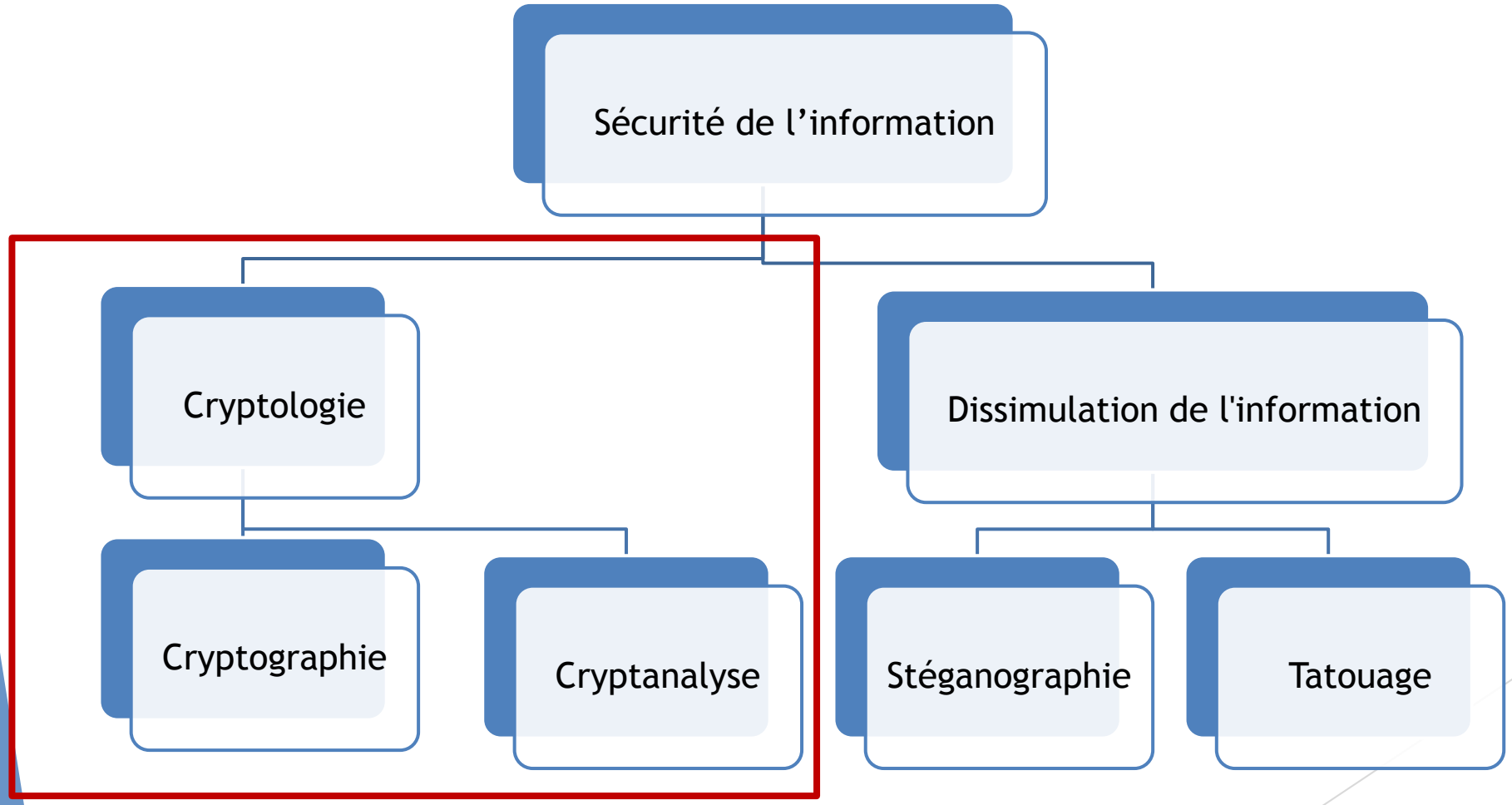
Concepts de base de la cryptographie

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

Plan du cours

- Terminologie
- Classification des algorithmes cryptographiques
- Historique
- Mathématiques pour la cryptographie

Terminologie



Terminologie

- **Stéganographie (couvert, écrire)**
  - C’st l’art de cacher un message secret au sein d’un autre message porteur (texte, image, son, vidéo...) de caractère anodin, de sorte que l’existence même du secret en soit dissimulée.
- **Tatouage**
  - C’est une technique permettant d'ajouter des informations de copyright ou d'autres messages de vérification à un document numérique.

Terminologie

- **Cryptologie (caché, science)**
  - C’est la science du secret. C’est une science mathématiques qui comporte deux branches: la cryptographie et la cryptanalyse.

Terminologie

Cryptologie = Science + Art

- Science: elle fait appel aux mathématiques et informatique.
- Art: elle fait appel aux talents d'intuition, d'imagination et d'invention du décrypteur.

- Didier Muller

Terminologie

- **Cryptographie (caché, écrire)**
  - Science qui utilise les mathématiques pour le cryptage et le décryptage de données.
  - C'est aussi l'étude des techniques mathématiques en rapport avec les propriétés de la sécurité informatique (confidentialité, intégrité et authentification).
- **Cryptanalyse**
  - C'est l'étude des informations cryptées, afin d'en découvrir le secret. Les cryptanalystes sont également appelés des « pirates ».

Terminologie

- Texte en clair (*Plaintext*)
  - Données lisibles et compréhensible sans intervention spécifique.
  - Texte chiffré (*Ciphertext*)
  - Texte inintelligible résultant du chiffrement.

Terminologie

- Cryptage (chiffrement)
  - Méthode permettant de convertir un texte clair en changeant son contenu. Cette opération permet s'assurer que seules les personnes auxquelles la clé de déchiffrement soient en mesure de les lire.
- Décryptage (déchiffrement):
  - Processus inverse de transformation du texte chiffré en texte clair.

Terminologie

- Cryptosystème
  - Il est défini comme l'ensemble des clés possibles (espace de clés), des textes clairs et chiffrés possibles associés à un algorithme donné.
  - Quintuplet $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$, tel que :
    - $\mathcal{P}$: ensemble de textes en clair
    - $\mathcal{C}$: ensemble fini de textes chiffrés
    - $\mathcal{K}$: espace de clés
    - Pour chaque $K \in \mathcal{K}$, il y a une fonction de cryptage $e_{K1} \in \mathcal{E}$, et une fonction de décryptage correspondante $d_{K2} \in \mathcal{D}$, tel que

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

Terminologie

- Chiffrement par substitution
  - Chaque caractère du texte en clair est remplace par un caractère dans un texte chiffré.
- Chiffrement par transposition
  - Les lettres dans le texte en clair demeurent inchangés mais dont les positions sont modifiées.

Terminologie

Principe de Kerckhoff

- Aucun secret ne doit résider dans l'algorithme mais plutôt dans la clé.
- Sans celle-ci, il doit être impossible de retrouver le texte clair à partir du texte chiffré.
- Par contre, si on connaît K, le déchiffrement est immédiat.

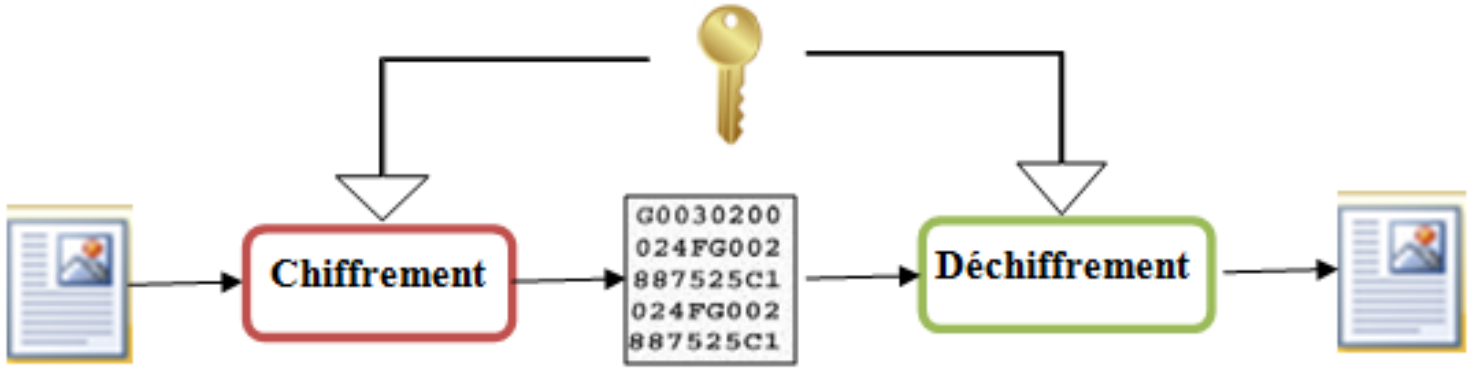
Classification des cryptosystèmes selon la nature de la clé

- Cryptographie symétrique
  - C’est appelé aussi la cryptographie de clé secrète.
  - Les deux entités partagent une clé secrète.
  - La clé sert au chiffrement et au déchiffrement.

Classification des cryptosystèmes selon la nature de la clé

- Cryptographie symétrique
  - Dans ce cas, pour un message « *m* », on écrit :

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



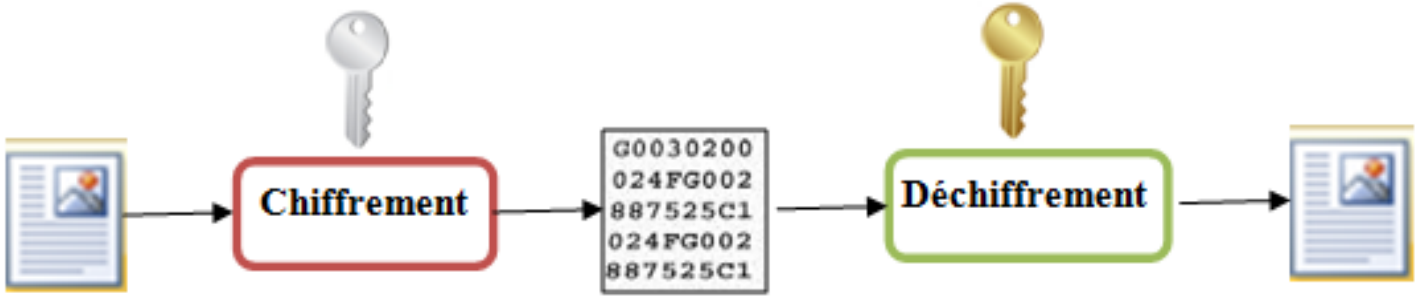
Classification des cryptosystèmes selon la nature de la clé

- Cryptographie asymétrique
  - C'est appelé aussi la cryptographie de clé publique.
  - On a deux types des clés:
    - Clé publique (K_1) diffusée à tout le monde, utilisée pour chiffrer le message,
    - Clé privée (K_2) tenue secrète, utilisée pour déchiffrer le message.

Classification des cryptosystèmes selon la nature de la clé

- Cryptographie asymétrique
  - On écrit :

$$e_{K1}(m) = c, \quad d_{K2}(c) = m \quad \text{et} \quad d_{K2}(e_{K1}(m)) = m.$$



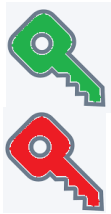
Chiffrement asymétrique (à clé publique)

Comment Amine peut envoyer un message à Salim en utilisant le chiffrement asymétrique?

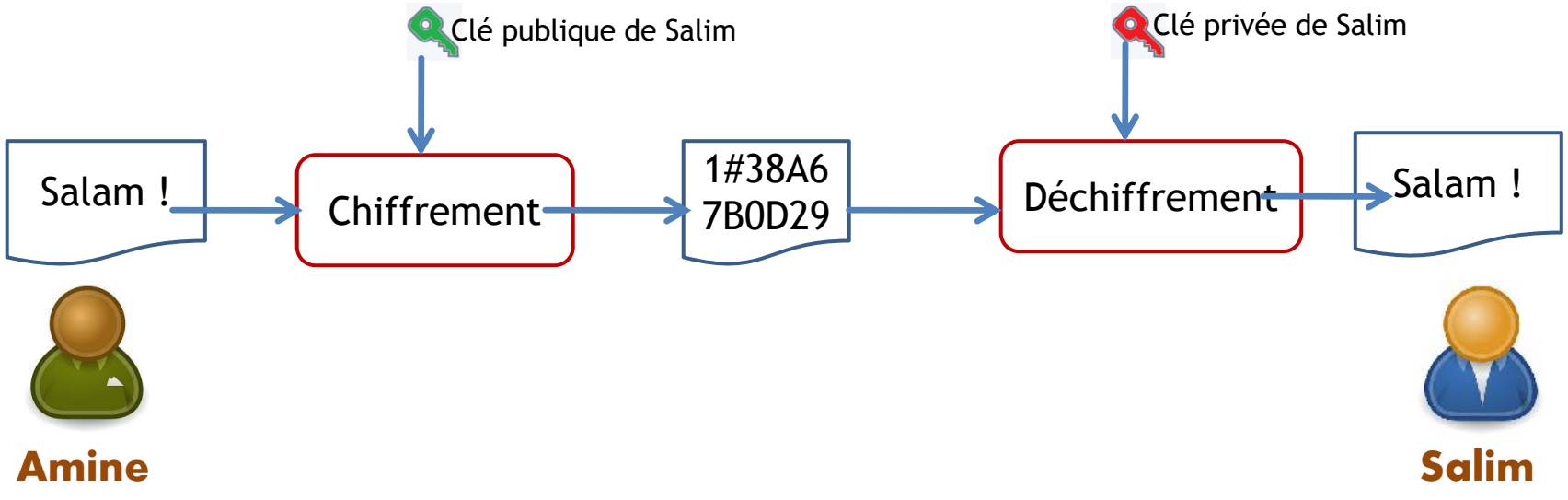
Salim possède une paire de clés

Clé publique

Clé privée



- L'algorithme de chiffrement est connu pour tout le monde.
- La fonction Déchiffrement est la fonction inverse de la fonction Chiffrement.
- Le clé privée de Salim ne circule jamais sur le réseau.
- Salim diffuse sa clé publique pour tout le monde.

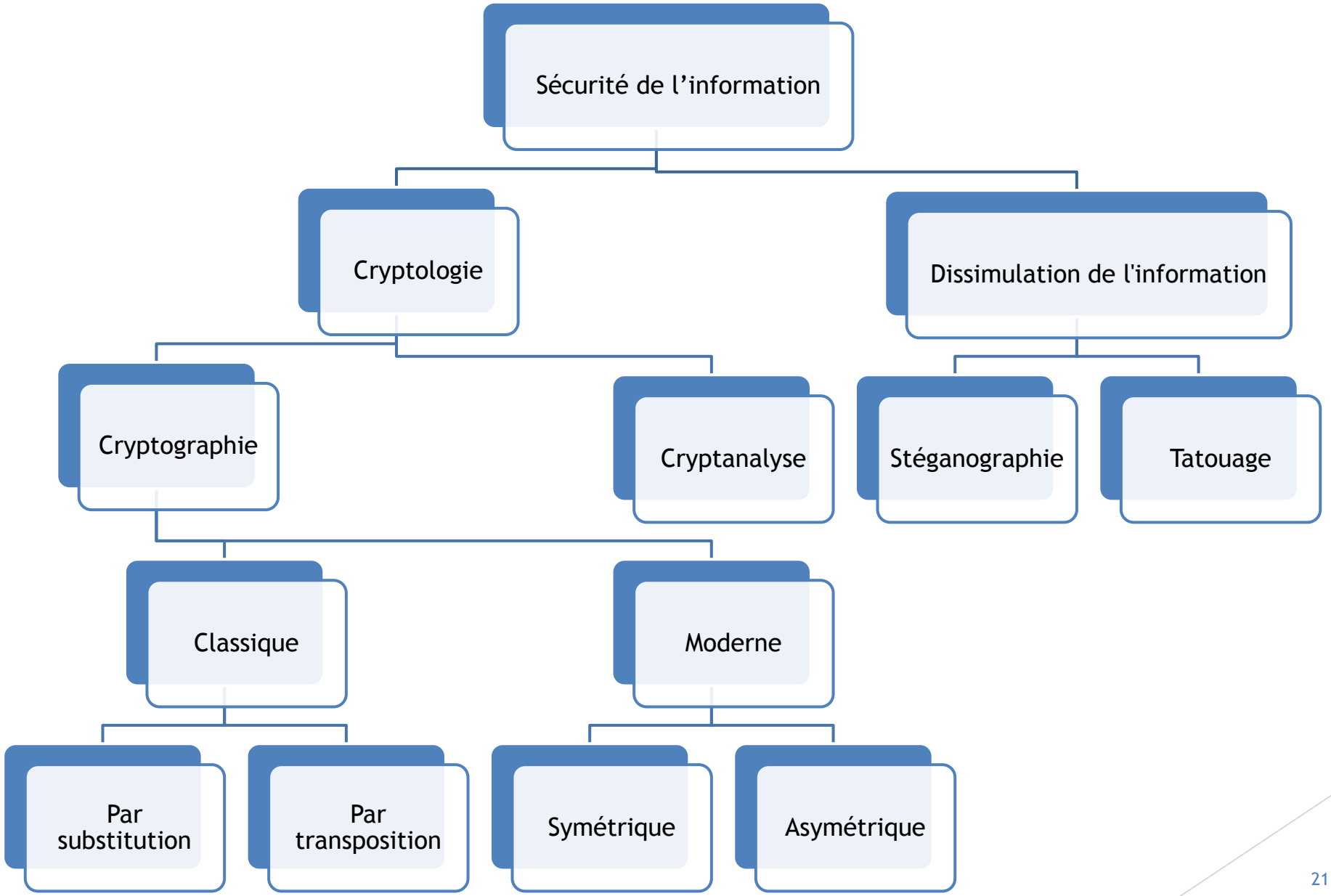


Classification des cryptosystèmes selon le temps

- Cryptographie classique
  - La science de la cryptographie est utilisée depuis l'antiquité.
  - Elle est basée sur l'utilisation des lettres de la langue pour le chiffrement des textes.
  - La même clé est utilisée pour le chiffrement et pour le déchiffrement.
  - Cette catégorie continué jusqu'à la fin de deuxième guerre mondiale.
  - Ces cryptosystèmes sont appliques pour protéger les documents physiques dans les domaines militaires et diplomatiques.

Classification des cryptosystèmes selon le temps

- Cryptographie moderne
  - Il dépend de l'apparition de l'informatique dans les années 60 et l'augmentation des systèmes de communications.
  - Elle est basée sur le langage machine 0/1.
  - Elle est appliquée dans la majorité des applications, telles que : commerciales, financières, militaires, communications, transports, santé, etc.

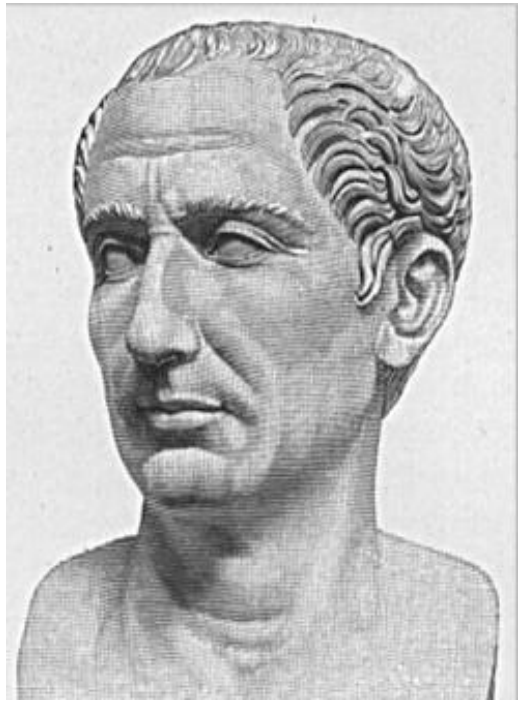

Sécurité de l’information
Cryptologie
Dissimulation de l'information
Cryptographie
Cryptanalyse
Stéganographie
Tatouage
Classique
Moderne
Par substitution
Par transposition
Symétrique
Asymétrique

Historique

- Chiffrement assyrienne (600 A.V J-C)

Historique

- César (50 A.V J-C)



Historique

- Al-Kindi (801-873)

Historique

- Vigénere (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

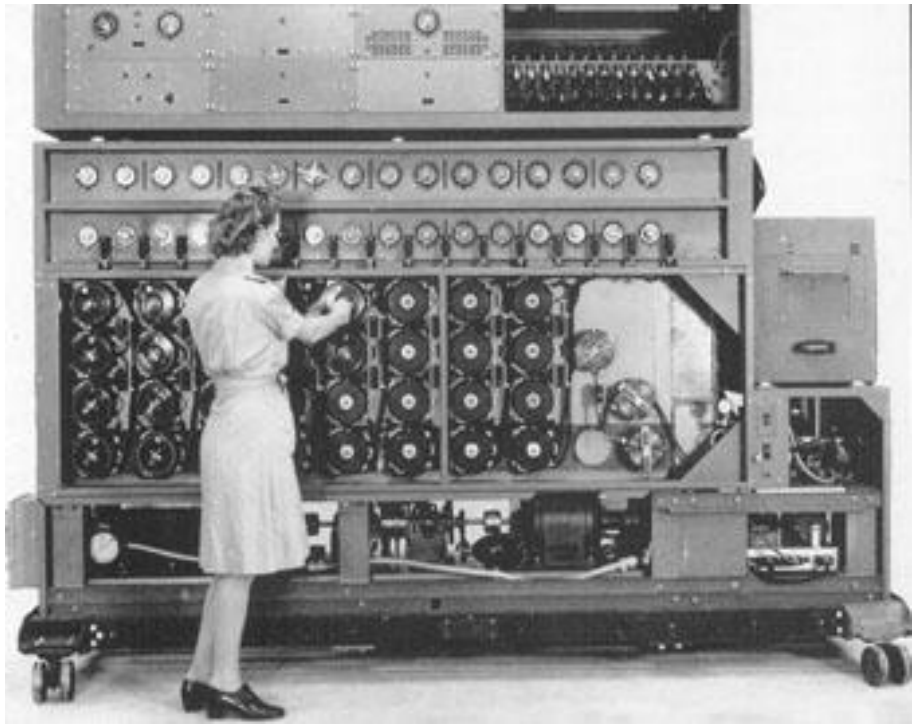
Geheimtext

Historique

- Vernam (1917)

Historique

- Alan M. Turing (1940)

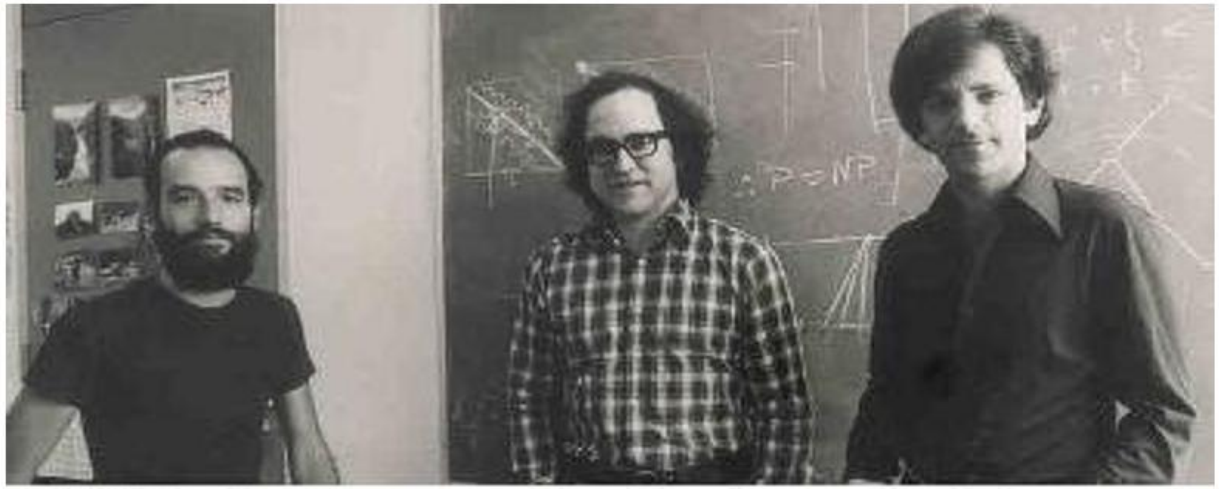


Historique

- Diffie & Hellman (1976)

Historique

- RSA (1977)



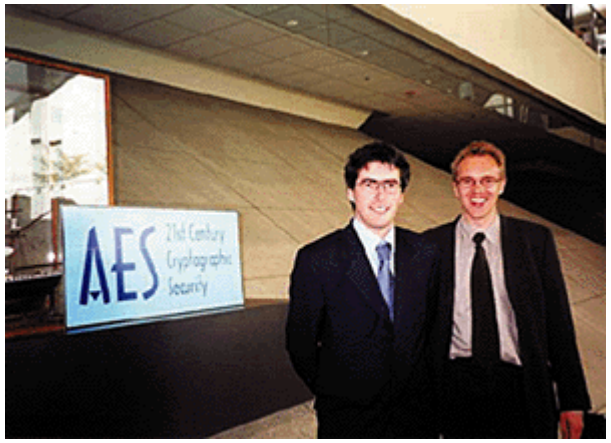
Adi Shamir Ron Rivest Len Adleman

Historique

- EL GAMAL(1984)

Historique

- Rijmen & Daemen(2001)



Advanced Encryption Standard (AES)

Mathématiques pour la cryptographie

Algorithme d'Euclide étendu

- Soient a et b deux entiers avec a≥b.
- Soit d est le PGCD de a et b.

> L'algorithme d'Euclide étendu permet de calculer les coefficients de Bézout (u et v) ainsi que le PGCD d.

- Tel que:

$$au + bv = d = pgcd(a, b)$$

- On utilise cet algorithme pour calculer la clé privée du cryptosystème RSA.

Algorithme d'Euclide étendu

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

Algorithme d'Euclide étendu

Exemple:

- Soit le calcul de pgcd(25,15).
- 25 = 15 * 1 + 10 → 10 = 25-15
- 15 = 10 *1 + 5 → 5 = 15-10 = 15*2-25
- 10= 5 *2 + 0

- Donc le pgcd(25,15)= (-1)*25 + (2)*15 =5.
  - u= -1
  - v= 2
  - d= 5

Algorithme d'Euclide étendu

Exercice:

Soit le calcul de pgcd(120,23).

120= 23x5 + 5 → 5= 120 – 23x5

23 = 5 x 4 + 3 → 3 = 23 – 5x4 = 23x21 – 120x4

5 = 3x1 + 2 → 2= 5- 3 = 120x5 – 23x26

3 = 2 x1 + 1 → 1 = 3 – 2 = 47x23 - 9x120

Donc le pgcd(120,23)= 120* (-9) + 23*47=1.

Inverse modulaire

- L'inverse modulo n de b est le nombre entier b^{-1} tel que:

$$b.b^{-1} \pmod{n} = 1$$

avec b et n sont premiers entre eux [$pgcd(b, n)=1$] .

Pour trouver b^{-1},on utilise l'algorithme Euclide étendu, tel que:

$$nu + bv = 1$$

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

Trouver $(17)^{-1}$ mod 26.

On applique l'algorithme Euclide étendu

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

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

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

$\rightarrow 8 = 2*17 - 1*26$

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

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

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

1

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

2 Tant que d = 1, alors v est l'inverse modulaire de17 mod 26.

v <0 → on calcule la valeur positive du v: -3 mod 26 = 23 mod 26 (26-3= 23)

3

4 L'inverse modulo 26 de 17est 23

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

Quiz

- Pour chiffrer un message utilisant le chiffrement asymétrique, on utilise:
  - Ma clé publique
  - Ma clé privée
  - La clé publique de destinataire
  - La clé privée de destinataire
- La science qui étudie la faiblesse des algorithmes de chiffrement est :
  - La cryptographie
  - La cryptanalyse
  - Le tatouage numérique
  - Stéganographie