Answers to Exercise 1

1. What is a cipher?
   - ☐ **An algorithm performing encryption/decryption**
   - ☐ An encrypted message
   - ☐ A method for breaking encrypted messages
   - ☐ An unencrypted message
2. The process of discovering a plaintext of a key is known as
   - ☐ Cryptography
   - ☐ **Cryptanalysis**
   - ☐ Steganography
   - ☐ Cryptoprocessing
3. The unencrypted message is called
   - ☐ **Plaintext**
   - ☐ **Cleartext**
   - ☐ Chiffre
   - ☐ Ciphertext
4. The order of letters in a message is rearranged by
   - ☐ Substitution cipher
   - ☐ Asymmetric cipher
   - ☐ **Transpositional cipher**
   - ☐ Symmetric cipher
5. Encryption protects against
   - ☐ Attacks
   - ☐ Loss of Data
   - ☐ Unavailability
   - ☐ **None of the mentioned**

Answer to Exercise 2

First, we need to count the frequencies of the characters in our cipher text:

Cipher	6	9	:	C	D	@	2	?	E	5	4	A	7	G	>	=	J	8
Frequency	12	7	7	7	6	6	5	5	5	3	3	3	3	2	2	2	2	1

Thus, we obtain:

```
6G6CJ@?6 92D E96 C:89E E@ C6DA64E 7@C 9:D AC:G2E6 2?5 72>:=J =:76 9:D 9@>6 2?5 9:D 4@CC6DA@?56?46

e_e____e ___ __e _____ __ _e__e__ ___ ___ ______e ___ ______ ___e ___ ___e ___ ___ ____e_____e__e
e_e____e h__ _he ___h_ __ _e__e__ ___ h__ ______e ___ ______ ___e h__ h__e ___ h__ ____e_____e__e
e_e____e h__ _he _i_h_ __ _e__e__ ___ hi_ __i___e ___ ___i__ _i_e hi_ h__e ___ hi_ __rre_____e__e
e_er___e h__ _he ri_h_ __ re__e__ __r hi_ _ri___e ___ ___i__ _i_e his h__e ___ his __rres____e__e
e_er___e h_s _he ri_h_ __ res_e__ __r his _ri___e ___ ___i__ _i_e his ho_e ___ his _orres_o__e__e
e_er_o_e h_s _he ri_h_ _o res_e__ _or his _ri___e ___ ___i__ _i_e his ho_e a__ his _orres_o__e__e
e_er_o_e has _he ri_h_ _o res_e__ _or his _ri_a_e a__ _a_i__ _i_e his ho_e an_ his _orres_on_en_e
e_er_one has _he ri_h_ _o res_e__ _or his _ri_a_e an_ _a_i__ _i_e his ho_e an_ his _orres_on_en_e
e_er_one has the ri_ht to res_e_t _or his _ri_ate an_ _a_i__ _i_e his ho_e and his _orres_onden_e
e_er_one has the ri_ht to res_e_t _or his _ri_ate and _a_i__ _i_e his ho_e and his _orres_onden_e
e_er_one has the ri_ht to res_ect _or his _ri_ate and _a_i__ _i_e his ho_e and his corres_ondence
e_er_one has the ri_ht to respect _or his pri_ate and _a_i__ _i_e his ho_e and his correspondence
e_er_one has the ri_ht to respect for his pri_ate and fa_i__ _ife his ho_e and his correspondence
ever_one has the ri_ht to respect for his private and fa_i__ _ife his ho_e and his correspondence
ever_one has the ri_ht to respect for his private and fami__ _ife his home and his correspondence
ever_one has the ri_ht to respect for his private and famil_ life his home and his correspondence
everyone has the ri_ht to respect for his private and family life his home and his correspondence
everyone has the right to respect for his private and family life his home and his correspondence
```

The plain text is a sentence from the European Convention on Human Rights.

The substitution table of the applied encryption scheme is:

Cipher	6	9	:	C	D	@	2	?	E	5	4	A	7	G	>	=	J	8
Plain	e	h	i	r	s	o	a	n	t	d	c	p	f	v	m	l	y	g

Further information: The applied substitution cipher is called ROT47, a variant of ROT13 that supports numbers, upper-case and lower-case letters.

Answer to Exercise 3

Round function is defined as below for each round:

$$f_1(x,K) = (1 \cdot x)^K \bmod 16 = x^K \bmod 16$$

$$f_2(x,K) = (2 \cdot x)^K \bmod 16 = (2x)^K \bmod 16$$

$$f_3(x,K) = (3 \cdot x)^K \bmod 16 = (3x)^K \bmod 16$$

$$f_4(x,K) = (4 \cdot x)^K \bmod 16 = (4x)^K \bmod 16$$

Encrypt ($(\underline{0001}\,|\,\underline{1001})_2$: $\underbrace{0001_2}_{L_0}\quad\underbrace{1001_2}_{R_0}$

Key $K = 0101_2 = 0.2^3+1.2^2+0.2^1+1.2^0 = 5_{10} = 5$

1. With $L_0 = 0001_2$, $R_0 = 1001_2$

   $L_1 = R_0 = 1001_2$

   $f_1(R_0,K) = f_1(1001_2,0101_2) = f_1(9,5) = (1 \cdot 9)^5 \bmod 16 = 9^5 \bmod 16 = 9 = 1001_2$

   $R_1 = L_0 \oplus f_1(R_0,K) = 0001_2 \oplus 1001_2 = 1000_2$

2. With $L_1 = 1001_2$, $R_1 = 1000_2$

   $L_2 = R_1 = 1000_2$

   $f_2(R_1,K) = f_2(1000_2,0101_2) = f_2(8,5) = (2 \cdot 8)^5 \bmod 16 = 16^5 \bmod 16 = 0 = 0000_2$

   $R_2 = L_1 \oplus f_2(R_1,K) = 1001_2 \oplus 0000_2 = 1001_2$

3. With $L_2 = 1000_2$, $R_2 = 1001_2$

   $L_3 = R_2 = 1001_2$

   $f_3(R_2,K) = f_3(1001_2,0101_2) = f_1(9,5) = (3 \cdot 9)^5 \bmod 16 = 27^5 \bmod 16 = 11 = 1011_2$

   $R_3 = L_2 \oplus f_3(R_2,K) = 1000_2 \oplus 1011_2 = 0011_2$

4. With $L_3 = 1001_2$, $R_3 = 0011_2$

   $L_4 = R_3 = 0011_2$

   $f_4(R_3,K) = f_4(0011_2,0101_2) = f_1(3,5) = (4 \cdot 3)^5 \bmod 16 = 12^5 \bmod 16 = 0 = 0000_2$

   $R_4 = L_3 \oplus f_4(R_3,K) = 1001_2 \oplus 0000_2 = 1001_2$

Thus, as $L_4 = 0011_2$ and $R_4 = 1001_2$, the ciphertext is

$00111001_2 = 0.2^7+0.2^6+1.2^5+1.2^4+1.2^3+0.2^2+0.2^1+1.2^0 = 57_{10} = 57$