Лекция 12. Дифференциальный криптоанализ

Цель лекции: рассмотреть один из универсальных методов криптоанализа.

План лекции:
Введение.
1 Дифференциальный криптоанализ
Заключение
Контрольные вопросы

Ключевые слова: [выбрать самостоятельно].

Содержание лекции:

Введение

1 Дифференциальный криптоанализ

Пусть некоторый блочный шифратор с длиной блока N строится по схеме.

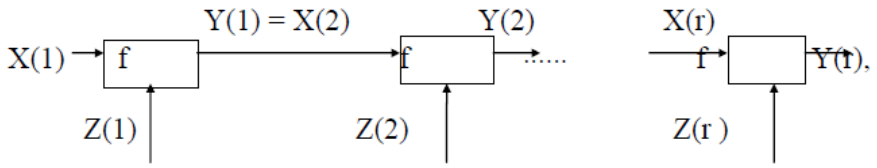

Рис. 1. Блочный шифратор

где Z = (Z(1), Z(2), …, Z(r)) получается по некоторой схеме из Z0, или независимо и равновероятно выбирается для каждого цикла. Пусть X(1) и $X^*(1)$ - пара открытых текстов. Рассмотрим следующие разности:

$$\Delta X(1) = X(1) - X^*(1),$$

$$\Delta Y(i) = Y(i) - Y^*(i).$$

Если мы знаем открытый и шифрованный текст в одном i-ом цикле DES, то несложно определить часть ключа Z(i), которая используется в i-ом цикле (идея Шеннона о суперпозиции простых шифров для получения сложного шифра). Но, если мы знаем ΔX(i), Y(i) и $Y^*(i)$, то задача становится более сложной, но также решается, если решается предыдущая задача.

Определение 1. Преобразование f называется криптографически слабым, если по ΔY(r – 1), Y(r) и $Y^*(r)$ для некоторого (малого) числа пар (X(1), $X^*(1)$) можно найти (хотя бы часть) Z(r).

Идея дифференциального криптоанализа [1] заключается в том, чтобы найти такие ΔX(1), что при случайном равновероятном выборе X(1), Z(1), Z(2), ..., Z(r-1) с вероятностью более $1/2^N$ появится ΔY(r-1).

Определение 2. Пара (α, β) возможных значений вектора (ΔX(1), ΔY(i)) называется дифференциалом i-ого цикла.

Тогда дифференциальный криптоанализ описывается следующей моделью.

---

[1] Biham E., Shamir A. Differential Cryptanalysis of the Data Encryption Standard, Springer- Verlag, 1993.

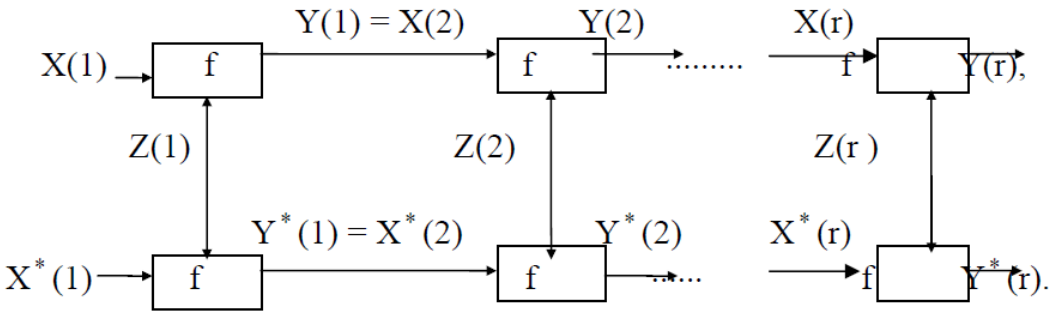

Рис. 2. Модель дифференциального криптоанализа

Пусть f определяет операции в Δ и f криптографически слаба. Тогда возможна следующая атака.

1. Выбираем дифференциал (r – 1)-го цикла (α, β), для которого вероятность P(ΔY(r – 1) = β|ΔX(1) = α) большая.
2. Случайно выбираем X(1) и подбираем $X^*(1)$, чтобы ΔX(1) = α. Пусть известны Y(r) и $Y^*(r)$.
3. Делаем предположение, что ΔY(r – 1) = β и, зная Y(r) и $Y^*(r)$, находим Z(r).
4. Повторяем 2 и 3 пока один (частичный) ключ не начнет появляться чаще других. Это и будет Z(r).
5. Повторяем 1 – 4 до нахождения полного ключа.

Заключение

Контрольные вопросы

Смотри руководство по организации самостоятельной работы магистрантов.