Segurança Computacional

João Pedro Carvalho de Oliveira Rodrigues - 221017032, Gabeiel Mauricio Chagas Silva - 221017097

18 de dezembro de 2024

1 Introdução

O S-DES é uma versão simplificada do algoritmo DES, utilizado como ferramenta educacional para ensinar conceitos básicos de criptografia de bloco. Ele foi projetado para ser mais fácil de entender e implementar, enquanto mantém os princípios fundamentais de algoritmos de criptografia modernos, como substituição e permutação. A implementação do programa foi feita em python.

2 Resolução da equação

2.1 Chaves

Definindo as chaves de 8 bits
Chave: 1010000010
Após realizar a permutação dos 10 bits temos: 1000001100
Então fazemos um shift circular de um bit para a esquerda separadamente nas duas metades da chave: 0000111000
Por fim a permutação com 8 elementos: k1 = 10100100
Repetimos um processo similar porem com o shift de 3 bits: k2 = 01000011

2.2 Encryption

Plaintext: 11010111
O primeiro passo é realizar a permutação inicial: 11011101
Separamos os lados da entrada L : 1101 , R: 1101
Essas serão as entradas da função F(R,SK)
Para realizar a função, fazemos uma expansão de R: 11101011
E um xor do resultado com a k1: 01001111
Usaremos então esses valores na tabela S0 e S1: 1111
Por fim realizamos uma permutação dos 4 elementos: 1111
Essa é a saída de F, que então realizamos um xor com L e trocamos de lado com R: 11010010
Esse procedimento é repetido mais uma vez usando k2, resultando em : 00110010
O último passo é reverter a IP : 10101000
Para decifrar a mensagem basta repetir o processo no sentido contrário

P10									
3	5	2	7	4	10	1	9	8	6

Figura 1: p10

P8							
6	3	7	4	8	5	10	9

Figura 2: p8

E/P							
4	1	2	3	2	3	4	1

Figura 3: Expansão/permutação

$$S0 = \begin{array}{c} \\ 0 \\ 1 \\ 2 \\ 3 \end{array} \begin{array}{c} \begin{array}{cccc} 0 & 1 & 2 & 3 \end{array} \\ \begin{bmatrix} 1 & 0 & 3 & 2 \\ 3 & 2 & 1 & 0 \\ 0 & 2 & 1 & 3 \\ 3 & 1 & 3 & 2 \end{bmatrix} \end{array} \qquad S1 = \begin{array}{c} \\ 0 \\ 1 \\ 2 \\ 3 \end{array} \begin{array}{c} \begin{array}{cccc} 0 & 1 & 2 & 3 \end{array} \\ \begin{bmatrix} 0 & 1 & 2 & 3 \\ 2 & 0 & 1 & 3 \\ 3 & 0 & 1 & 0 \\ 2 & 1 & 0 & 3 \end{bmatrix} \end{array}$$

Figura 4: Tabelas S

P4			
2	4	3	1

Figura 5: p4