# Review Questions

1. Compare between a monoalphabetic cipher and a polyalphabetic cipher in terms of speed, cryptanalysis complexity and ease of use.

2. Define “Diffusion” and explain why it is required for secure encryption.

3. Show that the round function F in Feistel Cipher does not have to be reversible.

4. What is the purpose of the S-boxes in DES?

5. Why the DES is currently considered insecure?

# Problems

1. How much time is needed to brute-force DES using a computer that can do 100 decryption/ microsecond?

2. This problem provides a numerical example of encryption using a one-round version of DES:

| Plaintext |  |
| --- | --- |
| in hexadecimal notation: | 93 DF AB C8 37 F2 14 38 |
| in binary notation: | 10010011 11011111 10101011 11001000  00110111 11110010 00010100 00111000 |
|  |  |
| Key |  |
| Hex | 3B 38 98 37 15 20 F7 5E |
| Binay | 00111011 00111000 10011000 00110111  00010101 00100000 11110111 01011110 |

1. Derive K1, the first-round subkey.
2. Derive L0, R0.
3. Expand R0 to get E[R0], where E[·] is the expansion function of Figure 3.8.
4. Calculate A = E[R0] ⊕ K1.
5. Group the 48-bit result of (d) into sets of 6 bits and evaluate the corresponding S-box substitutions.
6. Concatenate the results of (e) to get a 32-bit result, B.
7. Apply the permutation to get P(B).
8. Calculate R1 = P(B) ⊕ L0.
9. Write down the ciphertext.

This problem must be solved by hand.