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

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.

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

a. How important is the initial P10 permutation function?

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

6. (3.17) The equations for the variables q and r for S-DES are defined in the section on S-DES analysis. Provide the equations for s and t.

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_1 = 11011101
  - S0

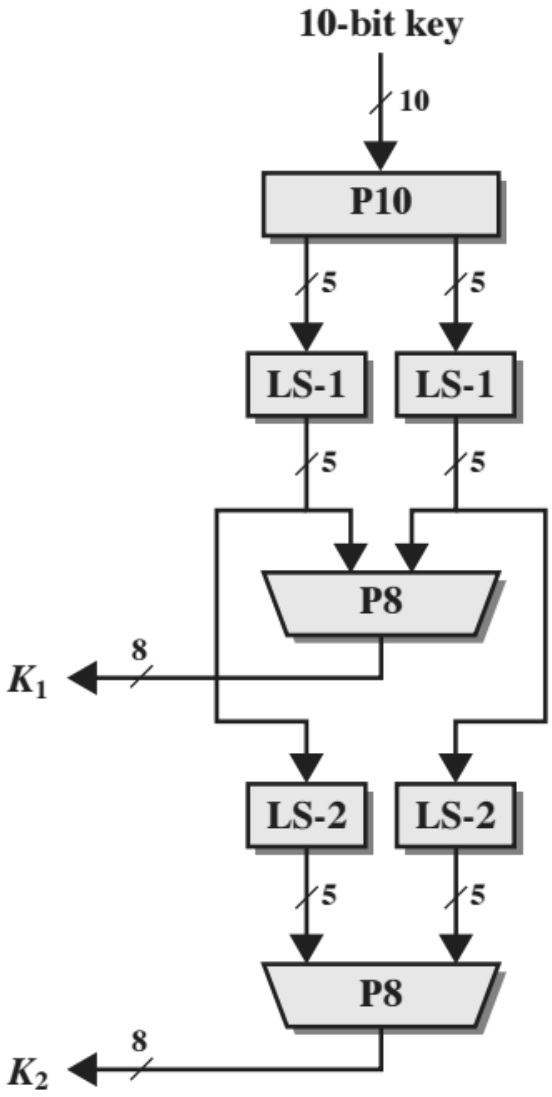

Figure G.2 Key Generation for Simplified DES

Figura 1: Figure G.2