

Solutions to Assignment 4

Question 1

For DES, let plain text m and $m' = IP(m)$. We write $m' = (a_0, a_1)$ where a_i 's are 32-bit vectors. Then the cipher text $c = IP^{-1}(c')$ where $c' = (a_{16}, a_{17})$ which is given by

$$a_{i+2} = f(a_{i+1}) \oplus a_i, i = 0, 1, \dots, 15$$

where \oplus is the bit-wise addition and f is a round function (see the notes). When the cipher text c is received, we have $c' = (a_{16}, a_{17}) = IP(c)$, the plain text $m = (a_0, a_1)$ can be obtained by

$$a_i = f(a_{i+1}) \oplus a_{i+2}, i = 15, 14, \dots, 1, 0,$$

and $m = IP^{-1}(a_0, a_1)$. Thus the operation of every round in decryption is identical to of every round in encryption except that the round keys are used in reverse order. Therefore DES decryption and encryption can use the same procedure, i.e., the same hardware.

Question 2

There are many candidates to propose as cipher algorithm. However, there is always a trade-off between cost of implementation and security of the scheme. To design some cipher in extremely resource-restrained environment, LFSR-based cipher is a better choice, because the operation in LFSR-Based cipher is very simple, and the implementation cost would be relatively lower than other kind of ciphers.

Question 3

(a) From the DES encryption, shown in the solution of Question 1, and the operation of f , we may write it in the way related to the round keys as follows

$$a_{i+2} = f_{k_i}(a_{i+1}) \oplus a_i, i = 0, 1, \dots, 15.$$

Note the operation f on the key bits is the bit-wise addition of a 48-bit vector extended from a_{i+1} by the operator E and 48-bit key k_i . Since $E(a^c) = E(a)^c$, we have

$$f_{k_i}(a_{i+1}) = f_{k_i^c}(a_{i+1}^c), i = 0, 1, \dots, 15.$$

Thus, if $Y = DES_K(X)$, then $Y^c = DES_{K^c}(X^c)$.

(b) The result of part (a) can reduce the search space of keys from 2^{56} to 2^{55} .

⁰Copyright ©2009 G. Gong. All rights reserved. May be freely reproduced for educational or personal use.

Question 4

(a) Complexity of placing a brute-force attack on RIJDAEL is 2^{128} .

(b) The RIJDAEL defines a round in terms of the following three transformations: byte substitution (ByteSub), shift row (ShiftRow) and mix columns (MixColumns). After performing these three operations, the round keys are XORed with the output of the round functions. Because ByteSub transform S and the shift row transform can be changed, we can represent RIJDAEL in word operations.

Question 5

We first divide the plain text $m = 1100010111110011$ into four blocks $m_1 = 1100$, $m_2 = 0101$, $m_3 = 1111$ and $m_4 = 0011$. Then we can find the corresponding cipher text as follows:

$$\begin{aligned} c_1 &= E(0011 \oplus 1100) = E(1111) = 1000, \\ c_2 &= E(0011 \oplus 0101) = E(0110) = 0111, \\ c_3 &= E(0011 \oplus 1111) = E(1100) = 1010, \\ c_4 &= E(0011 \oplus 0011) = E(0000) = 0000. \end{aligned}$$

Therefore, we get the cipher text which is 1000011110100000.