Rodrigo Seji Q. Hirao 186834

IA012 - Lista 02

01) Como temos que a cifra do complemento do texto original é o complemento da cifra original, podemos calcular apenas metade das cifras pois o complemento delas é previsível.

02)

a) No caso do DES em 2 camadas é esperado 2^{112} combinações porém é possível fazer apenas a primeira etapa 2^{56} vezes e o inverso da segunda mais 2^{56} vezes, resultando em, no máximo, 2^{57} tentativas. Enquanto com 3 camadas, usando o mesmo método, ainda terá uma camada intermediária, assim tendo que ser feita 2^{112} comparações.

b) Não há necessidade de usar uma terceira chave pois a terceira etapa será aplicada em uma cifra diferente do texto de entrada.

03) O módulo de Feistel é o processo de:

- separar o dado em 2 partes L (esquerda) e R (direita)
- $L_{i+1} = R_i$
- $R_{i+1} = L_i$ xor $f(R_i)$, onde f é uma função com base na subchave

04) Como a chave é calculada a partir da rotação de 28 bits, a segurança iria durar até 28 etapas, mas depois iria gerar chaves repetidas.

05) Criptoanálise Diferencial consta em encontrar pares equidistantes e comparar suas cifras $(\Delta x, \Delta y)$, tal que $\Delta y = S(x_1 \oplus \Delta x) \oplus S(x_2)$, assim podendo ser analizada estatisticamente de acordo com sua entropia.

06)

- AddRoundKey → cada byte é combinado, por um xor, com a chave round
- SubBytes → cada byte é substituido com outro na S-box (a posição na tabela é de acordo com seu valor)
- ShiftRows → As 3 últimas linhas de cada bloco são deslocadas
- MixColumns → É feito uma multiplicação matricial com cada coluna.

$$rcc_i = \begin{cases} 1 & , i=1 \\ 2 \cdot rcc_{i-1} & , i \neq 1 \text{ e } \dots \\ (2 \cdot rcc_{i-1}) \oplus 11B_{16} & , \text{e} \dots \end{cases}$$

07) $w_0 = w_1 = w_2 = w_3 = 18\,18\,68\,37 = 0001\ 1000\ 0001\ 1000\ 0110\ 1000\ 0011\ 0111$

↳ $= \begin{pmatrix} 18 & 18 & 18 & 18 \\ 18 & 18 & 18 & 18 \\ 68 & 68 & 68 & 68 \\ 37 & 37 & 37 & 37 \end{pmatrix}$ ↳ S-Box → $a_{ij} = i+j$ (para simplicidade)

→ Round Keys

↳ rcon → $\begin{matrix} 01 & 00 & 00 & 00 \\ 02 & 00 & 00 & 00 \\ 04 & 00 & 00 & 00 \\ 08 & 00 & 00 & 00 \\ 10 & 00 & 00 & 00 \\ 20 & 00 & 00 & 00 \\ 40 & 00 & 00 & 00 \\ 80 & 00 & 00 & 00 \\ 1B & 00 & 00 & 00 \\ 36 & 00 & 00 & 00 \\ 6C & 00 & 00 & 00 \end{matrix}$

↳ $w_4 = w_0 \oplus \text{subword}(\text{rotword}(w_0)) \oplus rcon_1$

$= w_0 \oplus \text{subword}(68\,37\,18\,18) \oplus rcon_1$

$= w_0 \oplus 0D\,0A\,09\,09 \oplus rcon_1$

$= 15\,12\,61\,35 \oplus rcon_1$

$= 14\,12\,61\,35$

↳ $w_5 = w_1 \oplus w_4 = 0C\ 0A\ 09\ 09$

↳ $w_6 = w_2 \oplus w_5 = 14\ 12\ 61\ 35$

↳ $w_7 = w_3 \oplus w_6 = 0C\ 0A\ 09\ 09$

↳ $W = \begin{matrix} w_4 & w_5 & w_6 & w_7 \end{matrix}$

$\begin{pmatrix} 14 & 0C & 14 & 0C \\ 12 & 0A & 12 & 0A \\ 61 & 09 & 61 & 09 \\ 35 & 09 & 35 & 09 \end{pmatrix}$

08) Pois para cifrar é possível calcular as chaves em paralelo, para decifrar é preciso feito em série

09) Ela deve ser resistente a ataques lineares e diferenciais minimizando a correlação entre transformação linear da entrada e da saída