MODULE-2

Symmetric Key Encipherment

Traditional Symmetric key cipher

The original message is called plaintext, the message that is sent through the channel is called ciphertext. To create the ciphertext from the plaintext, uses an encryption algorithm and a shared secret key. To create the plaintext from ciphertext, uses, a decryption algorithm, and the same secret key. We refer to encryption and decryption algorithms, as ciphers. A key is a set of values (numbers) that the cipher, as an algorithm operates on.

Symmetric key encipherment uses a single key for both encryption and decryption. The encryption and decryption algorithms are inverses of each other. If P is the plaintext, C is the ciphertext and K is the key then,

Encryption : $C = E_K(P)$

Decryption : $P = D_K(C)$

Using symmetric key encipherment two people can use the same key for communication on the both direction. This is why the method is called symmetric.

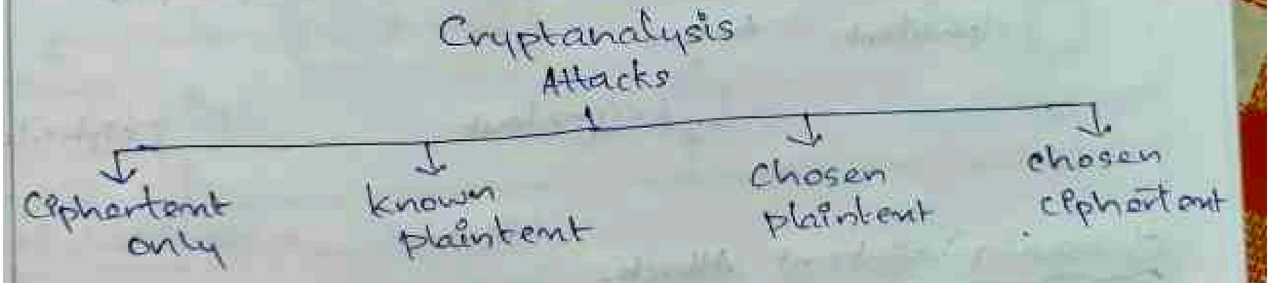
A person needs different keys to communicate with different persons. If there are m people in a group who need to communicate with each other they need $(m \times (m-1))/2$ keys.

Kerckhoff's Principle.

Although it may appear would be more secure if we hide both the encryption/decryption algorithm and the secret key, this is not recommended Based on Kerckhoff's principle, one should always assume that the adversary, Eve knows the encryption/decryption algorithm. The resistance of the cipher to attack must be based only on the secrecy of the key. In other words, gussing the key should be so difficult that there is no need to hide the encryption/decryption algorithm.

Cryptanalysis

As cryptography is the science and art of creating secret codes, cryptanalysis is the science and art of breaking those codes. This is to learn how ~~[illegible]~~ vulnerable our cryptosystem is There are four common types of cryptanalysis attacks



Ciphertext only Attack:

It is the most probable one because the attacker needs only the ciphertext for this attack. He has access to only ~~th~~ some ciphertext and tries to find corresponding key and plaintext.

1) Brute force Attack:

→ In this type of attack tries to use all possible key part of the key. Its value, 16, does not have a multiplicative inverse in Z_{26}.

To prevent this type of attack, the number of possible keys must be very large.

2) Statistical Attack:

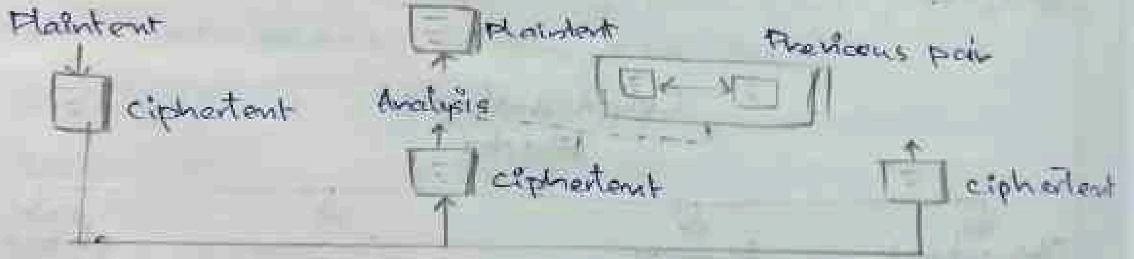
→ The cryptanalyst finds the mostly used character in the ciphertext and assumes that the corresponding plaintext character. To prevent this type g attack the cipher should hide the characteristics g the language.

3) Pattern Attack:

→ Cryptanalyst may use a pattern attack to break the cipher. Therefore, it is important to use ciphers that make the ciphertext look as possible.

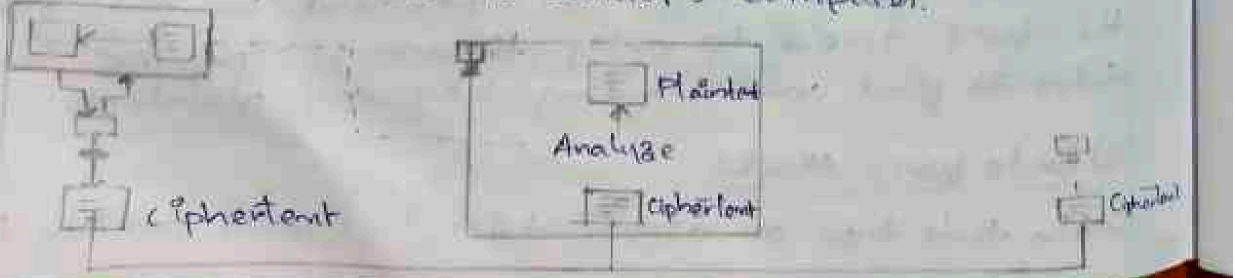
Known-Plain Text Attack:

Here attacker has access to some plaintext /ciphertext pairs in addition to the intercepted ciphertext that she wants to break.



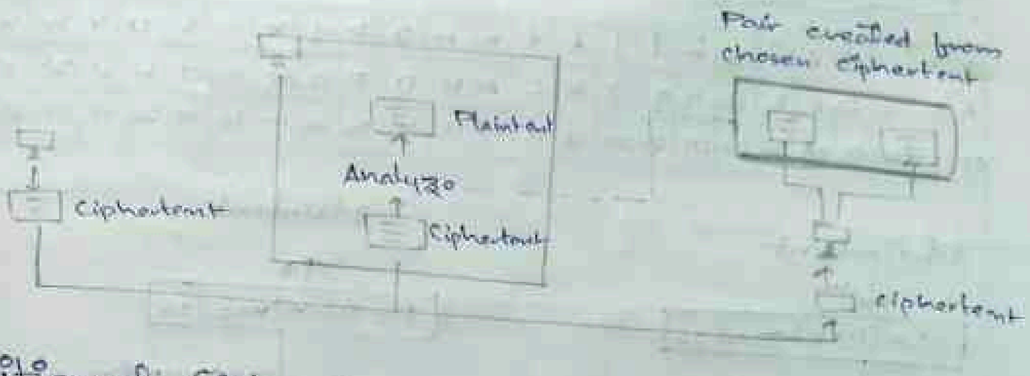
Chosen-plaintext Attack:

Here the plaintext or ciphertext pairs have been chosen by the attacker. This can happen when attacker has access to sender's computer.



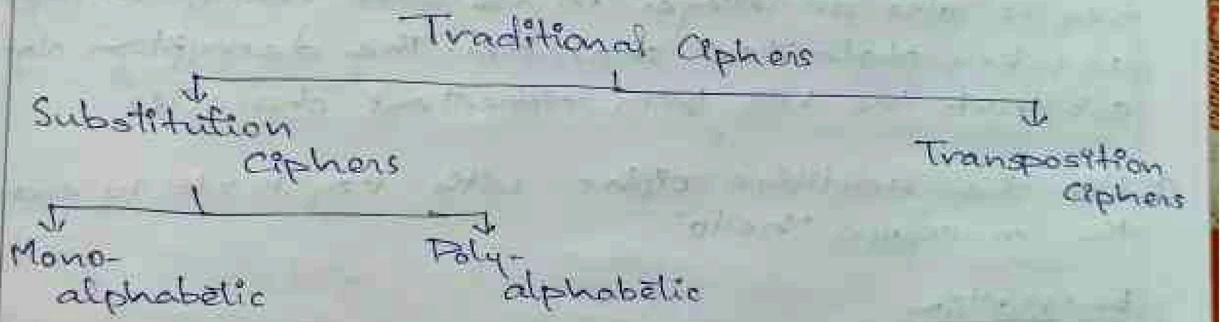
Chosen-ciphertext Attack:

Similar to chosen-plaintext, here attacker chooses some ciphertext and decrypts it to formal ciphertext/plaintext pair. Attacker has access to receivers computer.



Traditional Ciphers

We can divide traditional symmetric-key ciphers into two broad categories: substitution ciphers and transposition ciphers.



→Substitution Ciphers:

A substitution ciphers replaces one symbol with another symbol.

1) Monoalphabetic Cipher

A character or a symbol in the plaintext is always changed to same character or a symbol in the cipher-text regardless of its position in the text. The relationship between the symbol in plain text to a symbol in the cipher-text is always one to one.

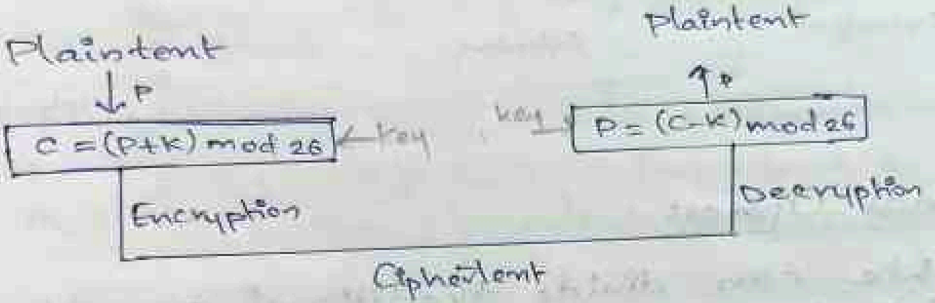
Eg:-

plaintext : hello

Ciphertext : khoor

→Additive Cipher

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
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
00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25



Each character is assigned Z_{26} the secret key is also an integer in Z_{26}. The encryption algorithm add key plain text character. The decryption algorithm substract the key from ciphertext character

Q. Use the additive cipher with key K = 15 to encrypt the message "hello".

Encryption

7 + 15 = 22 mod 26

22 → W

04 + 15 = 19 mod 26

19 → T

11 + 15 = 26 mod 26

0 → A

14 + 15 = 29 mod 26

3 → D

~~ciphertext~~ :

Ciphertext : WTAAD

Decryption

P = (C − K) mode 26

W = 22 − 15 = 7 → H

T = 19 − 15 = 4 → E

A = 00 − 15 = 15 → L

A = 00 − 15 = 15 → L

D = 03 − 15 = 14 → O

⇒ Shift Ciphers

Additive ciphers are called shift ciphers because the Encryption algorithm can be interpreted as "shift key characters down" and the encryption algorithm can be interpreted as " shift key character up". For example, if the key = 15, the encryption algorithm shifts 15 characters down (toward the end of of the alphabet). The decryption algorithm shifts 15 characters up (toward the beginning of the alphabet). Of course when we reach the end or the beginning of the alphabet.

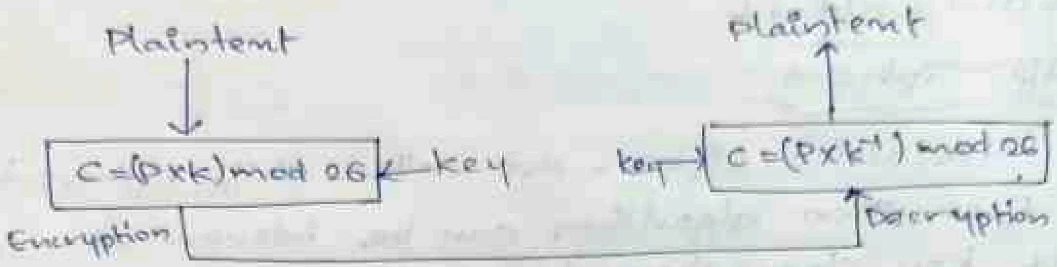
⇒ Caesar Cipher

Additive ciphers are sometimes refferred to as the caesar cipher. Caesare used a key of 3 for his communication.

* Additive ciphers are sometime reffered to as shift ciphers or caesar cipher.

⇒ Multiplicative Ciphers

In a multiplicative cipher, the encryption algorithms specifies multiplication of the plaintext by the key and the decryption algorithms specifies division of the ciphertext by the key as shown below:



However, since operations are in Z_{26}, decryption here means multiplying by the multiplicative inverse of the key. Note that, the key needs to belong to the set Z_{26}^{*} to guarantee that the encryption and decryption are inverses of each other.

Eg:-

We use a multiplicative cipher to encrypt the message "hello" with a key of 7.

Plaintext	Encryption	Ciphertext
h → 07	$(07\times07) \bmod 26$	23 → X
e → 04	$(04\times07) \bmod 26$	02 → C
l → 11	$(11\times07) \bmod 26$	25 → Z
l → 11	$(11\times07) \bmod 26$	25 → Z
o → 14	$(14\times07) \bmod 26$	20 → U

ie, ciphertext is "XCZZU".

⇒ Affine Cipher

We can combine the additive and multiplicative ciphers to get what is called the affine cipher — a combination of both ciphers with a pair of keys. The first key is used with the multiplicative cipher and