BVM Engineering College, VV Nagar

Gujarat Technological University

DATA COMMUNICATION

SEM 7
PRESENTATION

Digital Signature

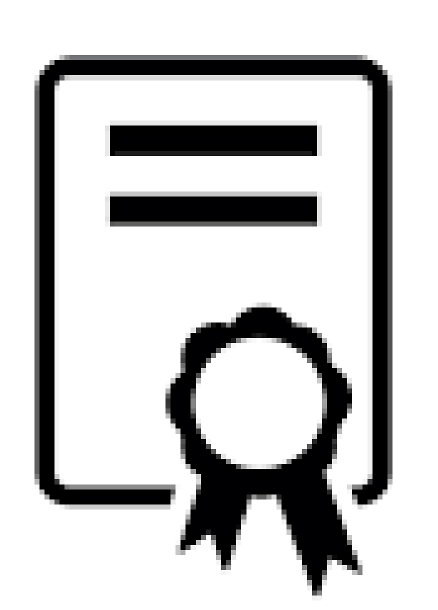
Electronics & Communication Dept.

Presented By :

- Anup Tiwari (140080111007)
- Chaitanya Tejaswi (140080111013)
- Nishant Kumar (140080111032)

Digital Signature

A **digital signature** is a mathematical scheme for demonstrating the authenticity of digital messages or documents.

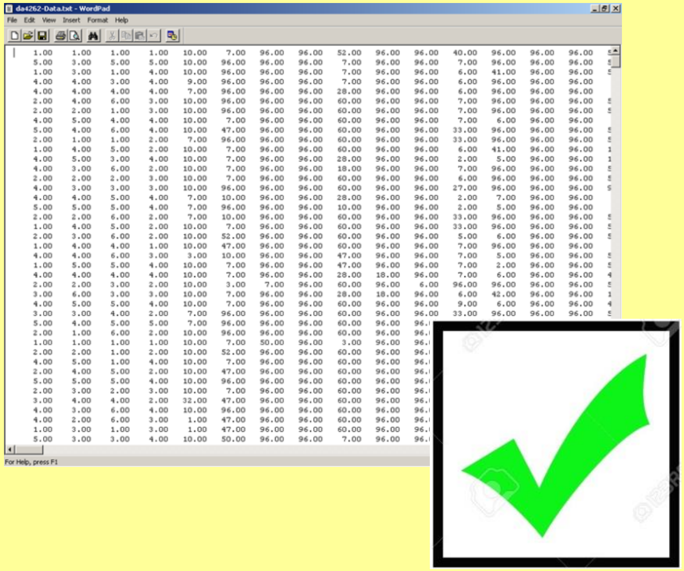


Digital Signature: Advantages

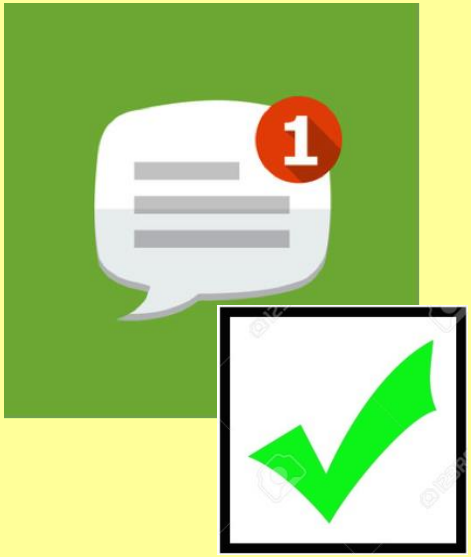
Data integrity

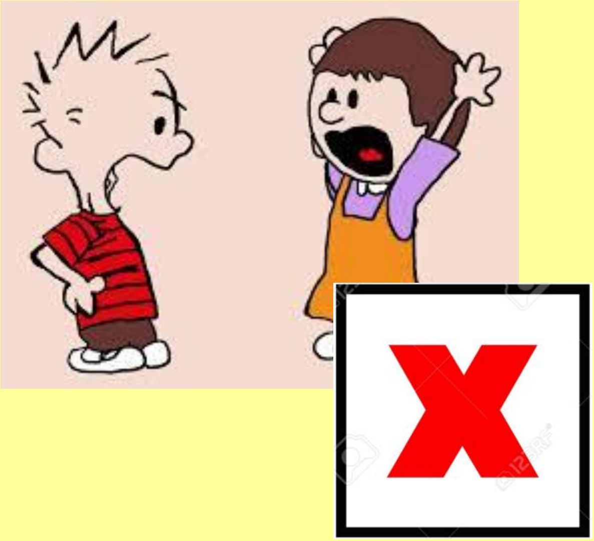
Message authentication

Non-repudiation



```
   1.00     1.00     1.00     1.00    10.00     7.00    96.00    96.00    52.00    96.00    96.00    40.00    96.00    96.00    96.00    5
   5.00     3.00     5.00     5.00    10.00    96.00    96.00    96.00     7.00    96.00    96.00     7.00    96.00    96.00    96.00    5
   1.00     3.00     1.00     4.00    10.00    96.00    96.00    96.00     7.00    96.00    96.00     6.00    41.00    96.00    96.00    5
   4.00     4.00     3.00     4.00     9.00    96.00    96.00    96.00     7.00    96.00    96.00     6.00    96.00    96.00    96.00
   4.00     4.00     4.00     4.00     7.00    96.00    96.00    96.00    28.00    96.00    96.00     6.00    96.00    96.00    96.00
   2.00     4.00     6.00     3.00    10.00    96.00    96.00    96.00    60.00    96.00    96.00     7.00    96.00    96.00    96.00    5
   2.00     2.00     1.00     3.00    10.00    96.00    96.00    96.00    60.00    96.00    96.00     7.00    96.00    96.00    96.00    5
   4.00     5.00     4.00     4.00    10.00     7.00    96.00    96.00    60.00    96.00    96.00     7.00     6.00    96.00    96.00
   5.00     4.00     6.00     4.00    10.00    47.00    96.00    96.00    60.00    96.00    96.00    33.00    96.00    96.00    96.00    5
   2.00     1.00     1.00     2.00     7.00    96.00    96.00    96.00    60.00    96.00    96.00    33.00    96.00    96.00    96.00    5
   1.00     4.00     5.00     2.00    10.00     7.00    96.00    96.00    60.00    96.00    96.00     6.00    41.00    96.00    96.00    1
   4.00     5.00     3.00     4.00    10.00     7.00    96.00    96.00    28.00    96.00    96.00     2.00     5.00    96.00    96.00    1
   4.00     3.00     6.00     2.00    10.00     7.00    96.00    96.00    18.00    96.00    96.00     7.00    96.00    96.00    96.00    5
   2.00     2.00     2.00     3.00    10.00     7.00    96.00    96.00    60.00    96.00    96.00     6.00    96.00    96.00    96.00    5
   4.00     3.00     3.00     3.00    10.00    96.00    96.00    96.00    60.00    96.00    96.00    27.00    96.00    96.00    96.00    5
   4.00     4.00     5.00     4.00     7.00    10.00    96.00    96.00    28.00    96.00    96.00     2.00     7.00    96.00    96.00
   5.00     5.00     5.00     4.00     7.00    96.00    96.00    96.00    10.00    96.00    96.00     2.00     5.00    96.00    96.00
   2.00     2.00     6.00     2.00     7.00    10.00    96.00    96.00    60.00    96.00    96.00    33.00    96.00    96.00    96.00    5
   1.00     4.00     5.00     2.00    10.00     7.00    96.00    96.00    60.00    96.00    96.00    33.00    96.00    96.00    96.00    5
   2.00     3.00     6.00     2.00    10.00    52.00    96.00    96.00    60.00    96.00    96.00     5.00     6.00    96.00    96.00    5
   1.00     4.00     4.00     1.00    10.00    47.00    96.00    96.00    60.00    96.00    96.00     7.00    96.00    96.00    96.00
   4.00     4.00     6.00     3.00     3.00    10.00    96.00    96.00    47.00    96.00    96.00     7.00     5.00    96.00    96.00    5
   1.00     5.00     5.00     4.00    10.00     7.00    96.00    96.00    47.00    96.00    96.00     7.00     2.00    96.00    96.00    5
   4.00     4.00     4.00     4.00    10.00     7.00    96.00    96.00    28.00    18.00    96.00     7.00     6.00    96.00    96.00    4
   2.00     2.00     3.00     2.00    10.00     3.00     7.00    96.00    60.00    96.00     6.00    96.00    96.00    96.00    96.00    5
   3.00     6.00     3.00     3.00    10.00     7.00    96.00    96.00    28.00    18.00    96.00     6.00    42.00    96.00    96.00    1
   4.00     5.00     5.00     4.00    10.00     7.00    96.00    96.00    60.00    96.00    96.00     9.00     6.00    96.00    96.00    4
   3.00     3.00     4.00     2.00     7.00    96.00    96.00    96.00    60.00    96.00    96.00    33.00    96.00    96.00    96.00    5
   5.00     4.00     5.00     5.00     7.00    96.00    96.00    96.00    60.00    96.00    96.
   2.00     1.00     6.00     2.00    10.00    96.00    96.00    96.00    60.00    96.00    96.
   1.00     1.00     1.00     1.00    10.00     7.00    50.00    96.00     3.00    96.00    96.
   2.00     2.00     1.00     2.00    10.00    52.00    96.00    96.00    60.00    96.00    96.
   4.00     5.00     1.00     4.00    10.00     7.00    96.00    96.00    60.00    96.00    96.
   2.00     4.00     5.00     2.00    10.00    47.00    96.00    96.00    60.00    96.00    96.
   5.00     5.00     5.00     4.00    10.00    96.00    96.00    96.00    60.00    96.00    96.
   2.00     3.00     2.00     3.00    10.00     7.00    96.00    96.00    60.00    96.00    96.
   3.00     4.00     4.00     2.00    32.00    47.00    96.00    96.00    60.00    96.00    96.
   4.00     3.00     6.00     4.00    10.00    96.00    96.00    96.00    60.00    96.00    96.
   4.00     2.00     6.00     3.00     1.00    47.00    96.00    96.00    60.00    96.00    96.
   1.00     3.00     1.00     3.00     1.00    47.00    96.00    96.00    60.00    96.00    96.
   5.00     3.00     3.00     4.00    10.00    50.00    96.00    96.00     7.00    96.00    96.
```





Digital Signature: Concepts

- Public & Private Keys
  - Example
- Hashing
  - Example
- Hashing v/s Encryption
- Public Key Encryption
- Digital Signature Scheme

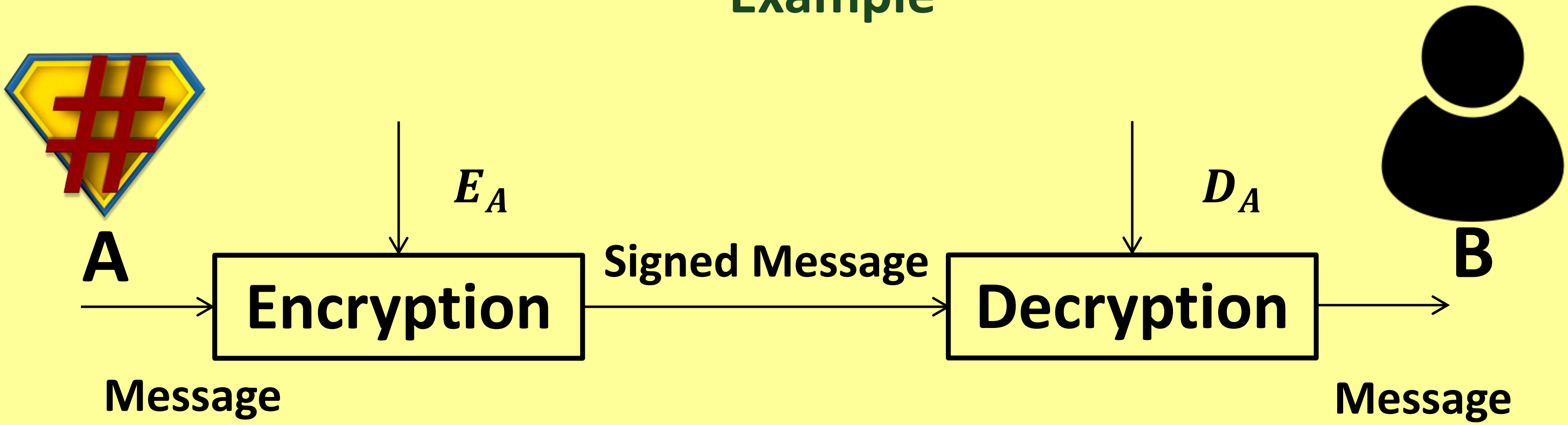
Public & Private Keys

Private Key is used to sign encrypted data. **Public Key** is used to retrieve data from encrypted form.

$\boldsymbol{E_{user}}$ **(Private Key)**

$\boldsymbol{D_{user}}$ **(Public Key)**

Example



A

Message

E_A

Encryption

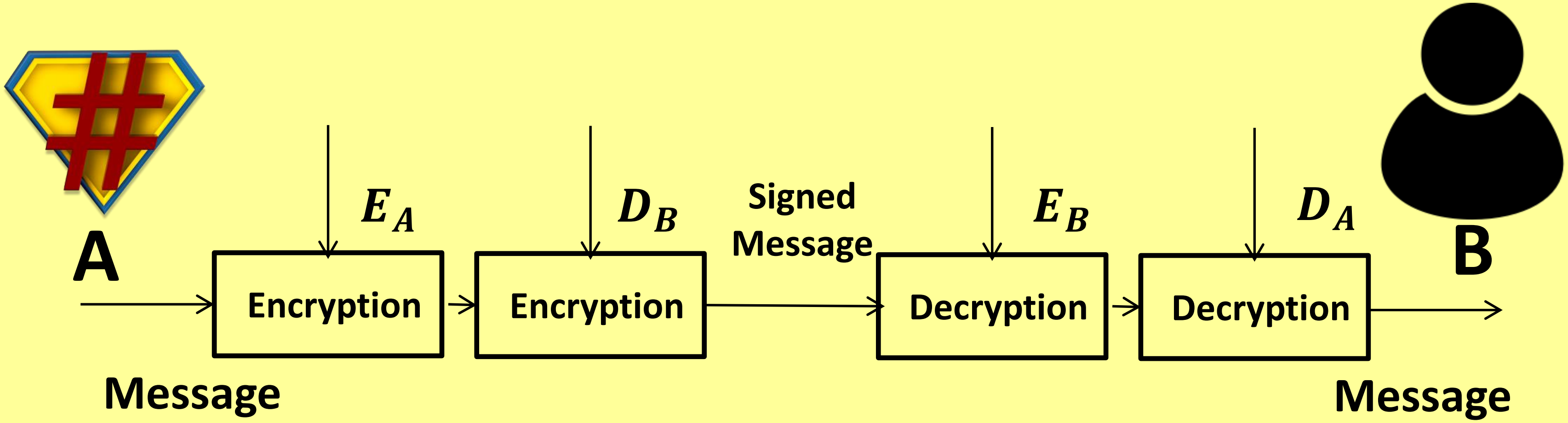
Signed Message

D_A

Decryption

B

Message



A

Message

E_A

Encryption

D_B

Encryption

Signed Message

E_B

Decryption

D_A

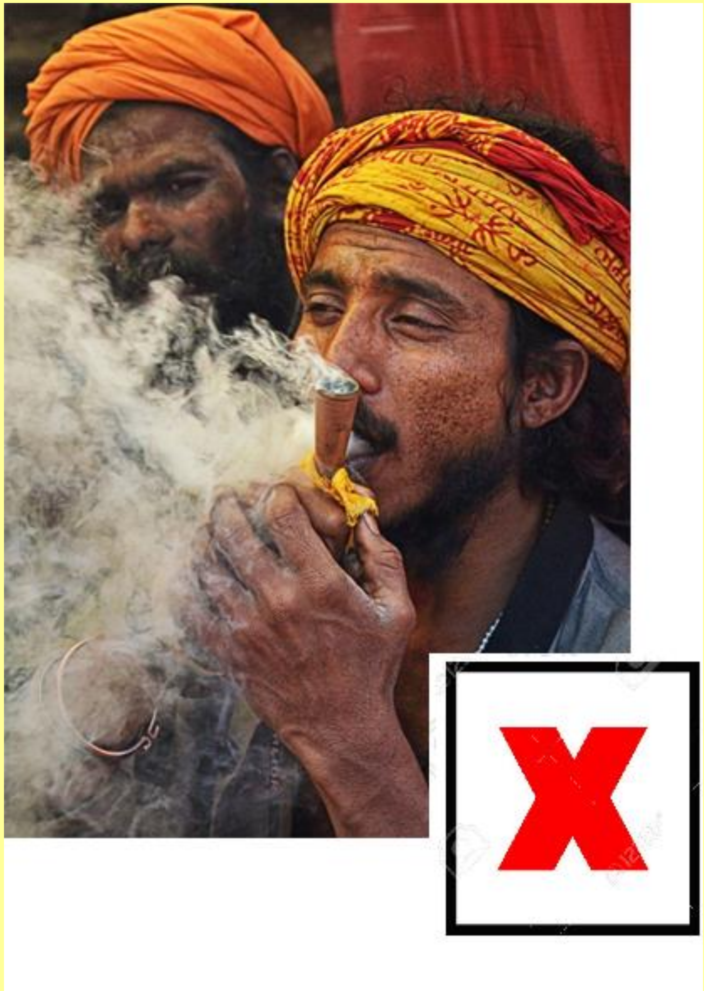
Decryption

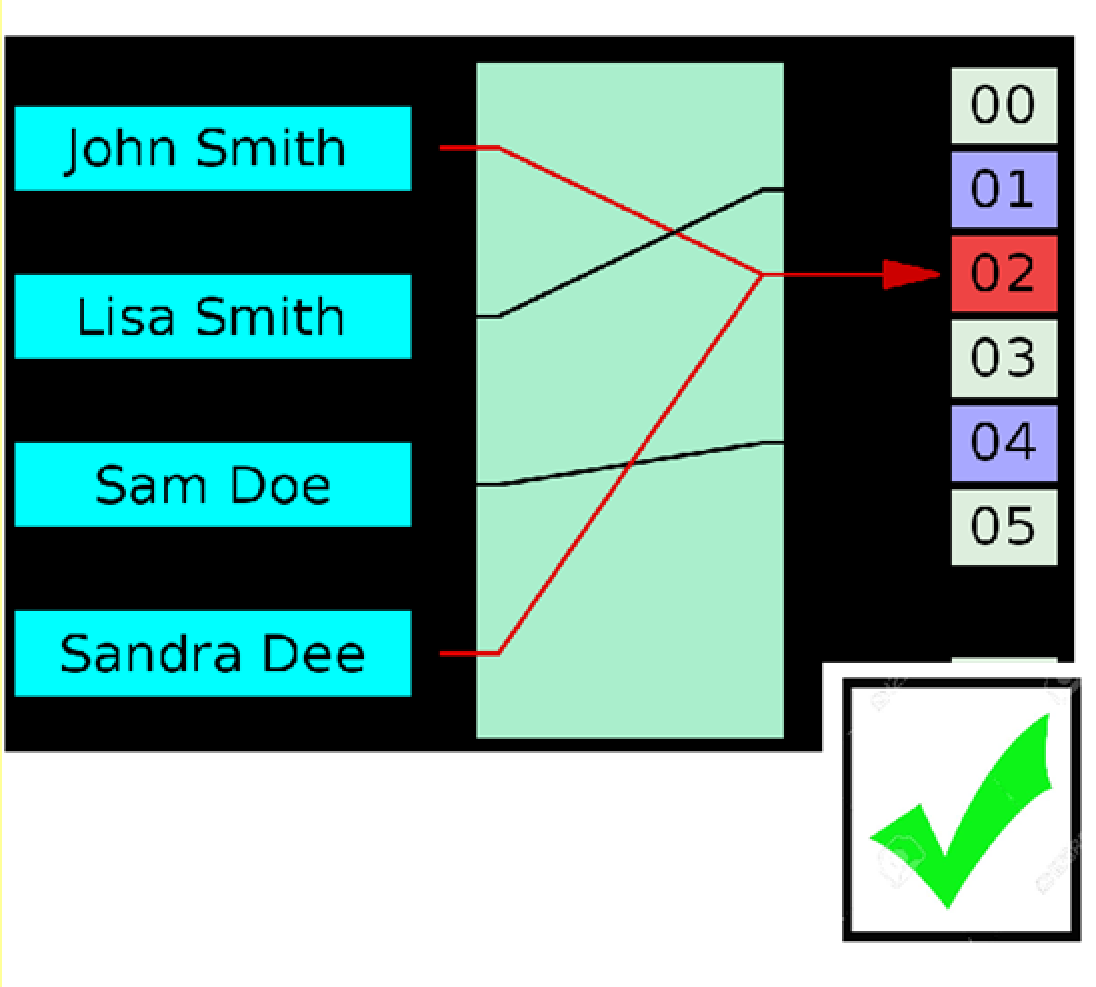
B

Message

More details will be given in **Public Key Encryption**.

Hashing

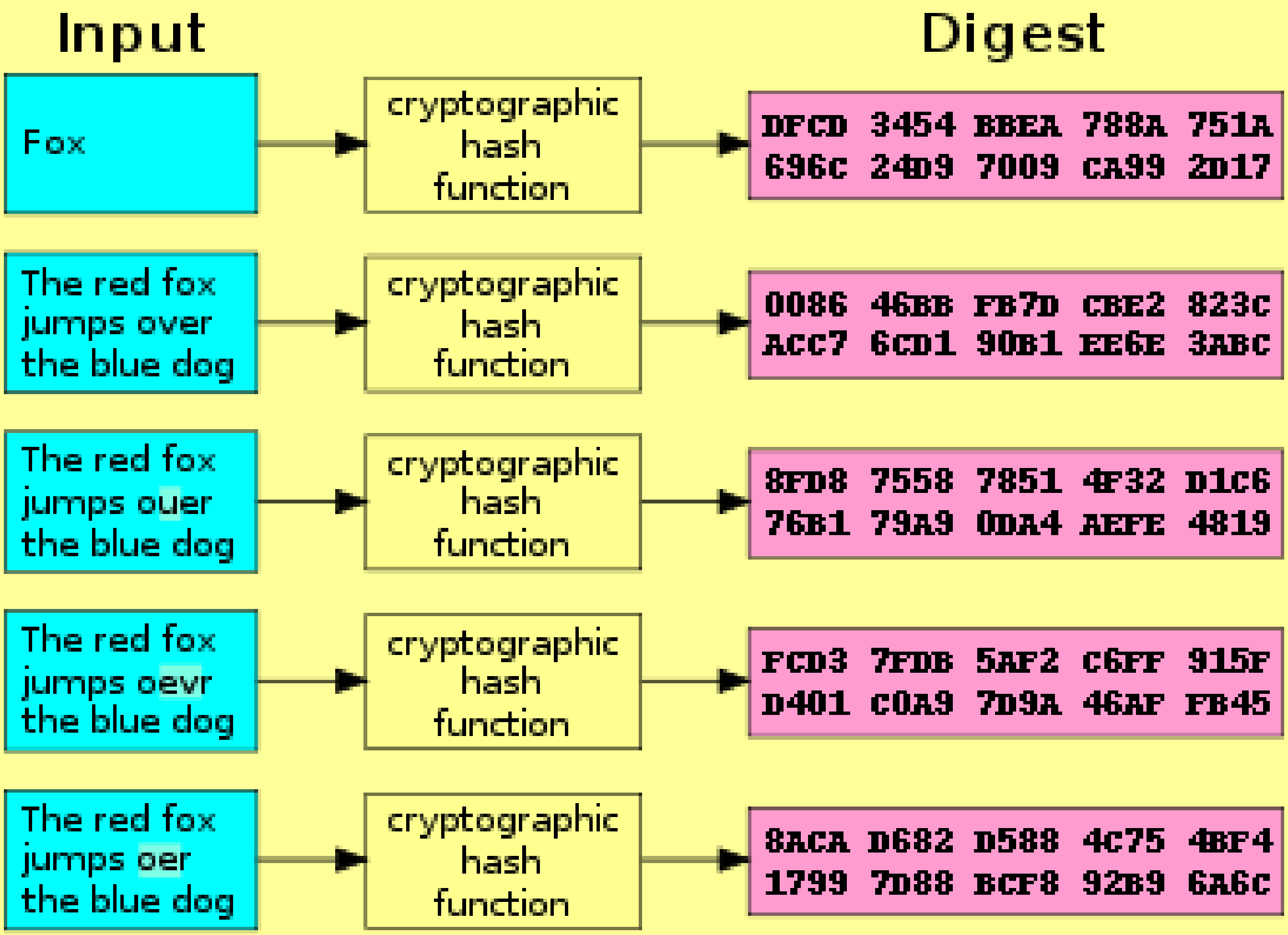




Hashing

A **Hash Function** is a cryptographic algorithm that transforms the given input (message) into a fixed length string, named **Hash Value**.

Example



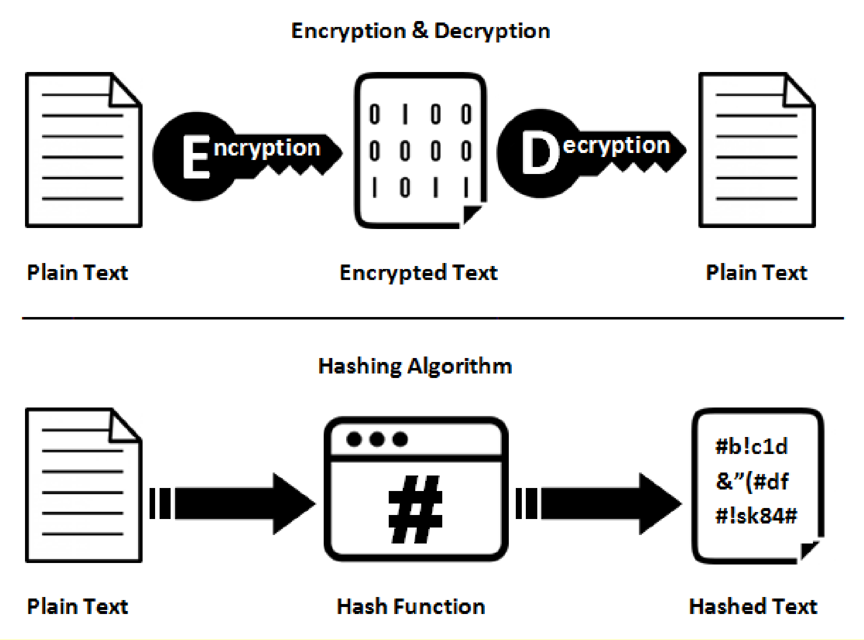
Input		Digest
Fox	cryptographic hash function	DFCD 3454 BBEA 788A 751A 696C 24D9 7009 CA99 2D17
The red fox jumps over the blue dog	cryptographic hash function	0086 46BB FB7D CBE2 823C ACC7 6CD1 90B1 EE6E 3ABC
The red fox jumps ouer the blue dog	cryptographic hash function	8FD8 7558 7851 4F32 D1C6 76B1 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

Hashing v/s Encryption

- Hashing is used to validate the integrity of the content by detecting all modifications and thereafter changes to a hash output.
- Encryption encodes data for the primary purpose of maintaining data confidentiality and security. It requires a private key to reversible function encrypted text to plain text.

In short, encryption is a two-way function that includes encryption & decryption whilst hashing is a one-way function that changes a plain text to a unique digest that is irreversible.

Also, encryption is reversible, hashing is not.



Hashing and encryption are different but also have some similarities.

They are both ideal in handling data, messages and information in computing systems. They both transform or change data into a different format.

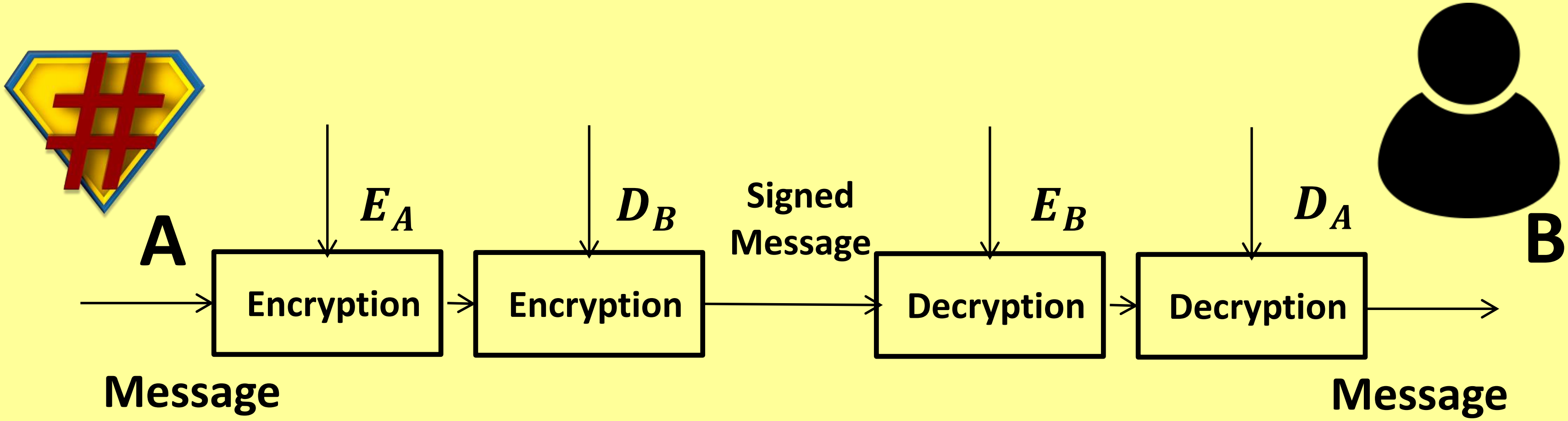
Public Key Encryption

Symmetric encryption (private-key encryption or secret-key encryption) utilizes the same key for encryption and decryption.

Asymmetric encryption utilizes a pair of keys like public and private key for better security where a message sender encrypts the message with the public key and the receiver decrypts it with his/her private key.

Asymmetric encryption, also known as **Public Key Encryption**, forms the basis for generating a **Digital Signature**.

This was **Asymmetric encryption**!



The algorithm produces a **Private-Public** key pair.

Digital Signature Scheme

A digital signature scheme typically consists of 3 algorithms:

A ***key generation*** algorithm that selects a *private key* uniformly at random from a set of possible private keys. The algorithm outputs the *private key* and a corresponding *public key*.

A ***signing*** **algorithm** that, given a message and a private key, produces a signature.

A ***signature verifying*** **algorithm** that, given the message, public key and signature, either accepts or rejects the message's claim to authenticity.

Algorithms

Rivest–Shamir–Adleman (RSA)

based on Public Key Cryptography.

Digital Signature Algorithm (DSA)

based on Hashing Function.

Elliptic Curve DSA (EC-DSA)