Unit V

Security

Introduction

Security Services:

The processing or communication service that is provided by a system

To give a specific kind of protection to system resources.

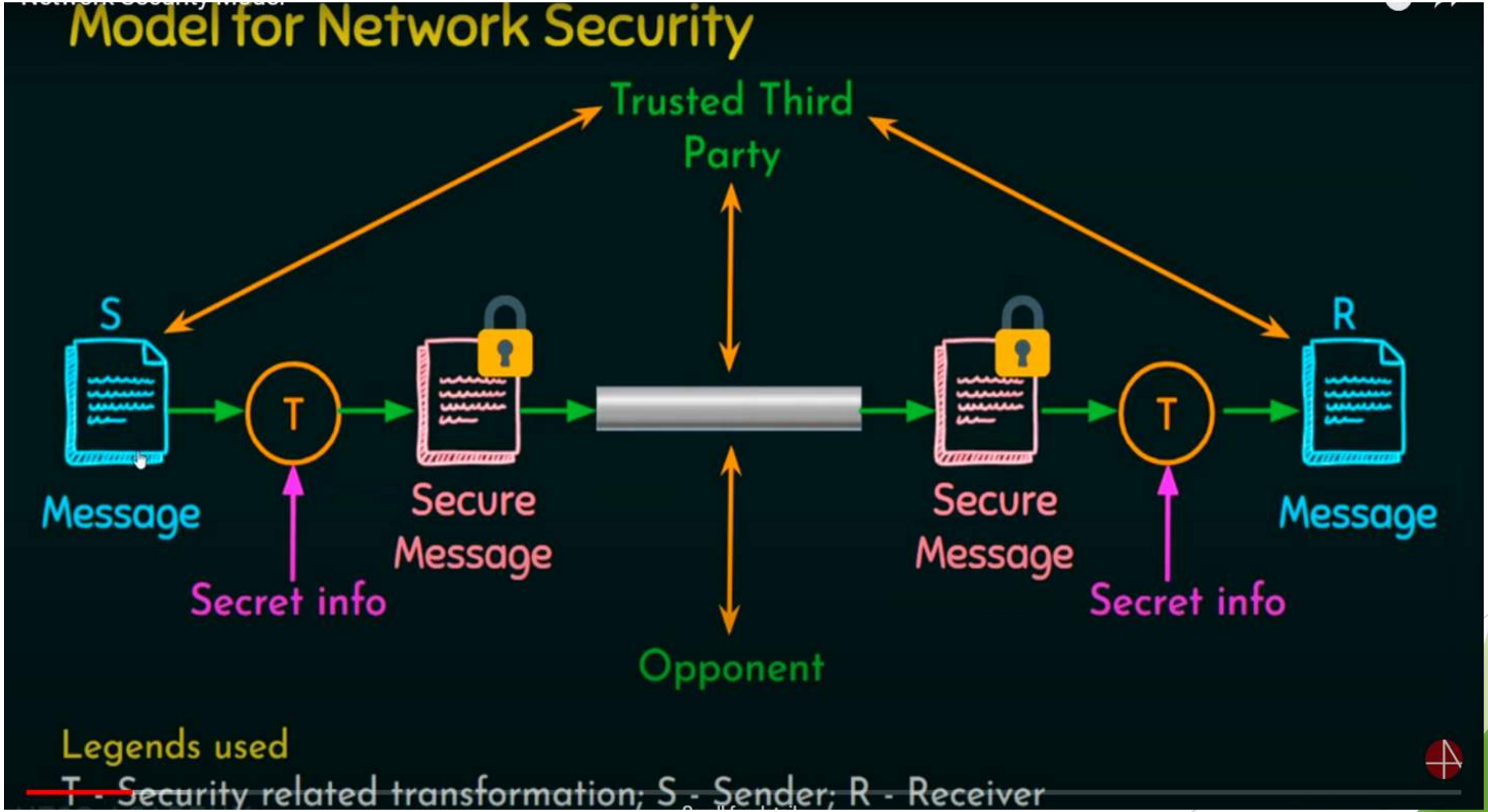
Security Services

- **1)Authentication: message authentication is a service to make the receiver sure of the sender identity.** Right user can accessing the system. Ex-Gmail, ATM,OTP
- **2)Authorization :** Whenever we have **multiple database ,or services. Authorization** defines which **services or database you should use**.It provides access control.Ex-Principal,professor, peon in organization.
- **3)Non-repudiation :**Nonrepudiation means a user cannot deny having performed a transaction.

Sender A
Receiver B

- **4)Message Privacy:**message privacy is that sender and receiver expect confidentiality & only intended receiver should able to decode the transmitted message correctly.

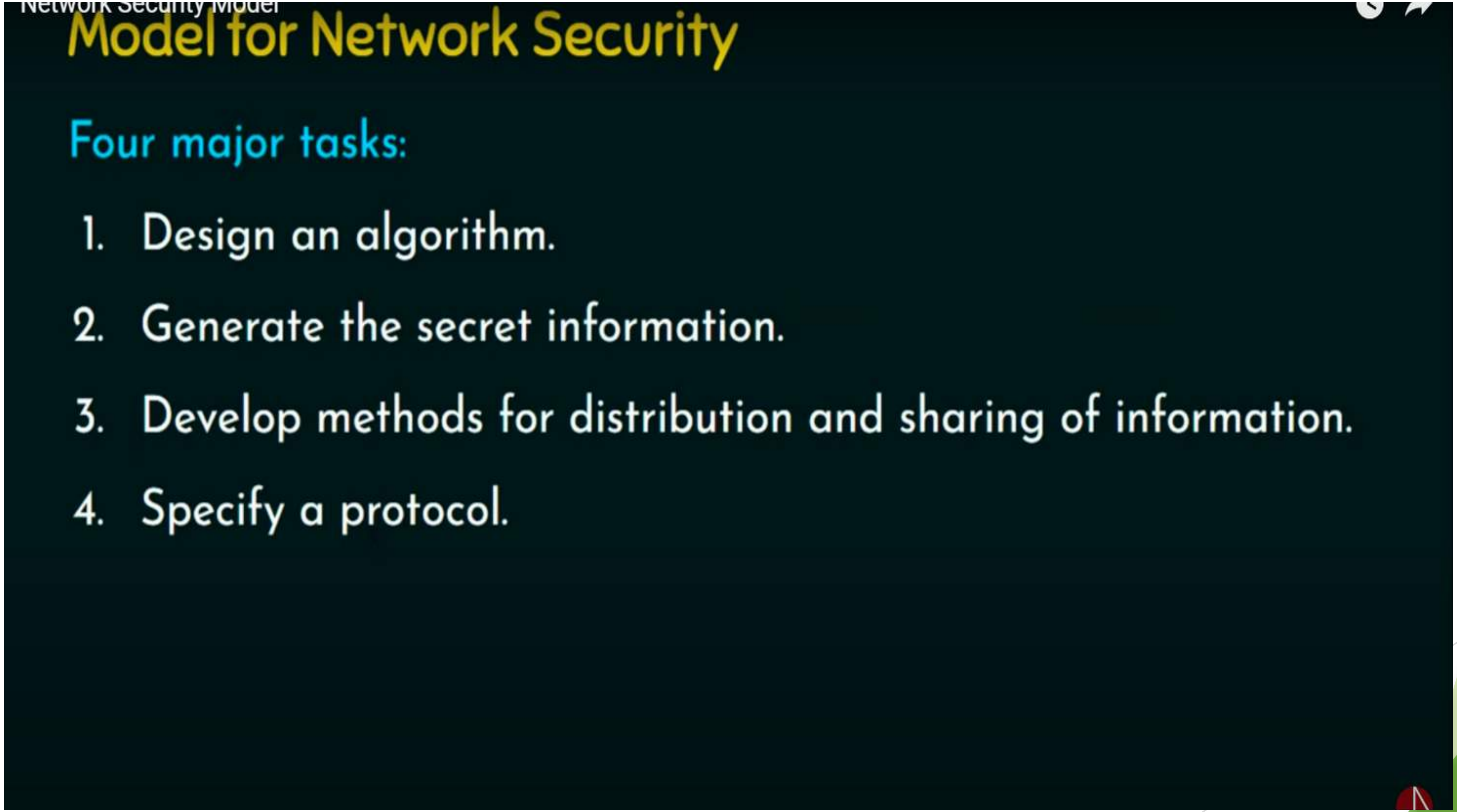
Network Security Model



Legends used

T - Security related transformation; S - Sender; R - Receiver

Network Security model

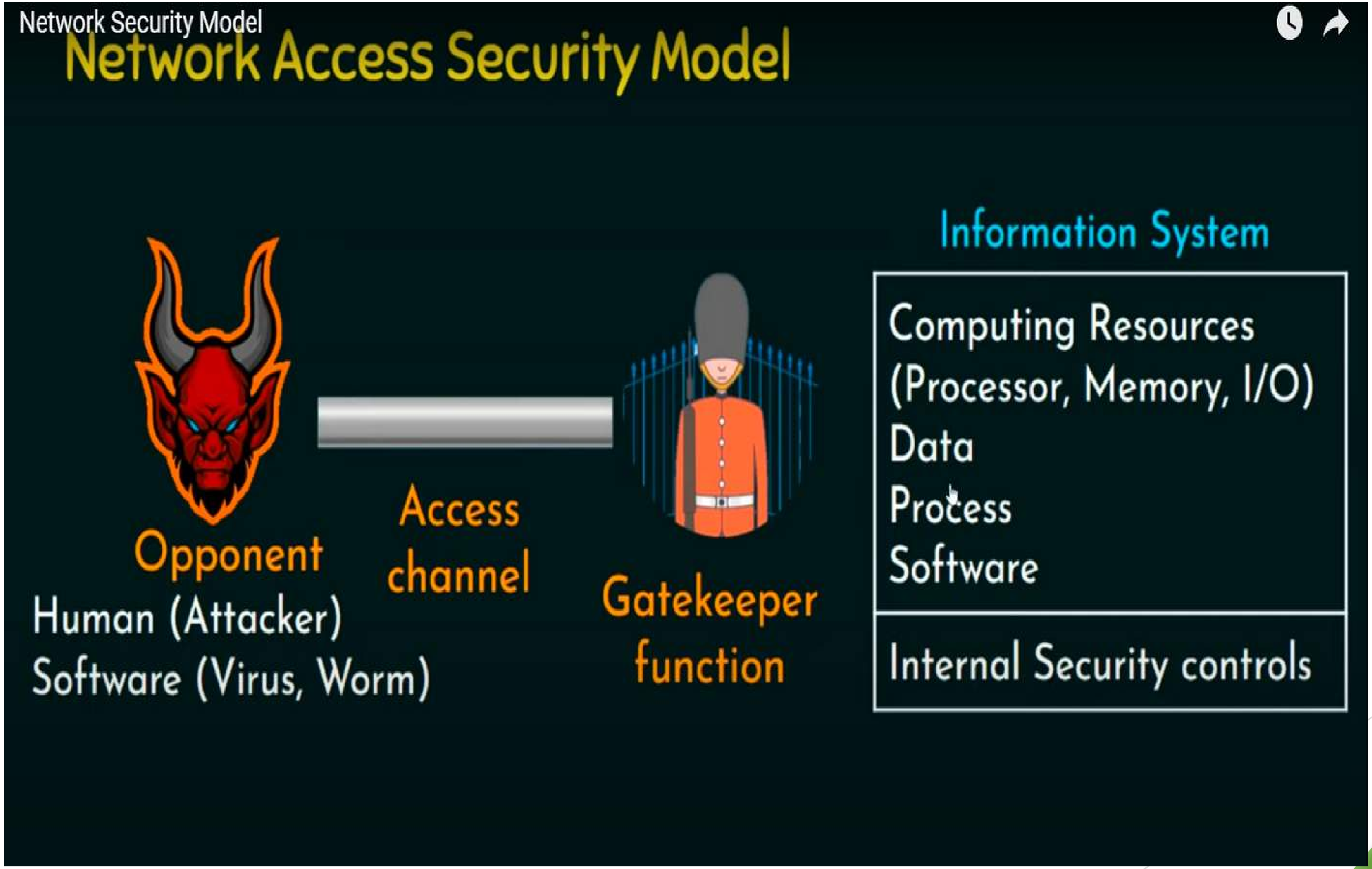


Network Security Model

Model for Network Security

Four major tasks:

1. Design an algorithm.
2. Generate the secret information.
3. Develop methods for distribution and sharing of information.
4. Specify a protocol.



Network Security Model

Network Access Security Model

Opponent

Human (Attacker)

Software (Virus, Worm)

Access channel

Gatekeeper function

Information System

Computing Resources
(Processor, Memory, I/O)
Data
Process
Software

Internal Security controls

Basics of network security

Plain Text

Cipher Text

Encryption

Decryption

Cryptography

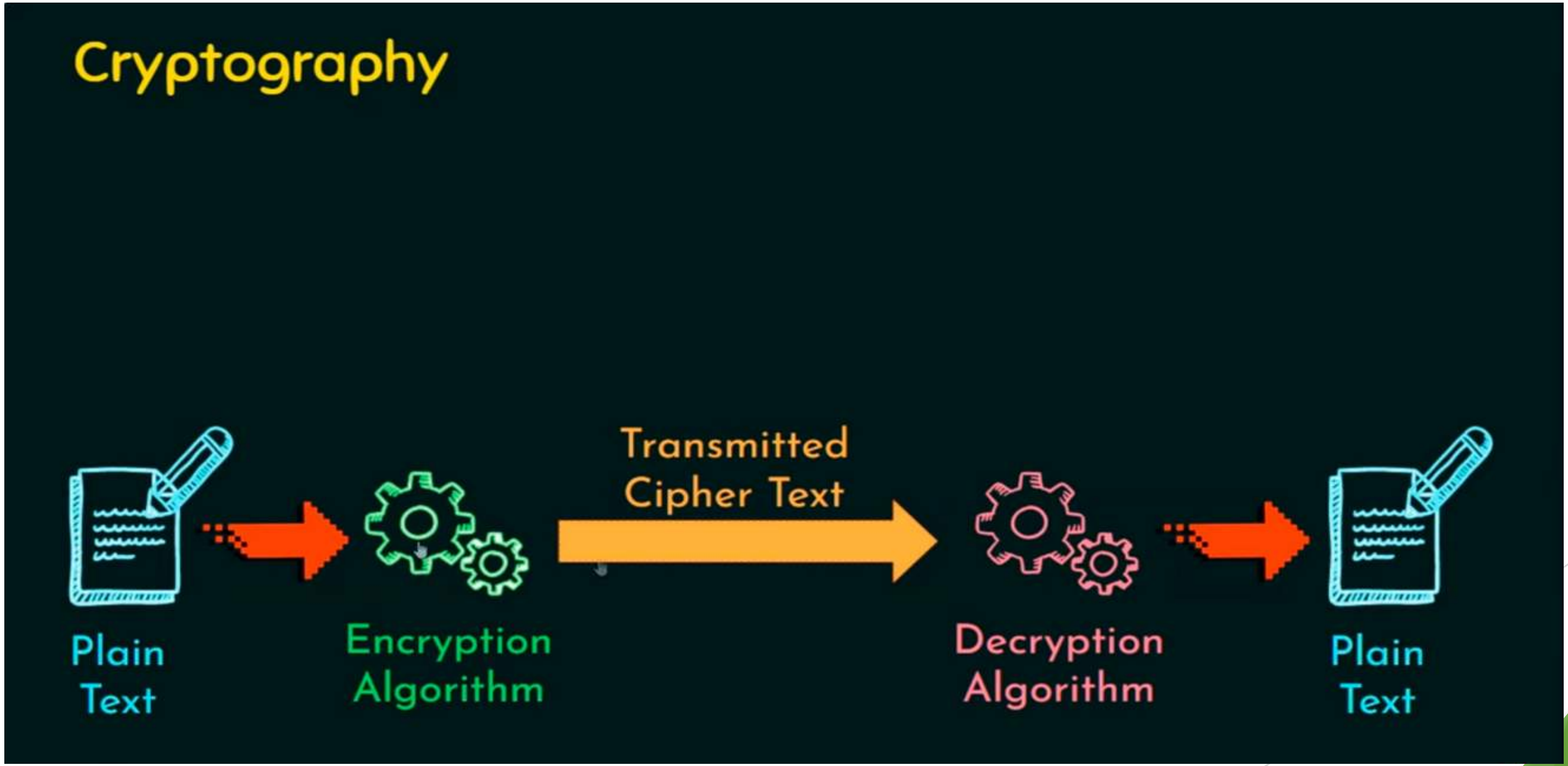
Cryptanalyst

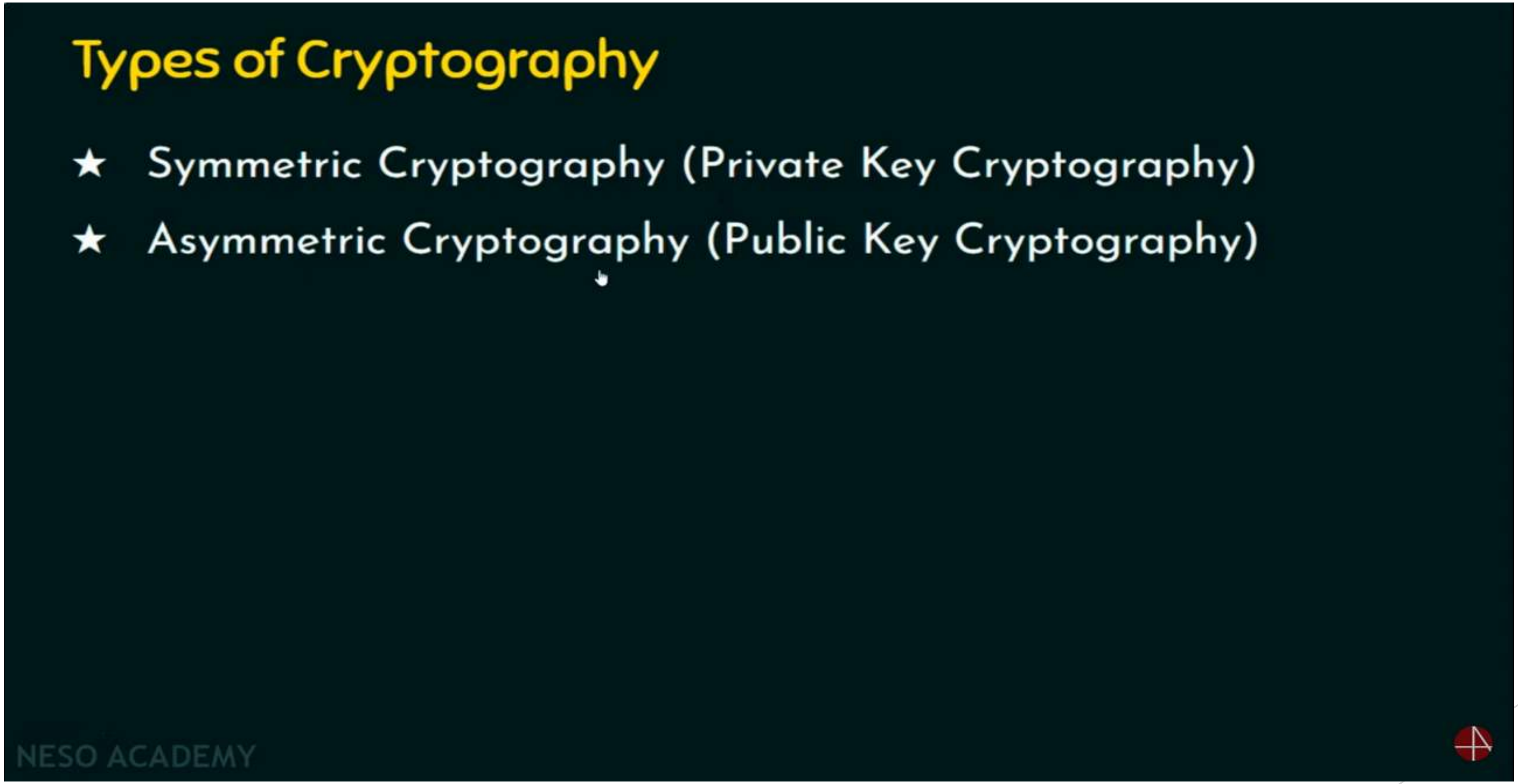
key

- **Plain text:** In cryptography, **plaintext is the original, readable form of data** before it is encrypted.
- **Ciphertext:**a cipher is a **set of algorithms that encrypts and decrypts data.**
- **Encryption:**Encryption is a cryptographic process that **convert data into an unreadable form,**called cipher text, so that **only authorized users can access it.**
- **Decryption:**In cryptography, decryption is the process of **converting encrypted data back into its original**, readable form.
- **Cryptography:**Cryptography is a method of **protecting information and communications using codes and mathematical concepts**
- **Key:**In cryptography, a key is a piece of information used to scramble data so that it appears random. It's usually a string of numbers or letters that's stored in a file.

Cryptography

The art or science that transforming an intelligible message into one that is unintelligible and then retransforming that message back to its original form

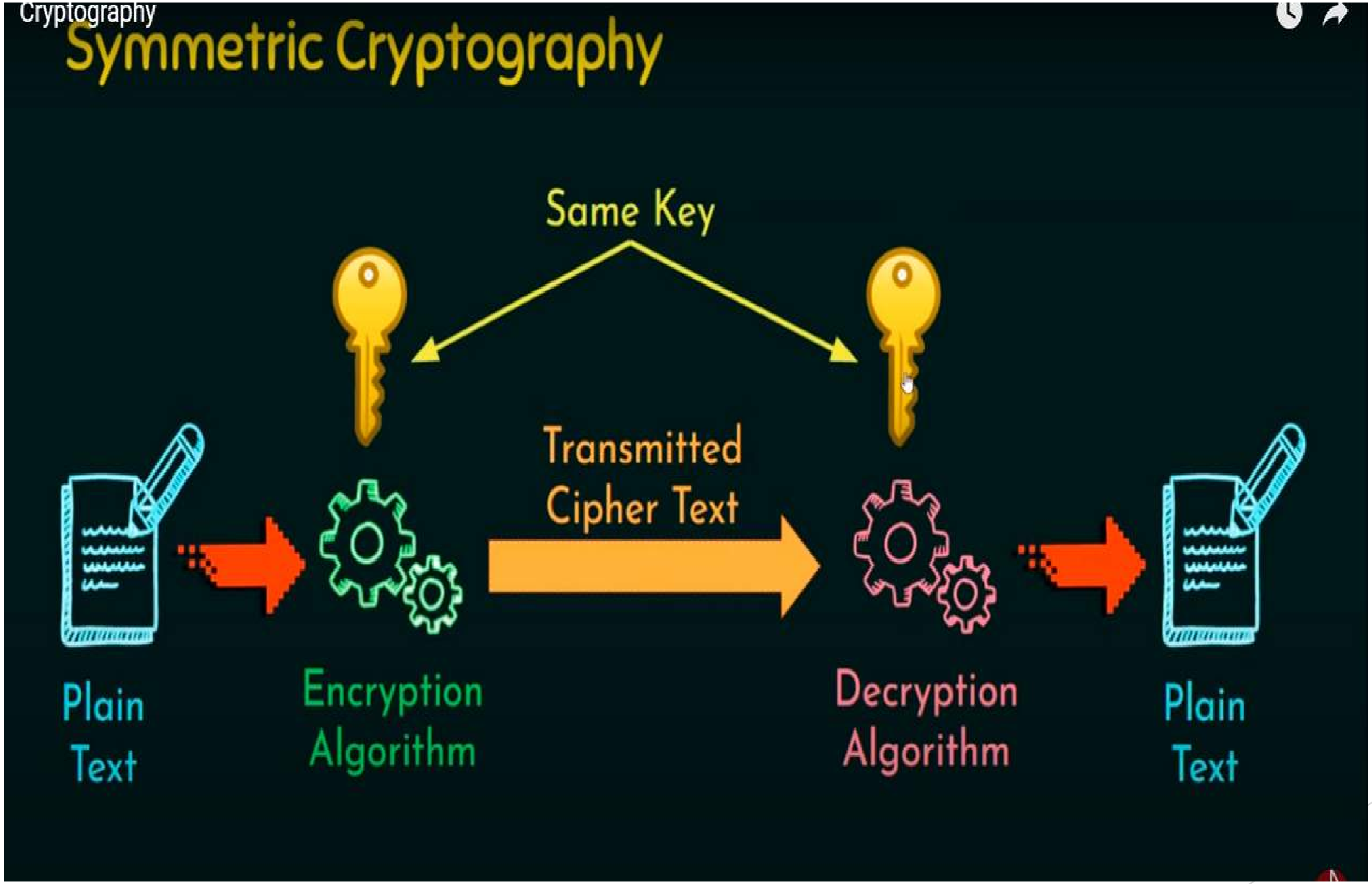




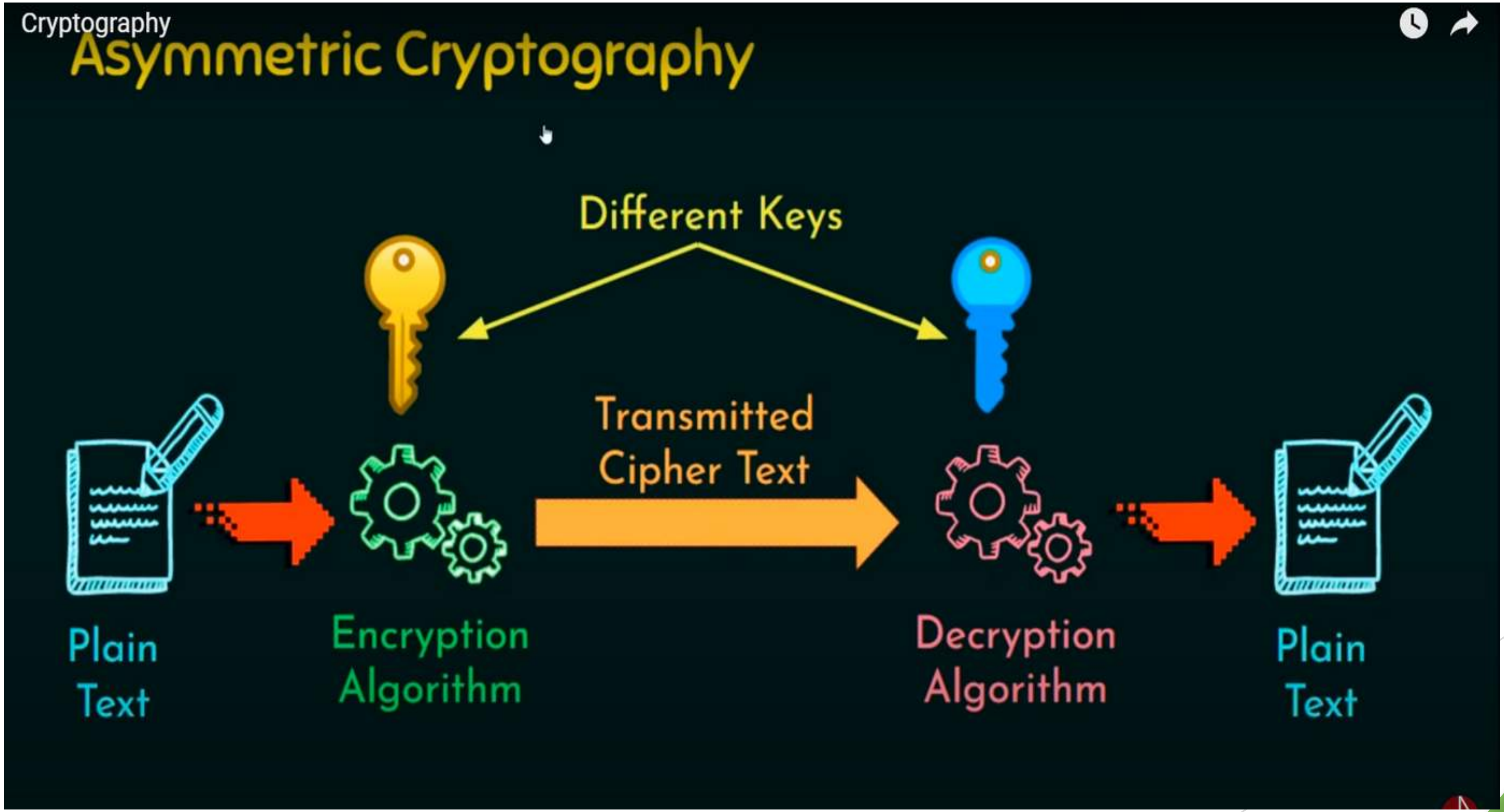
Types of Cryptography

- ★ Symmetric Cryptography (Private Key Cryptography)
- ★ Asymmetric Cryptography (Public Key Cryptography)

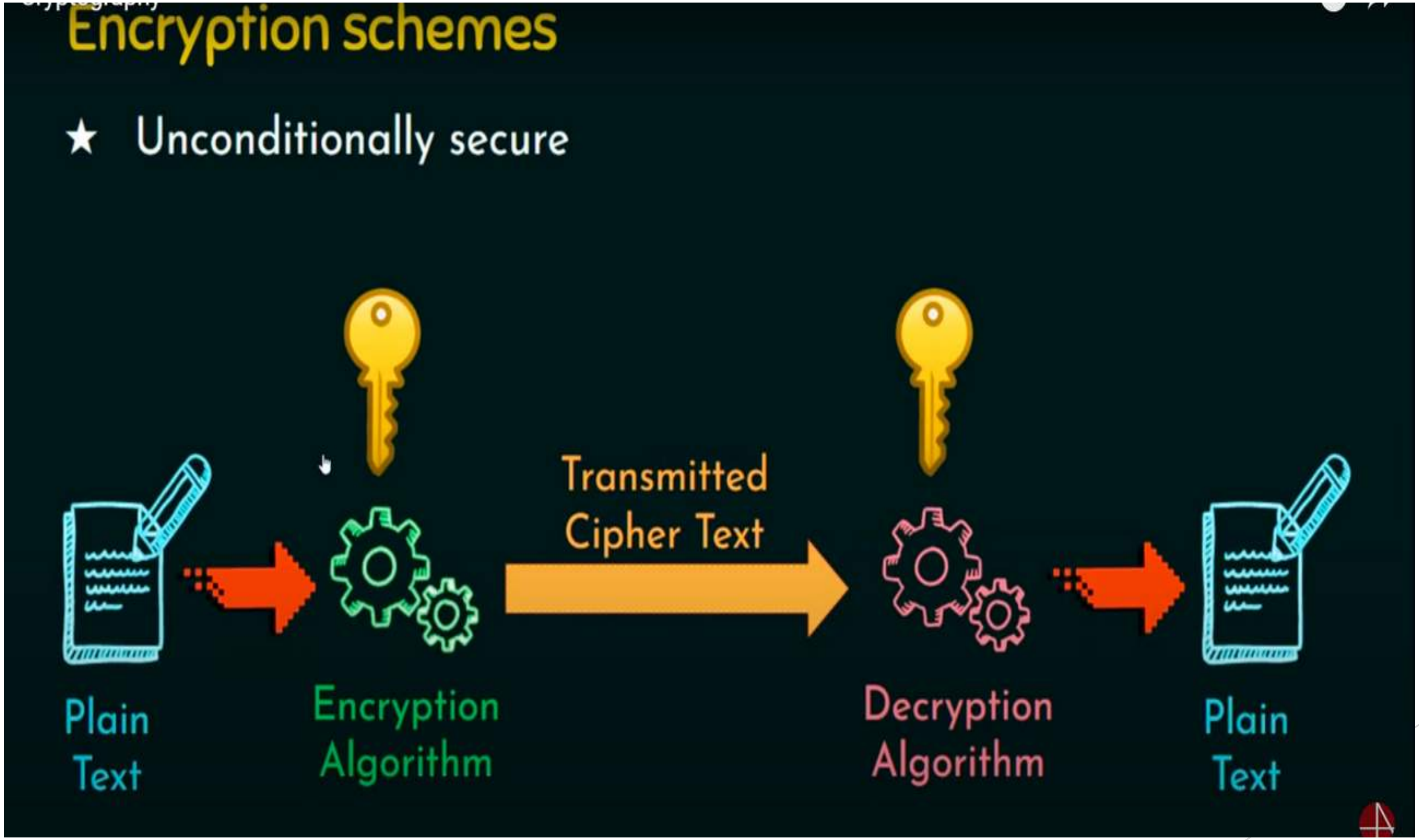
1)Symmetric Cryptography



2)Asymmetric cryptography

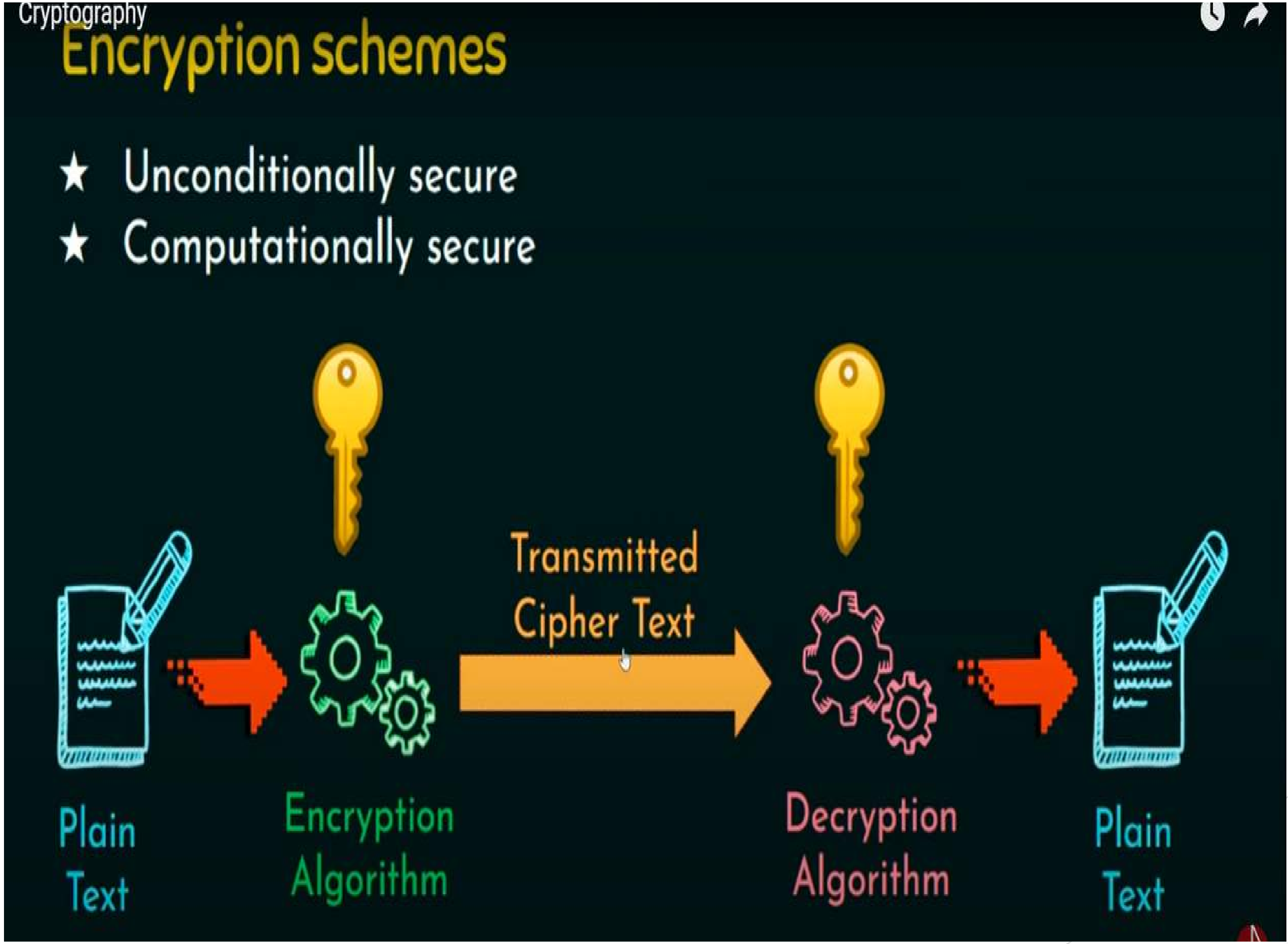


Whenever attacker is able to guess what is the plain text equivalent to the cipher text



Encryption schemes

- ★ Unconditionally secure



Cryptography

Encryption schemes

- ★ Unconditionally secure
- ★ Computationally secure

RSA (Rivest-Shamir-Adleman)

- Used to encrypt & decrypt message.
- It is asymmetric alg.
- **Encryption-**
- C=p^e mod n
- **Decryption-**
- P=c^d mod n
- Public Key={e,n}
- Private key={d,n}
- **Key Generation:**
- **1)consider two large number q,p**
- **2)calculate n=p*q**
- **3)Φ(n)=(p-1)(q-1)**
- **4)choose a small number e,co-prime to Φ(n) with GCD(Φ(n),e)=1 and 1<e< Φ(n)**
- **5)find d ,such that d*e mod Φ(n)=1**

- Example:Key generation
- 1)Two prime numbers p=3, q=5
- 2)n=p*q =3*5 =15
- n=15
- 3) **Φ(n)=(p-1)(q-1)**
- **=(3-1)(5-1)**
- **=8**
- **4)Assume e such that gcd(e, Φ(n)=1 & 1<e<Φ(n))**
- **e=3 gcd(3,8)=1**
- **gcd(5,8)=1**
- **gcd(7,8)=1**
- **5)find d**
- **d*e mod Φ(n)=1**
- **d*3 mod 8=1**
- **Cosider d=3**
- **3*3 mod 8=1 9mod 8=1 1=1 d=3**

- Public key={e,n} ={3,15}
- Private key={d,n}={3,15}
- **Encryption**
- Consider Plaintext p=8
- C=p^e mod n
- =8^3 mod 15
- **C=2**
- **Decryption**
- P=c^d mod n
- =2^3 mod 15
- =8 mod 15
- **P=8**