UNIVERSITY OF FRONTIER TECHNOLOGY, BANGLADESH

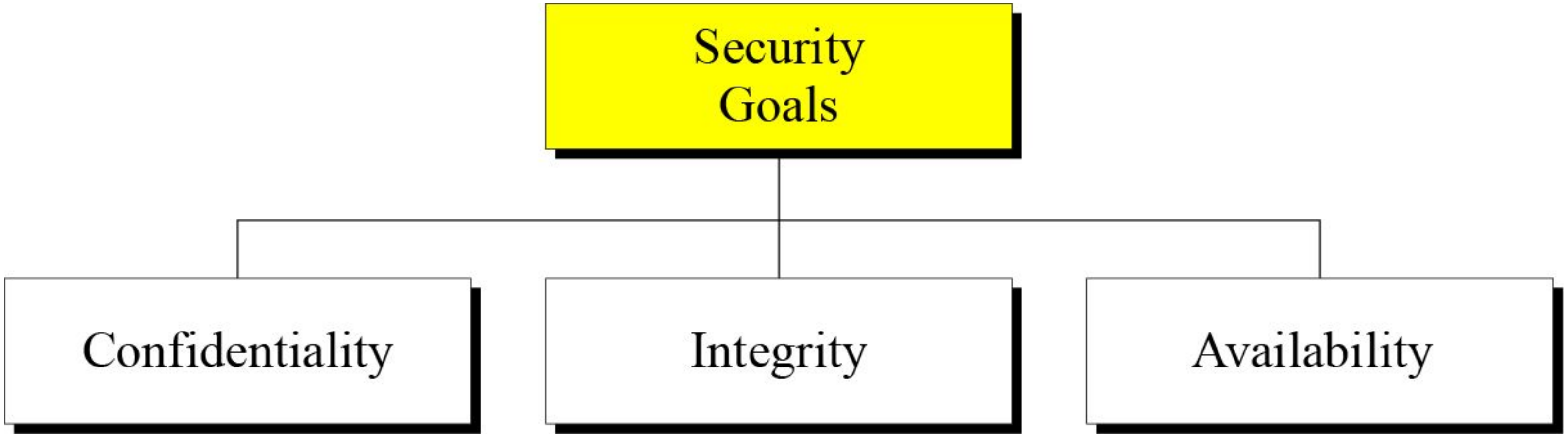
Topic: Introduction to Cryptography

Presented By:

Rakib Hossen
Assistant Professor
Dept. of Cyber Security Engineering (CySE), UFTB

SECURITY GOALS

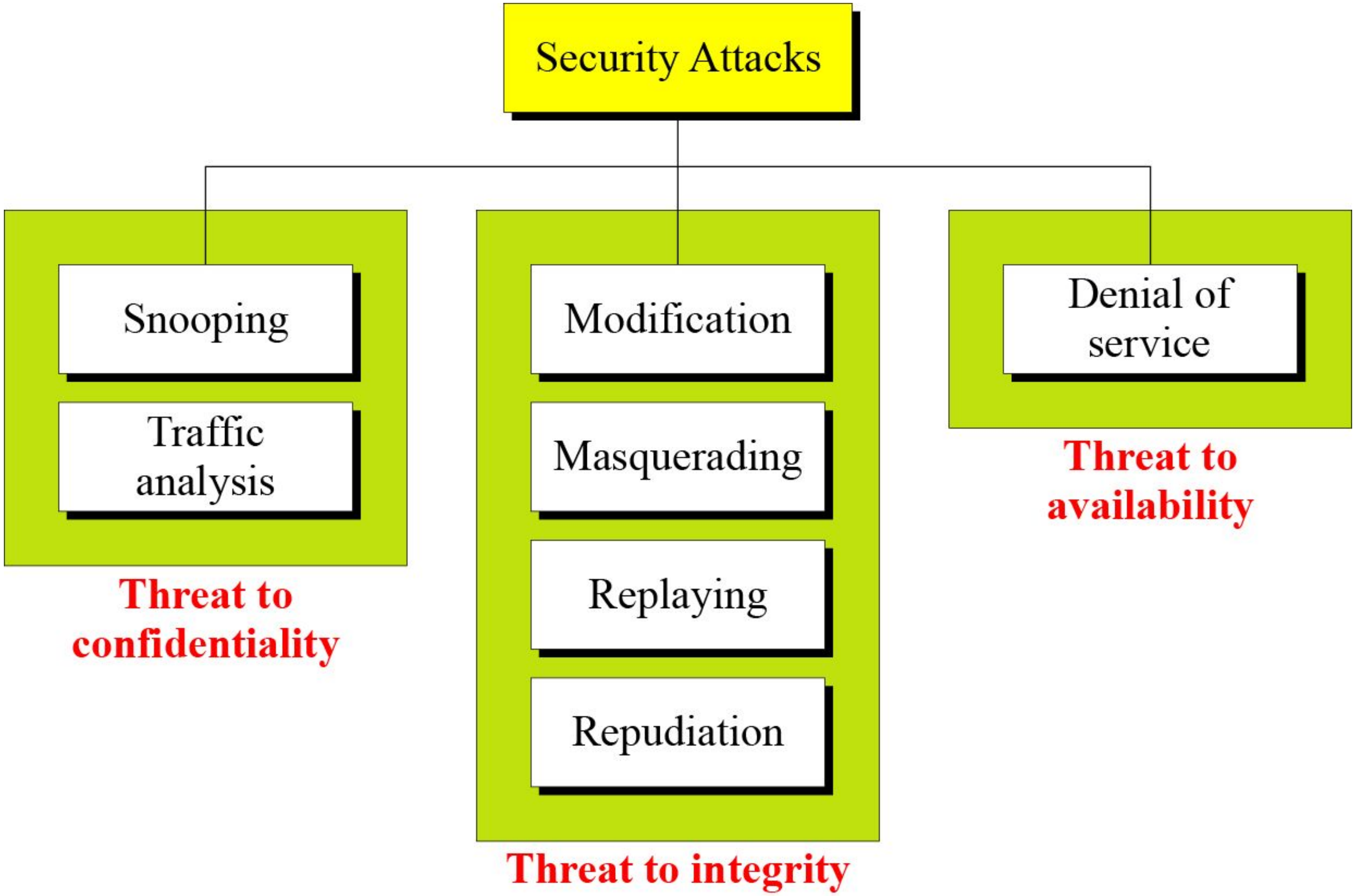
Taxonomy of security goals



The three goals of security —confidentiality, integrity, and availability —can be threatened by security attacks.

- ❖ **Attacks Threatening Confidentiality**
- ❖ **Attacks Threatening Integrity**
- ❖ **Attacks Threatening Availability**

Taxonomy of attacks with relation to security goals



Attacks Threatening Confidentiality

***Snooping** refers to unauthorized access to or interception of data.*

***Traffic analysis** refers to obtaining some other type of information by monitoring online traffic.*

Attacks Threatening Integrity

***Modification** means that the attacker intercepts the message and changes it.*

***Masquerading** or **spoofing** happens when the attacker impersonates somebody else.*

Attacks Threatening Integrity

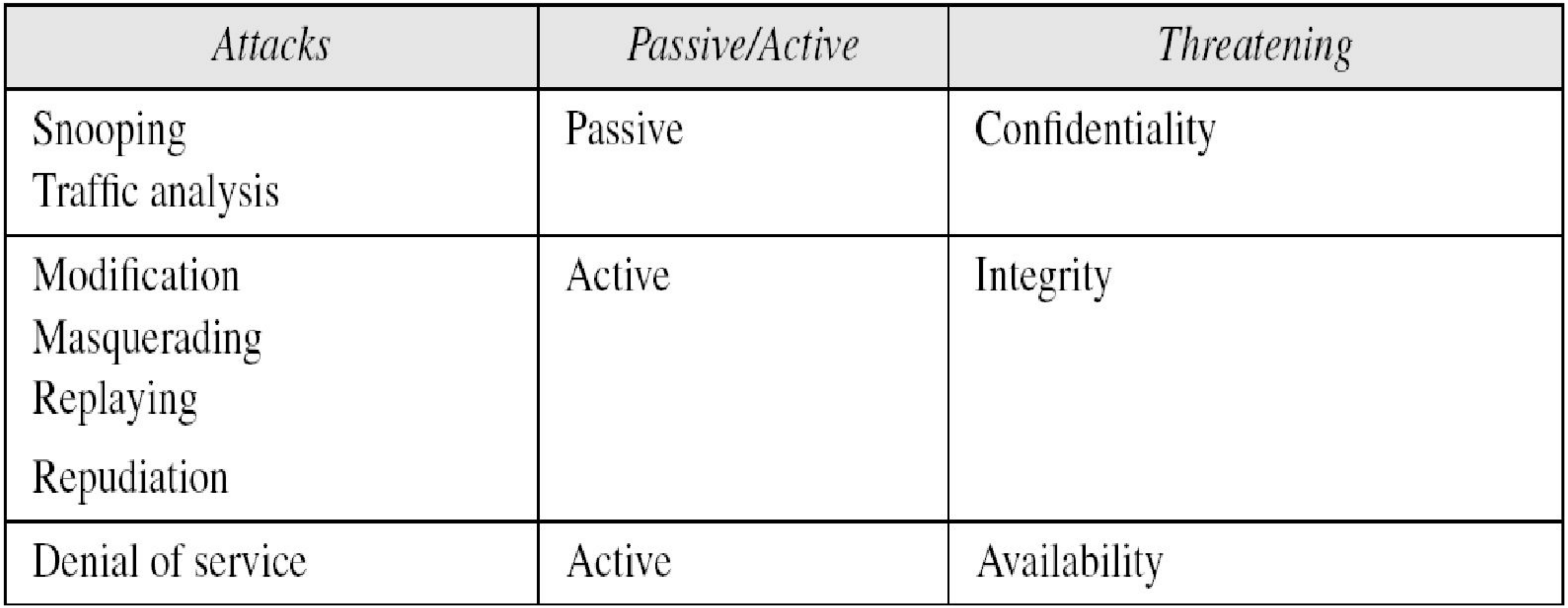
Repudiation means that sender of the message might later deny that she has sent the message; the receiver of the message might later deny that he has received the message.

Replaying means the attacker obtains a copy of a message sent by a user and later tries to replay it.

Attacks Threatening Availability

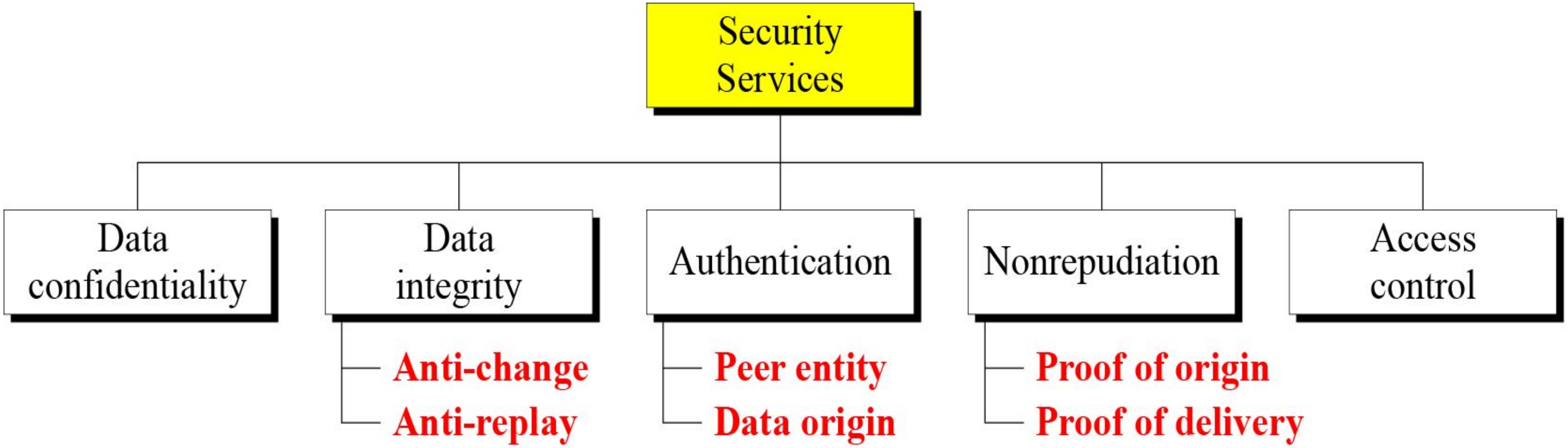
Denial of service (DoS) is a very common attack. It may slow down or totally interrupt the service of a system.

Categorization of passive and active attacks Based on threatened by security attacks

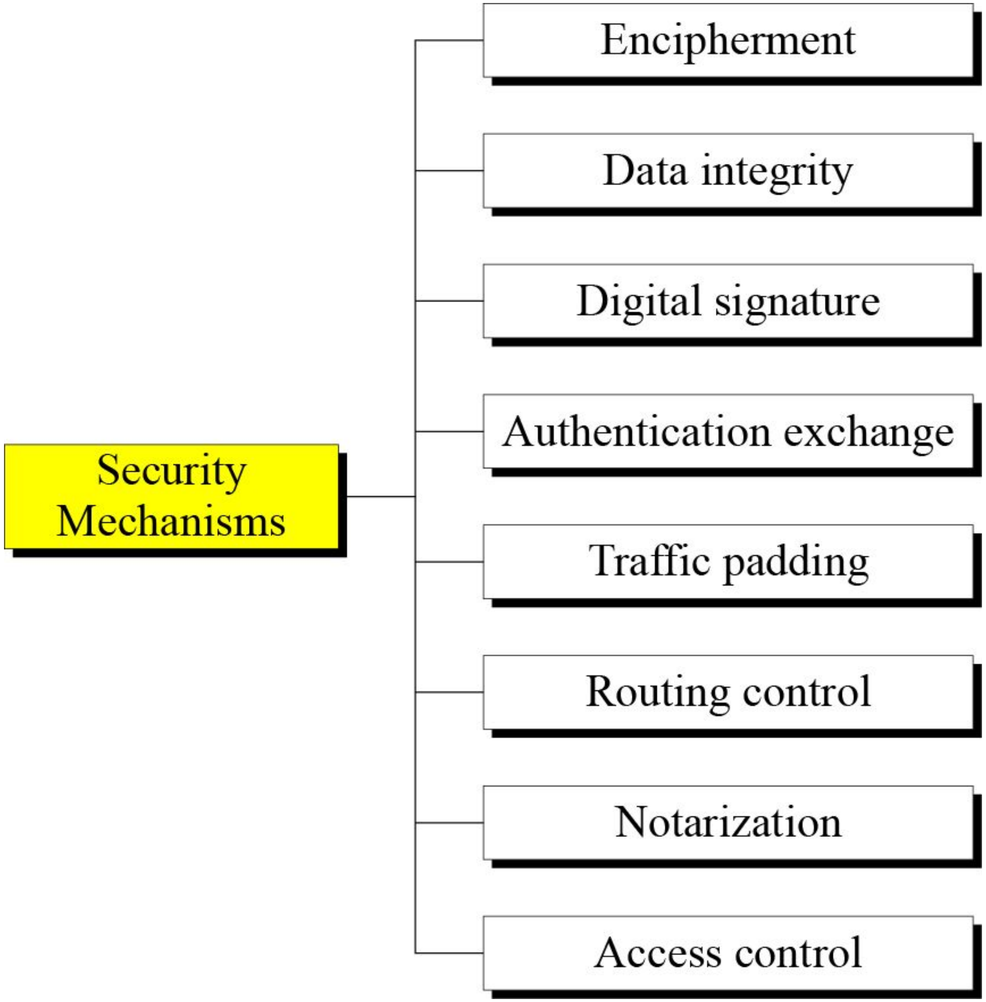


Attacks	*Passive/Active*	*Threatening*
Snooping Traffic analysis	Passive	Confidentiality
Modification Masquerading Replaying Repudiation	Active	Integrity
Denial of service	Active	Availability

Security Services



Security Mechanism



Security Mechanisms

Encipherment

Data integrity

Digital signature

Authentication exchange

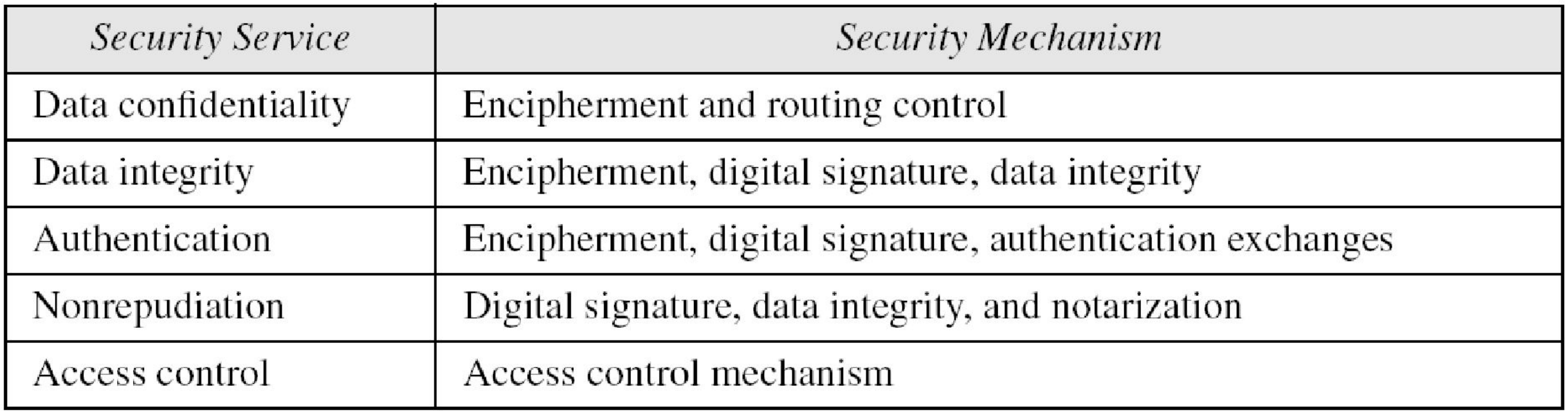
Traffic padding

Routing control

Notarization

Access control

Relation between Services and Mechanisms



Security Service	*Security Mechanism*
Data confidentiality	Encipherment and routing control
Data integrity	Encipherment, digital signature, data integrity
Authentication	Encipherment, digital signature, authentication exchanges
Nonrepudiation	Digital signature, data integrity, and notarization
Access control	Access control mechanism

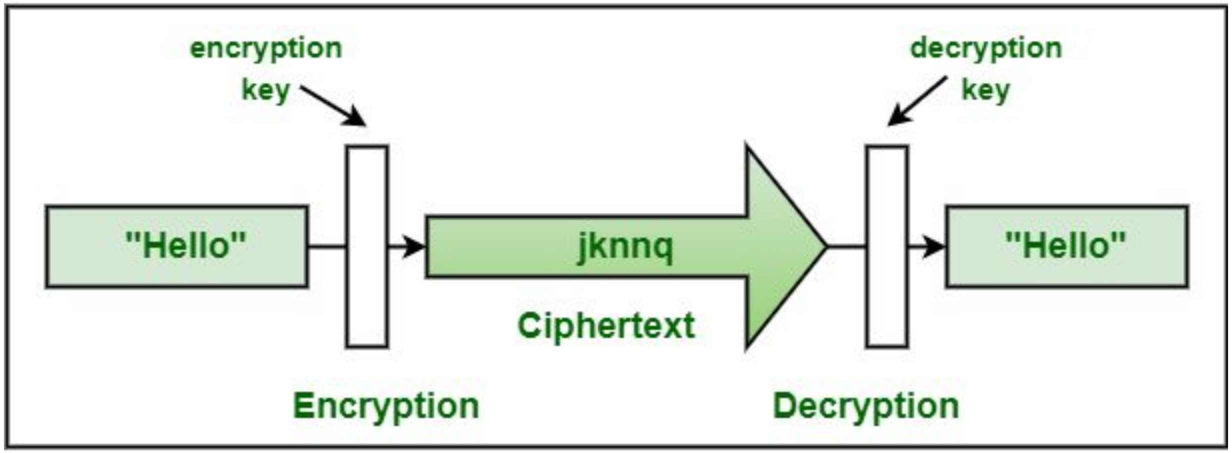
TECHNIQUES

- The actual implementation of **security goals needs some techniques.**
- Two techniques are prevalent today:

  - ❑ Cryptography
  - ❑ Steganography

Cryptography

- ***Cryptography, a word with Greek origins, means "secret writing."***
- **Cryptography is the process of hiding or coding information so that only the person a message was intended for can read it.**
- **The art of cryptography has been used to code messages for thousands of years and continues to be used in bank cards, computer passwords, and ecommerce**



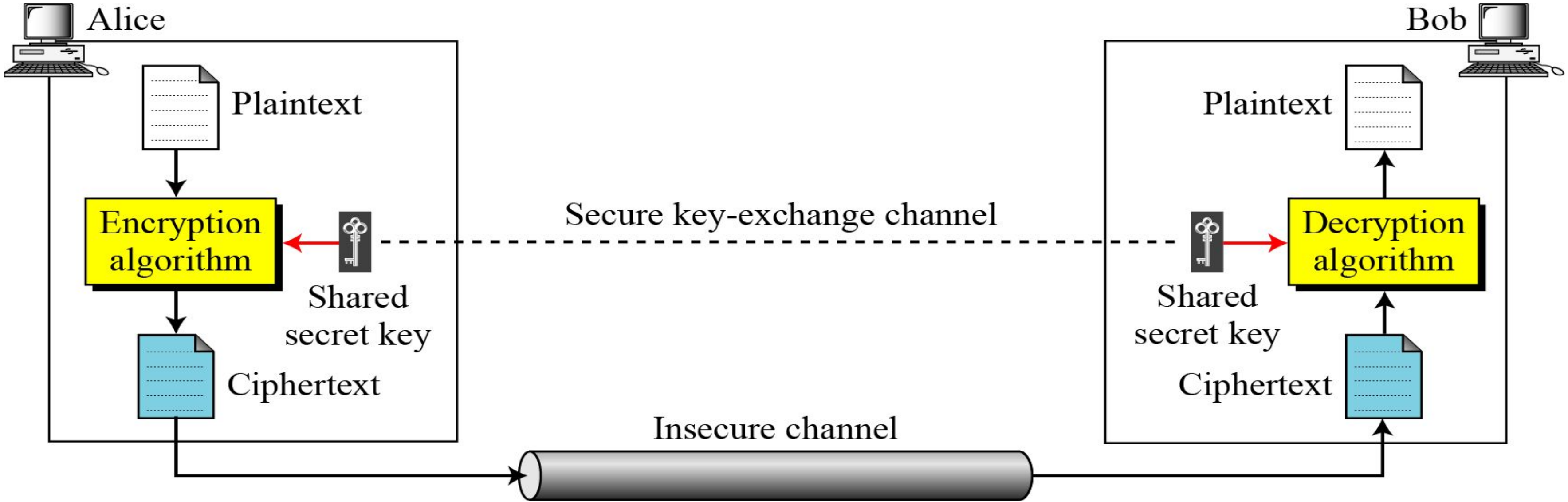
Cryptography

Types Of Cryptography

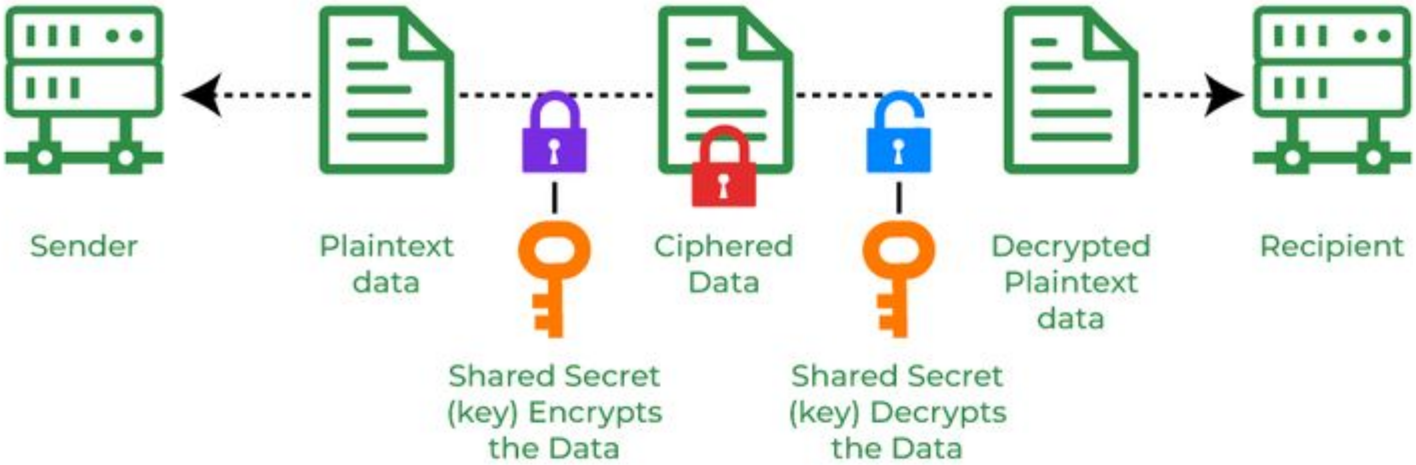
- **Symmetric Key Cryptography**
- **Hash Functions**
- **Asymmetric Key Cryptography**

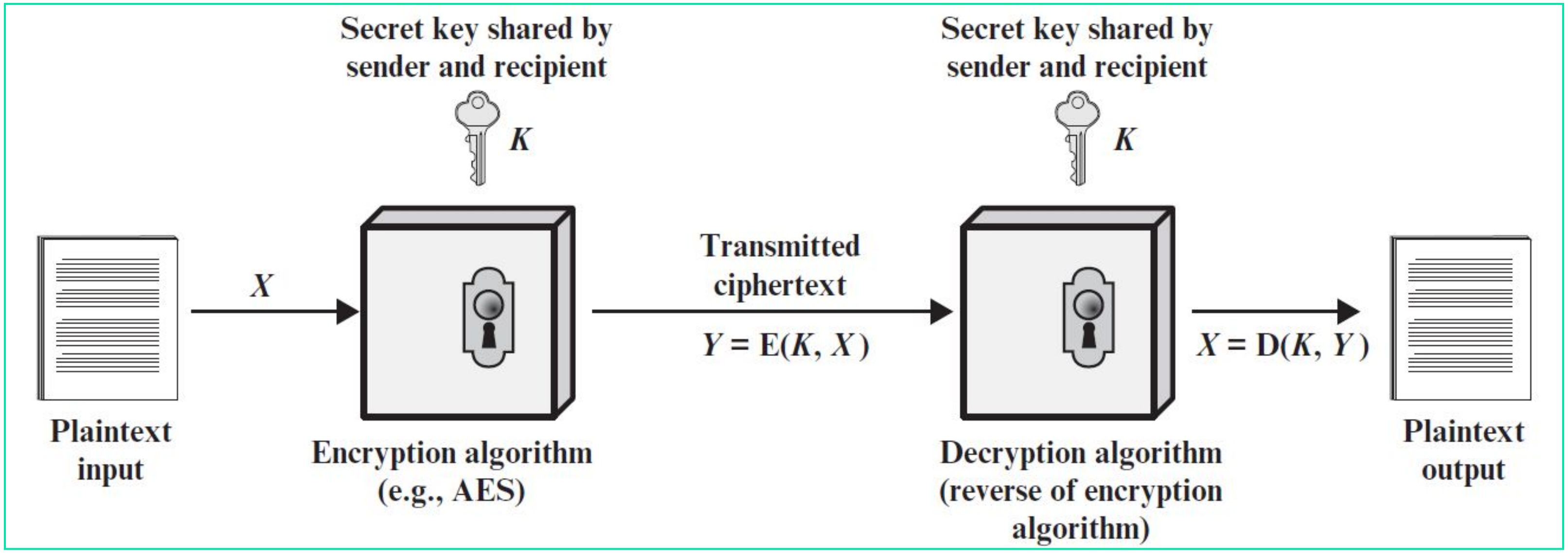
Symmetric Key Cryptography

- Symmetric encryption is a cryptographic technique where the same secret key is used for both the encryption and decryption processes.
- Symmetric Key cryptography is faster and simpler but the problem is that the sender and receiver have to somehow exchange keys securely.
- The most popular symmetric key cryptography systems are Data Encryption Systems (DES) and Advanced Encryption Systems (AES) .



Symmetric Key Cryptography Cont…

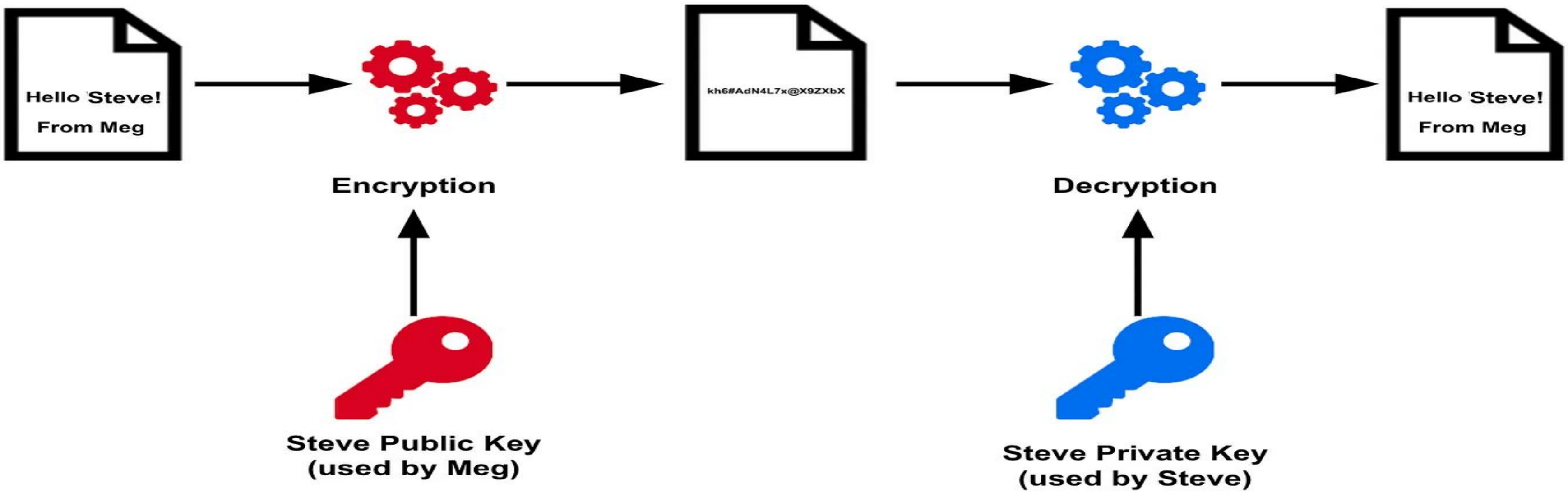

Sender
Plaintext data
Shared Secret (key) Encrypts the Data
Ciphered Data
Shared Secret (key) Decrypts the Data
Decrypted Plaintext data
Recipient

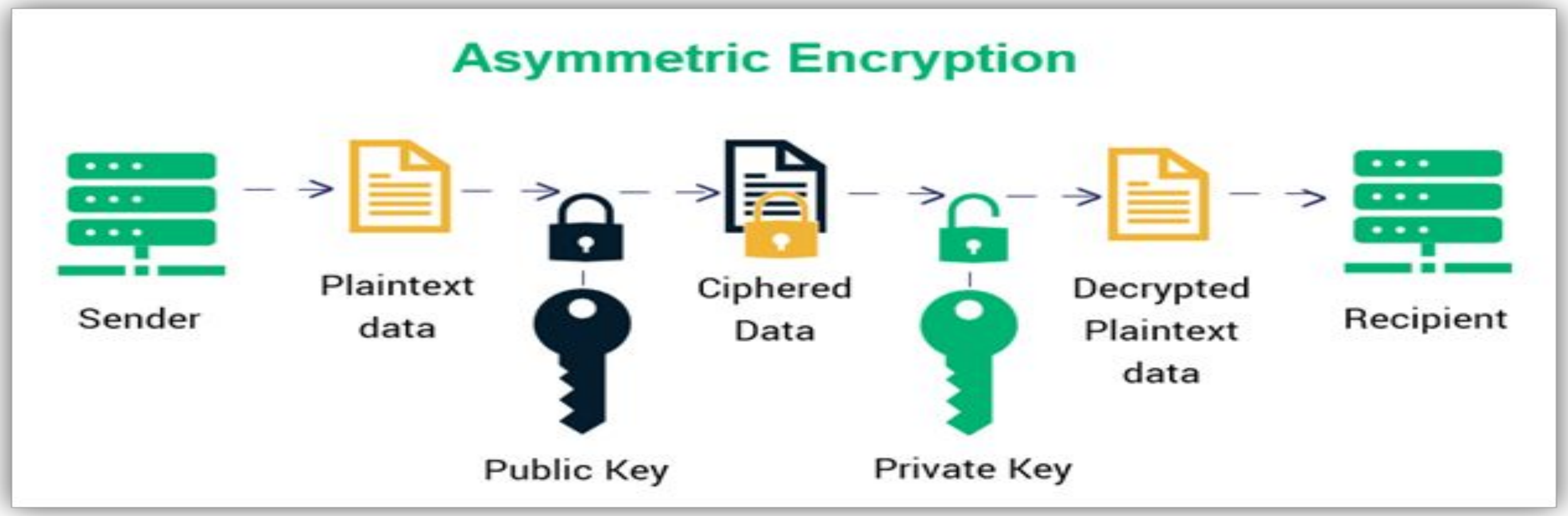

Secret key shared by sender and recipient
K
Secret key shared by sender and recipient
K
X
Transmitted ciphertext
Y = E(K, X)
X = D(K, Y)
Plaintext input
Encryption algorithm (e.g., AES)
Decryption algorithm (reverse of encryption algorithm)
Plaintext output

Asymmetric Key Cryptography

- In Asymmetric Key Cryptography, a pair of keys is used to encrypt and decrypt information.
- A sender's public key is used for encryption and a receiver's private key is used for decryption. Public keys and Private keys are different.
- Even if the public key is known by everyone the intended receiver can only decode it because he alone knows his private key.
- The most popular asymmetric key cryptography algorithm is the RSA algorithm

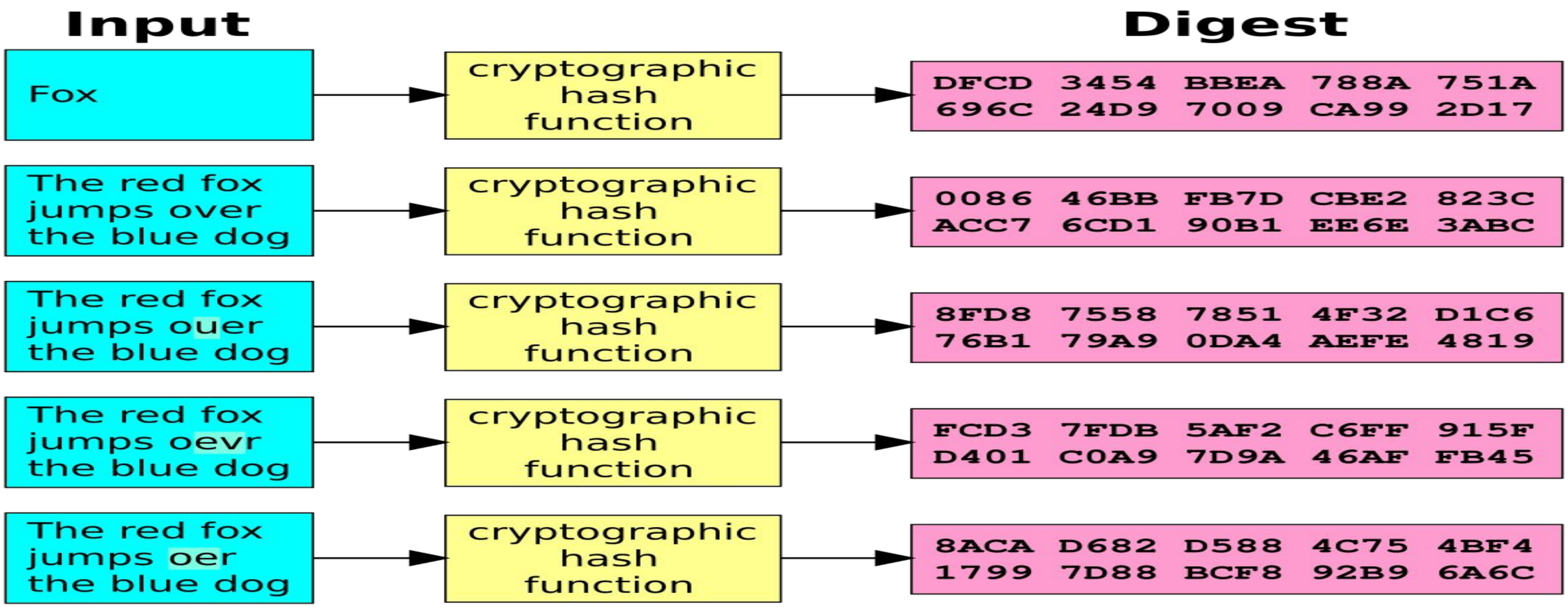
Asymmetric Key Cryptography Cont…





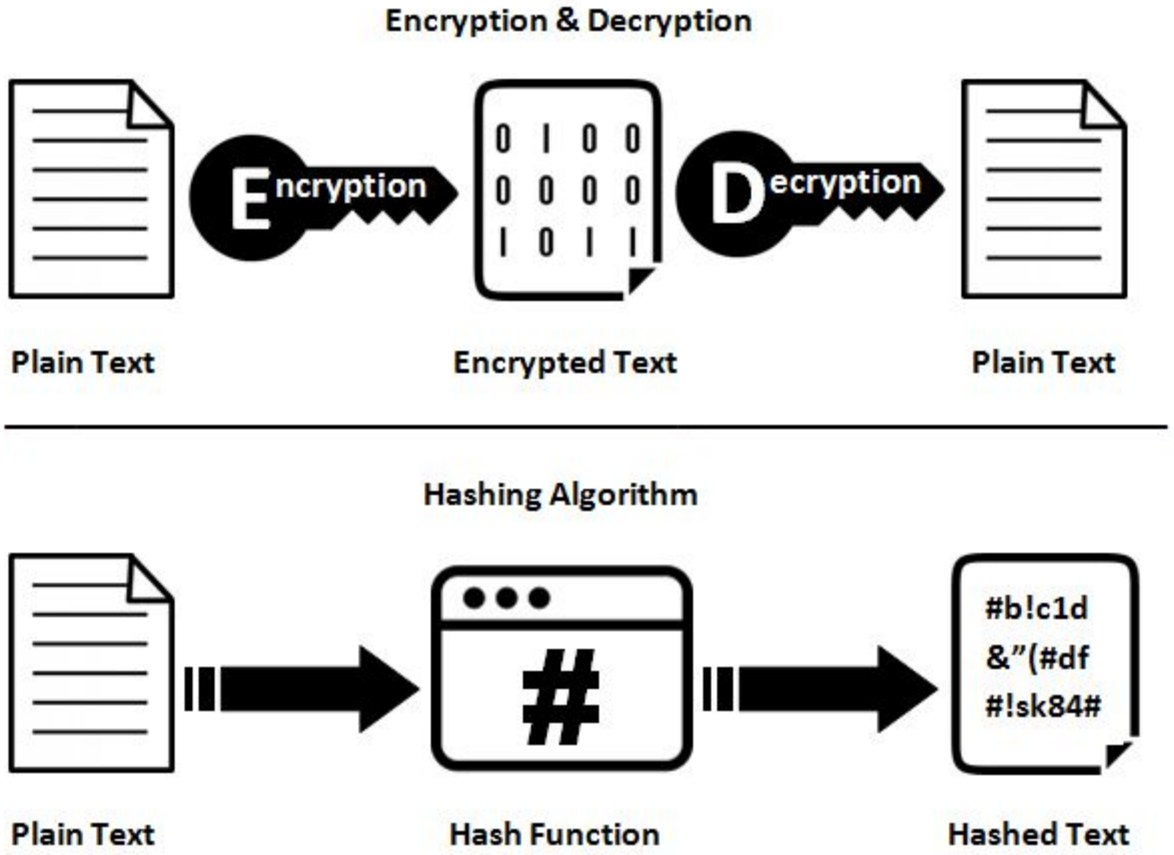
Hash Functions

- There is no usage of any key in this algorithm.
- A hash value with a fixed length is calculated as per the plain text which makes it impossible for the contents of plain text to be recovered.
- Many operating systems use hash functions to encrypt passwords.



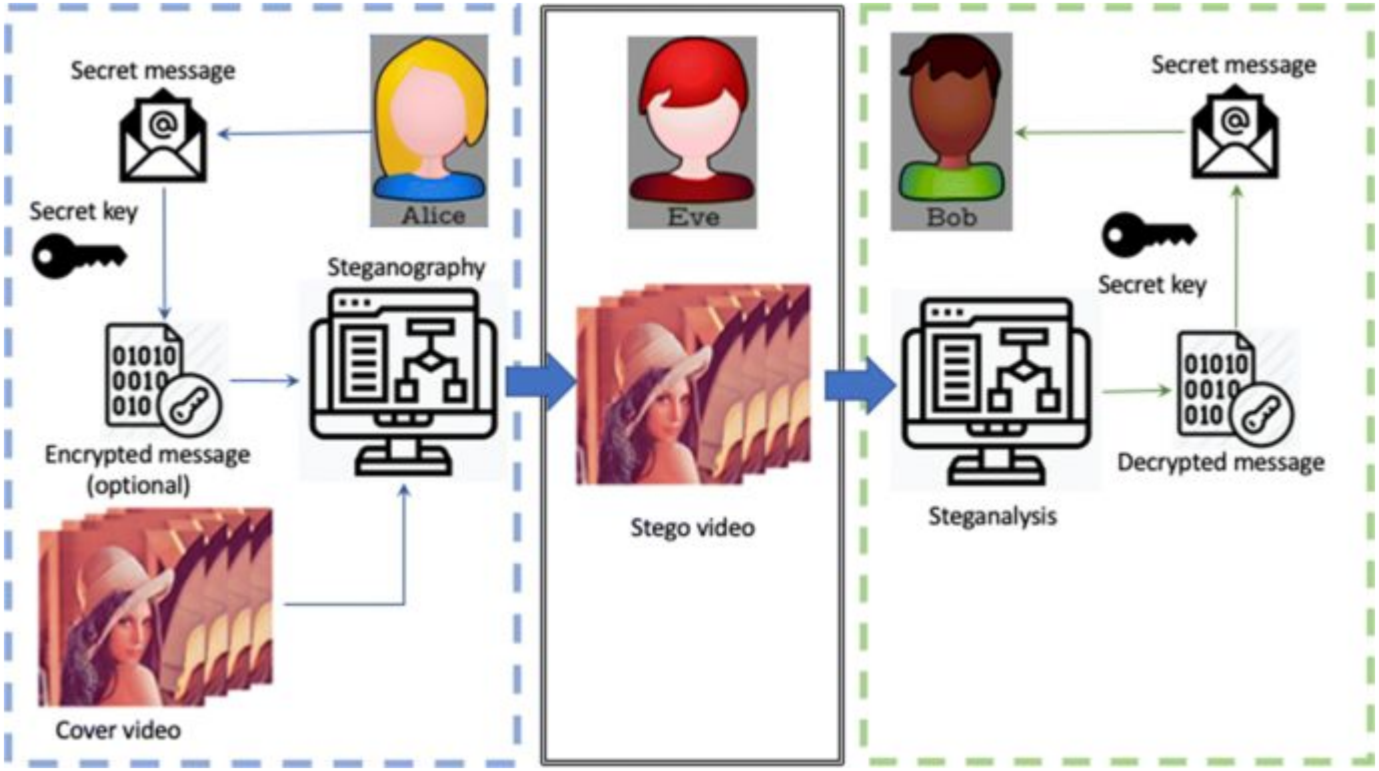
Input		Digest
Fox	cryptographic hash function	DFCD 3454 BBEA 788A 751A 696C 24D9 7009 CA99 2D17
The red fox jumps over the blue dog	cryptographic hash function	0086 46BB FB7D CBE2 823C ACC7 6CD1 90B1 EE6E 3ABC
The red fox jumps ouer the blue dog	cryptographic hash function	8FD8 7558 7851 4F32 D1C6 76B1 79A9 0DA4 AEFE 4819
The red fox jumps oevr the blue dog	cryptographic hash function	FCD3 7FDB 5AF2 C6FF 915F D401 C0A9 7D9A 46AF FB45
The red fox jumps oer the blue dog	cryptographic hash function	8ACA D682 D588 4C75 4BF4 1799 7D88 BCF8 92B9 6A6C

Hash Functions VS Cryptography



Steganography

The word steganography, with origin in Greek, means "covered writing," in contrast with cryptography, which means "secret writing."


Secret message
Alice
Secret key
01010
0010
010
Encrypted message
(optional)
Steganography
Cover video
Eve
Stego video
Bob
Secret message
Secret key
Steganalysis
01010
0010
010
Decrypted message