Лекция 6. Метод «разделяй и побеждай»

Цель лекции: рассмотреть один из универсальных методов криптоанализа.

План лекции:
Введение.
1 Метод «разделяй и побеждай»
Заключение
Контрольные вопросы

Ключевые слова: [выбрать самостоятельно].

Содержание лекции:

Введение

Рассмотрим метод, являющийся обобщением изложенного в лекции 3 аналитического метода.

1 Метод «разделяй и побеждай»

Пусть по-прежнему даны множества X открытых текстов, Y – шифрованных текстов, K – ключей, и шифр T: $X \times K \to Y$.

Предположим, что множество ключей K допускает представление $K = K_1 \times K_2$. То есть каждый ключ $k \in K$ может быть записан в виде вектора $k = (k_1, k_2)$, где $k_1 \in K_1$, $k_2 \in K_2$.

Предположим дополнительно, что существует критерий h, позволяющий при известных x и y проверять правильность компоненты k_1 в ключе $k = (k_1, k_2)$. То есть для любого k_2 функция $h(x, y, k_1) = 1$, если $\exists\, k_2 \in K_2$ такой, что $T(x, (k_1, k_2)) = y$, и $h(x, y, k_1) = 0$, если $\forall\, k_2 \in K_2$ $T(x, (k_1, k_2) \neq y$.

Если известные открытый и шифрованный тексты достаточно длинные, то достаточно часто существует единственный ключ k такой, что $T(x, k) = y$, поэтому сделанное предположение допустимо. Тогда метод «разделяй и побеждай» предлагает опробовать сначала элементы множества K_1, отбраковывая варианты k_1 по критерию h. Отсюда мы определим k_1 – первую компоненту вектора $k = (k_1, k_2)$. Затем, используя уравнение $T(x, (k_1, k_2)) = y$ относительно неизвестного параметра $k_2 \in K_2$, опробуем варианты k_2. Трудоемкость определения компоненты k_1 равна в среднем $|K_1|/2$ операций опробования, соответственно трудоемкость определения k_2 равна в среднем $|K_2|/2$ операций опробования. Тогда в среднем трудоемкость метода равна $|K_1|/2 + |K_2|/2$ против $|K_1| \cdot |K_2|/2$ при методе полного перебора.

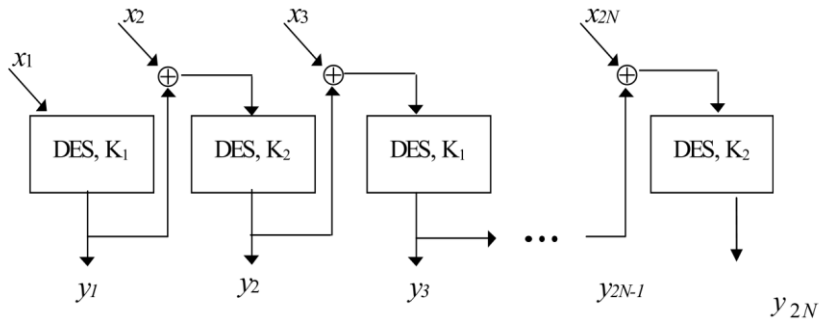

Рис. 6.1. Схема двойного DES

Пример. Рассмотрим вариант двойного DES. Пусть используются два ключа DES k_1 и k_2. Открытый текст x разбивается на последовательность 64-битных блоков $x = x_1, x_2, \ldots, x_{2N}$, а последовательность 64-битных блоков шифрованного текста $y = y_1, y_2, \ldots, y_{2N}$

получается поочередным применением алгоритма DES с ключами k_1 и k_2 к блокам открытого текста, сложенным с предыдущим блоком шифртекста. Схема шифрования приведена на рисунке 6.1.

Пусть известны открытый и шифрованный тексты x, y и N достаточно велико. Для применения метода «разделяй и побеждай» выделим четные и нечетные пары блоков в (x, y): A = {(x_{2k+1}, y_{2k+1}), k = 0, N – 1} и B = {x_{2k}, y_{2k}), k = 1, ..., N}. Преобразуем эти множества в следующие:

$$A' = \{(x_{2k+1} \oplus y_{2k}, y_{2k+1}), k = 0, \dots, N-1, y_0 = 0\},$$
$$B' = \{(x_{2k} \oplus y_{2k-1}, y_{2k}), k = \overline{1, N}\}.$$

Блоки из A' получены по ключу k_1. Определим его опробованием, затратив в среднем $2^{56}/2$ операций опробования. В качестве h здесь берем функцию равную единице, когда

$$DES(x_{2k+1} \oplus y_{2k}, k_1) = y_{2k+1}, \quad k = \overline{0, N-1}.$$

Затем ищем k_2, опираясь на множество B' и уравнение

$$DES(x_{2k} \oplus y_{2k-1}, k_2) = y_{2k}$$

Определение k_2 потребует в среднем $2^{56}/2$ операций опробования. Тогда трудоемкость определения ключа k = (k_1, k_2) в среднем равна 2^{56} операций опробования.

Заключение

Данный метод является обобщением изложенного в лекции 3 аналитического метода подбора системы уравнений, зависящих от части ключей.

Основная проблема при применении метода «разделяй и побеждай» [1] состоит в нахождении критерия h, который зависит от конкретного преобразования T или вообще может не существовать. Иногда критерий h может описываться вероятностно-статистической моделью. Мы рассмотрим такой пример в разделе «Статистические методы анализа».

Контрольные вопросы

Смотри руководство по организации самостоятельной работы магистрантов.

[1] Golic J. Intrinsic Statistical Weakness of Keystream generators//Advances in Cryptology - ASIACRYPT'94, Lecture Notes in Computer Science, Springer- Verlag, 1995, v. 917, c. 91-103.