Криптография

Кевролетин В.В.

27 декабря 2011 г.

Задание5.3

Условие

Доказать свойство дополнительности DES (1): если C=DES(M,K), то C'=DES(M',K') (Z' - обозначает слово, составленное из дополнений соответствующих битов бинарного слова Z). (Используйте следующее равенство для логических переменных (x+y)'=x'+y.) На первый взгляд, для анализа DES с помощью простого перебора ключей необходимо исследовать

$$2^{56}$$

вариантов. Как меняет приведенный результат эту оценку?

Решение

Сразу отмечу, что свойство комплиментарности приводит к тому, что для полного перебора ключей необходимо исследовать в 2 раза меньше ключей.

Первая и последняя перестановки лишь переставляют биты, не меняя их значения, поэтому не влияют на свойство дополнительности.

Так что надо более подробно рассмотреть механизмы генерации ключа и прменения функции f.

Для генерации ключей раундов используются операция циклического сдвига и перестановки. Циклический сдвиг является перестановкой и обладает свойством дополнительности.

Итак, возьмем форулы для сети Фейстеля:

$$L_1 = R_0$$

$$R_1 = L_0 \oplus f(R_0, K_0)$$

Если возьмём дополнения,

$$L'_i = \neg L_i; R'_i = \neg R_i$$

то будем иметь:

$$L'_1 = R'_0 = \neg R_0 = \neg L_0$$

$$R_1 = L_0 \oplus f(R_0, K_0) = \neg L0 \oplus f(\neg R_0, \neg K_0)$$

Последнее равенство верно, так как $f(R_i, K_i)$ применяет несколько перестановок к $R_i K_i$, а так же выбор значения из s-блоков: 1)как было ранее отмечено, перестановки не меняют значения битов, а лишь переставляют их

2) перед выборкой из s-блоков к ключу раунда и данным(прошедним расширяющую перестановку) применятся операция $\oplus$, но $\neg R_i \oplus \neg K_i = R_i \oplus K_i$ т.е. значение этой операции будет тем же самым, когда мы возьмём дополнения к ключу и входным данным. Суперпозиция нескольких операций, обладающих свойством дополнительности опять будет обладать этим свойством, так что функция f, а значит и весь процесс шифровиня обладает свойством дополнительности.

Задание5.4

Условие

Пусть

$$\phi_q$$

– подстановка, которая реализуется цикловой функцией шифра Файстеля,

$$T^n$$

– циклический сдвиг вправо, 2n – длина блока. Доказать, что

$$T^n, T^n\phi_q, \phi_q T^n$$

– инволюции

Решение

Преобразование P называется инволюцией, если для любого блока

$$PPw = w$$

Для простоты записи договоримся, что блок w длины 2n состоят из 2x блоков длины n: w = (A,B)

Для T^n:

$$T^n(T^n(A,B)) = T^n(B,A) = (A,B)$$

ч.т.д.

Для $T^n\phi_q$:

$$T^n\phi_q((A,B)) = T^n(B, A \oplus F(q,B)) = (A \oplus F(q,B), B) =$$
$$T^n\phi_q T^n\phi_q((A,B)) = T^n\phi_q(A \oplus F(q,B), B) =$$
$$T^n\phi_q(A \oplus F(q,B), B) = (A \oplus F(q,B) \oplus F(q,B), B) = (A,B)$$

ч.т.д.

Для $\phi_q T^n$:

$$\phi_q(T^n(A,B)) = \phi_q(B,A) = (A \oplus F(q,B), B)$$

Первое равенство аналогично первому равенству из предыдущего примера, а остальное аналогично. ч.т.д.