3.3. Дифференциальный и линейный криптоанализ

Понятие *дифференциального криптоанализа* было введено Эли Бихамом (Biham) и Ади Шамиром (Shamir) в 1990 году. Конечная задача ***дифференциального криптоанализа*** - используя свойства алгоритма, в основном свойства *S-box*, определить *подключ раунда*. Конкретный способ *дифференциального криптоанализа* зависит от рассматриваемого алгоритма шифрования.

Если в основе алгоритма лежит *сеть Фейштеля*, то можно считать, что блок m состоит из двух половин - m_0 и m_1. *Дифференциальный криптоанализ* рассматривает отличия, которые происходят в каждой половине при шифровании. (Для алгоритма *DES* "отличия" определяются с помощью операции XOR, для других алгоритмов возможен иной способ). Выбирается пара незашифрованных текстов с фиксированным отличием. Затем анализируются отличия, получившиеся после шифрования одним *раундом* алгоритма, и определяются вероятности различных ключей. Если для многих пар входных значений, имеющих одно и то же отличие X, при использовании одного и того же *подключа* одинаковыми (Y) оказываются и отличия соответствующих выходных значений, то можно говорить, что X влечет Y с определенной вероятностью. Если эта вероятность близка к единице, то можно считать, что *подключ раунда* найден с данной вероятностью. Так как *раунды* алгоритма независимы, вероятности определения *подключа* каждого *раунда* следует перемножать. Как мы помним, считается, что результат шифрования данной пары известен. Результаты *дифференциального криптоанализа* используются как при разработке конкретных *S-box*, так и при определении оптимального числа *раундов*.

Другим способом криптоанализа является *линейный криптоанализ*, который использует линейные приближения преобразований, выполняемых алгоритмом шифрования. Данный метод позволяет найти ключ, имея достаточно большое число пар (незашифрованный текст, зашифрованный текст). Рассмотрим основные принципы, на которых базируется *линейный криптоанализ*. Обозначим

P[1], … , P[n] - незашифрованный блок сообщения.

C[1], … , C[n] - зашифрованный блок сообщения.

K[1], … , K[m] - ключ.

$A[i, j, \ldots, k] = A[i] \oplus A[j] \oplus \ldots \oplus A[k]$

Целью *линейного криптоанализа* является поиск линейного уравнения вида

$P[\alpha_1, \alpha_2, \ldots, \alpha_a] \oplus C[\beta_1, \beta_2, \ldots, \beta_b] = K[\gamma_1, \ldots, \gamma_c]$

Выполняющееся с вероятностью $p <> 0.5$. α_i, β_i и γ_i - фиксированные позиции в блоках сообщения и ключе. Чем больше p отклоняется от 0.5, тем более подходящим считается уравнение.

Это уравнение означает, что если выполнить операцию XOR над некоторыми битами незашифрованного сообщения и над некоторыми битами зашифрованного сообщения, получится бит, представляющий собой XOR некоторых битов ключа. Это называется линейным приближением, которое может быть верным с вероятностью p.

Уравнения составляются следующим образом. Вычисляются значения левой части для большого числа пар соответствующих фрагментов незашифрованного и зашифрованного блоков. Если результат оказывается равен нулю более чем в половине случаев, то полагают, что $K[\gamma_1, \ldots, \gamma_c] = 0$. Если в большинстве случаев получается 1, полагают, что $K[\gamma_1, \ldots, \gamma_c] = 1$. Таким образом получают систему уравнений, решением которой является ключ.