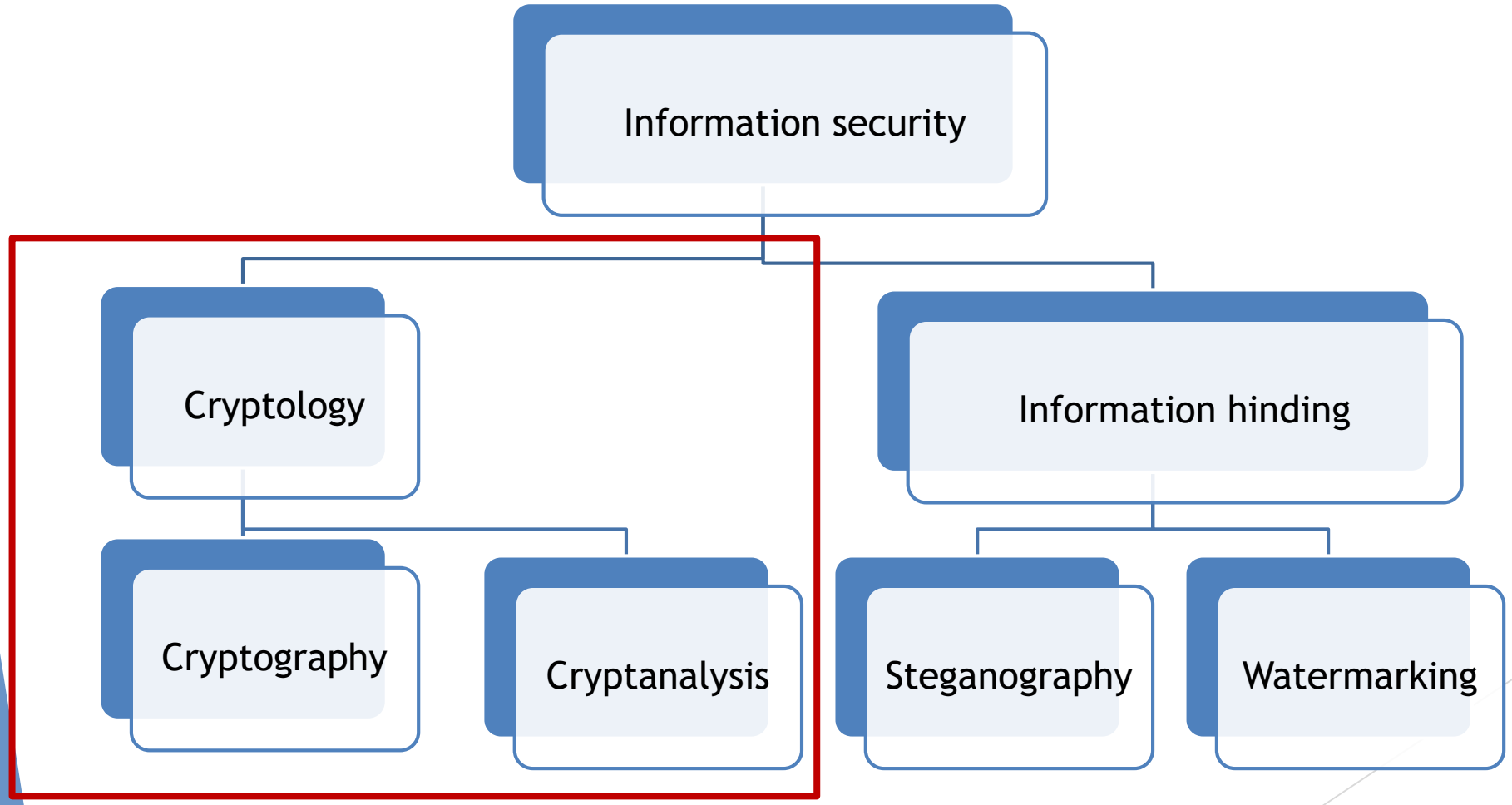
Basic concepts of cryptography

Pr. Noureddine Chikouche
noureddine.chikouche@univ-msila.dz
https://sites.google.com/view/chikouchenoureddine

Course outline

- Terminology
- Classification of cryptographic algorithms
- Historical
- Mathematics for Cryptography

Terminology



Terminology

- **Steganography (cover , write)**
  - It is the art of hiding a secret message within another message (text, image, sound, video...) of an innocuous nature, so that the very existence of the secret is hidded.
- Watermarking
  - This is a technique for adding copyright information or other verification messages to a digital document.

Terminology

- **Cryptology (hidden , science)**
  - It is the science of secrecy.
  - It is a mathematical science which has two branches: cryptography and cryptanalysis.

Terminology

Cryptology = Science + Art

- Science : it uses mathematics and computer science.
- Art : it calls upon the decrypter's talents of intuition , imagination , and invention .

- Didier Muller

Terminology

- **Cryptography (hidden , written)**
  - Science that uses mathematics for the encryption and decryption of data.
  - It is also the study of mathematical techniques related to the properties of computer security (confidentiality, integrity and authentication).
- **Cryptanalysis**
  - It is the study of encrypted information in order to uncover its secrets. Cryptanalysts are also called "hackers".

Terminology

- Plaintext
  - Data that is readable and understandable without specific intervention.
- Ciphertext
  - Unintelligible text resulting from encryption.

Terminology

- Encryption
  - A method for converting plaintext by changing its content. This operation ensures that only those with the decryption key can read it.
- Decryption:
  - The reverse process of transforming ciphertext into plaintext.

Terminology

- Cryptosystem
  - It is defined as the set of possible keys (key space), plaintexts and ciphertexts possible associated with a given algorithm.
  - Quintuplet ($\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D}$), such that:
    - $\mathcal{P}$: set of plain texts
    - $\mathcal{C}$: set of ciphertexts
    - $\mathcal{K}$: key space
    - For each $K \in \mathcal{K}$, there is an encryption function $e_{K1} \in \mathcal{E}$, and a corresponding decryption function $d_{K2} \in \mathcal{D}$, such that

$$d_{K2}(e_{K1}(x)) = x, \text{ for all } x \in \mathcal{P}$$

Terminology

- Substitution cipher
  - Each character in the plaintext is replaced by a character in ciphertext.
- Transposition cipher
  - The letters in the plain text remain unchanged, but their positions are modified.

Terminology

Kerckhoff's principle

- a cryptosystem must be secure even if everything about the system, with the exception of the key, is publicly known.
- No secret should reside in the algorithm, but rather in the key.
- However, if we know K, the decryption is immediate .

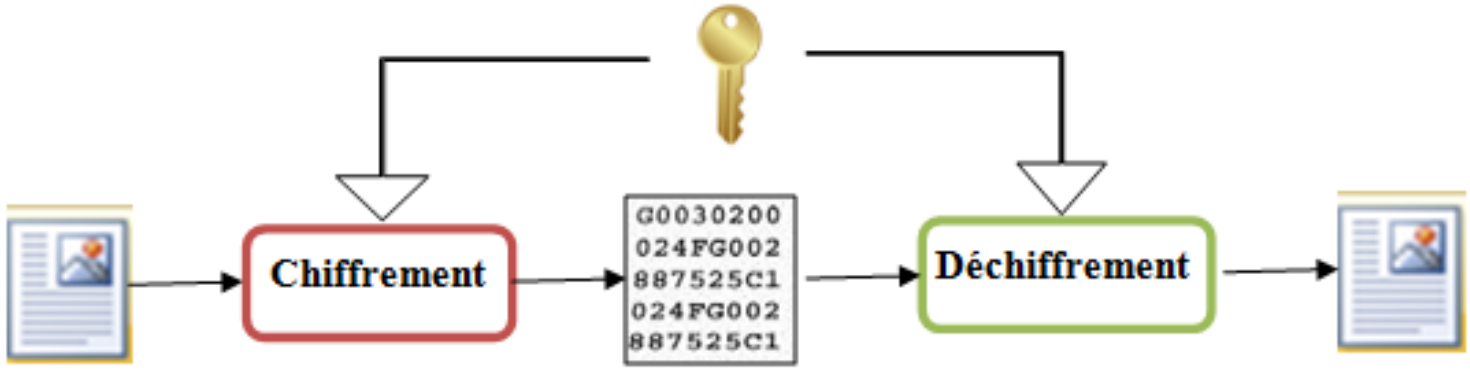
Classification of cryptosystems according to the nature of the key

- Symmetric cryptography
  - This is also called secret key cryptography .
  - The two entities share a secret key.
  - The key is used for encryption and decryption.

Classification of cryptosystems according to the nature of the key

- Symmetric cryptography
  - In this case, for a message " *m* ", we write:

$$e_K(m) = c,\ d_K(c) = m \text{ and } d_K(e_K(m)) = m.$$



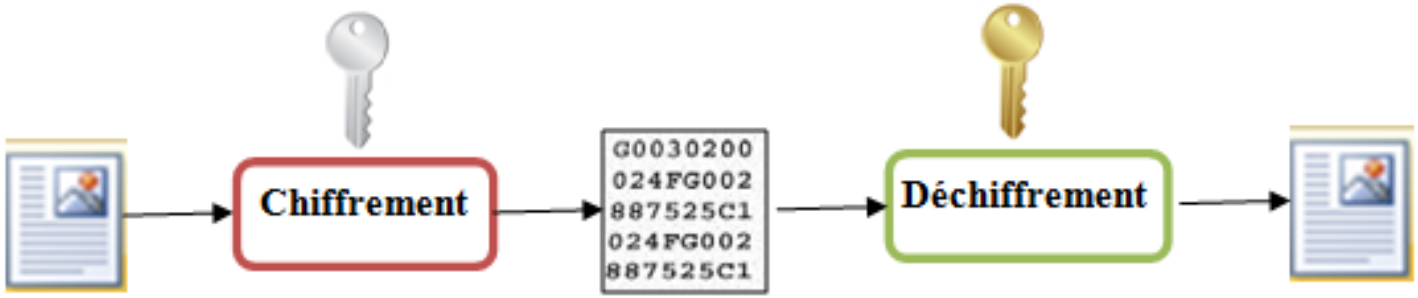
Classification of cryptosystems according to the nature of the key

- Asymmetric cryptography
  - This is also called public key cryptography .
  - There are two types of keys:
    - Public key (*K1*) is broadcast to everyone and used to encrypt the message.
    - Private key (*K2*) kept secret, used to decrypt the message.

Classification of cryptosystems according to the nature of the key

- Asymmetric cryptography
  - We write:

$$e_{K1}(m) = c,\ dK2(c) = m \text{ and } dK2(eK1(m)) = m.$$



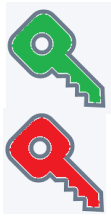
Asymmetric (public-key) encryption

How can Amine send a message to Salim using asymmetric encryption?

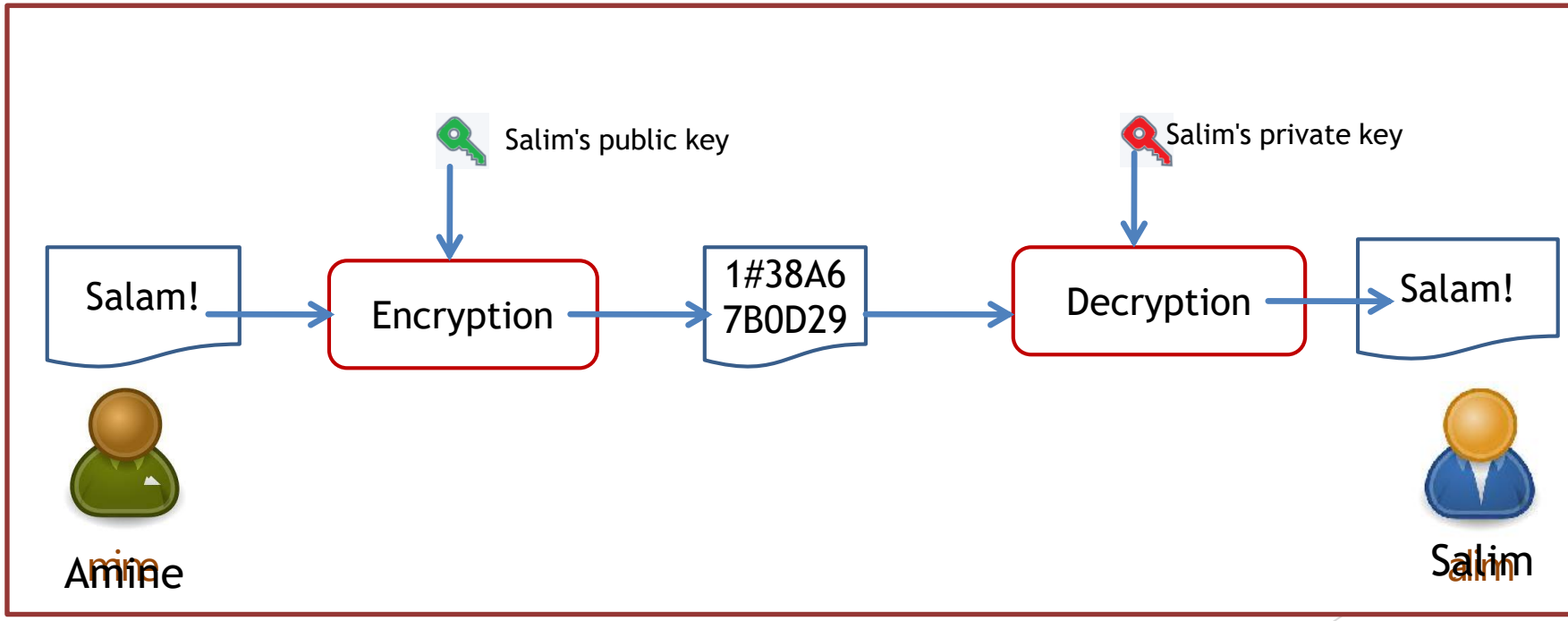
Salim has a pair of keys

Public key

Private key



- The encryption algorithm is known to everyone.
- The Decryption function is the inverse function of the Encryption function .
- Salim 's private key never circulates on the network.
- Salim is sharing his public key with everyone.

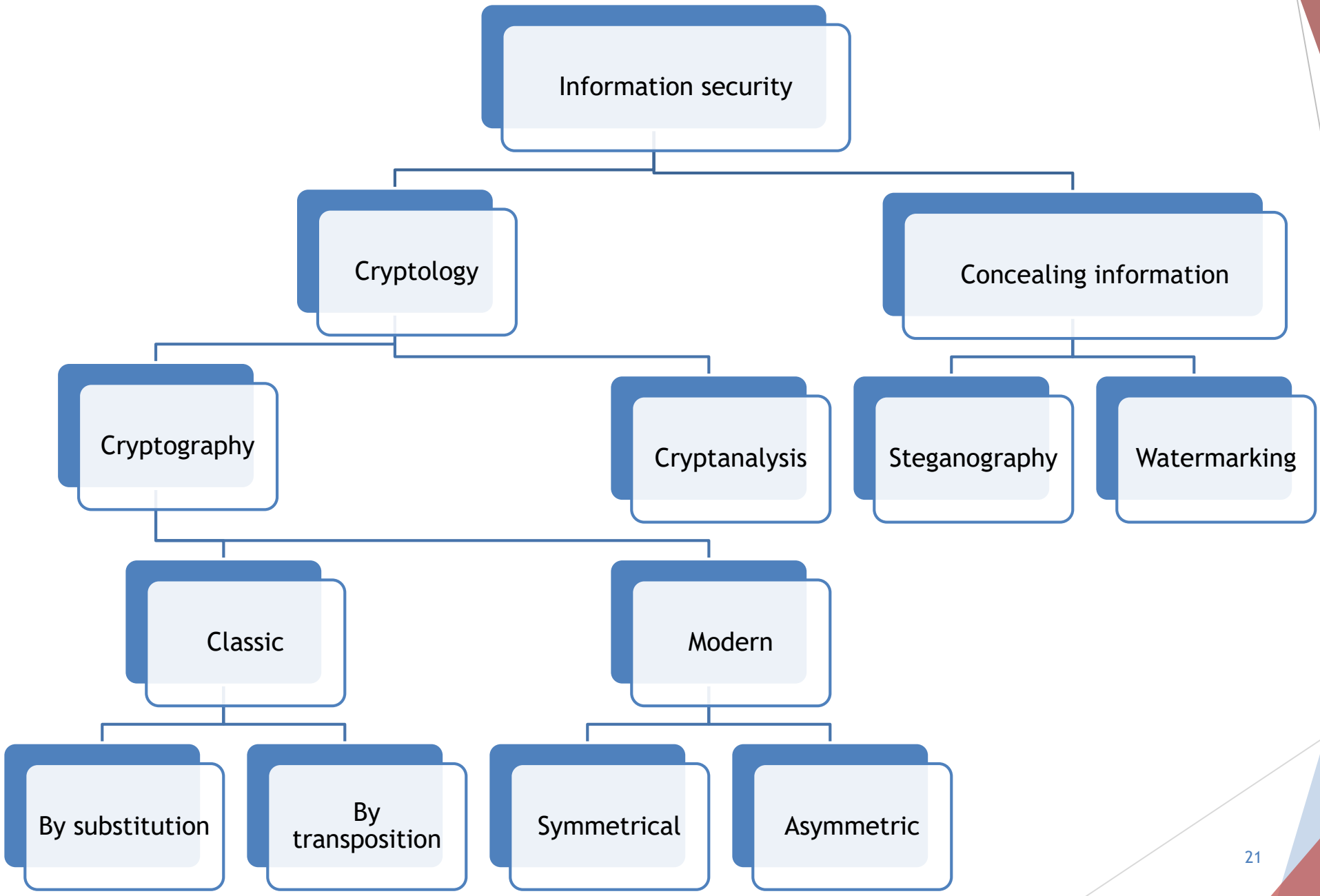


Classification of cryptosystems according to time

- Classical Cryptography
  - The science of cryptography has been used since antiquity.
  - It is based on the use of letters from the language for text encryption.
  - The same key is used for both encryption and decryption.
  - This category continued until the end of the Second World War.
  - These cryptosystems are used to protect physical documents in military and diplomatic applications.

Classification of cryptosystems according to time

- Modern Cryptography
  - It operates on binary data.
  - It uses advanced mathematical algorithms, such as number theory, probability, and computational complexity.
  - It is used in the majority of applications, such as: internet communication, commercial, financial transaction, military, transport, health, etc.

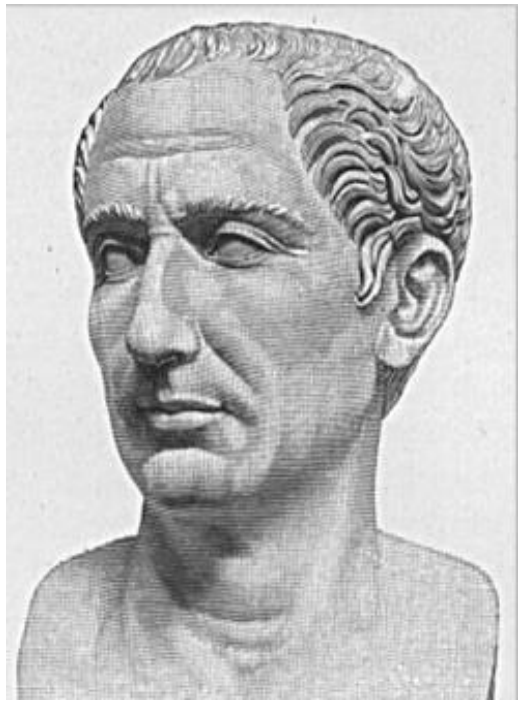

Information security
Cryptology
Concealing information
Cryptography
Cryptanalysis
Steganography
Watermarking
Classic
Modern
By substitution
By transposition
Symmetrical
Asymmetric

Historical

- Encryption Assyrian (600 BC)

History

- Caesar (50 BC)



History

- Al-Kindi (801-873)

History

- Vigenère (1553)

		Text																							
		A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Schlüssel	1	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	2	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
	3	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
	4	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
	5	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
	6	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
	7	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
	8	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
	9	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
	10	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
	11	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
	12	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
	13	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
	14	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
	15	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
	16	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
	17	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
	18	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
	19	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
	20	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
	21	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
	22	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
	23	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
	24	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
	25	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
	26	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

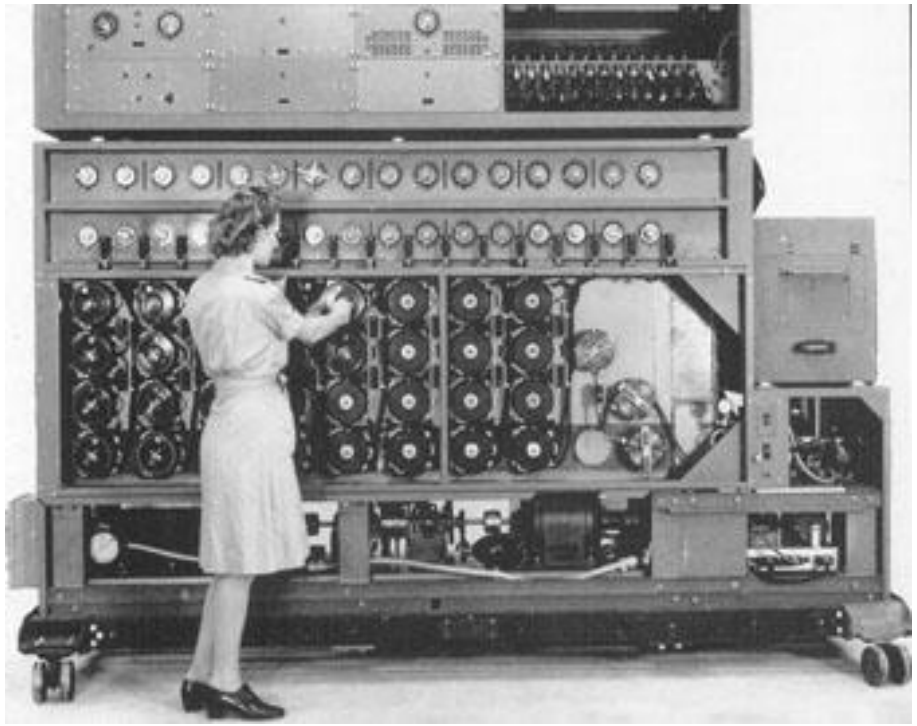
Geheimtext

History

- Vernam (1917)

History

- Alan M. Turing (1940)

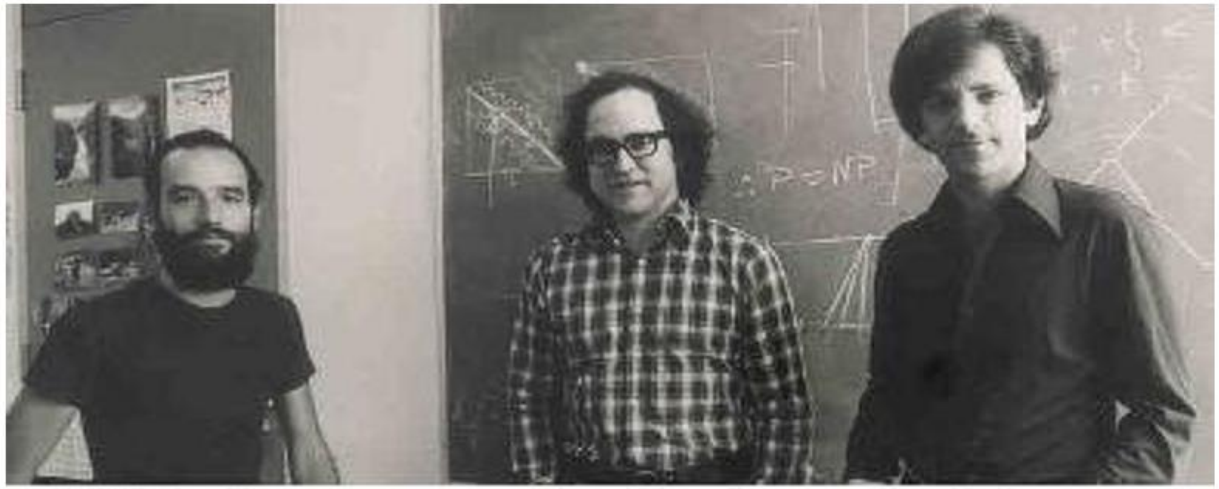


History

- Diffie & Hellman (1976)

History

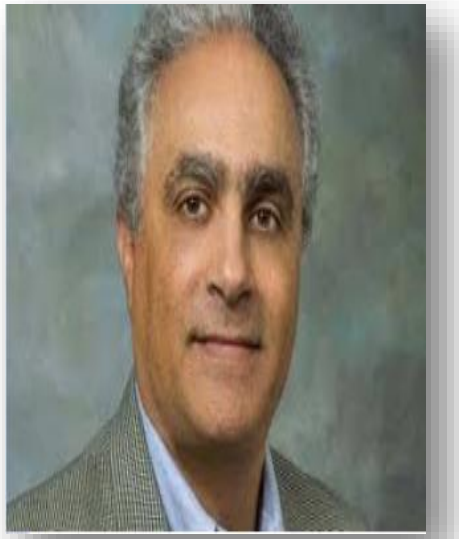
- RSA (1977)



Adi Shamir Ron Rivest Len Adleman

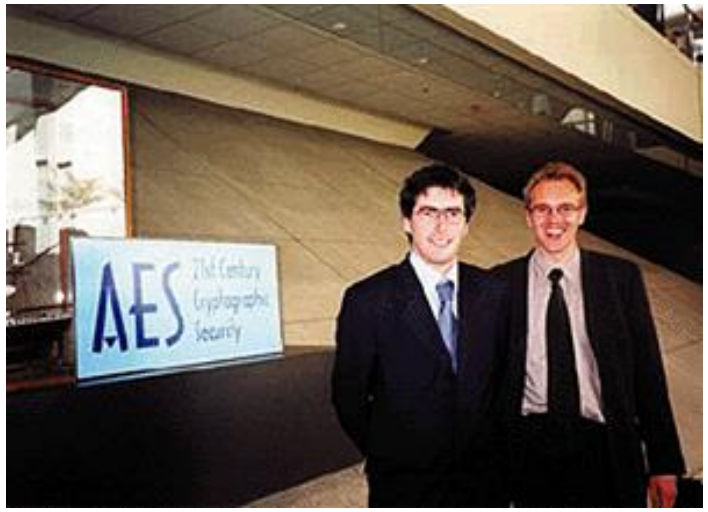
History

- EL GAMAL (1984)



History

- Rijmen & Daemen (2001)



Advanced Encryption Standard (AES)

Mathematics for Cryptography

Extended Euclid's Algorithm

- Let a and b be two integers with $a \geq b$.
- Let d be the GCD of a and b .

> The extended Euclid algorithm allows the calculation of Bézout's coefficients (u And v) as well as the GCD d .

- Such as:

$$a\,u + b\,v = d = \gcd(a, b)$$

- This algorithm is used to calculate the private key of the RSA cryptosystem .

Extended Euclid's Algorithm

Fonction PGCDE(a, b) ; *[la fonction retourne 3 entiers]*
$a \leftarrow |a|$; $b \leftarrow |b|$;
Si $(b > a)$ **Alors**
  $a \leftrightarrow b$;
Fin Si
Effectuer la division euclidienne de a par b ; $r \leftarrow$ reste ;$q \leftarrow$ quotient ;
Si (r est nul) **Alors**
  Retourner $(b, 0, 1)$;
Sinon
  $(d, u', v') \leftarrow PGCDE(b, r)$;
  $u \leftarrow v'$; $v \leftarrow (u' - qv')$;
  Retourner (d, u, v) ;
Fin Si

Extended Euclid's Algorithm

Example:

- Let's calculate gcd(25,15).
- 25 = 15 * 1 + 10 → 10 = 25-15
- 15 = 10 * 1 + 5 → 5 = 15 - 10 = 15 * 2 - 25
- 10 = 5 * 2 + 0

- So the gcd(25,15)= (-1) *25 + (2)* 15 = 5 .
  - u= -1
  - v = 2
  - d = 5

Extended Euclid's Algorithm

Exercise:

Let's calculate gcd(120 , 23).

120= 23x5 + 5 → 5= 120 - 23 x 5

23 = 5 x 4 + 3 → 3 = 23 - 5 x 4 = 23 x 21 - 120 x 4

5 = 3 x 1 + 2 → 2= 5- 3 = 120 x 5 - 23 x 26

3 = 2 x 1 + 1 → 1 = 3 - 2 = 47 x 23 - 9 x 120

So the gcd(120,23)= 120* (-9) + 23*47=1 .

Modular Invert

The inverse modulo n of b is the integer b^{-1} such that:

$$bb^{-1} \pmod{n} = 1$$

with b and n are coprime [gcd(b, n)=1] .

To find b^{-1} , we use the extended Euclid algorithm , such that:

$$n\,u + b\,v = 1$$

So, $b^{-1} \bmod n = v$

Find $(17)^{-1} \bmod 26$.

We apply the algorithm Extended Euclid

$26 = 17 * 1 + 9 \rightarrow 9 = 26 - 1 * 17$

$17 = 9*1 + 8 \rightarrow 8 = 17 - 1*9$

$\rightarrow 8=17-1*(26-1*17)$

$8 = 2 * 17 - 1 * 26$

$9 = 8 * 1 + 1 \rightarrow 1 = 9 - 1 * 8$

$\rightarrow 1=(26-1*17)-1\ (2*17-1*26)$

$\rightarrow 1 = 2 * 26 - 3 * 17$

1

d=1, u=2 and v= -3

2 As long as d = 1 , then v is the modular inverse of 17 mod 26.

3 v <0 → We calculate the positive value of v : -3 mod 26 = 23 mod 26 (26-3= 23)

4 The inverse modulo 26 of 17 is 23

$(17)^{-1} \bmod 26 = 23$

Quiz

- To encrypt a message using asymmetric encryption, we use:
  - My public key
  - My private key
  - The recipient's public key
  - The recipient's private key
- The science that studies the weakness of encryption algorithms is:
  - Cryptography
  - Cryptanalysis
  - Digital tattooing
  - Steganography