций, с длиной блока $n = 128$ бит. Из мастер ключа $K = (K_1, K_2, K_3, K_4)$, где $K_1, \ldots, K_4 \in V_{64}$, итерационные ключи (на итерациях $1, 2, 3, \ldots, 8$) получаются вырабаютываются как последовательность $K_3, K_2, K_4, K_1, K_3, K_2, K_4, K_1$. Обозначим за $E : V_{128} \times V_{256} \to V_{128}$ алгоритм зашифрования.

Описать трудоемкость, вероятность успеха, затраты по памяти и объём материала для методов тотального опробования и слайд-атаки.

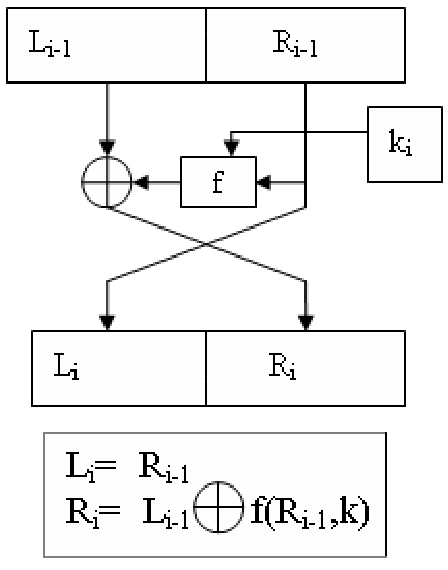

Рис. 1: Раунд сети Фейстеля

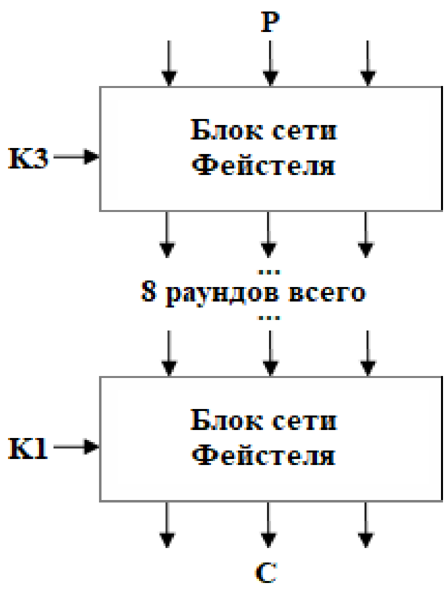

Рис. 2: Шифр из задачи

Метод тотального опробования

Для начала определим количество материала, необходимое для однозначного опредления ключа. Поскольку одной на паре (P, C) открытого и шифрованного текста, где $P, C \in V_{128}$, можно отбраковать 2^{128} ключей, то потребуется $\lceil \frac{256}{128} \rceil = 2$ различные пары: $(P_1, C_1), (P_2, C_2)$. Будем дальше считать, что они нам даны.

Алгоритм 1: Метод тотального опробования

Вход: Пары открытого и шифрованного текста $(P_1, C_1), (P_2, C_2)$
Выход: Ключ шифрования K
1. **Для каждого** $\tilde{k} \in V_{256}$ **:**
2. Вычислить $B_1 = E(P_1, \tilde{k})$
3. **Если** $B_1 = C_1$, **то**
4. Вычислить $B_2 = E(P_2, \tilde{k})$
5. **Если** $B_2 = C_2$, **то**
6. Закончить алгоритм и вернуть $\tilde{k}$

Трудоёмокстъ Q этого алгоритма будем измерять в количествах зашифрования, а необходимую для работы алгоритма память M в битах. Тогда имеем

$$Q = 2^{256} + 2^{128} + 1 \approx 2^{256}$$

$$M = (128 + 128) * 2 = 512$$

Вероятность успеха алгоритма $P = 1$, поскольку алгоритм гарантированно находит ключ шифрования.

Слайд-атака

Заметим, что алгоримт зашфирования E представим как $E = G \circ G$, где $G : V_{128} \times V_{256} \to V_{128}$ – работа первых 4 раундов сети Фейстеля представленного в задаче шифра. Точно так же, как и в методе тотального опробования, после нахождения слайд-пары необоходимо будет доопробовать найденный ключ. В общем итоге для восстановления ключа нам потребуется $\lceil \frac{256}{128} \rceil = 2$ различные пары: $(P_1, C_1), (P_2, C_2)$. Будем дальше считать, что они нам даны. Также будем считать, что нам дана возможность по любому открытому тексту получить его зашифрованную версию, иными словами для любого открытого текста P мы можем вычислить $E(P, K)$ даже не зная K.

Алгоритм 2: Метод скольжения

Вход: Пары открытого и шифрованного текста $(P_1, C_1), (P_2, C_2)$

Выход: Ключ шифрования K

```
Принять i = 1
Пока ключ не найден или i > 2^64
    i = i + 1
    Выберем случайно P ∈ V_128 – открытый текст
    Посчитаем C = E(P, K)
    Выберем случайно P' ∈ V_128 – другой открытый текст
    Посчитаем C' = E(P', K)
    Если пары (P, C) и (P', C') совпали, то
        Перейти на новую итерацию цикла
    Решим уравнение P' = G(P) и результат занесём в K_first
    Решим уравнение C' = G(C) и результат занесём в K_last
    Если K_first = K_last то
        Доопробуем ключ K_first на парах (P_1, C_1), (P_2, C_2) и в
         случае успеха вернём ключ K_first
```

Алгоритм 2 был сформулирован как вероятностный, чтобы продемонстрировать его основные характеристики. Детеременированная версия алгоритма (вероятность успеха которой равна 1) легко получается заменой случайного выбора на перебор всевозможных значений.

Трудоёмкость Q этого алгоритма будем измерять в количествах зашифрования, а необходимую для работы алгоритма память M в битах. Тогда имеем

$$Q = 2^{64} \cdot 2q$$

$$M = (128 + 128) * 2 = 512,$$

где q – это сложность решения уравнения $P' = G(P)$ относительно ключа k.

Согласно парадоксу дней рождений вероятность успеха алгоритма $P \gg 0.9999$.