Sobre o DES

Lucas João Martins

1. (3.7) Show that DES decryption is, in fact, the inverse of DES encryption.

2. (3.9) Consider the substitution defined by row 1 of S-box S_1 in Table S.2. Show a block diagram similar to Figure 3.2 that corresponds to this substitution

S_1	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

Figura 1: S-box S_1

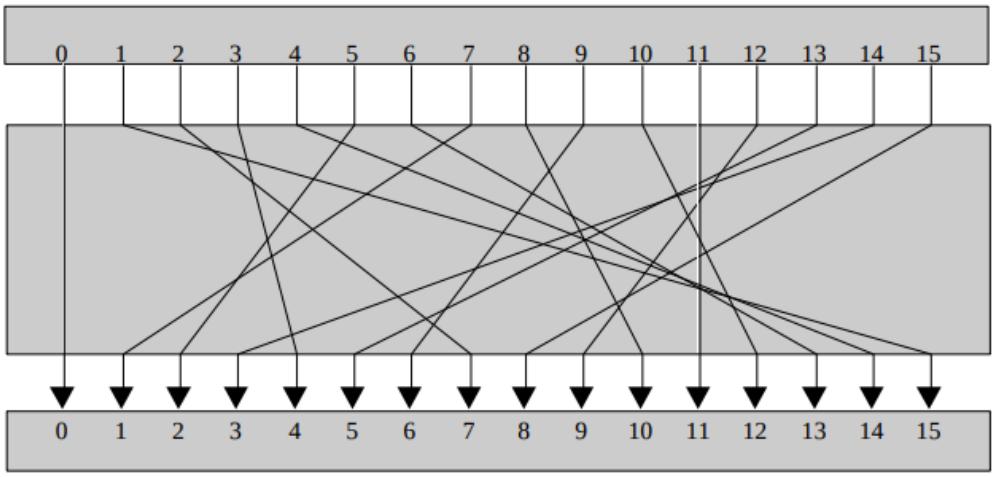

Figura 2: Resposta

3. (3.10) Compute the bits number 1, 16, 33, and 48 at the output of the first round of the DES decryption, assuming that the ciphertext block is composed of all ones and the external key is composed of all ones.

4. (3.15) Show that in DES the first 24 bits of each subkey come from the same subset of 28 bits of the initial key and that the second 24 bits of each subkey come from a disjoint subset of 28 bits of the initial key.

Basta observar a tabela de escolha de chave no DES (*compreension D-box*), onde é visto que os primeiros 24 bits são selecionados dos primeiros 28 bits e os últimos 24 bits são selecionados dos últimos 28 bits.

5. (3.16) Refer to Figure G.2, which depicts key generation for S-DES.

a. How important is the initial P10 permutation function?

Perceba que antes da realização de P10 existem 2^{10} possíveis chaves únicas. Após a aplicação de P10, que se trata de uma permutação sim-

14	17	11	24	01	05	03	28
15	06	21	10	23	19	12	04
26	08	16	07	27	20	13	02
41	52	31	37	47	55	30	40
51	45	33	48	44	49	39	56
34	53	46	42	50	36	29	32

Figura 3: Tabela de escolha de chave no DES

ples, ainda irá existir 2^{10} possíveis chaves únicas. Com isso, essa permutação não adiciona em nada na segurança do algoritmo.

b. How important are the two LS-1 shift functions?

Pelo mesmo motivo explicado na resposta da alternativa anterior, os dois deslocamento a esquerda de 1 bit não adicionam em nada na segurança do algoritmo.

7. (3.18) Using S-DES, decrypt the string (10100010) using the key (0111111101) by hand. Show intermediate results after each function (IP, F_K, SW, F_K , IP^{-1}). Then decode the first 4 bits of the plaintext string to a letter and the second 4 bits to another letter where we encode A through P in base 2 (i.e., A = 0000, B = 0001, ..., P = 1111). Hint: As a midway check, after the application of SW, the string should be (00010011).

Geração das subchaves:

- chave = 0111111101
- P10 = 1111110011
- Shift = 1111100111
- P8 = 01011111

- **K_1 = 01011111**
- Shift = 1111111100
- P8 = 11111100
- **K_2 = 11111100**

Processo de decifrar:

- Texto cifrado = 10100010
- IP = 00110001
- F_K:
  - E/P = 10000010
  - E/P xor K_2 = 01111110
  - S0 = 00
  - S1 = 00
  - P4 = 0000
  - P4 xor 4 bits iniciais da entrada = 0011
  - Saída = 00110001
- SW = 00010011
- F_K:
  - E/P = 10010110
  - E/P xor K_1 = 11001001
  - S0 = 01
  - S1 = 10
  - P4 = 0110
  - P4 xor 4 bits iniciais da entrada = 0111
  - Saída = 01110011
- IP^{-1} = 10101110
- Texto original = 10101110
- Texto traduzido = JN

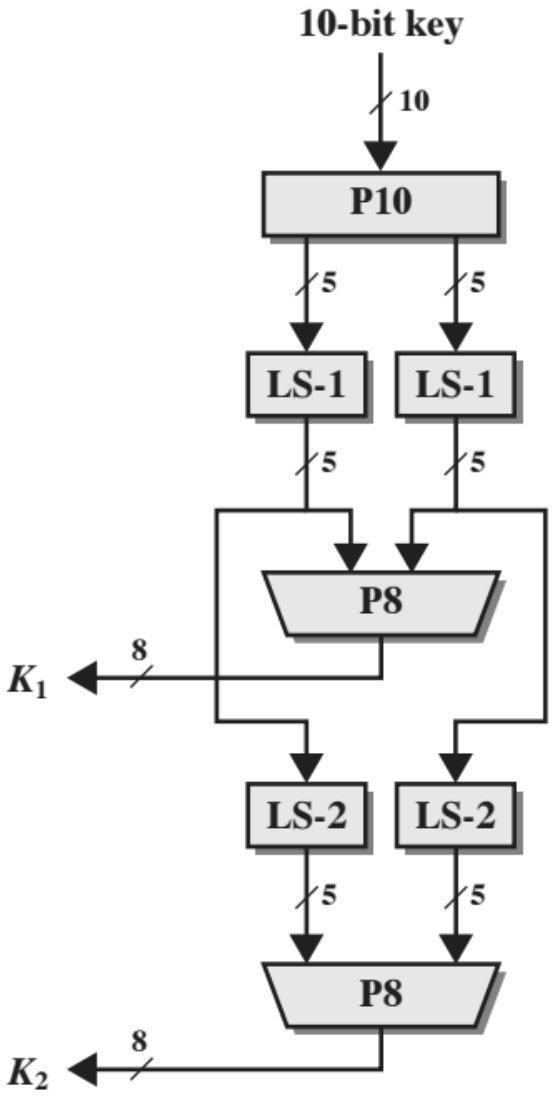

Figure G.2 Key Generation for Simplified DES

Figura 4: Figure G.2