**Lab1**

**Shafiya Heena Najmun Nahar  
(301199792) (301160081)**

**Secret Message:** This is my fifth semester

**Encryption: FTUE UE YK RURFT EQYQEFQD**

T 🡪 F

H 🡪 T

I 🡪 U

S 🡪 E

I 🡪 U

S 🡪 E

M 🡪 Y

Y 🡪 K

F 🡪 R

I 🡪 U

F 🡪 R

T 🡪 F

H 🡪T

S 🡪 E

E 🡪 Q

M 🡪 Y

E 🡪 Q

S 🡪 E

T 🡪 F

E 🡪 Q

R 🡪 D

**Decryption:**

**FTUE UE YK RURFT EQYQEFQD**   
key = 12

F 🡪 5 Decryption: (5-12)mod26 plainText: 19 🡪 T

T 🡪 19 Decryption: (19-12)mod26 plainText: 07 🡪 H

U 🡪 20 Decryption: (20-12)mod26 plainText: 08 🡪 I

E 🡪 4 Decryption: (4-12)mod26 plainText: 18 🡪 S

U 🡪 20 Decryption: (20-12)mod26 plainText: 08 🡪 I

E 🡪 4 Decryption: (4-12)mod26 plainText: 18 🡪 S

Y 🡪 24 Decryption: (24-12)mod26 plainText: 12 🡪 M

K 🡪 10 Decryption: (10-12)mod26 plainText: 24 🡪 Y

R 🡪 17 Decryption: (17-12)mod26 plainText: 05 🡪 F

U 🡪 20 Decryption: (20-12)mod26 plainText: 08 🡪 I

R 🡪 17 Decryption: (17-12)mod26 plainText: 05 🡪 F

F 🡪 5 Decryption: (5-12)mod26 plainText: 19 🡪 T

T 🡪 19 Decryption: (19-12)mod26 plainText: 07 🡪 H

E 🡪 4 Decryption: (4-12)mod26 plainText: 18 🡪 S

Q 🡪 16 Decryption: (16-12)mod26 plainText: 04 🡪 E

Y 🡪 24 Decryption: (24-12)mod26 plainText: 12 🡪 M

Q 🡪 16 Decryption: (16-12)mod26 plainText: 04 🡪 E

E 🡪 4 Decryption: (4-12)mod26 plainText: 18 🡪 S

F 🡪 5 Decryption: (5-12)mod26 plainText: 19 🡪 T

Q 🡪 16 Decryption: (16-12)mod26 plainText: 04 🡪 E

D 🡪 3 Decryption: (3-12)mod26 plainText: 17 🡪 R

**Caesar cipher:**key: 3  
  
T 🡪 19 Encrypted: (19+3) mod26 Cipher Text: W

H 🡪 07 Encrypted:(07+3)mod26 Cipher Text: K

I 🡪 08 Encrypted:(08+3)mod26 Cipher Text: L

S 🡪 18 Encrypted:(18+3)mod26 Cipher Text: V

I 🡪 08 Encrypted:(08+3)mod26 Cipher Text: L

S 🡪 18 Encrypted:(18+3)mod26 Cipher Text: V

M 🡪 12 Encrypted:(12+3)mod26 Cipher Text: P

Y 🡪 24 Encrypted:(24+3)mod26 Cipher Text: B

F 🡪 05 Encrypted:(05+3)mod26 Cipher Text: I

I 🡪 08 Encrypted:(08+3)mod26 Cipher Text: L

F 🡪 05 Encrypted:(05+3)mod26 Cipher Text: I

T 🡪 19 Encrypted:(19+3)mod26 Cipher Text: W

H 🡪07 Encrypted:(07+3)mod26 Cipher Text: K

S 🡪 18 Encrypted:(18+3)mod26 Cipher Text: V

E 🡪 04 Encrypted:(04+03)mod26 Cipher Text: H

M 🡪 12 Encrypted:(12+3)mod26 Cipher Text: P

E 🡪 04 Encrypted:(4+3)mod26 Cipher Text: H

S 🡪 18 Encrypted:(18+3)mod26 Cipher Text: V

T 🡪 19 Encrypted:(19+3)mod26 Cipher Text: W

E 🡪 04 Encrypted:(04+3)mod26 Cipher Text: H

R 🡪 17 Encrypted:(17+3)mod26 Cipher Text: U

**Decryption:**

Key =3

W 🡪 22 Decryption: (22-3)mod26 plainText: T

K 🡪 10 Decryption: (10-3)mod26 plainText: H

L 🡪 11 Decryption: (11-3)mod26 plainText: I

V 🡪 21 Decryption: (21-3)mod26 plainText: S

L 🡪 11 Decryption: (11-3)mod26 plainText: I

V 🡪 21 Decryption: (21-3)mod26 plainText: S

P 🡪15 Decryption: (15-3)mod26 plainText: M

B 🡪 01 Decryption: (01-3)mod26 plainText: Y

I 🡪08 Decryption: (08-3)mod26 plainText: F

L 🡪 11 Decryption: (11-3)mod26 plainText: I

I 🡪08 Decryption: (08-3)mod26 plainText: F

W 🡪22 Decryption: (22-3)mod26 plainText: T

K 🡪 10 Decryption: (10-3)mod26 plainText: H

V 🡪 21 Decryption: (21-3)mod26 plainText: S

H 🡪07 Decryption: (07-3)mod26 plainText: E

P 🡪 15 Decryption: (15-3)mod26 plainText: M

H 🡪 07 Decryption: (07-3)mod26 plainText: E

V 🡪 21 Decryption: (21-3)mod26 plainText: S

W 🡪 22 Decryption: (22-3)mod26 plainText: T

H 🡪 07 Decryption: (07-3)mod26 plainText: E

U 🡪20 Decryption: (20-3)mod26 plainText: R

**Software security best practices:**

**1.Create a Robust IR plan:**

By creating a strong Incident response plan we can stop the attackers from breach and helps to detect and limit the damage.

**2.Integrate security into your SDLC (Software development life cycle):**

Implementing integration of software security activities in an organization is cheaper and faster which ultimately reduces the exposure to security risks. This integration includes architecture risk analysis, static, dynamic and interactive application security testing, SCA and pen testing.

**3. Segment your network:**

Performing proper segment networking limits the movement of attackers. In this we need to identify the critical data storage and use appropriate security controls to limit the traffic to and from those networking segments.

**4.Educate and train users:**

Having an organized and maintained security training curriculum for employees will be an organization’s security DNA where employee gets awareness about security and developers learn the secure coding . This regular practice help employees in spotting and shut downing the social engineering attacks.