Лекция 14. Анализ схем шифрования, использующих многократно один блочный шифр

Цель лекции: провести анализ схем шифрования, использующих многократно один блочный шифр.

План лекции:
Введение.
1 Анализ схем шифрования, использующих многократно один блочный шифр
Заключение
Контрольные вопросы

Ключевые слова: [выбрать самостоятельно].

Содержание лекции:

Введение

1 Анализ схем шифрования, использующих многократно один блочный шифр

Пусть для определенности используется DES. Достижения в криптографии и электронике в 90-х годах позволили снизить время дешифрования DES, что позволяет делать недорогие системы для его дешифрования. Возникла идея построения нового алгоритма, у которого стойкость выше, чем у DES, а в качестве компоненты алгоритма используется DES. Наибольшую потребность в этом испытывают финансовые структуры, которые не хотели бы отказываться от DES из-за значительных дополнительных вложений и других трудностей, но нуждаются в стойких системах шифрования. В этих структурах наиболее употребительным является режим с зацеплением блоков (CBC).

Режимы использования DES [1, с. 229].

1. Режим электронной книги (ECB).

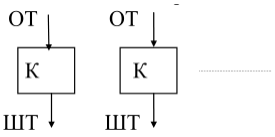

Рис. 1. Схема режима ECB

2. Режим с зацеплением (CBC).

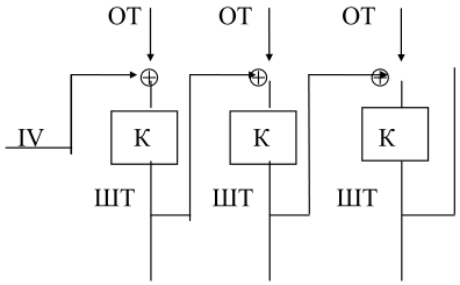

Рис. 2. Схема режима CBC

Здесь IV - инициальное значение.

3. Режим с обратной связью по шифртексту (CFB).

[1] Menzes A., van Oorschot P., Vanstone S. Hadbook of Applied Cryptography, CRC Press, 1997.

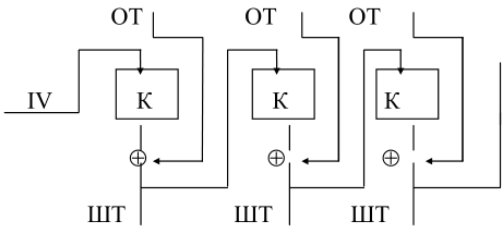

Рис. 3. Схема режима CFB

4. Режим с обратной связью (асинхронный) (OFB).

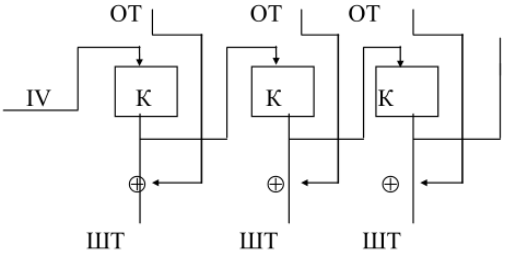

Рис. 4. Схема режима OFB

Были придуманы схемы шифрования, многократно использующие DES.
Пример 1. Двойной DES в режиме электронной книги.

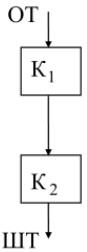

Рис. 5. Схема двойного DES в режиме электронной книги

Двойной DES не стоек к методу «встреча посередине».
Пример 2. Тройной DES в режиме электронной книги [[2], с. 272]. Стойкость данного алгоритма не превосходит стойкости DES, если используется атака с выделенным открытым текстом.

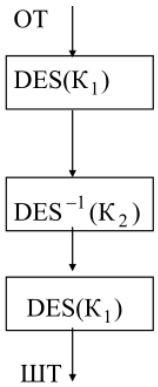

Рис. 6. Схема тройного DES в режиме электронной книги

Пример 3. Тройной DES с зацеплением.

[2] Menzes A., van Oorschot P., Vanstone S. Hadbook of Applied Cryptography, CRC Press, 1997.

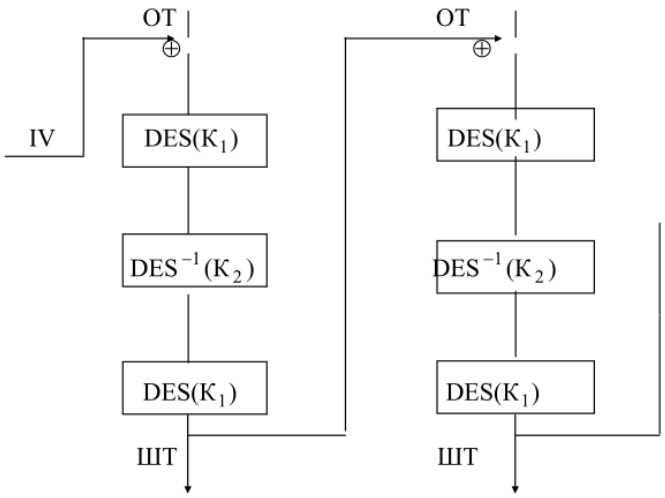

Рис. 7. Схема тройного DES с зацеплением

Оказывается, что стойкость данного тройного DES такая же как стойкость в режиме электронной книги при атаке с выбранным шифртекстом. Слабость данного алгоритма заключается в том, что шифртекст известен и он же идет на вход следующего блока.

Пример 4. [3]. Возникло много модификаций тройного DES, когда зацепление проходит внутри. Рассмотрим следующий вариант тройного DES: CBC/CBC/ECB.

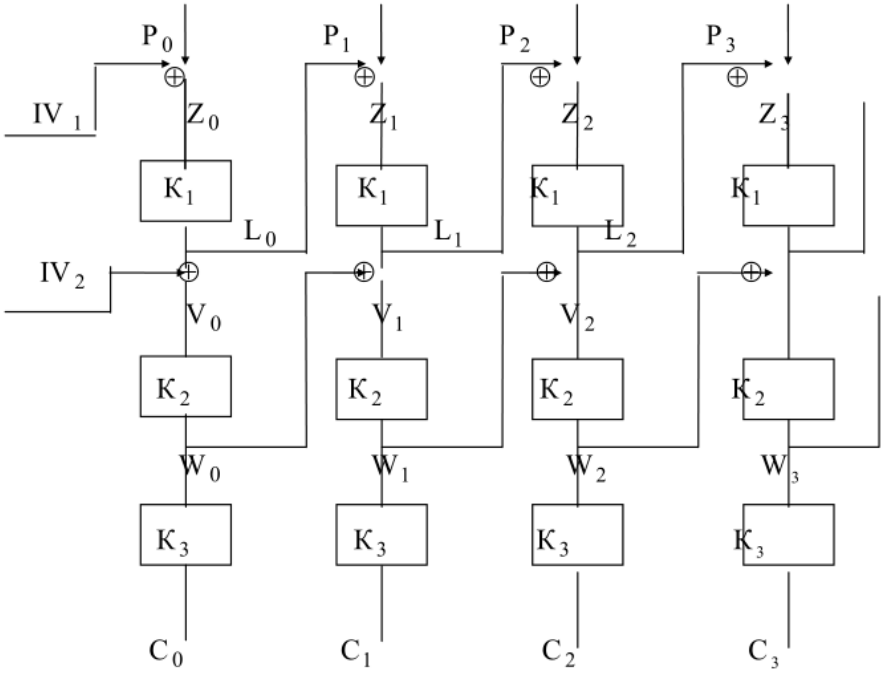

Рис. 8. Схема тройного DES: CBC/CBC/ECB

Рассмотрим один из вариантов дешифрования этой схемы методом выбранного шифртекста. Сначала будем искать ключ K_3. Пусть известны открытые и шифрованные тексты. Среди всех шифртекстов выберем две тройки блоков следующего вида (C_0, C_1, C_2) и (C_0^*, C_1, C_2), где $C_0 \neq C_0^*$. Обозначим для первой тройки через W_i – вход последнего блока, V_i – вход второго блока и через Z_i, L_i – вход и выход первого блока соответственно, P_i – открытый текст. Соответствующие обозначения для второй тройки – W_i^*, V_i^*, Z_i^*, L_i^*, P_i^*. Для выбранных троек имеем следующие соотношения.

Из того, что $C_1 = C_1^*$, $C_2 = C_2^*$, следует

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

$$W_1 = W_1^*, \quad W_2 = W_2^*, \quad V_1 = V_1^*, \quad V_2 = V_2^*. \tag{1}$$

Отсюда $L_2 = L_2^*$, и, следовательно, $Z_2 = Z_2^*$. Тогда

$$V_1 = W_0 + L_1,$$

$$V_1^* = W_0^* + L_1^*.$$

Из этих соотношений с учетом (1) получим

$$W_0 + W_0^* = L_1 + L_1^*. \tag{2}$$

Аналогично,

$$Z_2 = P_2 + L_1,$$

$$Z_2^* = P_2^* + L_1^*.$$

Откуда следует, что

$$P_2 + P_2^* = L_1 + L_1^*. \tag{3}$$

Из соотношений (2) и (3) получим

$$P_2 + P_2^* = W_0 + W_0^*. \tag{4}$$

Так как мы знаем открытый текст, то нам известно $P_2 + P_2^*$. Тогда мы знаем $W_0 + W_0^*$ и C_0, C_0^* и можем опробовать ключ K_3, что в среднем потребует 2^{55} операций.

Нахождение вероятностей таких пар троек, у которых $C_1 = C_1^*$ и $C_2 = C_2^*$ следует из задачи о днях рождения. А именно, если вероятность такой пары при произвольном C0 есть $1/2^{128}$, то вероятность хоть какой-нибудь пары $\sim\sqrt{\frac{1}{2^{128}}} = \frac{1}{2^{64}}$. Значит надо иметь ~ 2^{64} блоков шифртекста для определения ключа K_3.

Зная K_3, находим W_i и, применяя аналогичную технику, определяем K_2 и K_1. Для данной атаки потребуется 3×2^{55} операций опробования и 3×2^{64} блоков шифртекста.

Заключение

Контрольные вопросы

Смотри руководство по организации самостоятельной работы магистрантов.