# **Question 10 a)** Illustrate Ciphertext only attack

Ciphertext-only attacks refer to a situation where an attacker has access to only the encrypted form of a message or data, and does not have any knowledge about the original plaintext. The goal of the attacker in this case is to analyse the ciphertext and try to derive information about the original plaintext, such as its content or its meaning. Ciphertext-only attacks are often considered the most difficult type of attack because the attacker has no knowledge or information about the original message or data.

For example:-

An attacker has access to following two cipher texts possibly encoded with same key.

1) dwwdfn dw gdzq 2) zh zloo iljkw

Attacker begins decoding the ciphertext assuming that it was encoded using Monoalphabetic cipher.

CT : dwwdfn dw gdzq CT : zh zloo iljkw

Key: 1 Key: 1

PT : cvvcem cv fcyp PT : yg yknn hkijv

CT : dwwdfn dw gdzq CT : zh zloo iljkw

Key: 2 Key: 2

PT : buubdl bu ebxo PT : xf xjmm gjhiu

CT : dwwdfn dw gdzq CT : zh zloo iljkw

Key: 3 Key: 3

PT : attack at dawn PT : we will fight

Thus, by guessing the key, attacker was able to decode the messages. Attacker can also use strategies like frequency distribution of alphabets, repetitive pairs of texts in ciphertext, etc.

# **Question 10 b)** Illustrate Known Plaintext attack

A known plaintext attack occurs when the attacker has access to both the plaintext and the corresponding ciphertext. The goal of the attacker in this case is to analyse the relationship between the plaintext and the ciphertext, and use that information to try to derive the secret key used to encrypt the message. Known plaintext attacks are often easier than ciphertext-only attacks because the attacker has access to both the plaintext and ciphertext, which can reveal important information about the encryption algorithm used.

For example:-

An attacker has access to following ciphertext and its corresponding plaintext .

CT : HCRZ

PT : hill

He also have access to another cipher text encoded with same secret key but don’t know its corresponding plaintext. So, his goal is to guess the secret key.

CT : SSXNSP

Attacker begins to guess the encryption algorithm used in encryption. Several algorithms like Caesar Cipher, Playfair seems to fail, now attacker assumes that hill cipher might be used in this case.

|  |  |
| --- | --- |
| 𝑘11  Let Key (K) =  𝑘21 | 𝑘12    𝑘22 |

CT = PT K mod 26

 [7 2] = [7 8] K mod 26

 [17 25] = [11 11] K mod 26

7 2 7 8

 = K mod 26 17 25 11 11

K= PT-1.CT mod 26

7 8

Finding Inverse of

11 11

Determinant = -11 mod 26

= 15

11 −8

Inverse = 1/15 mod 26

−11 7

=> 1/15 mod 26 = a

=> 1 mod 26 = 15a

=> a=7

11 −8

 7 mod 26

−11 7

77 −56 25 22

 mod 26 =

−77 49 1 23

25 22 7 2

 mod 26

1 23 17 25

549 600

 mod 26

398 577

3 2

 K =

8 5

Now, Decoding other ciphertext

Det K = -1 mod 26 = 25

K-1 = 1/25 5 −2 mod 26

−8 3

K-1 = 25 5 −2 mod 26

−8 3

-1 = 21 2 K

8 23

18 18

CT =

23 13

18 18 21 2

PT= mod 26

23 13 8 23

522 450 2 8

 mod 26 = = ciph

587 345 15 7

CT = [18 15]

21 2

PT = [18 15] mod 26

8 23

 [498 381] mod 26 = [4 17] = er

Decoded Text = cipher