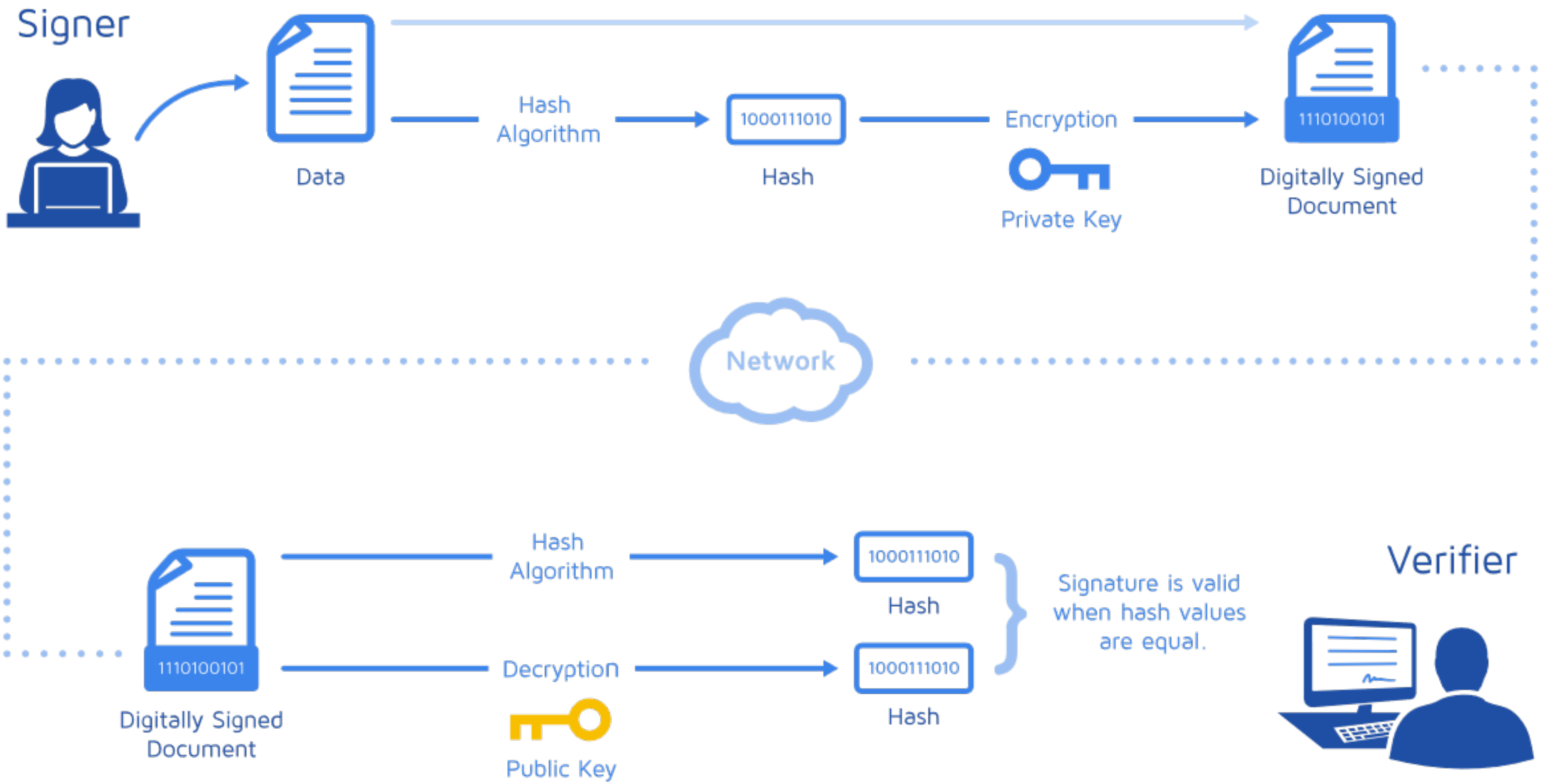
Crypto intro

Badis HAMMI

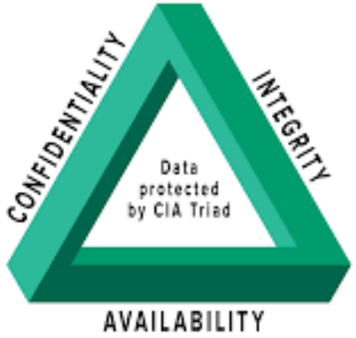
Authentication: Digital (cryptographic) signature



Introduction to cryptography and security services

- Confidentiality
- Integrity
- Availability
- Authentication

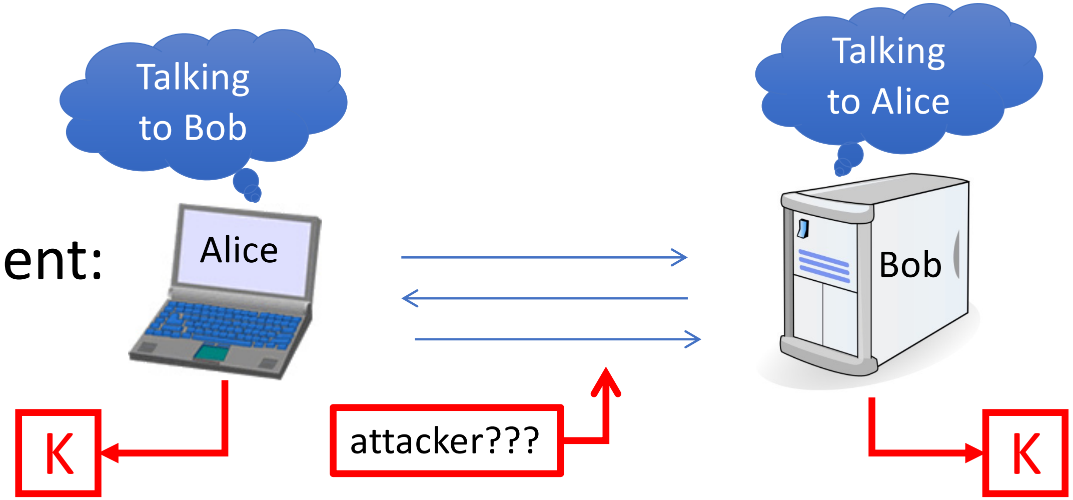
- Identification
- Non Repudiation
- Authorization
- Anonymity



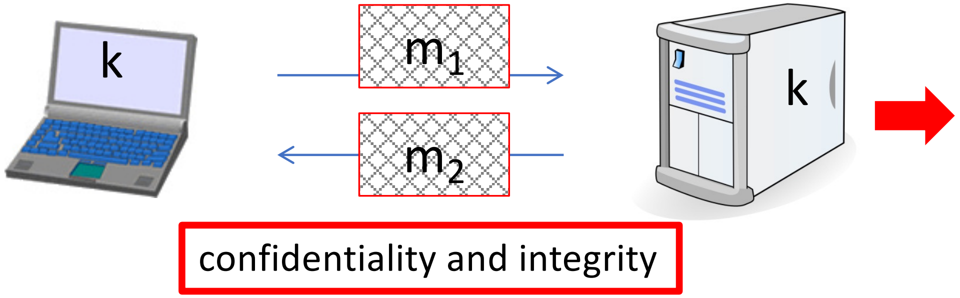
What is cryptography

Crypto core

1 - Secret key establishment:



2 - Secure communication:



First part pf the chapter

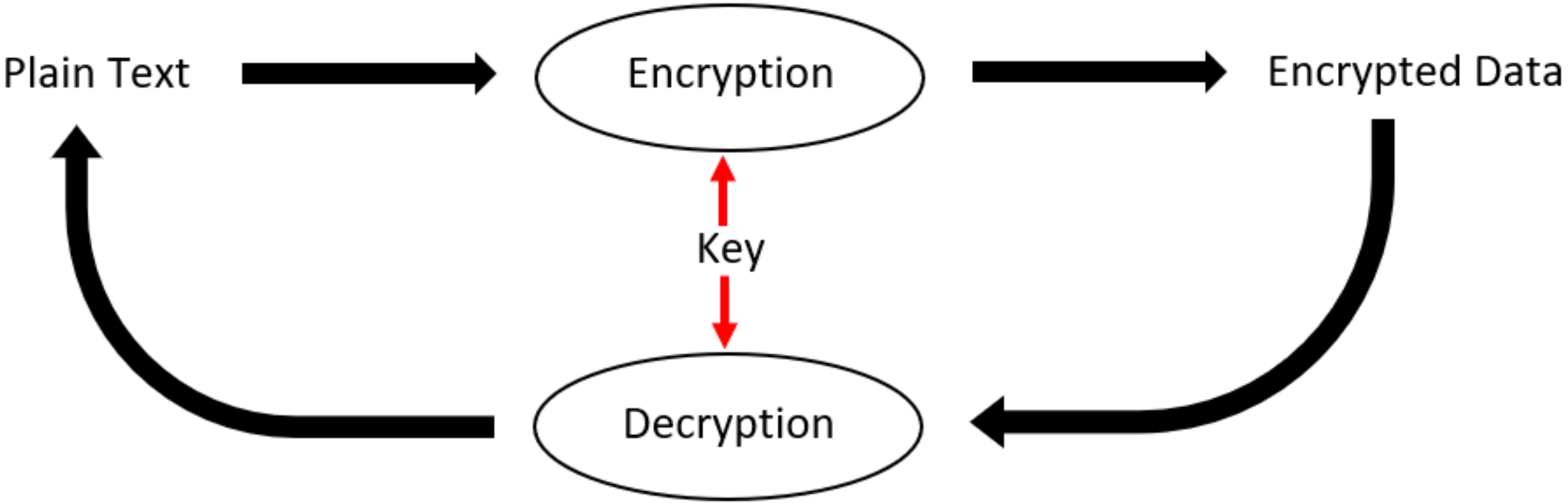
Confidentiality

"Ensuring that information is only accessible to those whose access is authorized"

International Organization for Standardization (ISO)

- Reserved nature of an information whose access is limited to those who are authorized to know it
- ***ISO 7498-2***:
  - the property that information is neither available nor disclosed to unauthorized persons, entities or processes.
- Information exchanged between two or more entities is only accessible by them.

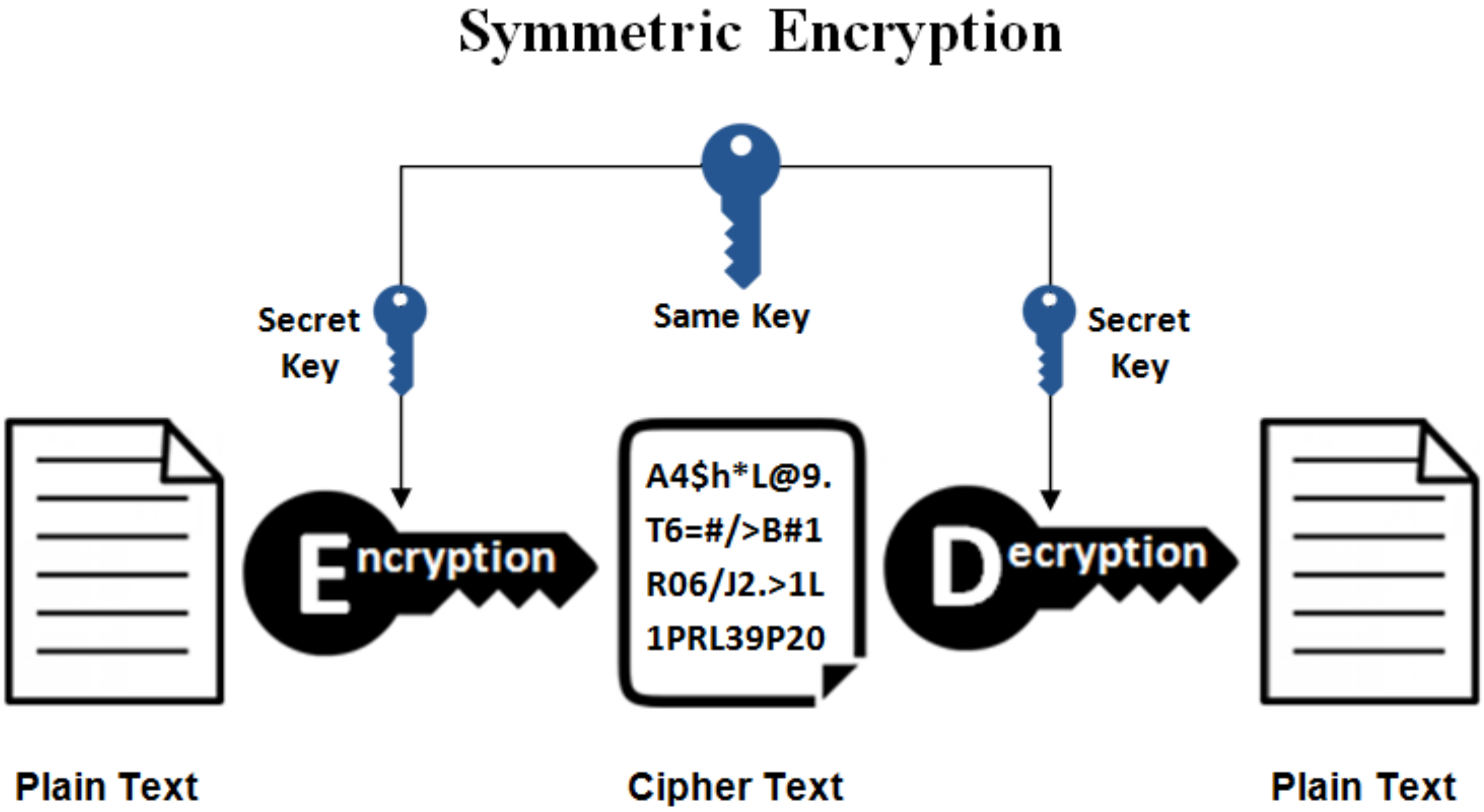
Ciphers



1. Symmetric ciphers (Symmetric Cryptography)

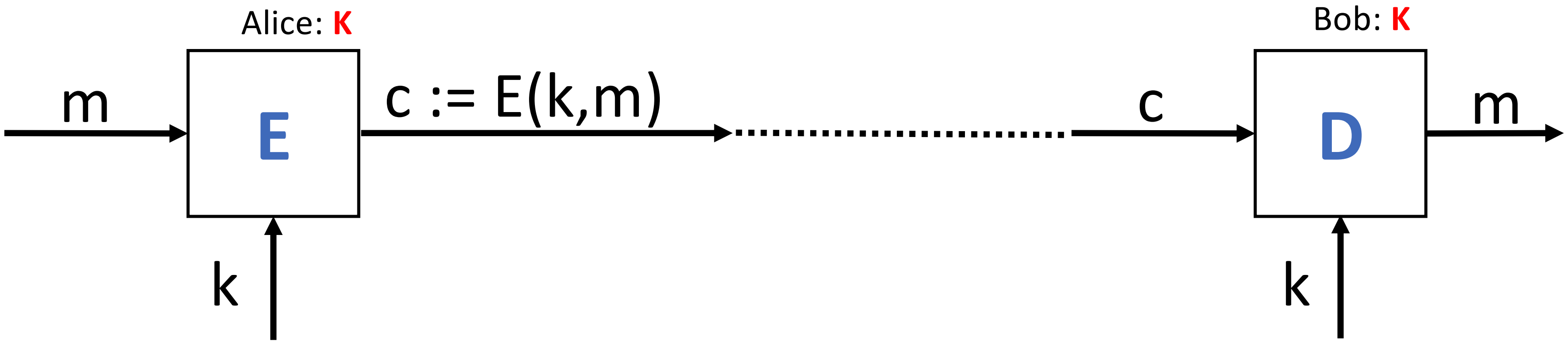
2. Asymmetric ciphers (Asymmetric Cryptography)

Symmetric ciphers



Symmetric ciphers

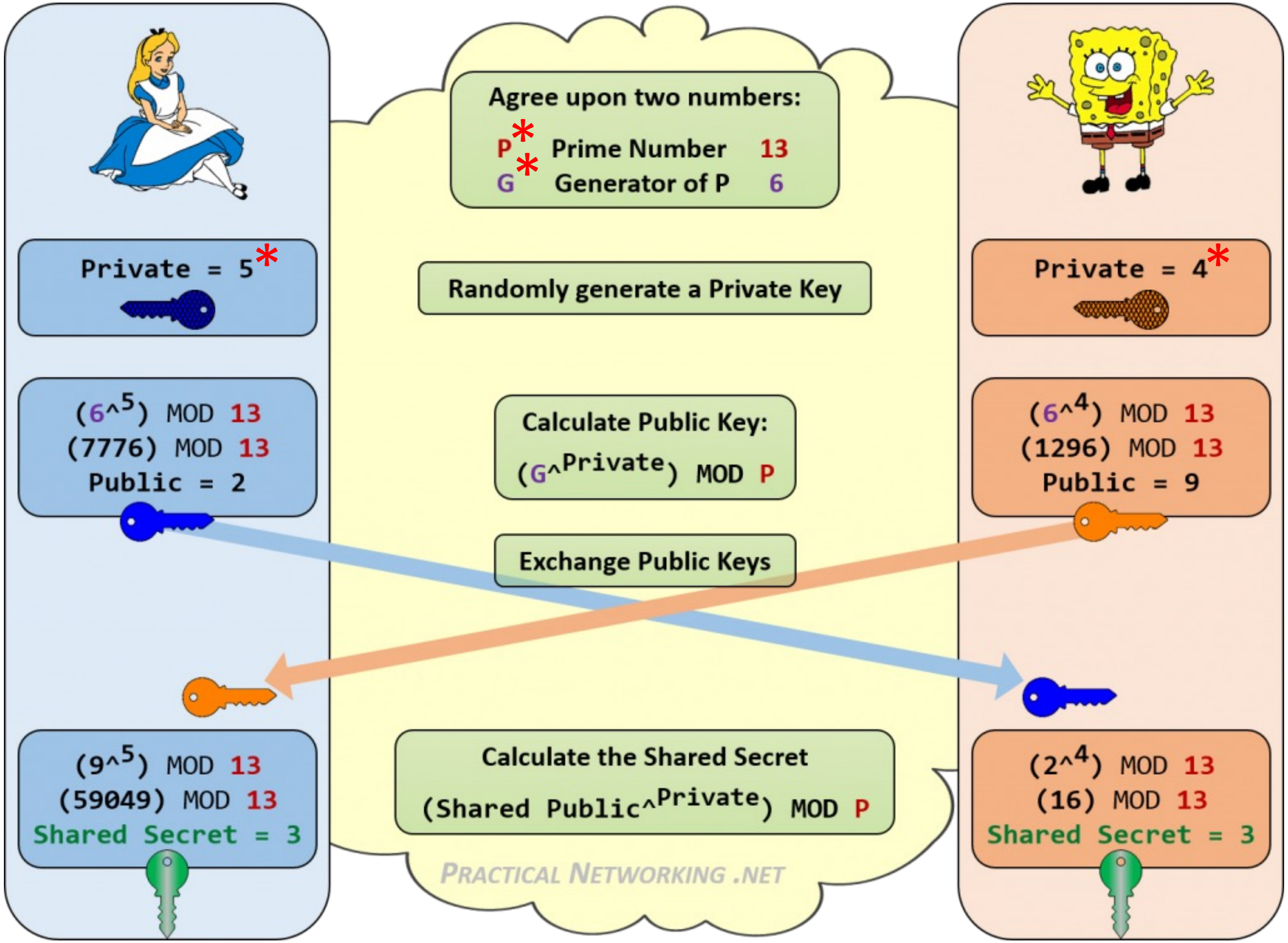
Symmetric Cipher



$D(k,E(k,m)) = m$

Symmetric ciphers: Keys exchange: Diffie-Hellman

*Very Big



Agree upon two numbers:

P*	Prime Number	13
G*	Generator of P	6

Randomly generate a Private Key

Private = 5*

Private = 4*

Calculate Public Key:

$(G^{\wedge \text{Private}})$ MOD P

$(6^{\wedge 5})$ MOD 13
(7776) MOD 13
Public = 2

$(6^{\wedge 4})$ MOD 13
(1296) MOD 13
Public = 9

Exchange Public Keys

Calculate the Shared Secret

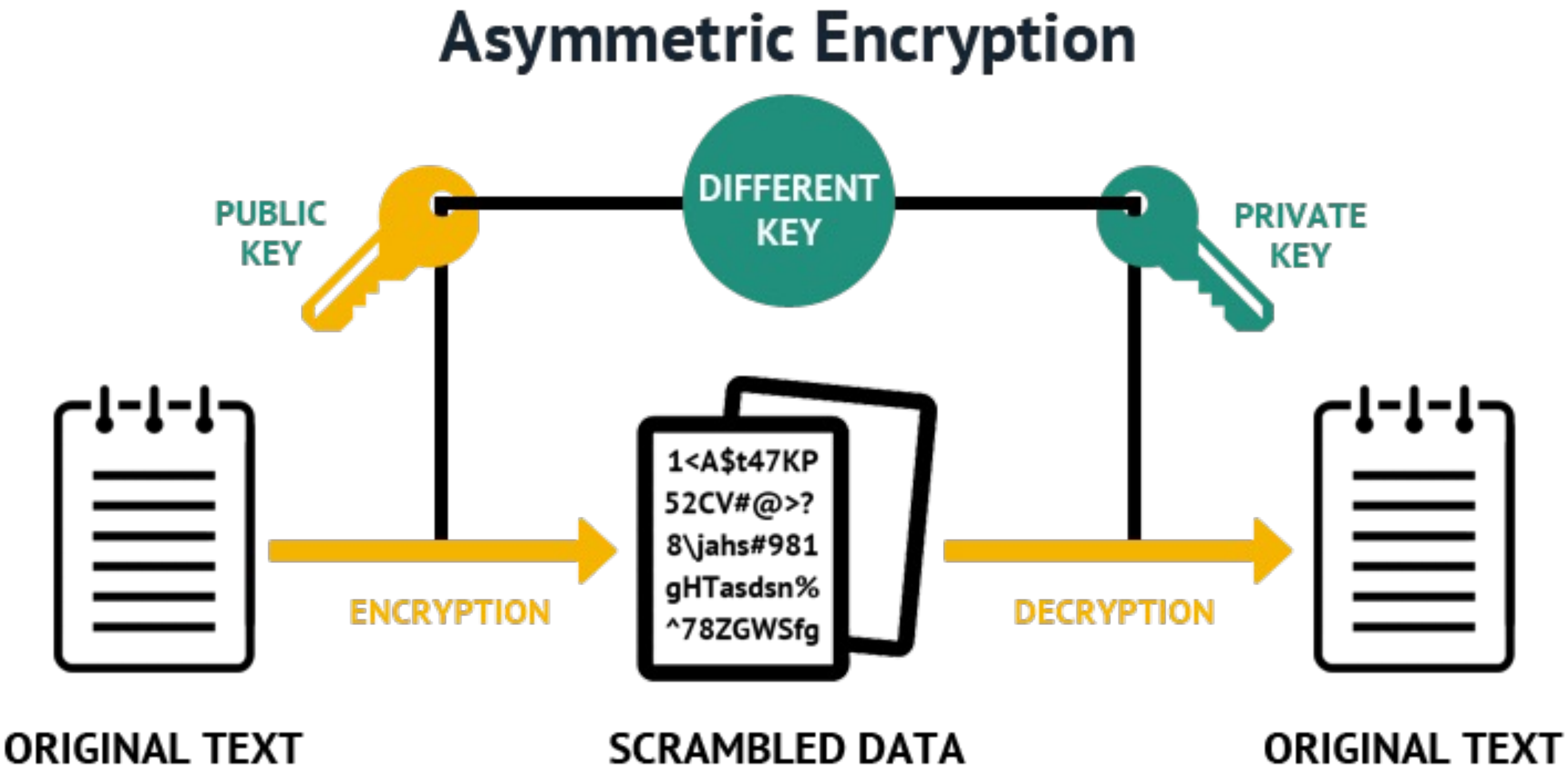
$(\text{Shared Public}^{\wedge \text{Private}})$ MOD P

$(9^{\wedge 5})$ MOD 13
(59049) MOD 13
Shared Secret = 3

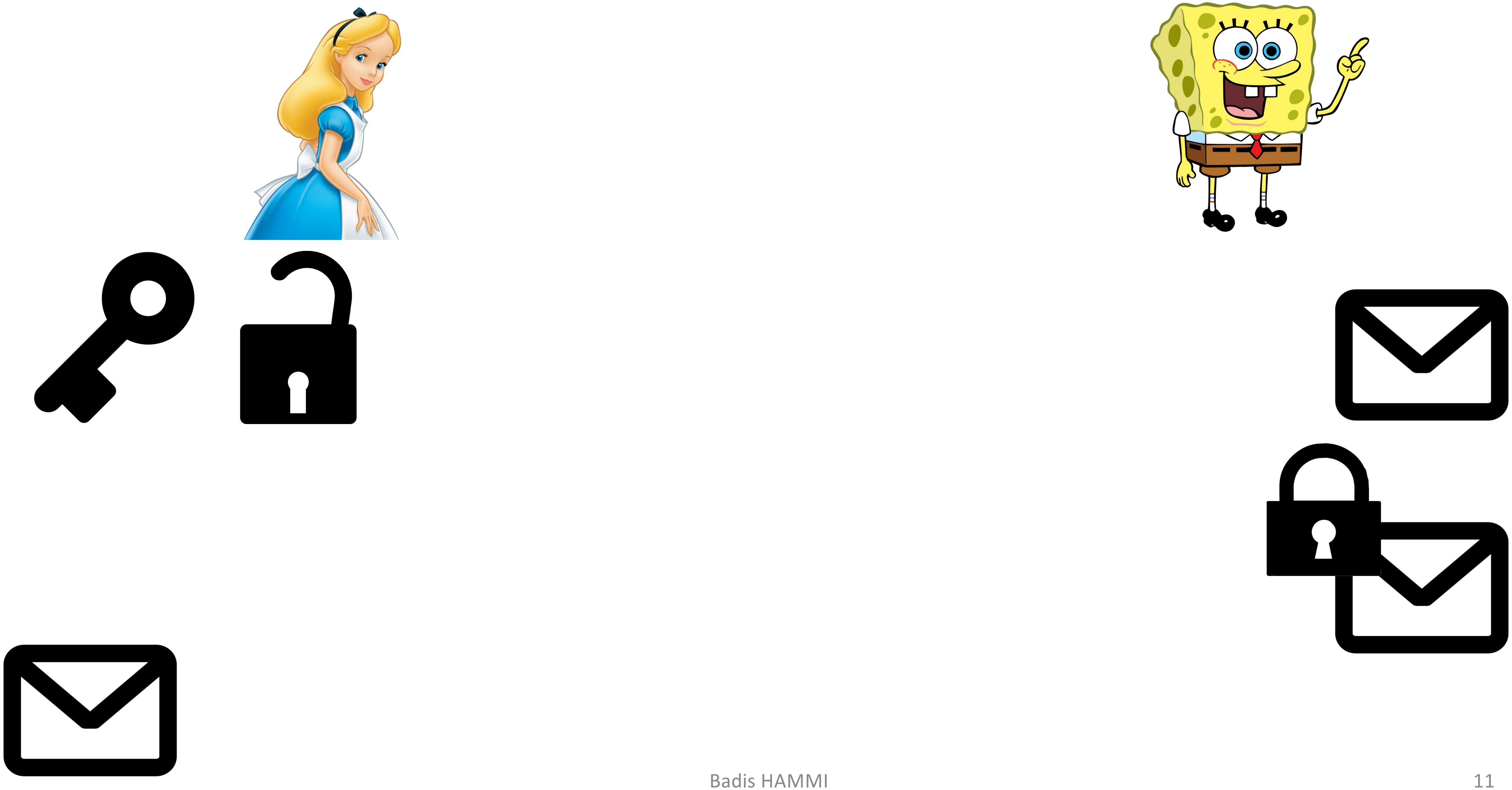
$(2^{\wedge 4})$ MOD 13
(16) MOD 13
Shared Secret = 3

Asymmetric ciphers

Two keys: One for encryption, the other one for decryption



Asymmetric ciphers



Data Integrity

The fact that ensures that the data always remains intact, that is to say, that it has not been modified by an unauthorized third party. This principle should be respected throughout the data lifecycle. Guaranteeing the integrity of data means ensuring that the data has remained reliable since its creation.

- Property guaranteeing that information has not been modified without authorization
- ISO 7498-2 :
  - property ensuring that data has not been altered or destroyed in an unauthorized manner
- Information exchanged between two or more entities is received by all as it was issued
  - In an exchange (communication) context, authentication of origin accompanies the integrity service.

Data Integrity: Hash functions

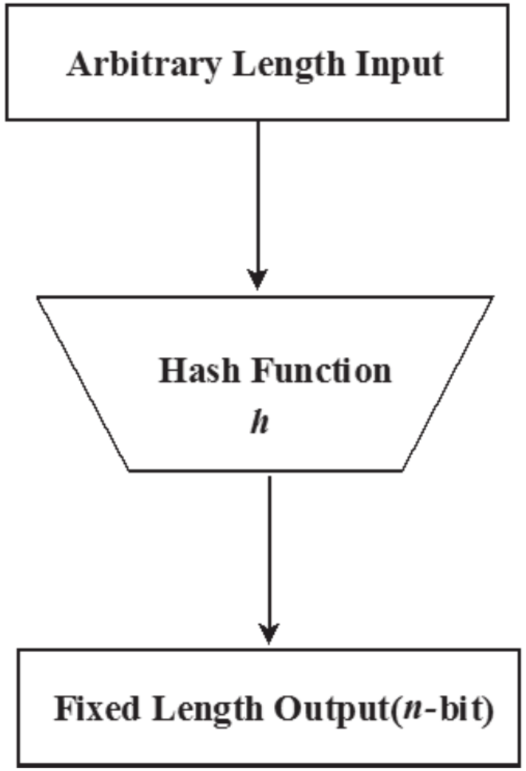
Hash function

- Takes any string as input
- Fixed size output (e.g. 256 bits)
- Efficiently computable

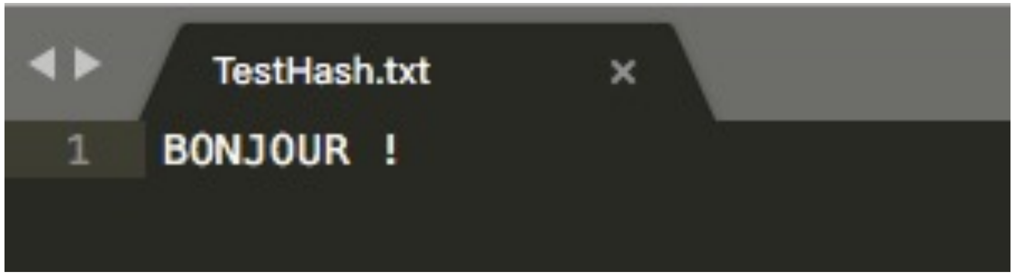
H: $\{0,1\}^n$ → $\{0,1\}^s$ with n >> s

Security properties

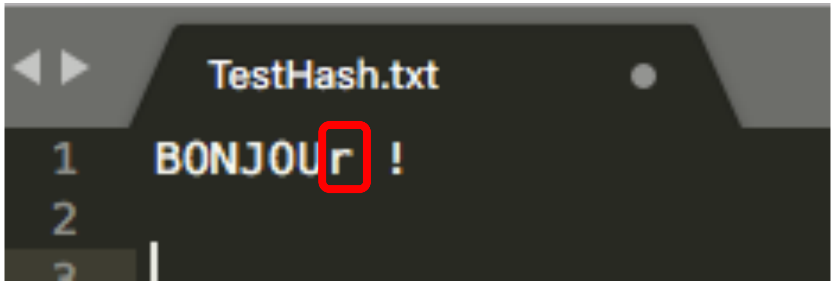
- Collision-free
- Hiding
- Puzzle friendly



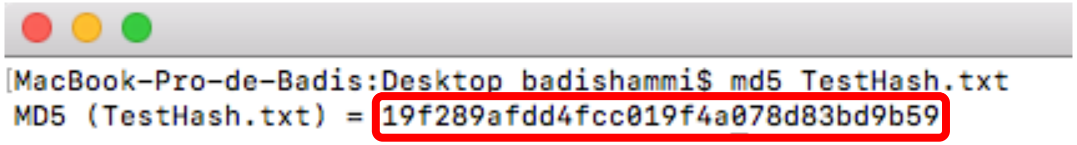
Data Integrity: Hash functions



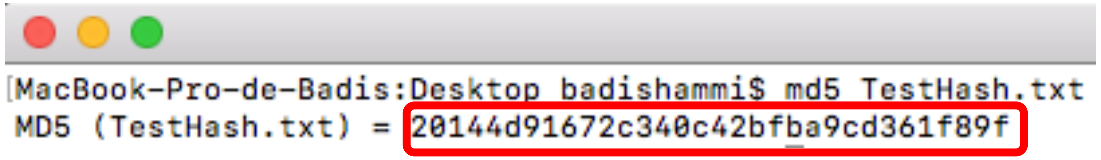
```
BONJOUR !
```



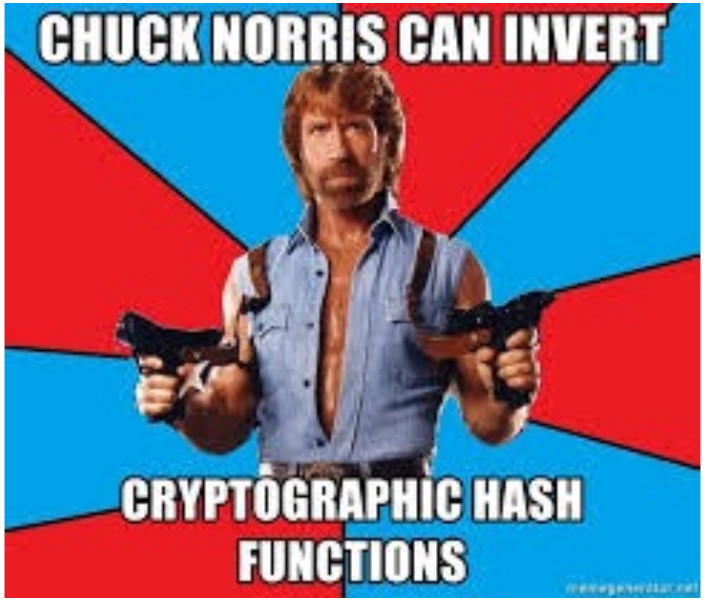
```
BONJOUr !

```



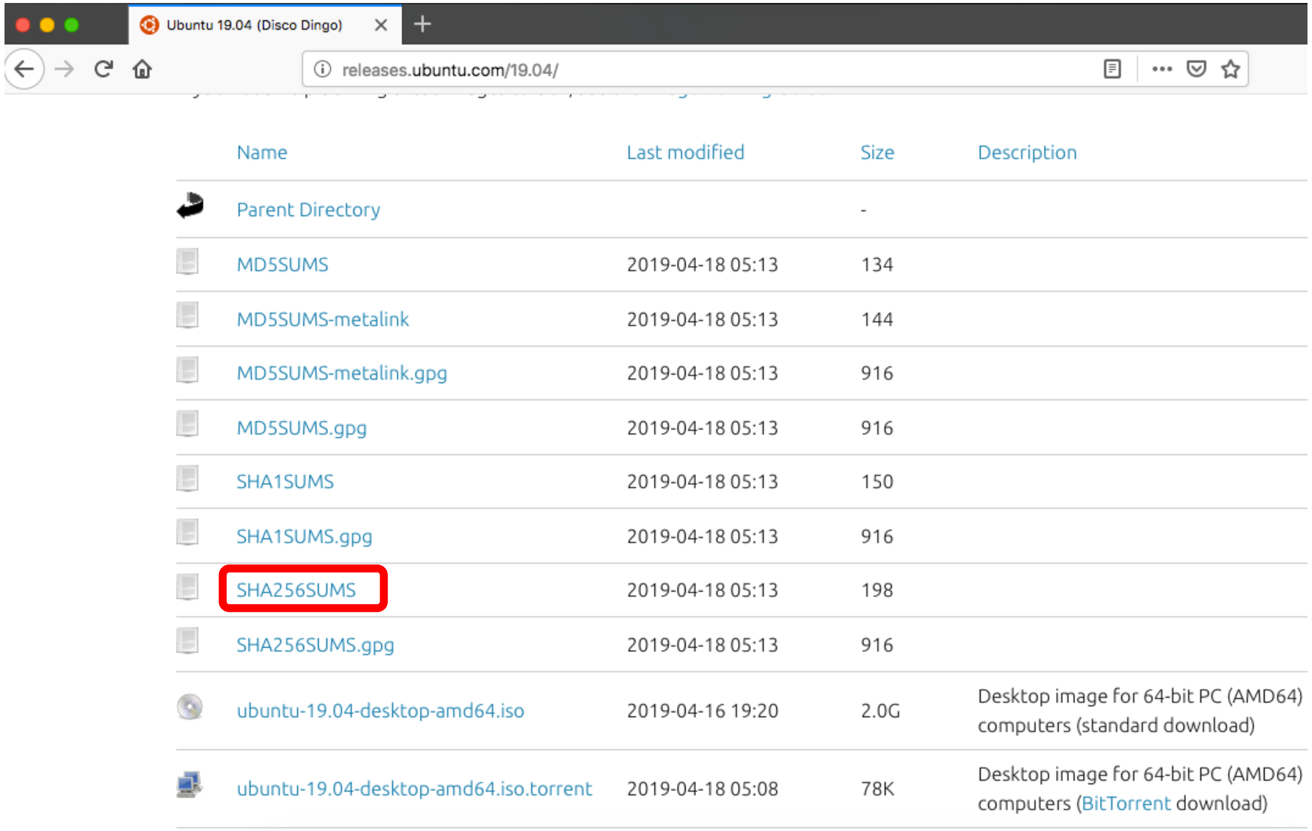
```
[MacBook-Pro-de-Badis:Desktop badishammi$ md5 TestHash.txt
 MD5 (TestHash.txt) = 19f289afdd4fcc019f4a078d83bd9b59
```



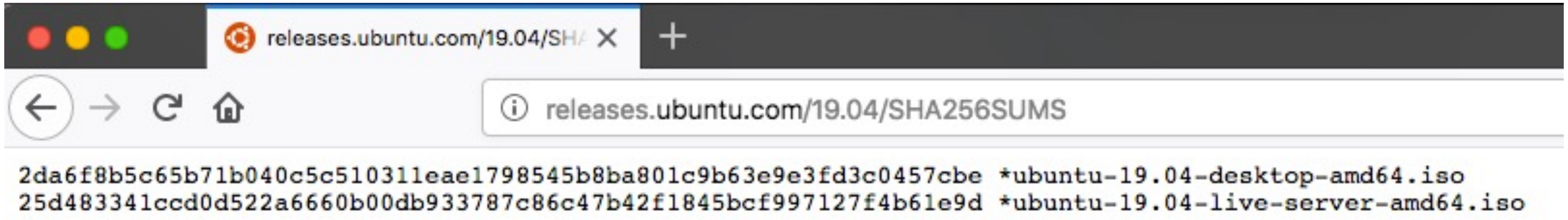
```
[MacBook-Pro-de-Badis:Desktop badishammi$ md5 TestHash.txt
 MD5 (TestHash.txt) = 20144d91672c340c42bfba9cd361f89f
```



Data Integrity: Hash functions: Security properties

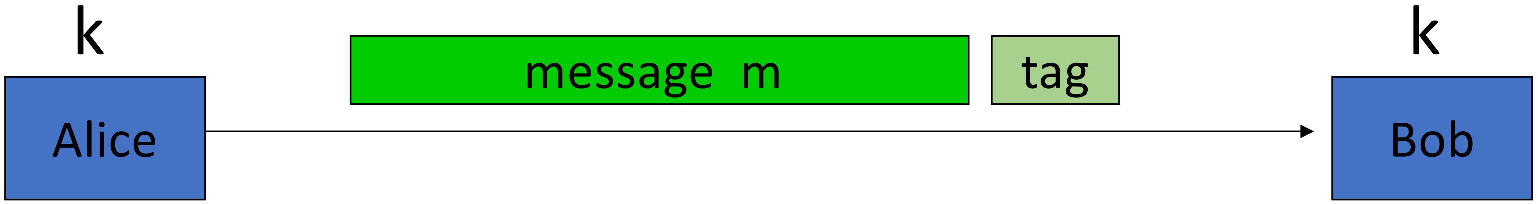


	Name	Last modified	Size	Description
	Parent Directory		-	
	MD5SUMS	2019-04-18 05:13	134	
	MD5SUMS-metalink	2019-04-18 05:13	144	
	MD5SUMS-metalink.gpg	2019-04-18 05:13	916	
	MD5SUMS.gpg	2019-04-18 05:13	916	
	SHA1SUMS	2019-04-18 05:13	150	
	SHA1SUMS.gpg	2019-04-18 05:13	916	
	SHA256SUMS	2019-04-18 05:13	198	
	SHA256SUMS.gpg	2019-04-18 05:13	916	
	ubuntu-19.04-desktop-amd64.iso	2019-04-16 19:20	2.0G	Desktop image for 64-bit PC (AMD64) computers (standard download)
	ubuntu-19.04-desktop-amd64.iso.torrent	2019-04-18 05:08	78K	Desktop image for 64-bit PC (AMD64) computers (BitTorrent download)


releases.ubuntu.com/19.04/SHA
releases.ubuntu.com/19.04/SHA256SUMS

```
2da6f8b5c65b71b040c5c510311eae1798545b8ba801c9b63e9e3fd3c0457cbe *ubuntu-19.04-desktop-amd64.iso
25d483341ccd0d522a6660b00db933787c86c47b42f1845bcf997127f4b61e9d *ubuntu-19.04-live-server-amd64.iso
```

Data Integrity: Hash functions: Security properties



Generate tag:

tag ← H(m)

Verify tag:

V(m, tag) $\overset{?}{=}$ `yes'

Authentication

Authentication is a process allowing the system to ensure the legitimacy of the access request made by an entity (human being, process or another system) in order to authorize the access of this entity to system’s resources.

Entity authentication service

- Confirmation of the veracity of the identity or of a specific element to a declared entity

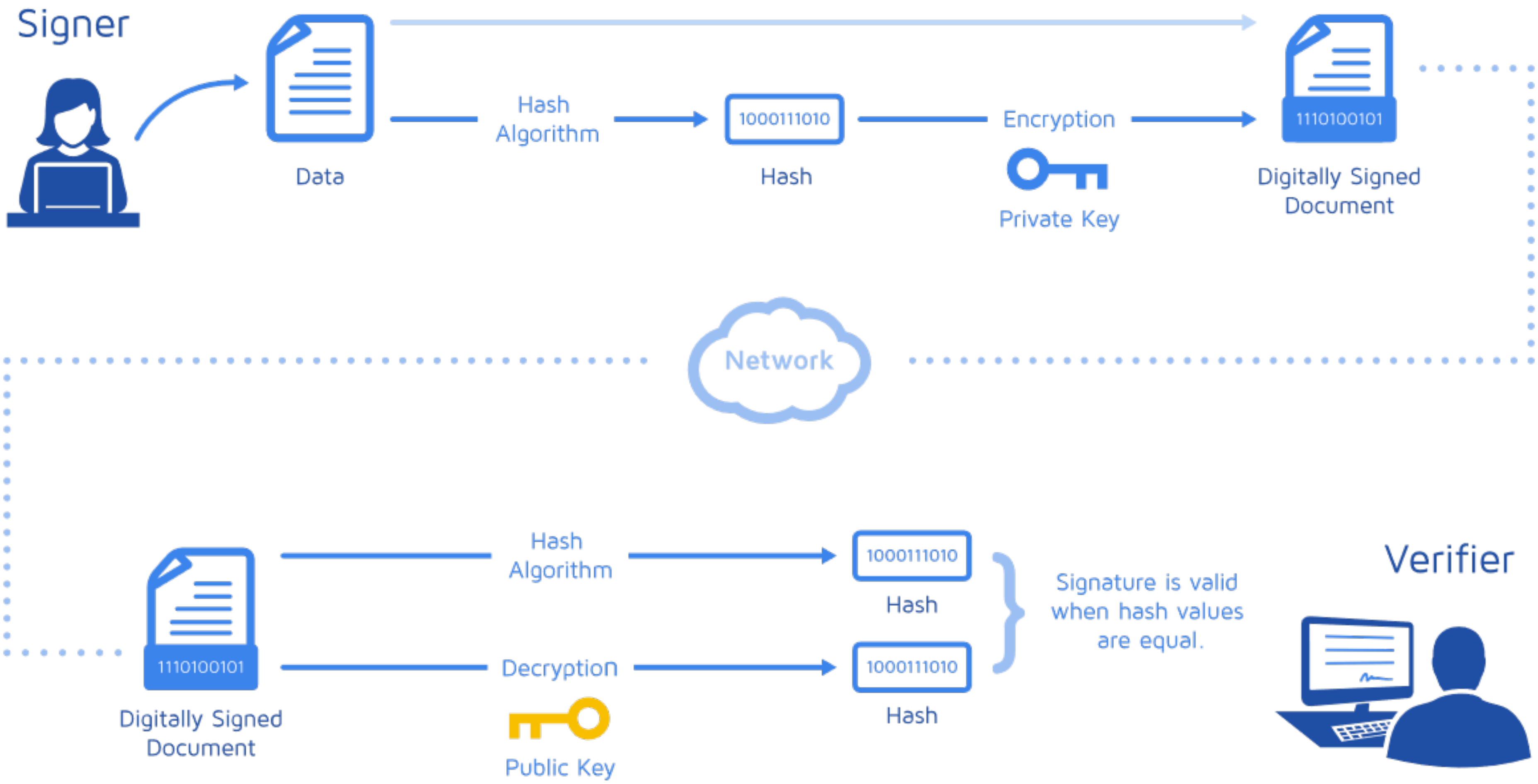
ISO/IEC 2382/8:

- Ensures that the identity of the data origin is the identity claimed

In practice:

- Consists of linking information together with generally an element allowing to specify an entity

Authentication: Digital (cryptographic) signature


Signer
Data
Hash
Algorithm
1000111010
Hash
Encryption
Private Key
1110100101
Digitally Signed
Document
Network
1110100101
Digitally Signed
Document
Hash
Algorithm
1000111010
Hash
Decryption
Public Key
1000111010
Hash
Signature is valid
when hash values
are equal.
Verifier