CRYPTOGRAPHY AND NETWORK SECURITY

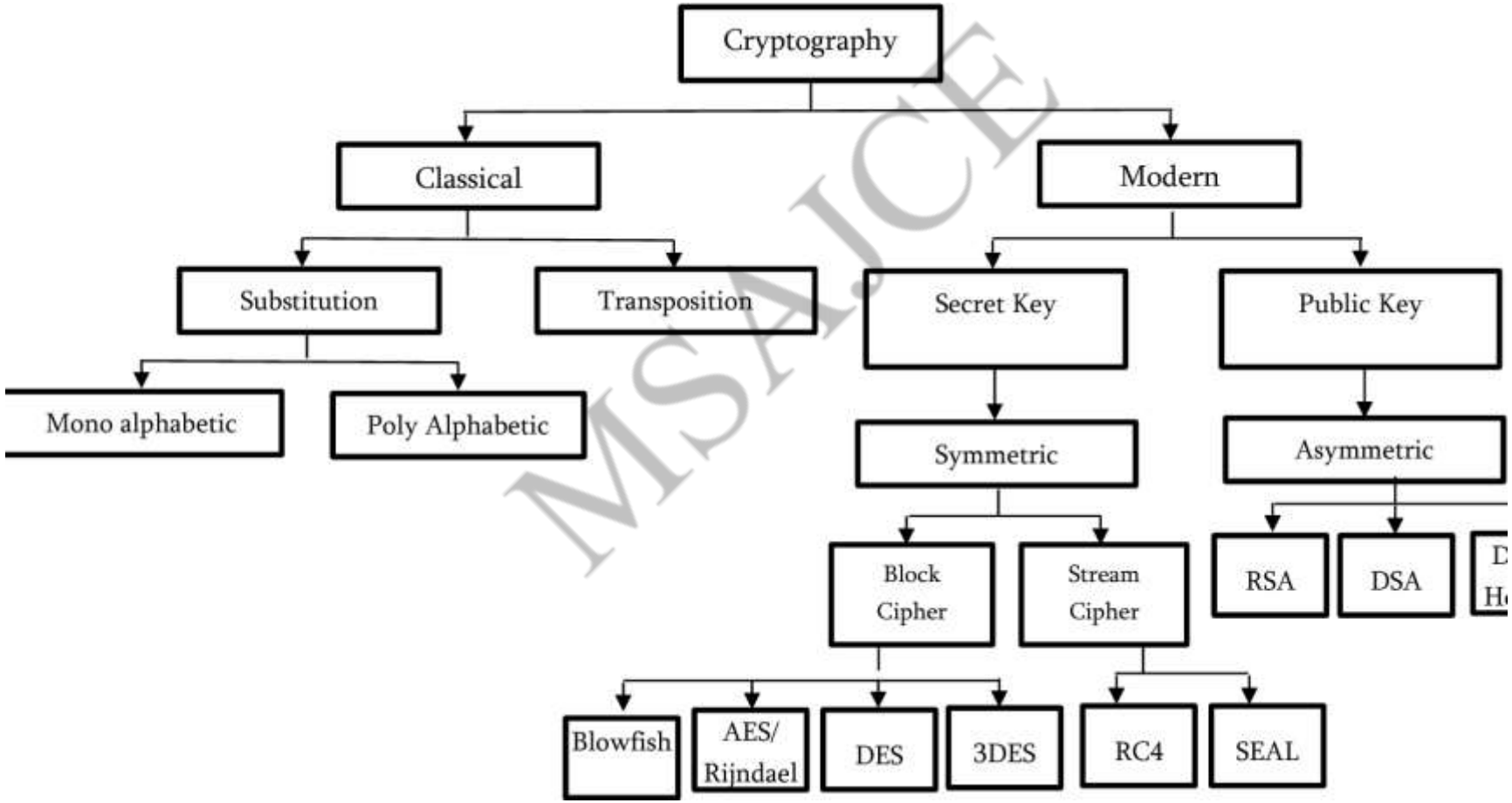
BY

M.A.AYSHA SUFREEN

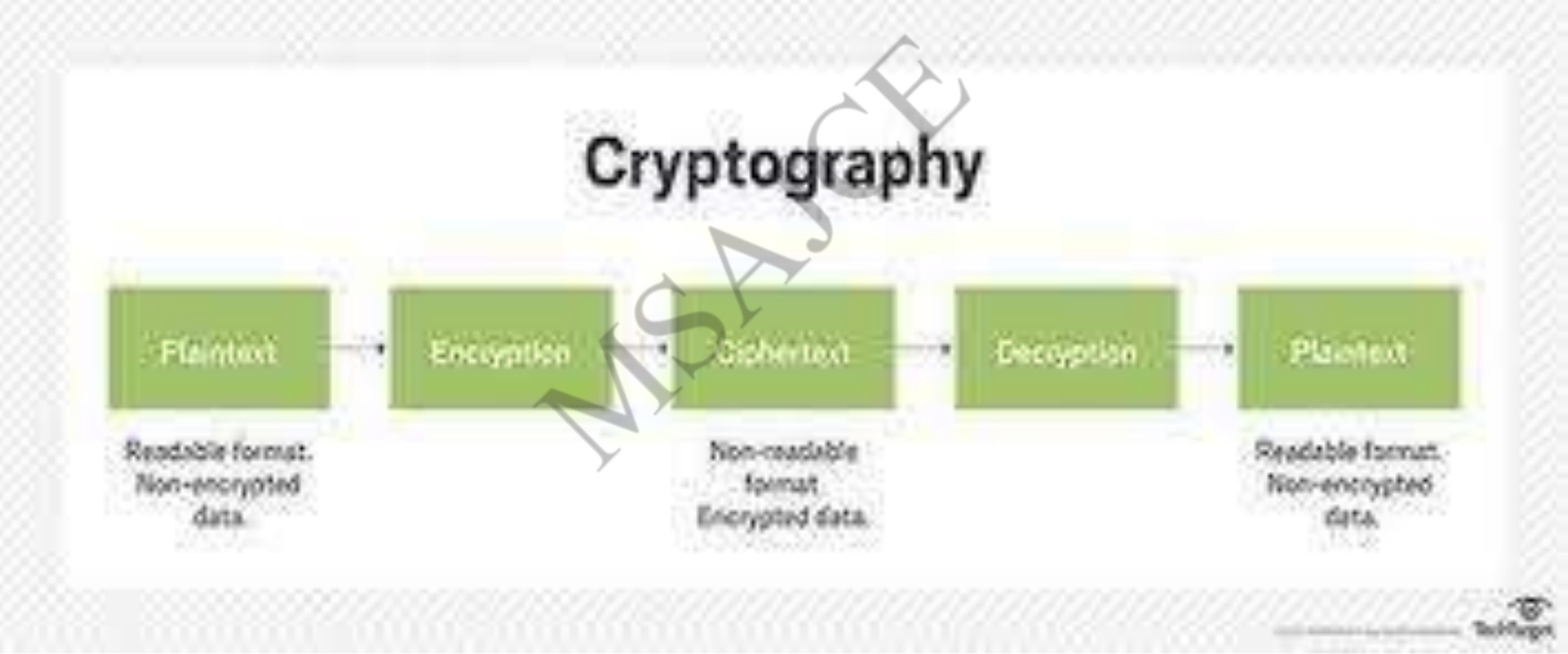
What is Cryptography ?

- Cryptography is the science of encryption and decryption written communication.
- It comes from the Greek word “krptos” = hidden “graphia” = writing.
- Cryptography is sending information (sensitive information) confidentially.

Classification of Cryptography:



Encrypting and decrypting method:



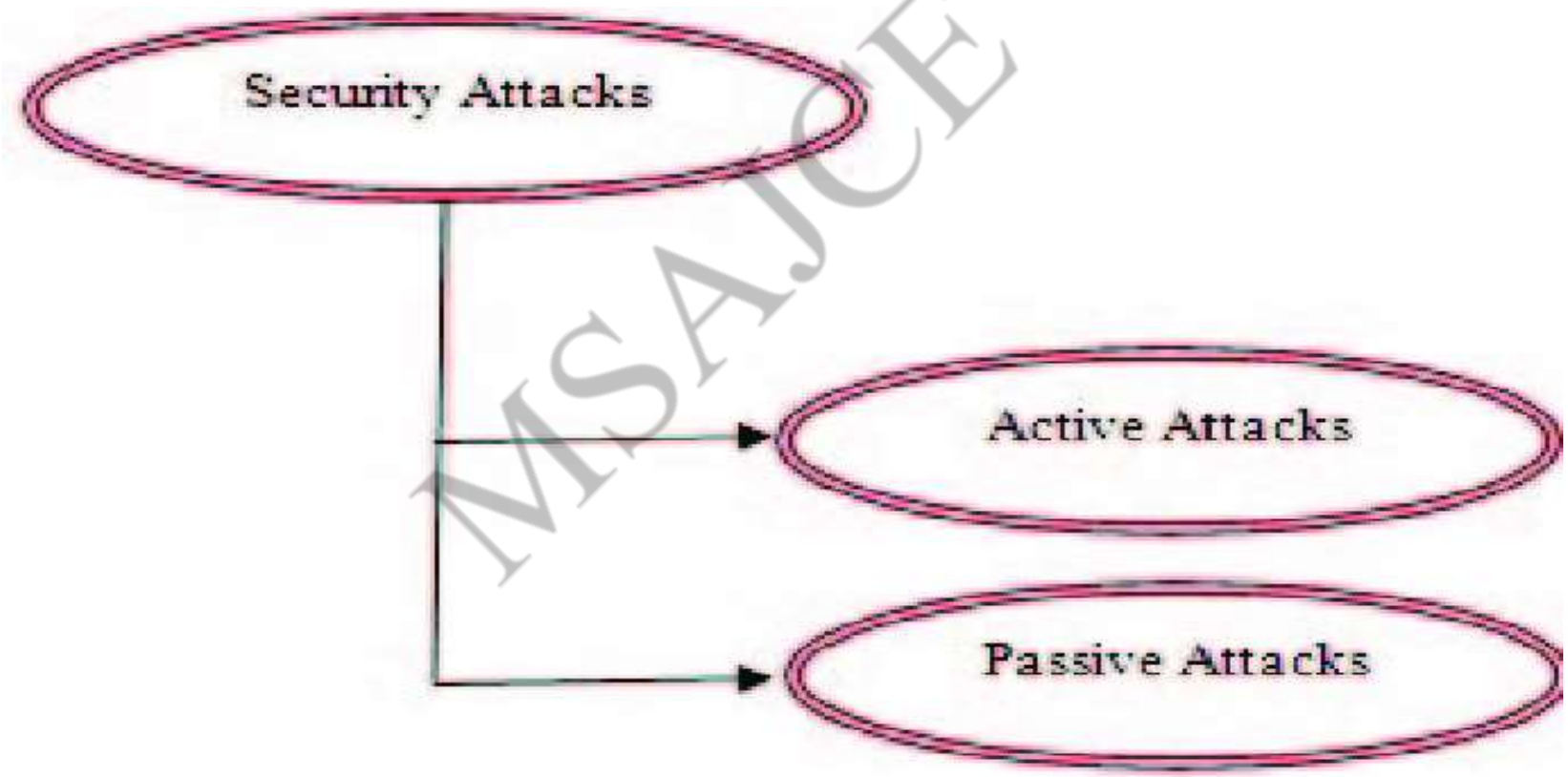
Security Attack, Mechanism and Service:

- Security Attack : Any action that compromises the security of information by an organization.

- Security Mechanism: A mechanism that is designed to Detect , Prevent and Recover.

- Security Service: A service that enhances the security of the data processing system and the information transfers of an organization.

Security Attack:



Active vs Passive (attack):

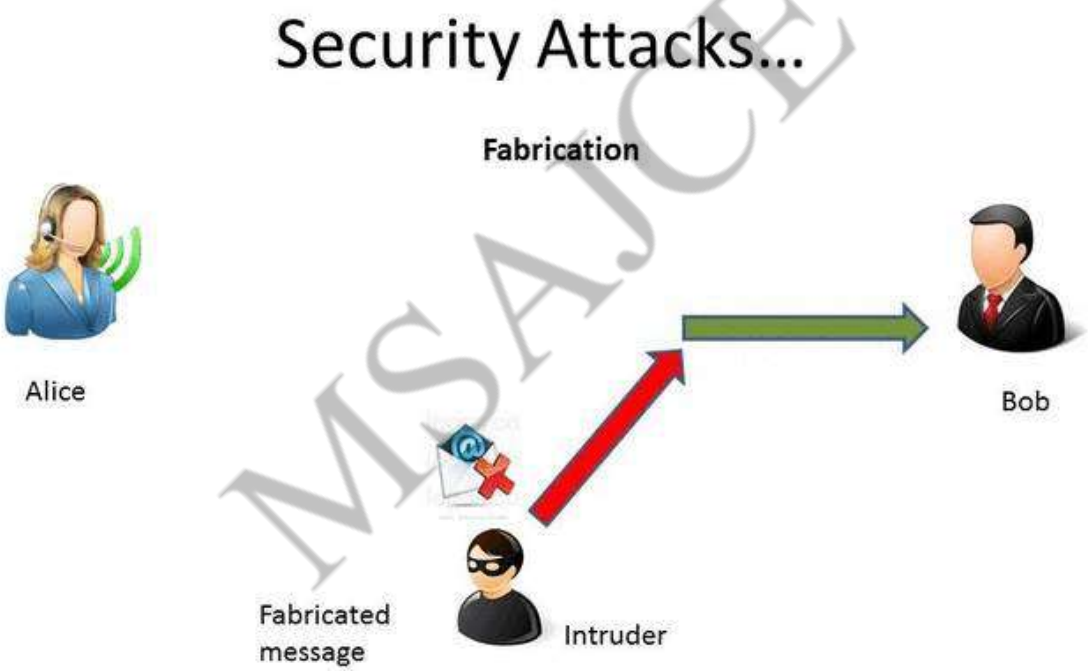
Active Attack

- Modify.
- Affect the system(information).
- Can be easily detected.

Passive Attack

- Monitor the data.
- Does not affected the system.
- Can not be easily detected.

Cont…


Security Attacks…
Fabrication
Alice
Bob
Fabricated message
Intruder
Intruder fabricate a message and send impersonating the sender
This is an attack on authenticity
An active intruder
Summer Workshop on Cyber Security August 12- 16 , 2013 – Network Security, TTU

Types of Cryptography

1. Asymmetric

2. Symmetric

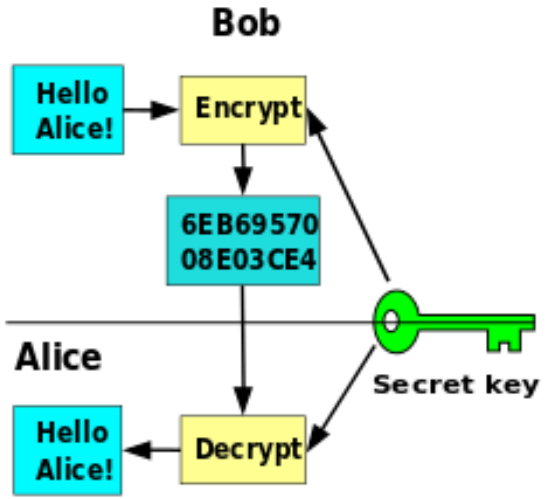
1.Asymmetric:

- Asymmetric cryptography (Public Key Cryptography) uses two different keys for encryption and decryption.
- Each user has a pair of keys, one is called a public key and the other is called a private key.
- The public key is made public, while the private key is always kept secret.

Cont..

2.Symmetric Cryptography

- In Symmetric Cryptography or Secret -Key Cryptography, the sender and recipient of a message know and use the same secret key.
- The sender uses the secret key to encrypt the message and the recipient uses the same key to decrypt the message. This method is called symmetric cryptography or secret key cryptography.



RSA (**Rivest–Shamir–Adleman**) algorithm:

- RSA algorithm is asymmetric cryptography algorithm.
- Asymmetric actually means that it works on two different keys i.e. **Public Key** and **Private Key.**
- As the name describes that the Public Key is given to everyone and Private key is kept private.
- The idea of RSA is based on the fact that it is difficult to factorize a large integer.
- The public key consists of two numbers where one number is multiplication of two large prime numbers. And private key is also derived from the same two prime numbers.

Cont..

- So if somebody can factorize the large number, the private key is compromised. Therefore encryption strength totally lies on the key size and if we double or triple the key size, the strength of encryption increases exponentially.
- RSA keys can be typically 1024 or 2048 bits long.

>>

Generating public key:

Public key:

- Select two prime no's. Suppose **P = 53 and Q = 59**.
- Now First part of the Public key : **n = P*Q = 3127**.
- We also need a small exponent say **e** :
- But e Must be an integer now we consider **e =3**

Generating Private Key :

We need to calculate Φ(n) :

$$\Phi(n) = (P-1)(Q-1)$$
$$= (53-1)(59-1)$$

so, Φ(n) = 3016 .

Now calculate Private Key,

K=2 , e=3, Φ(n) = 3016

$$d : d = (k*\Phi(n) + 1) / e$$
$$=(2*(3016)+1)/3$$
$$d = 2011$$

Now we are ready with our – Public Key (n = 3127 and e = 3) and Private Key(d = 2011)

Encryption and Decryption:

Now we will encrypt **“HI”** :

Convert letters to numbers : H = 8 and I = 9

Thus **Encrypted Data c = 89^e mod n**.

= 89^3 mod 3016

c = 1394

Thus our Encrypted Data comes out to be 1394

Now we will decrypt **1394** :

Decrypted Data = c^d mod n. =1394^2011 mod 3016

= 89

Thus our Decrypted Data comes out to be 89

8 = H and I = 9 i.e. "HI".