1-

One time pad (OTP)

a.

The key is random string of letters that has the same length of the message

b.

E(k,m) = m + k mod 26 where m is the numerical representation of each plaintext's letter as well as for the key

c.

D(k,c) = c – k mod 26 where c is the numerical representation of each ciphertext's letter as well as for the key

d.

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Ciphertext: | b | s | a | s | p | p | k | k | u | o | s | p |
| Numerical Ciphertext: | 1 | 18 | 0 | 18 | 15 | 15 | 10 | 10 | 20 | 14 | 18 | 15 |
| OTP: | r | s | i | d | p | y | d | k | a | w | o | y |
| Numerical OTP: | 17 | 18 | 8 | 3 | 15 | 24 | 3 | 10 | 0 | 22 | 14 | 24 |
| Numerical Plaintext: | 10 | 0 | 18 | 15 | 0 | 17 | 7 | 0 | 20 | 18 | 4 | 17 |
| Plaintext: | k | a | s | p | a | r | h | a | u | s | e | r |

2-

In Caesar cipher, the following formula is used for encryption.

$$E_n(x) = (x + n) \ mod \ 26, where \ x \ is \ the \ letter \ being \ encrypted$$

By using a shift of 3 as an example, the following is acquired.

A: (0+3) mod 26 = 3 mod 26 = 3: D

B: (1+3) mod 26 = 4 mod 26 = 4: E

C: (2+3) mod 26 = 5 mod 26 = 5: F

D: (3+3) mod 26 = 6 mod 26 = 6: G

E: (4+3) mod 26 = 7 mod 26 = 7: H

F: (5+3) mod 26 = 8 mod 26 = 8: I

G: (6+3) mod 26 = 9 mod 26 = 9: J

3-

| | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z |
| u | p | i | j | g | d | t | e | h | m | v | a | x | r | k | y | q | z | l | b | o | c | s | f | w | n |

Ciphertext: h akcg izwybktzuyew

Plaintext: i love cryptography