

Information Security-LAB



Submitted By:

Raja Umer Saleem 2023-CS-609

Submitted To:

Ms. Shanfa

Dated: 20th Jan 2025

Department of Computer Science

University of Engineering and Technology Lahore, New Campus

1. Crack the following plaintext TRVJRI TZGYVIJ RIV HLZKV VRJP KF TIRTB

```
Text : TRVJRI TZGYVIJ RIV HLZKV VRJP KF TIRTB
Shift: 1
Cipher: USWKSJUUAHZWJKUSJWUIMALWUWSKQULGUUJSUC
De-cipher: TRVJRITTZGYVIJTRIVTHLZKVTVRJP TKFTTIRTB9
Text : TRVJRI TZGYVIJ RIV HLZKV VRJP KF TIRTB
Shift: 9
Cipher: CAESAR]CIPHERS]ARE]QUITE]EASY]TO]CRACK
De-cipher: TRVJRInTZGYVIJnRIVnHLZKVnVRJPnKFnTIRTB
```

Crack text:

CAESAR CIPHERS ARE QUITE EASY TO CRACK

2. What encryption key was used?

The Key was 9.

3. Make you own cipher text using the Caesar cipher.

```
D:\4rd sem Allah krm kry ga\ISL\encryption.exe
Text : OWN TEXT
Shift: 1
Cipher: PXOUUFYU
De-cipher: OWNTTEXT3
Text : OWN TEXT
Shift: 3
Cipher: RZQWWHAW
De-cipher: OWNTTEXT
```

4. Can you crack other people's ciphertexts?

Yes, I guess the the key.

5. What key do we need to make "CAESAR" become "MKOCKB"?

```
Text : CAESAR
Shift: 10
Cipher: MKOCKBKey matched 10
```

Key =10

6. What key do we need to make "CIPHER" become "SYFXUH"?

```
Text : CIPHER
Shift: 16
Cipher: SYFXUHKey matched 16
```

Key=16

7. Use the Caesar cipher to encrypt your first name

```
D:\4rd sem Allat
Text : Umer
Shift: 3
Cipher: Xphu
De-cipher: Umer
```

8. How can we find the decryption key from the encryption key?

The key used in encryption just simple "subtract" it.

2nd Manual

```
-----
a = 56
b = 98
Euclidean_GCD = 14
-----
Process exited after 0.1666 seconds with return value 0
Press any key to continue . . .
```

