

Prepared by Dr. Mohammed Anbar

Network Security CYB 630
An Overview of Cryptography

Lecture 6



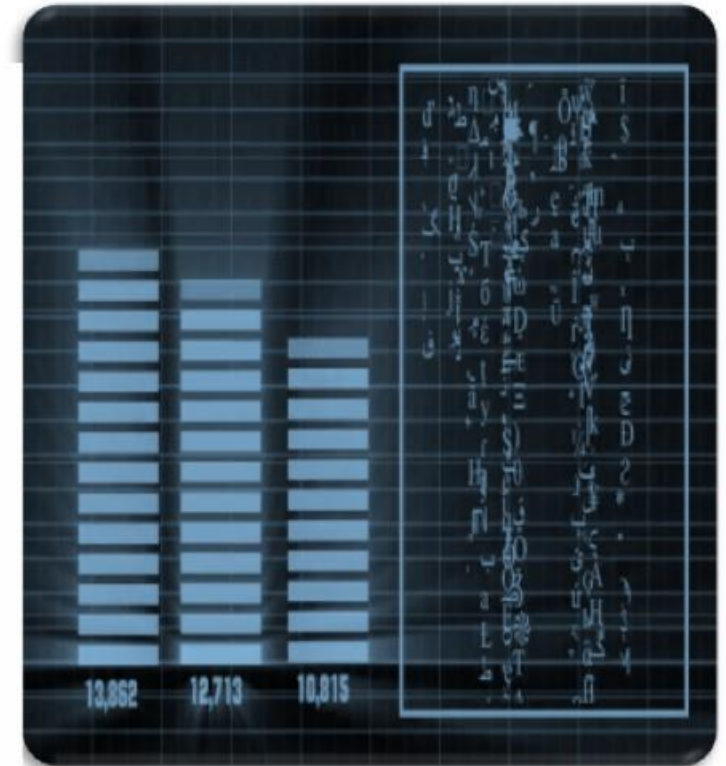
- Define the cryptography concepts,
- Understand Caesar cipher substitution technique,
- Explain symmetric and asymmetric encryption algorithms,
- Explain Diffie-Hellman Key Exchange,
- Explain Hash functions,
- Explain keyed-hash message authentication code,
- Explain the basics of cryptanalysis.

- Cryptography is the science of secret or hidden writing
- It has two main components:
 1. Encryption
 - Practice hiding messages so that they can not be read by anyone other than the intended recipient
 2. Authentication & Integrity
 - Ensuring that users of data/resources are the persons they claim to be and that a message has not been altered



Encryption and
decryption
use the same key

Uses different keys
for encryption
and decryption.

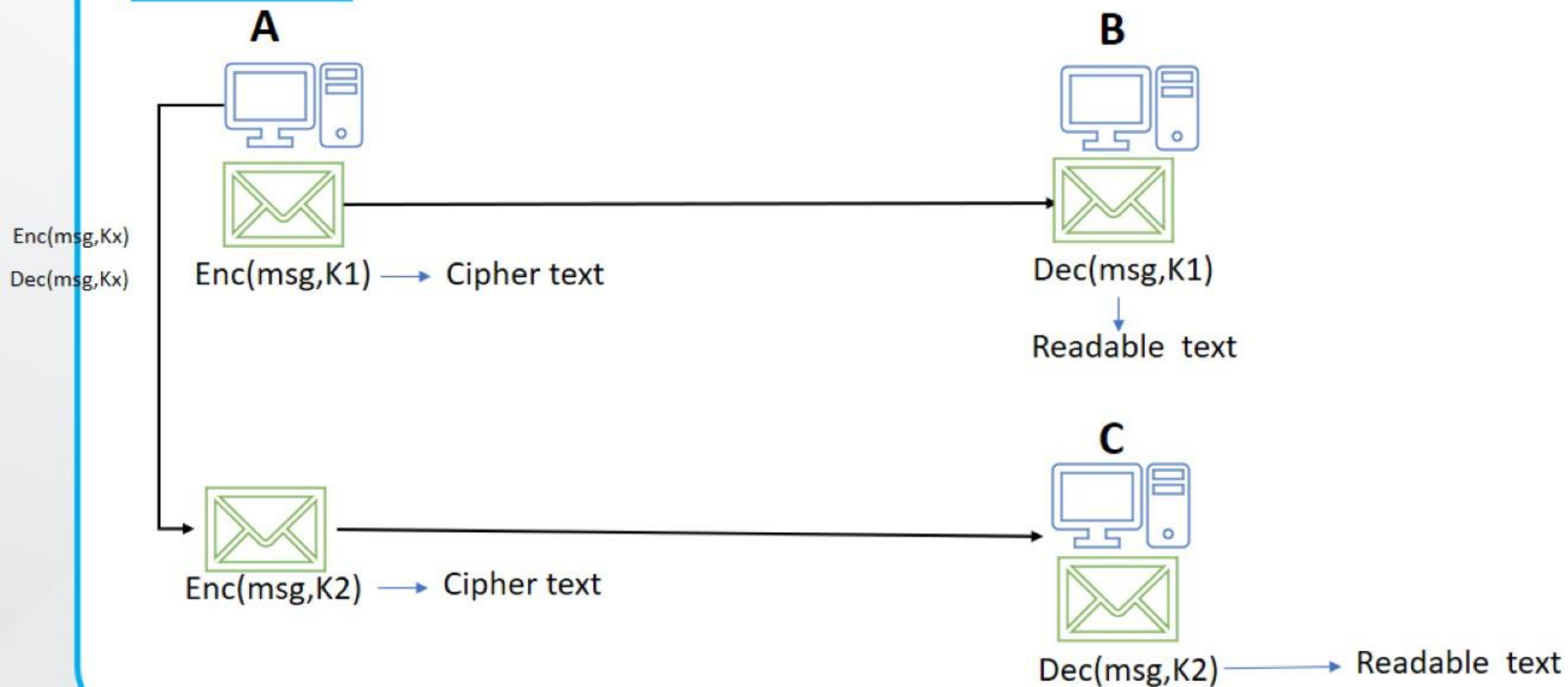




AES

DES

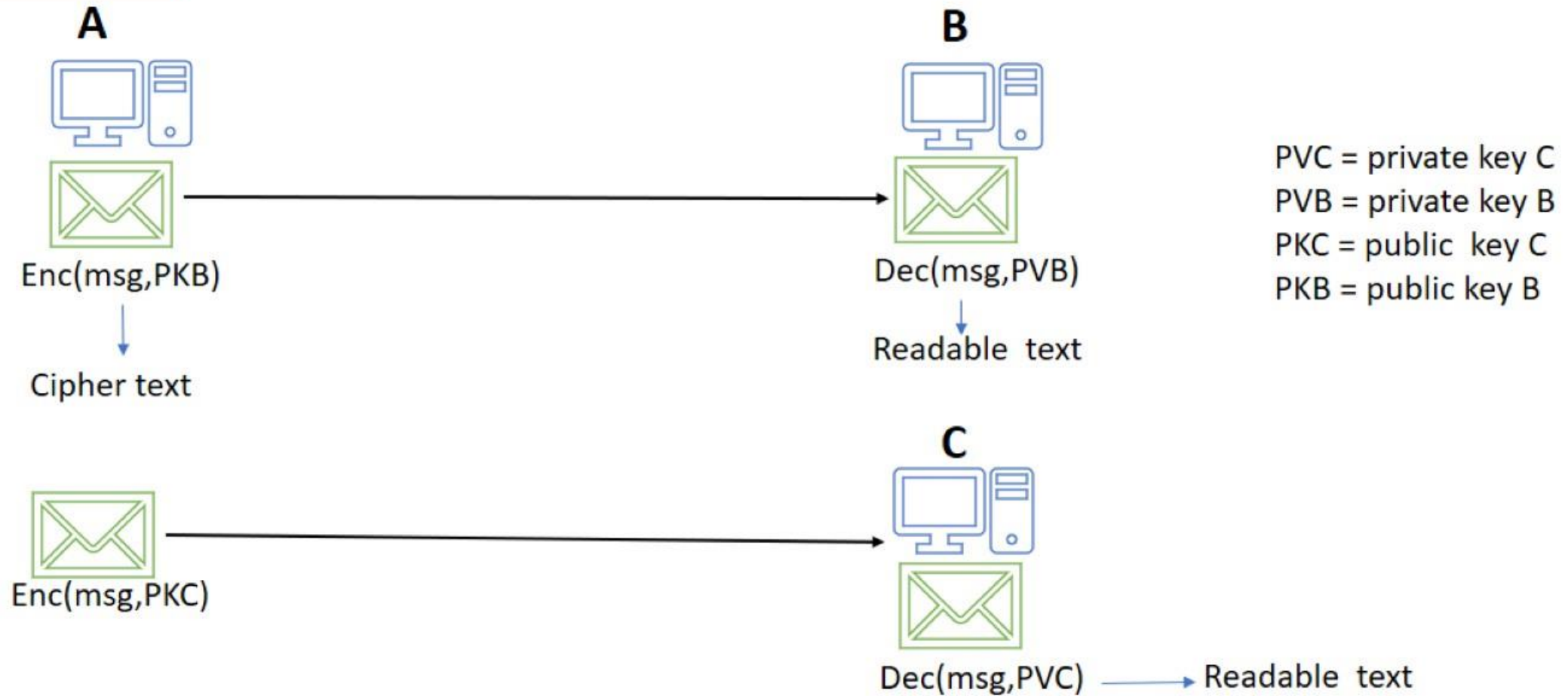
IDEA





Elliptic curve

Digital
signature



- Algorithms in which the key for encryption and decryption are the same are Symmetric
 - Example: Caesar Cipher
- Types:
 1. Block Ciphers
 - Encrypt data one block at a time (typically 64 bits, or 128 bits)
 - Used for a single message
 2. Stream Ciphers
 - Encrypt data one bit or one byte at a time

- Strength of the algorithm is determined by the size of the key
 - The longer the key the more difficult it is to crack
- Key length is expressed in bits
 - Typical key sizes vary between 48 bits and 448 bits
- Set of possible keys for a cipher is called keys-space
 - For a 40-bit key there are 2^{40} possible keys
 - For 128-bit key there are 2^{128} possible keys
 - Each additional bit added to the key length doubles the security

- To crack the key the hacker must use brute-force

(i.e. try all the possible keys till a key that works is found)

- Supercomputer can crack a 56-bit key in 24 hours
- It will take 2^{72} times longer to crack a 128-bit key (Longer than the age of the universe)

* A supercomputer is a computer with a high level of performance as compared to a general-purpose computer

- Caesar Cipher is a method in which each letter in the alphabet is rotated by three letters.
- Caesar cipher substitution technique is vulnerable to brute-force cryptanalysis because its key space is small, i.e., there are only 25 possible keys. In addition, the Caesar cipher substitution technique is vulnerable to frequency analysis.

ABCDEFGHIJKLMNOPQRSTUVWXYZ



DEFGHIJKLMNOPQRSTUVWXYZABC

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
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
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

- Let us try to encrypt the message

ATTACK AT DAWN

DWWDFN DW GDZQ

Encryption $\Rightarrow c = E(K, P) = (K + P) \bmod 26$

Decryption $\Rightarrow p = D(k, C) = (C - k) \bmod 26$

Encryption

$$A = 3 + 0 \bmod 26 = 3 = D$$

$$T = 3 + 19 \bmod 26 = 22 = W$$

$$C = 3 + 2 \bmod 26 = 5 = f$$

Decryption

$$D = 3 - 3 \bmod 26 = 0 = A$$

$$W = 22 - 3 \bmod 26 = 19 = T$$

$$f = 5 - 3 \bmod 26 = 2 = c$$

- Monoalphabetic cipher is a substitution cipher in which for a given key, the cipher alphabet for each plain alphabet is fixed throughout the encryption process. For example, **if 'A' is encrypted as 'D', for any number of occurrences in that plaintext, 'A' will always get encrypted to 'D'.**
- Any letter can be substituted for any other letter. Each letter must have a unique substitute
- The **monoalphabetic substitution** consists in using a **mixed alphabet** (with the letters in an unusual order) and **replacing the letters** of the alphabet normal with it.
- The key is changed for every message (possibly 26!).

ABCDEFGHIJKLMNOPQRSTUVWXYZ
MNBVCXZASDFGHJ KLPO IUYTREWQ

26! means

- For the plaintext letter A you can use the ciphertext letter A, B, C, ... , X, Y, or Z. (26 possible letters.)
- For B you can use A, B, C, ... , X, Y, or Z, but not the letter you did use for A. (25 possible letters.)
- For C you can use A, B, C, ... , X, Y, or Z, but not the letter you did use for A or B. (24 possible letters.)
- For Z you can only use the remaining letter. (1 possible letter.)
- The whole number of possible keys is $26 \times 25 \times 24 \times \dots \times 2 \times 1 = 26!$ (The exclamation mark denotes the factorial of a number.)

- Developed by Blaise de Vigenere. Also, called Vigenere cipher
- Vigenere Cipher is a method of encrypting alphabetic text.
- It uses a simple form of polyalphabetic substitution. A polyalphabetic cipher is any cipher based on substitution, using multiple substitution alphabets.
- The encryption of the original text is done using the Vigenère square or Vigenère table.

Substitution Cipher - Polyalphabetic Caesar Cipher (cont.)

Encryption

Plaintext: ATTACKATDAWN

Key: Lemon

Keystream: lemonlemonle

Cipher text:

LXFOPVEFRNHR

Plain text

	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	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
B	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
C	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
D	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
E	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
F	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
G	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
H	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
I	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
J	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
K	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
L	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
M	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
N	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
O	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
P	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
Q	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
R	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
S	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
T	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
U	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
V	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
W	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
X	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
Y	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
Z	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

Key

Vigenère square or Vigenère table

Decryption

Key: Lemon

Cipher text:

LXFOPVEFRNHR

Keystream: lemonlemonle

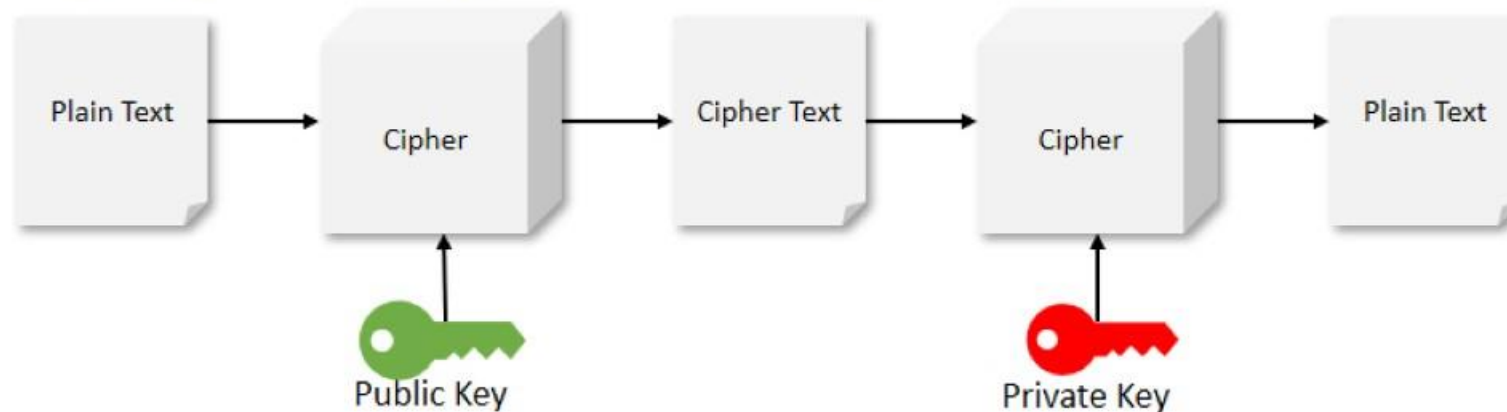
Plaintext: ATTACKATDAWN

		Plain text																									
		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
Key	A	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
	B	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
	C	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
	D	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
	E	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
	F	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
	G	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
	H	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
	I	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
	J	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
	K	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
	L	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
	M	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
	N	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
	O	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
	P	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
	Q	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
	R	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
	S	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
	T	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
	U	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
	V	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
	W	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
	X	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
	Y	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
	Z	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

Vigenère square or Vigenère table

- Any exposure to the secret key compromises the secrecy of the ciphertext.
- A key needs to be delivered to the recipient of the coded message for it to be decrypted.
- Potential for eavesdropping attack during transmission of key.

- Uses a pair of keys for encryption
 - Public key for encryption
 - Private key for decryption
- Messages encoded using the public key can only be decoded by the private key
 - Secret transmission of key for decryption is not required
 - Every entity can generate a key pair and release its public key

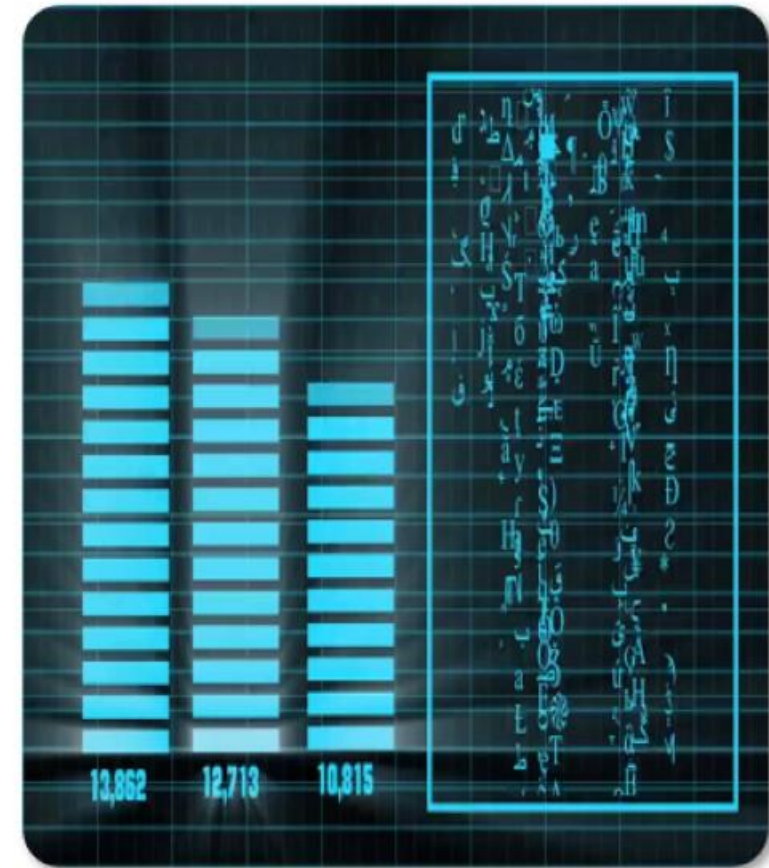
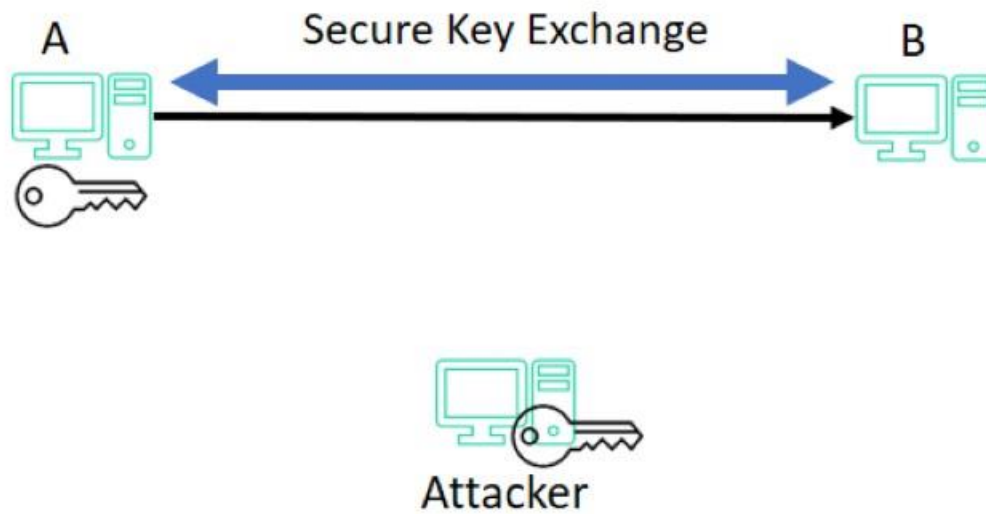


Two most popular algorithms are RSA & El Gamal

- RSA
 - Developed by Ron Rivest, Adi Shamir, Len Adelman
 - Both public and private key are interchangeable
 - Variable Key Size (512, 1024, or 2048 bits)
 - Most popular public key algorithm
- El Gamal
 - Developed by Taher ElGamal
 - Variable key size (512 or 1024 bits)
 - Less common than RSA, used in protocols like PGP

- Efficiency is lower than Symmetric Algorithms. It's a slow process compared to symmetric cryptography. Therefore, it's not appropriate for decrypting bulk messages.
- Potential for a man-in-the-middle attack
- Since public keys aren't authenticated, nobody can be certain that a public key belongs to the person supplied.

- Diffie-Hellman is the first key agreement algorithm
 - Invented by Whitfield Diffie & Martin Hellman
 - Provided the ability for messages to be exchanged securely without having to have shared some secret information previously
 - Inception of public key cryptography which allowed keys to be exchanged in the open
- No exchange of secret keys
 - Man-in-the-middle attack avoided



Diffie-Hellman Key Exchange

Public key = Generator ^{private key} mod Prime

Public key (A) = $3^{15} \bmod 17 = 6$

Public key (B) = $3^{13} \bmod 17 = 12$

Attacker



Prime = 17

Generator = 3

Public(A) = 6

Public(B) = 12

A



Public(B) = 12

Prime = 17

Generator = 3

Private key(A) = 15

Public key(A) = 6

Secret key = $12^{15} \bmod 17 = 10$
 $(3^{13})^{15}$

B



Public(A) = 6

Prime = 17

Generator = 3

Private key (B) = 13

Public key(B) = 12

Secret key = $6^{13} \bmod 17 = 10$

$(3^{15})^{13}$

$3^{15 \cdot 13}$

ABC

Lorem ipsum dolor sit amet,
consectetur adipiscing elit.
Donec at metus at est eleifend
tempus. Phasellus blandit
sollicitudin justo. Placerat,
sem eget consequat sodales.

#

#b!c1d

&"(#df

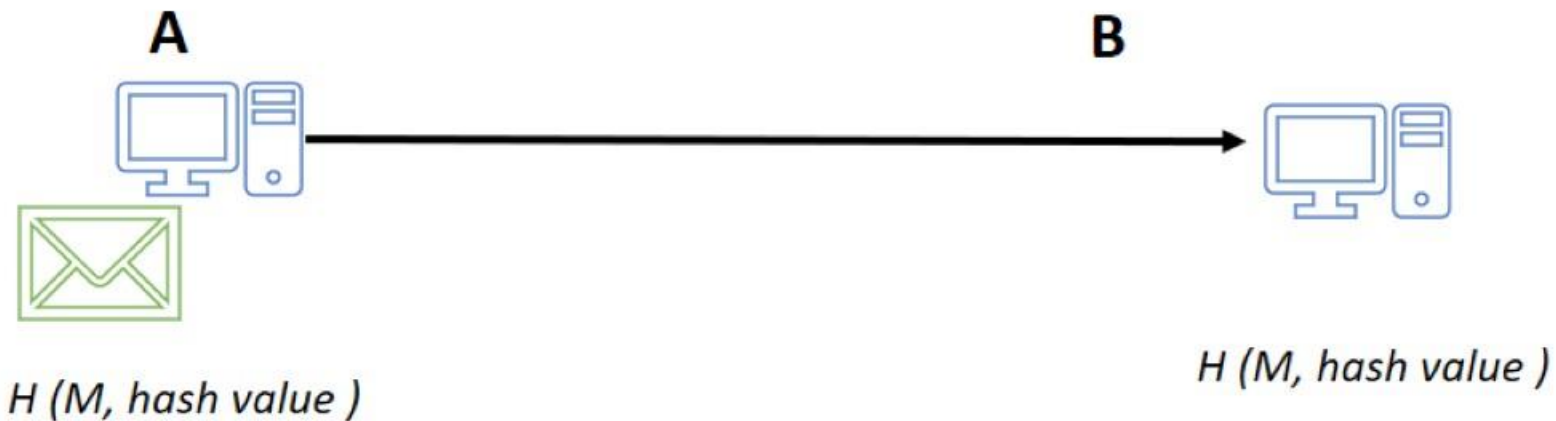
#!sk84#

The MD5 hash for hello world is : 5eb63bbbe01eeed093cb22bb8f5acdc3

The MD5 hash for Hello world is : 3e25960a79dbc69b674cd4ec67a72c62



- Hash functions represent a third cryptography type alongside symmetric and asymmetric cryptography.
- A hash function is a function that maps data of any size to data of a fixed size.
- The value returned by a hash function is called hash value or simply h which It is often viewed as a digital fingerprint.
- Hashing only provides integrity services; confidentiality services are not supported. A one-way cryptographic algorithm is a hash function. The adoption of a one-way cryptographic algorithm prevents the ciphertext from being decoded to expose the original plaintext.
- A hashing function's able to produce completely distinct hash values even when the input plaintext is slightly altered is another noteworthy feature. This characteristic is helpful for data security since it produces clearly different hashes whenever an attacker makes even a small alteration to the original data.



If the hash value generated by A =
the hash value generated by B then
integrity achieved

Random-length message

MD5

Hash value: fixed-length output of 128 bits

Random-length message

SHA-256

Hash value: fixed-length output of 256 bits

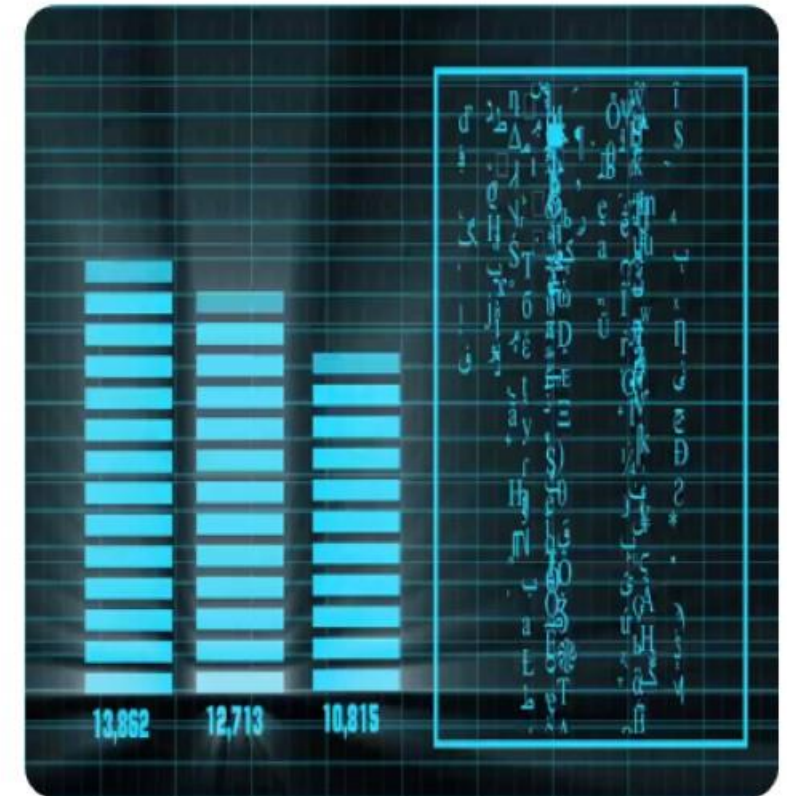
- In cryptography, an HMAC (sometimes expanded as either keyed-hash message authentication code or hash-based message authentication code) is a specific type of message authentication code (MAC) involving a cryptographic hash function and a secret cryptographic key.
- As with any MAC, it may be used to simultaneously verify both the data integrity and authenticity of a message.
- HMAC can provide authentication using a shared secret instead of using digital signatures with asymmetric cryptography.
- It trades off the need for a complex public key infrastructure by delegating the key exchange to the communicating parties, who are responsible for establishing and using a trusted channel to agree on the key prior to communication.

- The key length plays an important role in hashing algorithm. The bigger the key size, the harder to break in the key while the smaller the key size, the easier to break in the key and the algorithm is more vulnerable to collision attack where the hashing algorithm generates the same hash value for different input
- **MD5** – Uses a 128-bit shared secret key. The variable-length message and 128-bit shared secret key are combined and run through the HMAC-MD5 hash algorithm. The output is a 128-bit hash. The hash is appended to the original message and forwarded to the remote end.
- **SHA – SHA-1** uses a 160-bit secret key. The variable-length message and the 160-bit shared secret key are combined and run through the HMAC-SHA1 hash algorithm. The output is a 160-bit hash. The hash is appended to the original message and forwarded to the remote end.

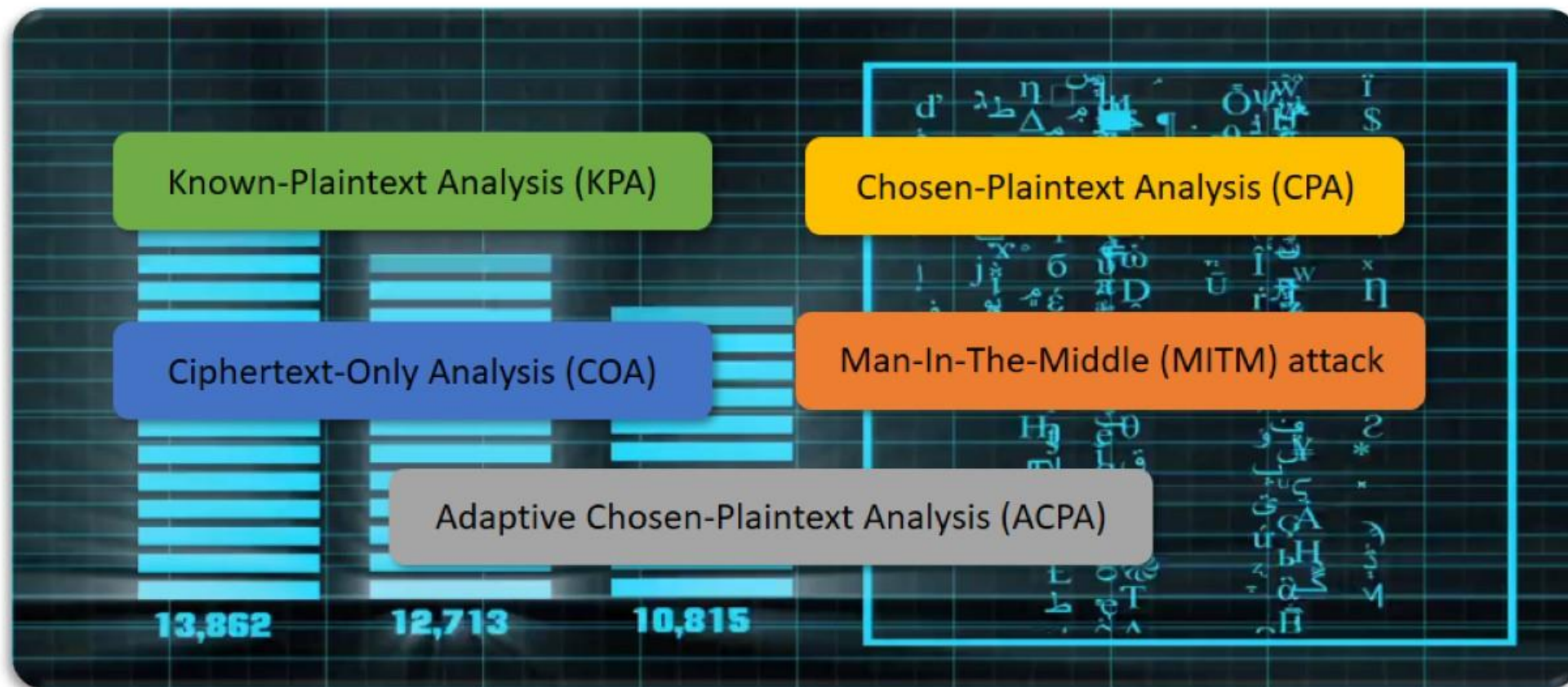
Cryptanalysis= the
science of breaking
encryption



- To determine the weak points of a cryptographic system, it is important to attack the system. These attacks are called Cryptanalytic attacks.
- The main goal of a Cryptanalysis attack is to recover the key in use rather than simply to recover the plaintext of a single ciphertext.



- Attempt to infer some meaning without even breaking the encryption, such as noticing an unusual frequency of communication or determining something by whether the communication was short or long.
- Attempt to deduce the key, in order to break subsequent messages easily
- Attempt to find weaknesses in the implementation or environment of the use of encryption.
- Attempt to find general weaknesses in an encryption algorithm, without necessarily having intercepted any messages.



- **Known-Plaintext Analysis (KPA) :**

In this type of attack, some plaintext-ciphertext pairs are already known. The attacker maps them in order to find the encryption key. This attack is easier to use as a lot of information is already available.

- **Chosen-Plaintext Analysis (CPA) :**

In this type of attack, the attacker chooses random plaintexts and obtains the corresponding ciphertexts and tries to find the encryption key. It's very simple to implement like KPA but the success rate is quite low.

- **Ciphertext-Only Analysis (COA) :**

In this type of attack, only some ciphertext is known and the attacker tries to find the corresponding encryption key and plaintext. It's the hardest to implement but is the most possible attack as only ciphertext is required.

- **Man-In-The-Middle (MITM) attack :**

In this type of attack, the attacker intercepts the message/key between two communicating parties through a secured channel.

- **Adaptive Chosen-Plaintext Analysis (ACPA) :**

This attack is like CPA. Here, the attacker requests the cipher texts of additional plaintexts after they have ciphertexts for some texts.

- Stallings, W. (2006). Cryptography and network security principles and practices 4th edition
- Vincent Nestler, Gregory White, wm. Arthur Conklin, Principles of Computer Security: CompTIA Security+ and Beyond – Lab Manual, ISBN: 978-0-07-174856-8, MHID: 0-07-174856-3, McGraw Hill, 2011



Thank You