Лекция 15. Атака на тройной DES с помощью линейного криптоанализа

Цель лекции: обсудить возможные варианты атак на тройной DES.

План лекции:
Введение.
1 Атака на тройной DES с помощью линейного криптоанализа
2 Техника атаки на тройной DES, основанная на задаче о днях рождения.
3 Криптоанализ режима DES, предложенного в качестве стандарта ANSI X9.52.
Заключение
Контрольные вопросы

Ключевые слова: [выбрать самостоятельно].

Содержание лекции:

Введение

1 Атака на тройной DES с помощью линейного криптоанализа

Рассмотрим схему тройного DES в режиме CBC/ECB/CBC [1].

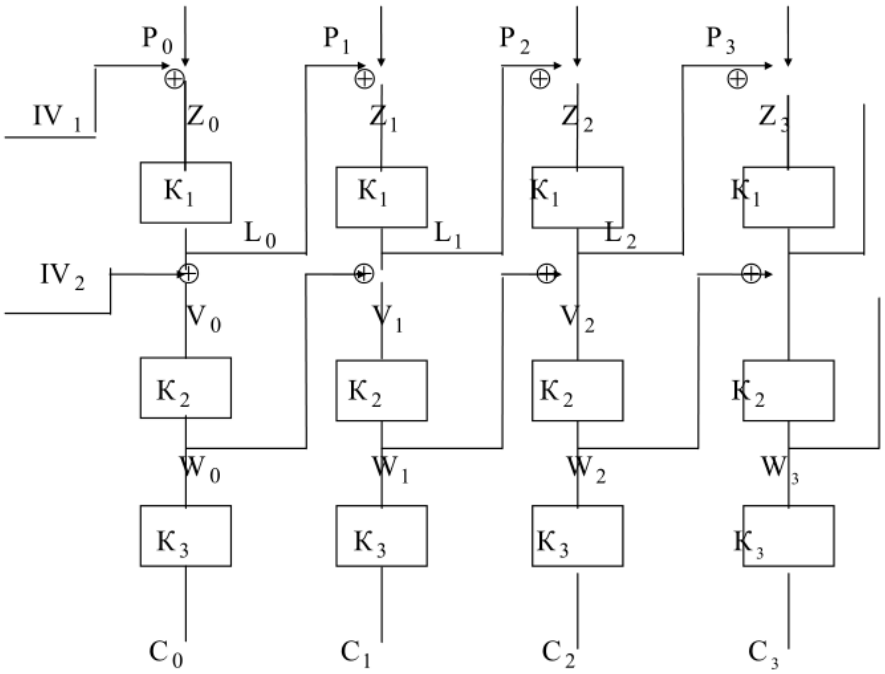

Рис. 1. Схема тройного DES: CBC/CBC/ECB

Пусть найдено достаточно много шифртекстов (C_0, C_1, C_2), где C_1 и C_2 – фиксированы, а C_0 – произвольные и различные.

1) Сначала атакуем ключ K_2. Обозначим через W_i – вход последнего блока, V_i – выход второго блока и через Z_i, L_i – вход и выход первого блока соответственно, P_i – открытый текст. Для всех векторов

$$L_1 = D_{K_2}(V_1), \quad V_1 = C_0 + W_1.$$

[1] Biham E. Cryptanalysis of Multiple Modes of Operation // Proc. ASIACRYPT'94, Springer-Verlag, 1994, с. 278 – 291.

Отсюда

$$L_1 = D_{K_2}(C_0 + W_1). \quad (1)$$

Для всех векторов $V_2 = W_2 + C_1$ одно и то же, так как $W_2 = D_{K_3}(C_2)$. Следовательно, для них $L_2 = D_{K_2}(V_2)$ одно и то же. Отсюда получаем

$$P_2 = D_{K_3}(C_0 + W_1) + Z_2, \quad (2)$$

где для всех C_0 векторы W_1 и Z_2 остаются одинаковыми. Нам известны P_2 и C_0, а неизвестны K_2, W_1 и Z_2. Пусть $D^*_{K_2}(\cdot)$ – линейный статистический аналог $= D_{K_2}(\cdot)$. Тогда

$$P_2 = D^*_{K_2}(C_0 + W_1) + Z_2 + \quad (3)$$

– линейное уравнение относительно K_2, W_1 и Z_2. Набирая и решая системы при различных (C_0, P_2), статистически выделяем решение K_2, W_1 и Z_2.

2) $E_{K_3}(W_1) = C_1$.

Отсюда с помощью метода полного перебора получим K_3.

3) Зная K_2, K_3, получим L_2 и, зная Z_2, методом полного перебора из соотношения $E_{K_1}(Z_2) = L_2$ находим K_1.

2 Техника атаки на тройной DES, основанная на задаче о днях рождения.

Рассмотрим схему тройного DES CBC/CBC/CBC [2].

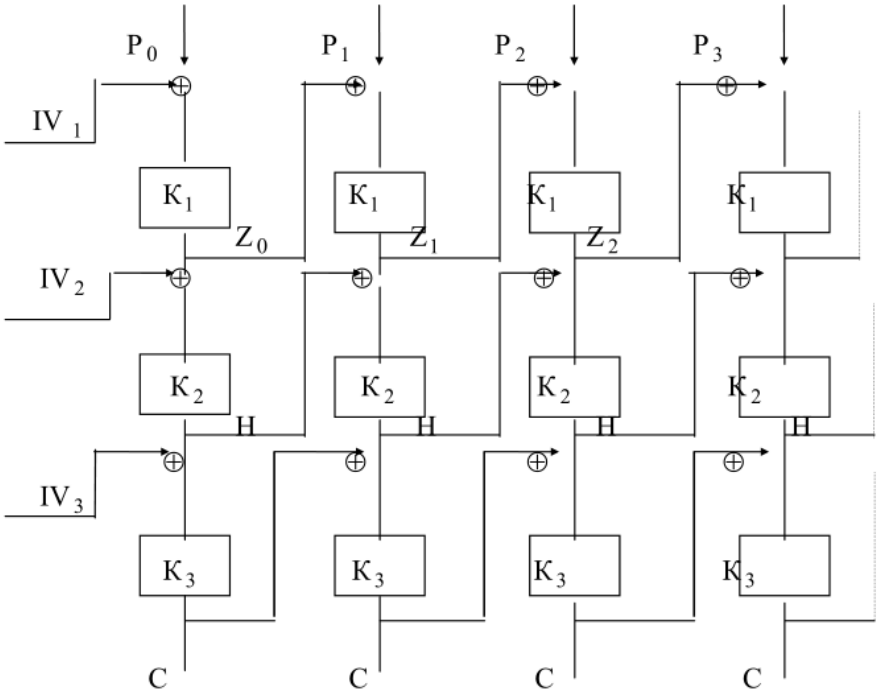

Рис. 2. Схема тройного DES CBC/CBC/CBC

Пусть найдено 2^{33} шифртекстов вида (C, C, C, C). Атака сначала ведется на ключ K_3. На выходе второго блока шифрования имеем четверку вида (?, H, H, H), где

[2] Biham E. Cryptanalysis of Multiple Modes of Operation // Proc. ASIACRYPT'94, Springer-Verlag, 1994. – С. 278 – 291.

$$H = C + D_{K_3}(C).$$

H – это случайная функция от C, не являющаяся подстановкой. По результатам задачи о днях рождения с большой вероятностью существуют C и C^*, дающие одно и то же H, так как H – не взаимно-однозначное отображение. Тогда для двух C и C^* появится одно и то же P_3. Действительно, для C и C^*

$$Z_2 = D_{K_2}(H) + H.$$

Отсюда

$$P_3 = Z_2 + D_{K_1}(Z_3) = Z_2 + D_{K_1}\big(D_{K_2}(H) + H\big).$$

Для такой пары C и C^* имеем уравнение

$$C + D_{K_3}(C) = C^* + D_{K_3}(C^*),$$

где C и C^* известны. Методом полного перебора находим ключ K_3. Аналогичным образом находим K_2 и K_3.

3 Криптоанализ режима DES, предложенного в качестве стандарта ANSI X9.52.

Для повышения стойкости тройного DES было предложено усилить режим с зацеплением тройного DES маскировками (CBCM). Biham и Knudsen [3] построили атаку на эту систему, значительно снижающую стойкость. Поэтому данный алгоритм в последний момент был снят с голосования по принятию его как стандарта.

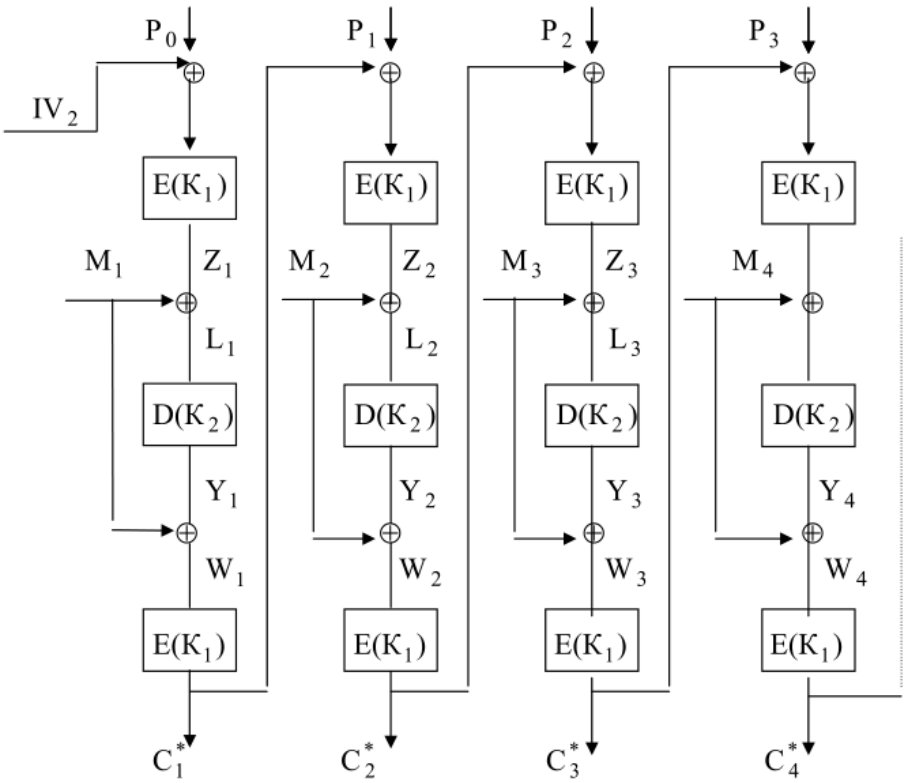

Рис. 3. Схема CBCM

[3] Biham E., Knudsen L. Cryptanalysis of the ANSI X.9.52 CBCM Mode/Technion – Computer Science Department – Technical Report CS 0928, 1998.

Схема маскировки выглядит следующим образом (OFB).

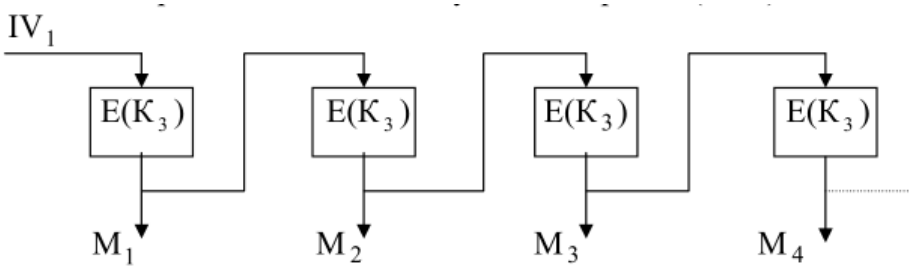

Рис. 4. Схема маскировки OFB

Рассмотрим два блока шифртекста длины 2^{64} C_1 и C_2. Ключи K_1, K_2, K_3 и произвольные IV неизвестны. Допустим, что дан такой открытый текст, что получено 2^{64} C_1, а затем 2^{64} C_2. Период схемы OFB самое большее 2^{64} (в среднем 2^{63}). Поскольку IV2 неизвестно, то не будем принимать во внимание первый блок C_1 и первый блок C_2. Обозначим блоки открытого текста (после удаления первых блоков) в первых p шагах через $P_{1,1}$, …, $P_{1,p}$. Тогда входы на первые блоки шифрования DES на ключе K_1 равны

$$Q_{1,i} = P_{1,i} + C_1, \qquad i = 1, \ldots, p.$$

$Q_{1,i}$ и зашифровываются в C_1 при использовании маскирующего блока M_i. Аналогично для любого i $P_{2,i}$ – блок открытого текста, который под действием той же маскировки M_i переводится в C_2.

$$Q_{2,i} = P_{2,i} + C_2, \qquad i = 1, \ldots, p.$$

Опробуем ключ K_1. Если мы угадали ключ, то должно выполняться равенство

$$E_{K_1}(P_{1,i} + C_1) + D_{K_1}(C_1) = L_i + Y_i, \quad i = 1, \ldots, p.$$

Аналогичное равенство выполняется и для C_2:

$$E_{K_1}(P_{1,i} + C_2) + D_{K_1}(C_2) = L_i + Y_i, \quad i = 1, \ldots, p.$$

Рассмотрим отображение

$$E_{K_2}(\cdot) + V,$$

где V – фиксировано. Это отображение пространства 64-мерных выборок в себя. Пусть V – случайно. Тогда с большой вероятностью существует ровно одна неподвижная точка этого отображения. Эта задача может быть проинтерпретирована следующим образом. Пусть N = 2^{64} дробинок размещают по 2^{64} ящикам. Какова вероятность того, что ровно одна дробинка попадет в свой ящик? N^N общее число размещений N дробинок по N ящикам. Тогда число благоприятных событий (ровно одна дробинка попадет в свой ящик) будет равно N и, соответствующая вероятность

$$p = \frac{N(N-1)^{N-1}}{N^N} = \left(1 - \frac{1}{N}\right)^N \sim e^{-1}.$$

Если для некоторого i эта точка равна $M_i = D_{K_1}(C_{K,i})$, то тогда

$$Q_{K,i} = D_{K_1}\left(M_i + E_{K_2}\left(M_i + D_{K_1}(C_{K,i})\right)\right) =$$
$$= D_{K_1}\left(M_i + V + \left(M_i + D_{K_1}(C_{K,i})\right)\right) =$$
$$= D_{K_1}\left(V + D_{K_1}(C_{K,i})\right).$$

Тогда атака состоит из следующих шагов:

1. Выбираем произвольный блок V.
2. Опробуем ключ K_1. Пусть K' – очередной проверяемый ключ.
3. Вычисляем

$$T_1(K') = D_{K'}\left(V + D_{K'}(C_1)\right),$$
$$T_2(K') = D_{K'}\left(V + D_{K'}(C_2)\right). \quad (4)$$

Находим подходящие тексты такие, что

$$Q_{1,i} = T_1(K'), \quad Q_{2,j} = T_2(K').$$

4. Если нашли такие открытые тексты, то вычисляем U = D K (C1) + D K (C 2).

$$U = D_{K'}(C_1) + D_{K'}(C_2).$$

С учетом (4) последнее равенство влечет

$$U = E_{K'}\left(Q_{1,i}\right) + E_{K'}\left(Q_{2,j}\right).$$

Теперь проверяем равенство

$$U = E_{K'}\left(Q_{2,i}\right) + E_{K'}\left(Q_{1,j}\right).$$

5. Если равенство выполняется, то ключ K_1 = K'. Если равенство не выполняется, то опробуем новый K'.
6. Если ключ K_1 не найден, то опробуем другое V и повторяем действия 1 – 5.

Объясним причину работы атаки. Поскольку неподвижная точка одна, то

$$M_i + D_{K'}(C_1) = M_j + D_{K'}(C_2).$$

Тогда

$$D_{K'}(C_1) + D_{K'}(C_2) = M_i + M_j = U. \quad (5)$$

Рассмотрим теперь $Q_{1,j}$ и $Q_{2,i}$. Для них соответствующие маскировки M_j и M_j, а выходы из блока расшифрования на ключе K_2 равны

$$D_{K'}(C_1) + M_j \text{ и } D_{K'}(C_2) + M_i.$$

Отсюда, согласно (5),

$$Y_{1,j} = D_{K'}(C_1) + M_j = D_{K'}(C_2) + M_i = Y_{2,i}.$$

Раз равны выходы, то равны и входы:

$$L_{1,j} = L_{2,i}.$$

Тогда

$$Z_{1,j} = M_j + L_{1,j}$$

$$Z_{2,i} = M_i + L_{2,i}.$$

Сложив два последние равенства, получим

$$E_{K'}(Q_{1,j}) + E_{K'}(Q_{2,i}) = Z_{1,j} + Z_{2,i} = M_i + M_j = U.$$

Если $K_1 \neq K'$, то последнее равенство не выполняется.

Ключ K_2 затем находится проще. Общая сложность атаки 2^{58} при известных выбранных шифртекстах длины $2 \times 2^{64} = 2^{65}$.

Заключение

Контрольные вопросы

Смотри руководство по организации самостоятельной работы магистрантов.