La cryptographie

Sécurité des Systèmes & Réseaux

Animé par :

Samir DIABI

Contenu du chapitre

- Introduction
- Services de la cryptographie
- Les bases de l'intégrité et de l'authenticité.
- La confidentialité
- La cryptographie à clé publique

Introduction

- Depuis fort longtemps, les hommes ont tenté de rendre sécuritaires leurs communications confidentielles.
- Au début, il s'agissait seulement de cacher l'existence du message.
- Puis, des techniques de plus en plus sophistiquées furent utilisées pour rendre les messages compréhensibles seulement par leurs destinataires légitimes.
- Tout au cour de l'histoire, une difficile bataille eut lieu entre les constructeurs de code (cryptographes) et ceux qui essayaient de les briser (les cryptanalystes).

Contenu du chapitre

- Introduction
- Services de la cryptographie
- Les bases de l'intégrité et de l'authenticité.
- La confidentialité
- La cryptographie à clé publique

La stéganographie

- La **stéganographie** est l'art de la dissimulation : son objet est de faire passer inaperçu un message dans un autre message.
- Damaratus inscrivait son message sur des tablettes de bois et les recouvrit de cire.
- Histaïaeus, pour transmettre un message, rasa la tête de son messager et inscrivit le message sur son crane. Une fois les cheveux repoussés, le messager put circuler sans attirer l'attention.

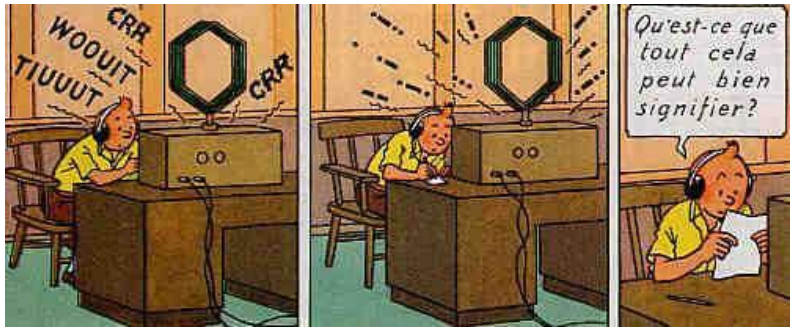
Le cryptage

- **La cryptologie :** Il s'agit d'une science mathématique comportant deux branches : la cryptographie et la cryptanalyse.

- En **cryptographie**, un algorithme de chiffrement transforme un message, appelé texte clair en un texte chiffré (cryptogramme) qui ne sera lisible que par son destinataire légitime.

- Dans la **cryptographie moderne**, les transformations en question sont des fonctions mathématiques, appelés algorithmes cryptographiques qui dépendent d'un paramètre appelé clé.

- **Cryptanalyse :** Opposée à la cryptographie, elle a pour but de retrouver le texte clair à partir de textes chiffrés en déterminant les failles des algorithmes utilisés.



Sécuriser les communications

- Il existe trois objectifs majeurs liés à la sécurisation des communications :
  - **Authentification** : L'assurance que chaque personne faisant parti de l'échange est bien celui qu'il prétend être.
  - **Intégrité** : Le but est de s'assurer que le message envoyé n'a pas été altéré de manière volontaire ou involontaire.
  - **Confidentialité** : Le but est de s'assurer que seul la personne qui est destinataire du message pourra comprendre le message.

C.I.A

Confidentialit

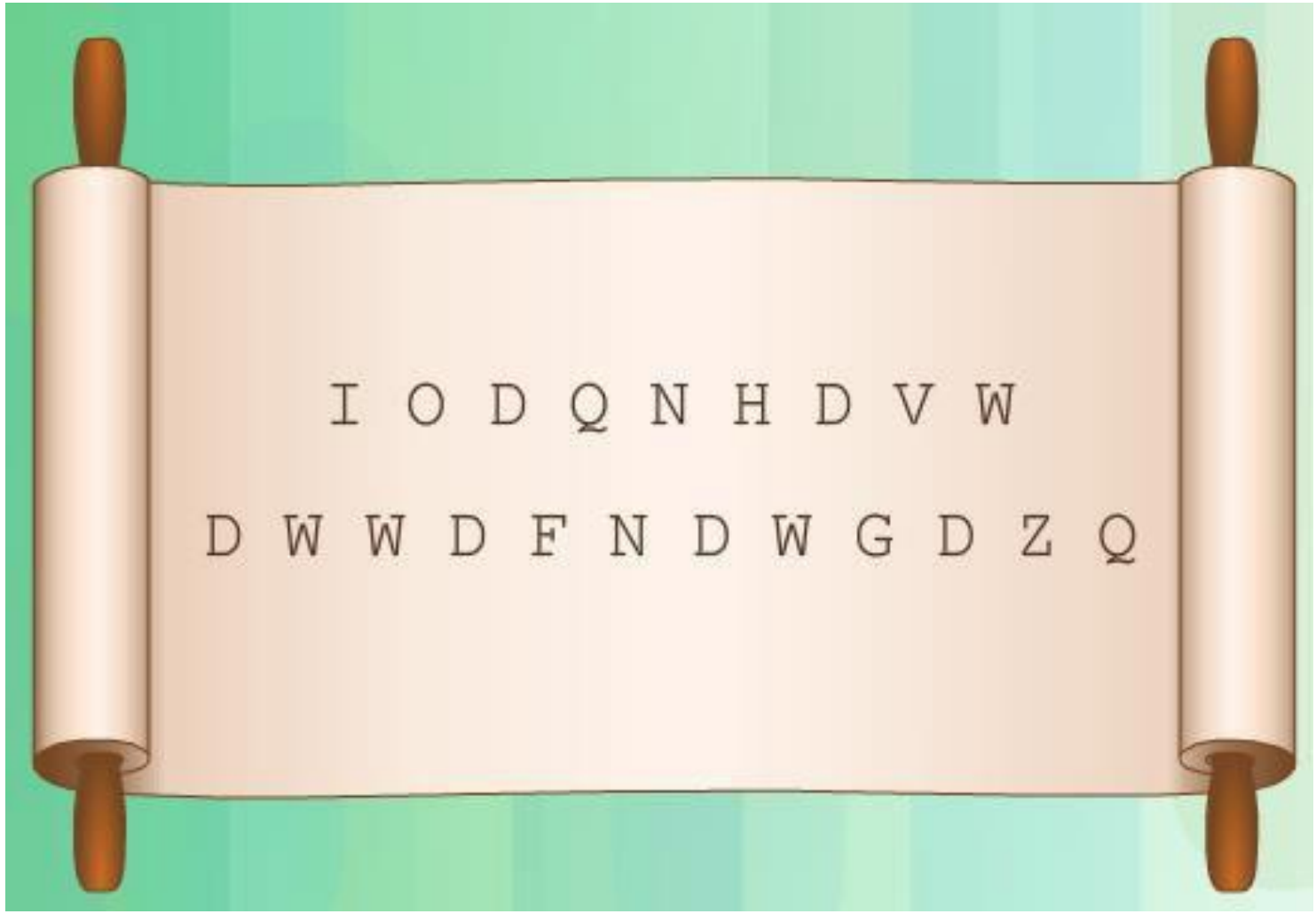
Integrity

Authenticity

L'authentification

L'integrité

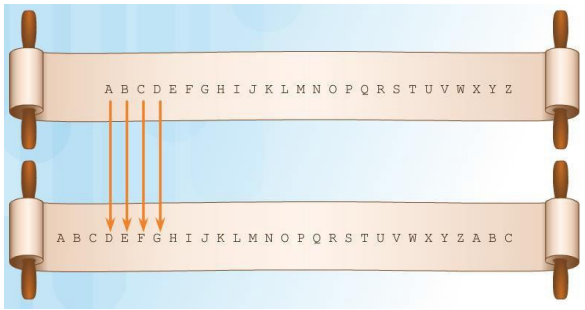
La confidentialité



Systèmes de cryptage

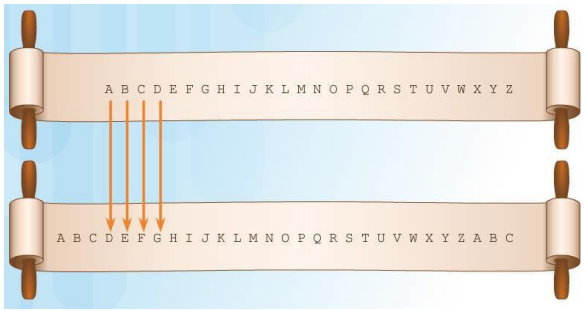
- À travers le temps, différentes méthodes de codage furent utilisées :
  - Scytale.
  - Le chiffre de César.
  - Le chiffrement de Vigenère.
  - La machine Enigma.

	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
A	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
B	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
C	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
D	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
E	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
F	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
G	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
H	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
I	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
J	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
K	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
L	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
M	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
N	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
O	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
P	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
Q	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
R	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
S	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
T	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
U	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
V	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
W	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
X	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
Y	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
Z	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



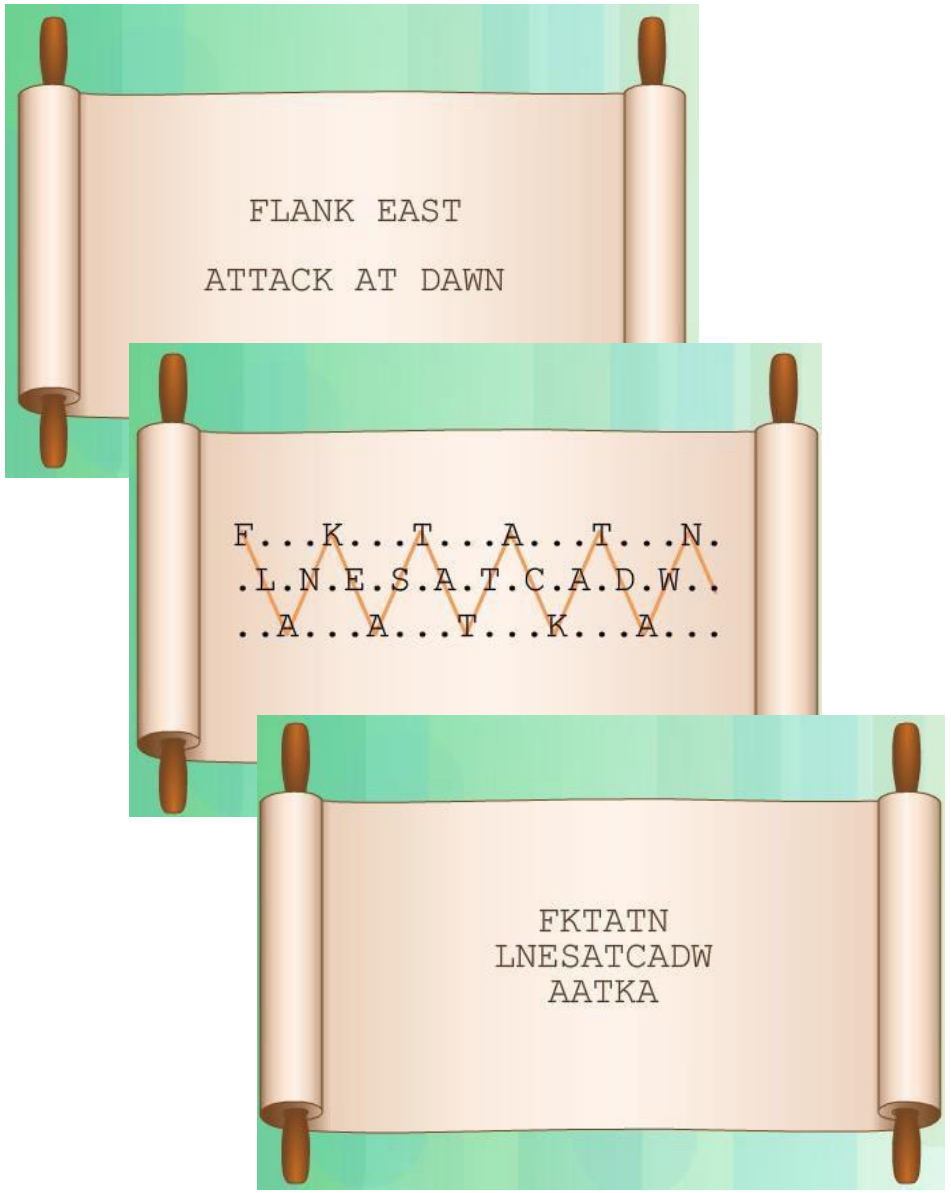
Types des systèmes de cryptage

- Toute méthode de cryptage utilise un algorithme spécifique utilisé pour chiffrer et déchiffrer les messages.
- L'algorithme de chiffrement est un ensemble d'étapes à suivre dans le cadre de chiffrement/déchiffrement de messages.
- Différentes approches peuvent être utilisées :
  - Transposition.
  - Substitution.
  - Masque jetable (One-time pad).



Chiffrement par transposition

- Un chiffrement par transposition est un chiffre qui consiste à changer l'ordre des lettres, donc à construire des anagrammes. Cette méthode est connue depuis l'Antiquité, puisque les Spartiates utilisaient déjà une scytale.
- Le chiffrement par transposition demande de découper le texte clair en blocs de taille identique.
- La même permutation est alors utilisée sur chacun des blocs.
- La clef de chiffrement est la permutation elle-même.
- Parmi les protocoles modernes, DES et 3DES utilisent tous les deux la méthode de transposition.



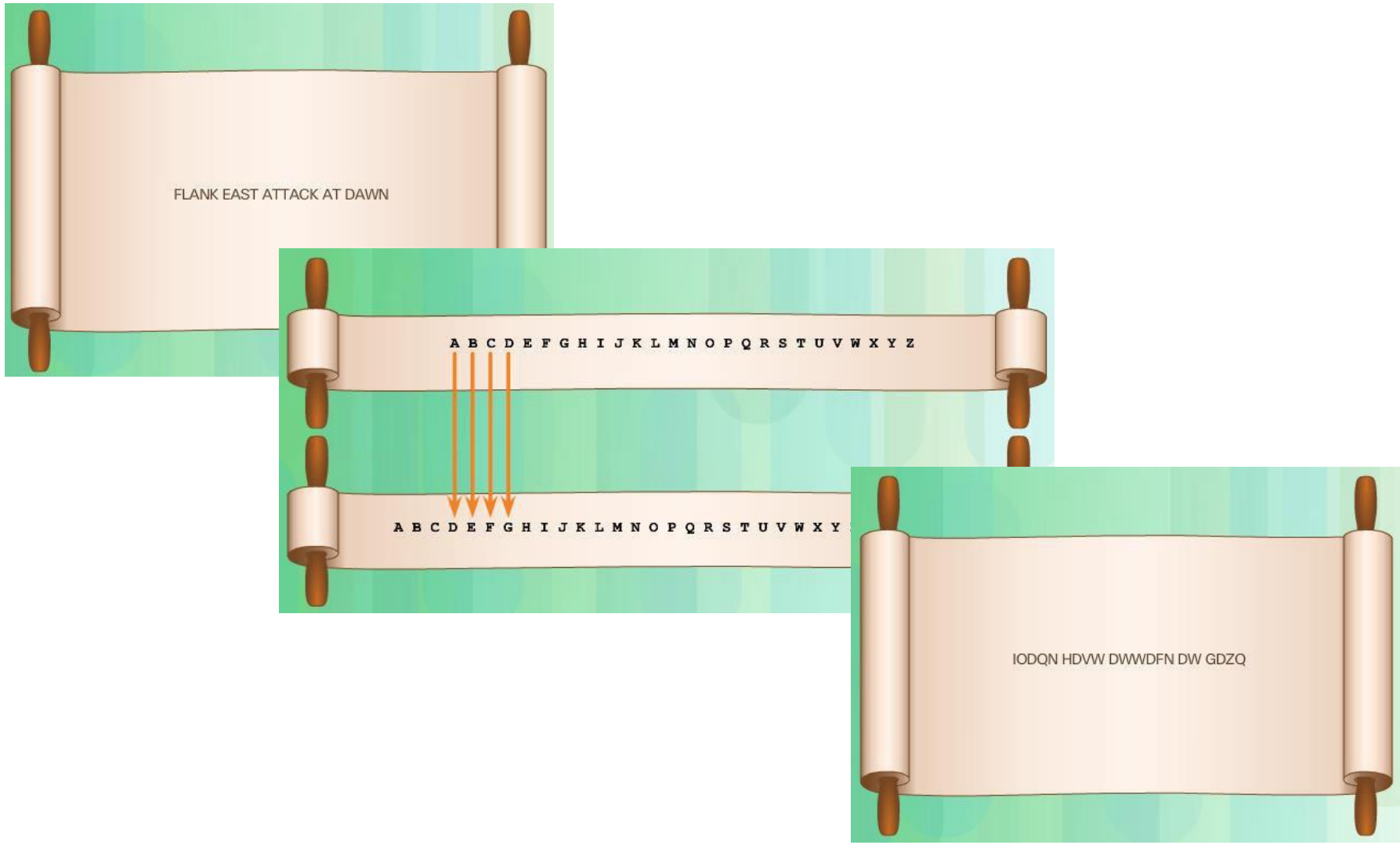
Exemple

- Chiffrer le texte « **rendez vous mercredi** » en utilisant la méthode de transposition Rail fence cipher et une clé égale à trois.

Exemple

- Déchiffrer le texte « CNTOOFNIDCIEEEDL » en utilisant la méthode de transposition Rail fence cipher et une clé égale à quatre.

Chiffrement par substitution



Le chiffre de César

- En cryptographie, le chiffrement par décalage, aussi connu comme le chiffre de César ou le code de César, est une méthode de chiffrement très simple utilisée par Jules César dans ses correspondances secrètes.
- Le texte chiffré s'obtient en remplaçant chaque lettre du texte clair original par une lettre à distance fixe, toujours du même côté, dans l'ordre de l'alphabet.
- Pour les dernières lettres (dans le cas d'un décalage à droite), on reprend au début.
- Dans le cas de l'alphabet latin, le chiffre de César n'a que 26 clés possibles (y compris la clé nulle, qui ne modifie pas le texte).
- Il s'agit d'un cas particulier de chiffrement par substitution monoalphabétique.
- Voici un exemple de rotation avec un clé égale à 13:

ROT13

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
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

Exemple

- Chiffrer le texte « **rendez vous mercredi** » en utilisant la méthode de substitution le chiffre de César avec une rotation à 13 positions.

Exemple

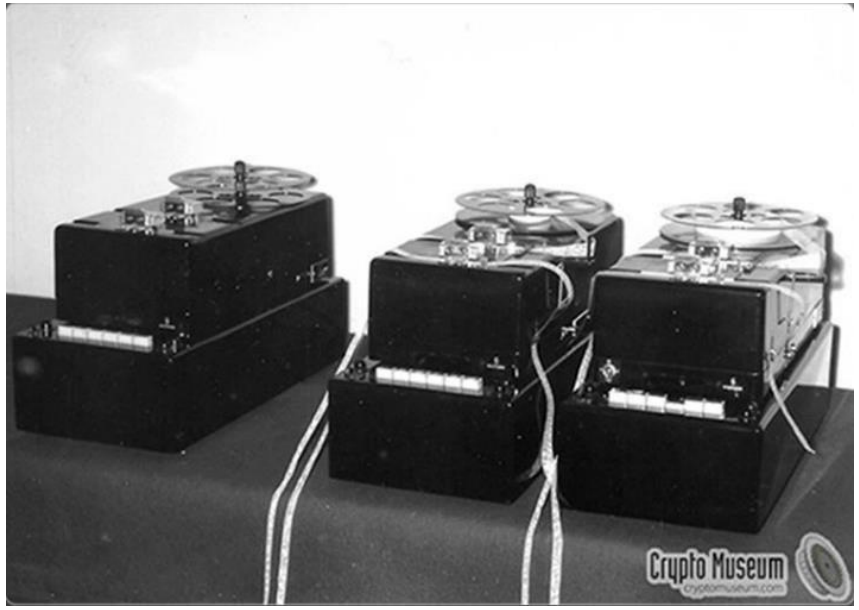
- Déchiffrer le texte « **nggndhr qvznapur zngva** » en utilisant la méthode de substitution le chiffre de César avec une rotation à 13 positions.

ROT13

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
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

Chiffrement One-Time Pad

- Le chiffrement par la méthode du masque jetable consiste à combiner le message en clair avec une clé présentant les caractéristiques très particulières suivantes :
  - La clé doit être une suite de caractères au moins aussi longue que le message à chiffrer.
  - Les caractères composant la clé doivent être choisis de façon totalement aléatoire.
  - Chaque clé, ou « masque », ne doit être utilisée qu'une seule fois (d'où le nom de *masque jetable*).
- L'intérêt considérable de cette méthode de chiffrement est que si les trois règles ci-dessus sont respectées strictement, le système offre une sécurité théorique absolue.



Exemple

- Chiffrer le texte « **KO** » en utilisant la clé suivante :

  0 1 0 0 1 0 0 0 1 0 0 0 1 0

Opération XOR

A	*B*	$C = A \oplus B$
0	0	0
0	1	1
1	0	1
1	1	0

Exemple

- Déchiffrer le texte

« **UHv** » en utilisant la clé :

01000000100001000000110

Opération XOR

A	*B*	$C = A \oplus B$
0	0	0
0	1	1
1	0	1
1	1	0

Contenu du chapitre

- Introduction
- Services de la cryptographie
- **Les bases de l'intégrité et de l'authenticité.**
- La confidentialité
- La cryptographie à clé publique

Cracker le code

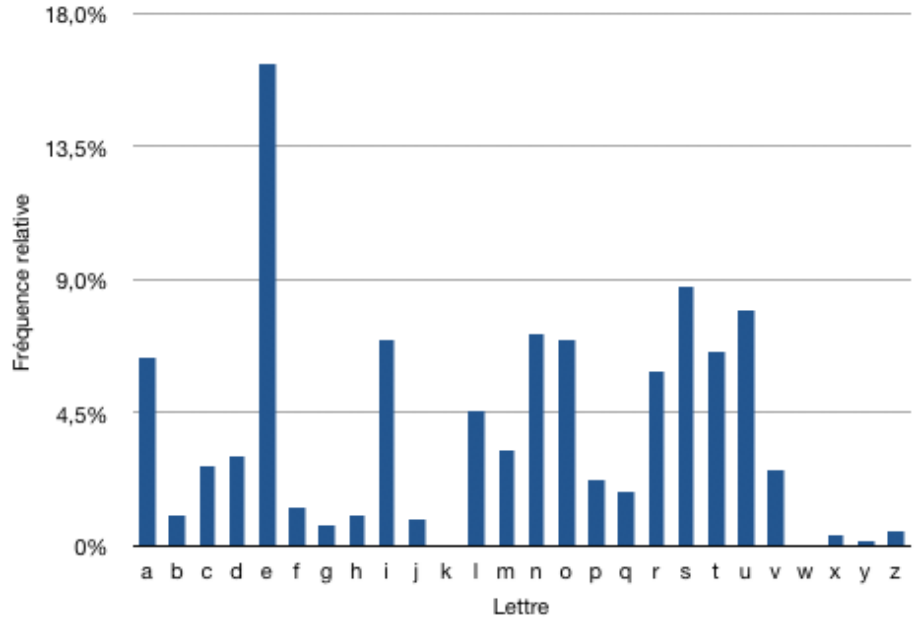
- Pendant que la cryptographie évoluait, la cryptanalyse faisait de même.
- La cryptanalyse est la pratique qui consiste à chercher à déchiffrer un message sans aucune connaissance de la clé secrète utilisée pour le chiffrement.

Méthodes pour faire cracker le code

Méthodes utilisées pour la cryptanalyse :

- Méthode par force brute.
- Méthode de texte chiffré.
- Méthode de texte en clair connu.

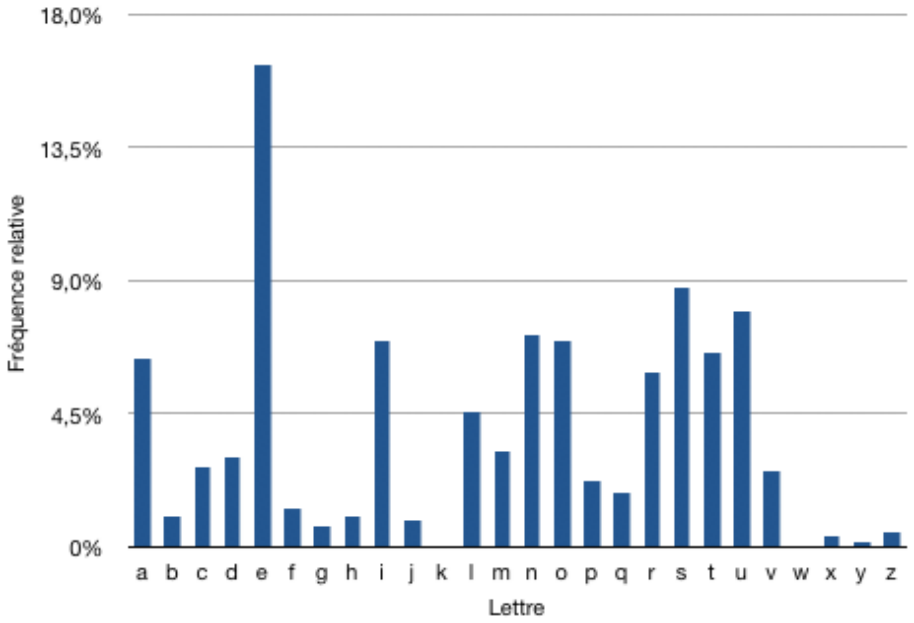
Méthodes pour faire cracker le code



- *Analyse fréquentielle des alphabets de la langue française*

- *Déchiffrer en utilisant L'analyse fréquentielle*

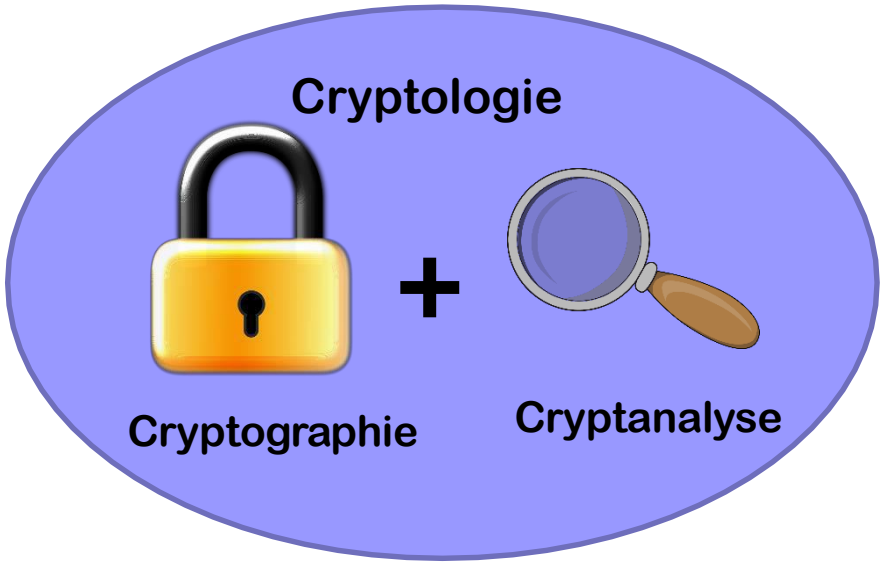
wr frenv yn onf qrznva fbve



BWDDC YASWY WDTWD CTIHX DZWDS UHBWD NWYWI
SVGWD UXSDZ WDXHC DIXID WIUWU WZXMX TIXPW UXSDC
GIYWB WYWTS WUWTI AWDIX GJZWU CTDWG JUWUW
DVGWB BWDDW BSMYW TICFF YXTIB NCUUX PWZWB WGYDA
CYHDW IZWBW GYDXU WDWID SBWTW DIXST DSXGT SMWXG
ZWBXF XGIWH CGYVG CSTWT DWYXS ISBHX DXSTD SXGTS
MWXGZ GANXI SUWTI STFWY TXBTC GDXMC TDYWA WUUWT
IXHHY SDXMW AIYSD IWDDW VGGTA WYIXS TTCUT YWZWH
WYDCT TWDZW DZWGJ DWJWD CGTBS WGDWD ZWBWG
YDXBG IWIAC TIYXS YWUWT IXBXF CSAXI NCBSV GWDWD
CTIZC TTWDX GJZWU CTDDC GDBXF CYUWD ZSTAG TWDWI
ZWDGA AGTWD WIHXY BWGYD STAXT IXISC TDDCY IDAYS
UWDWI XAISC TDSTF XUXTI WDZWI YGSDW TIBWF YGSIZ
WDWTI YXSBB WDZWD FWUUW DZWDI YCGHW XGJZW
ZSMWY DXTSU XGJFC TIUCG YSYBW TBWBX MCSTW ZWASU
WTIBW DYWAC BIWDT XHHCY IWTIV GWZCG BWGYD WIXFF
BSAIS CTDWU HWANW TIBWD NCUUW DZWHY CAYWW
YWIBW DFWUU WDZWA CTAWM CSY

Cryptologie

- La **cryptologie** est la science à créer et à faire cracker des codes secrets.
- Cryptographie : développement et utilisation des codes secrets.
- Cryptanalyse : Faire craquer ces codes.



Un secret : la clé

- Dans le monde des communications réseaux, l'implémentation de l'authentification, l'intégrité et la confidentialité est assurée par différents protocoles et algorithmes.
- Auparavant, la réussite d'un système de chiffrement était basée sur le fait de tenir au secret l'algorithme utilisé.
- Avec les technologies modernes, déchiffrer suppose une connaissance de la clé de cryptage.
- Autrement dit, l'enjeu aujourd'hui est de garder secret la clé de cryptage.

Integrity	Authentication	Confidentiality
MD5	HMAC-MD5	DES
SHA	HMAC-SHA-1	3DES
	RSA and DSA	AES

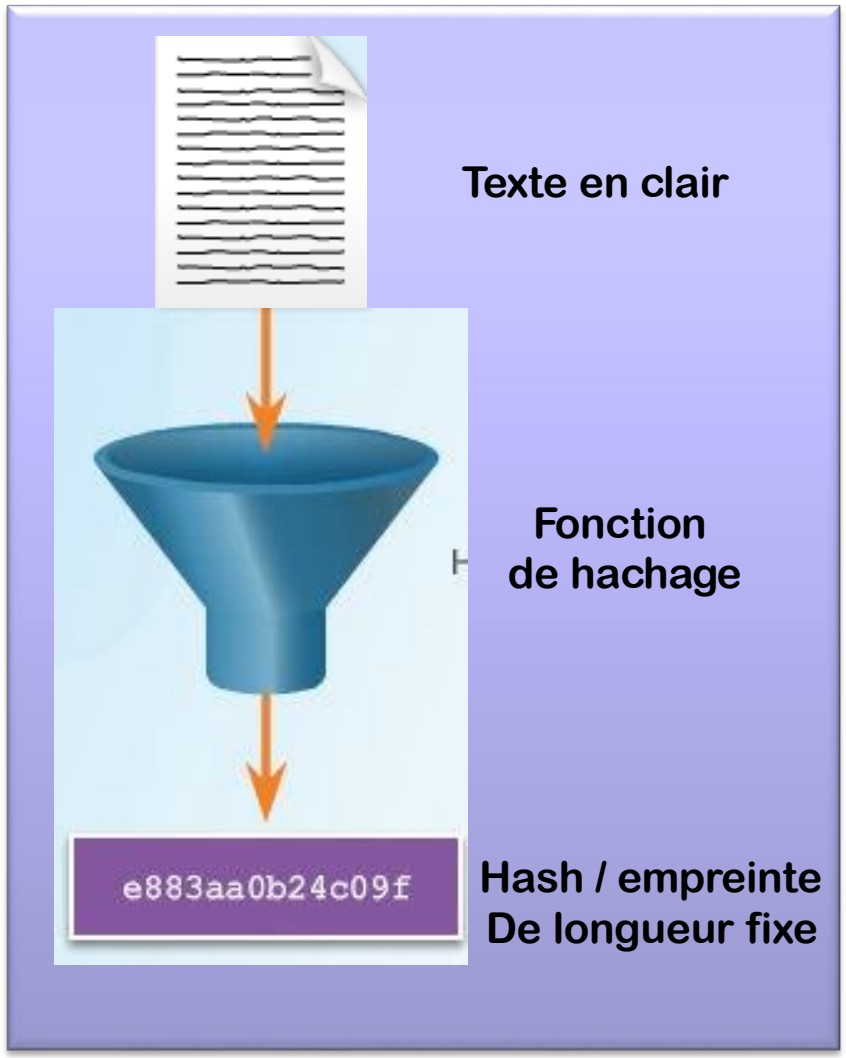
Contenu du chapitre

- Introduction
- Services de la cryptographie
- **Les bases de l'intégrité et de l'authenticité.**
- La confidentialité
- La cryptographie à clé publique

Les fonctions d'intégrité

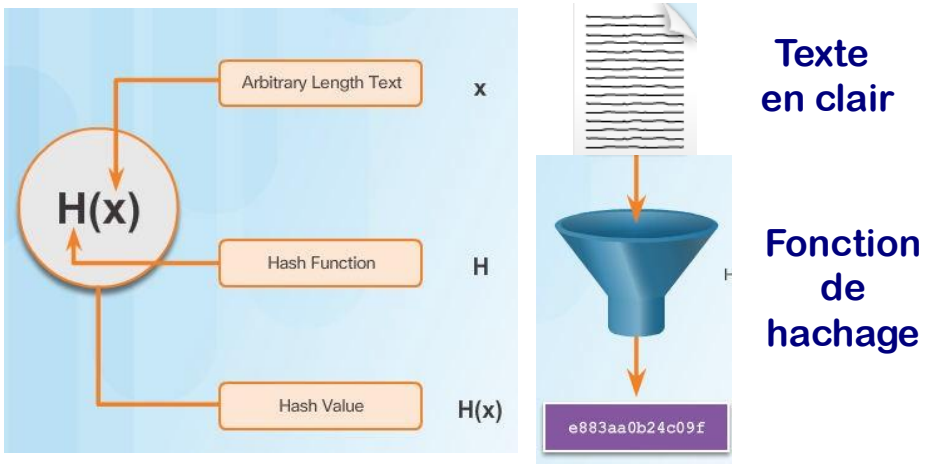
Fonctions de hachage

- La hachage est utilisé pour assurer l'intégrité des données.
- Une fonction de hachage est une fonction à sens unique qui va calculer une empreinte (ou signature) unique à partir des données fournies.
- Le hash a une longueur fixe.



Propriétés des fonctions de hachage

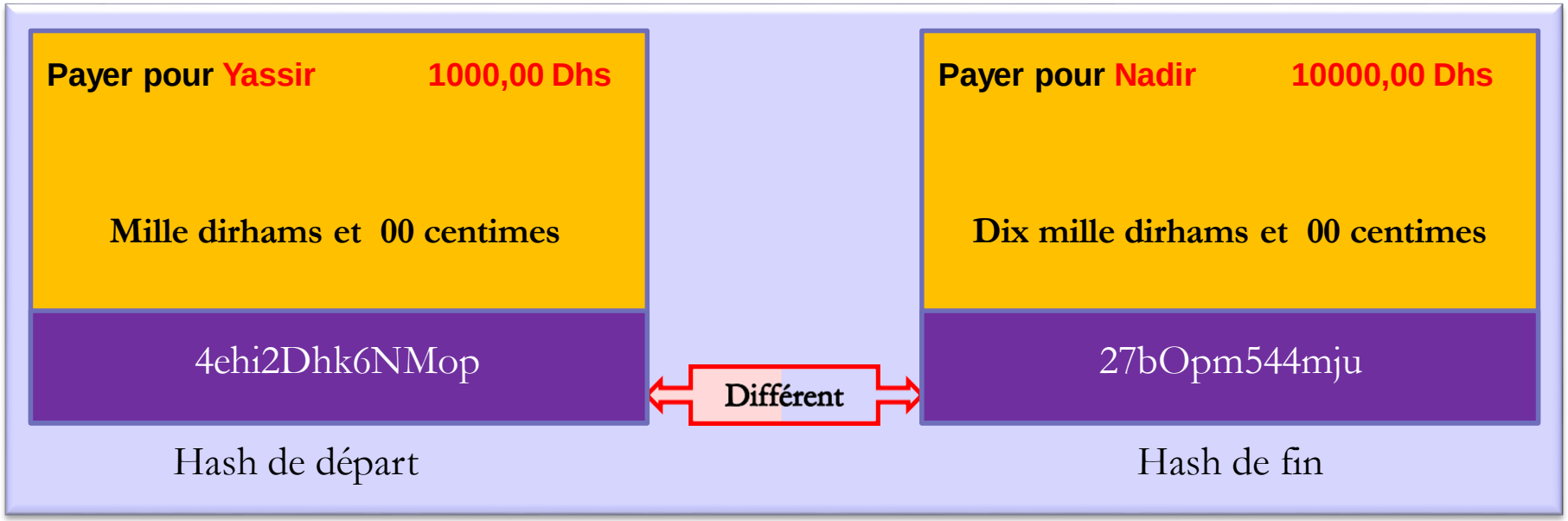
- La longueur de la signature doit être toujours la même.
- Il n'est pas possible de trouver les données originales à partir des empreintes : Les fonctions de hachage ne fonctionnent que dans un seul sens.
- Il ne doit pas être possible de prédire une signature.
- Et enfin, évidemment pour des données différentes : les signatures doivent être différentes (Pas de collision).
- Fonctions de hachage connues : MD5, SHA-2 …



Texte en clair

Fonction de hachage

Fonctions du hachage

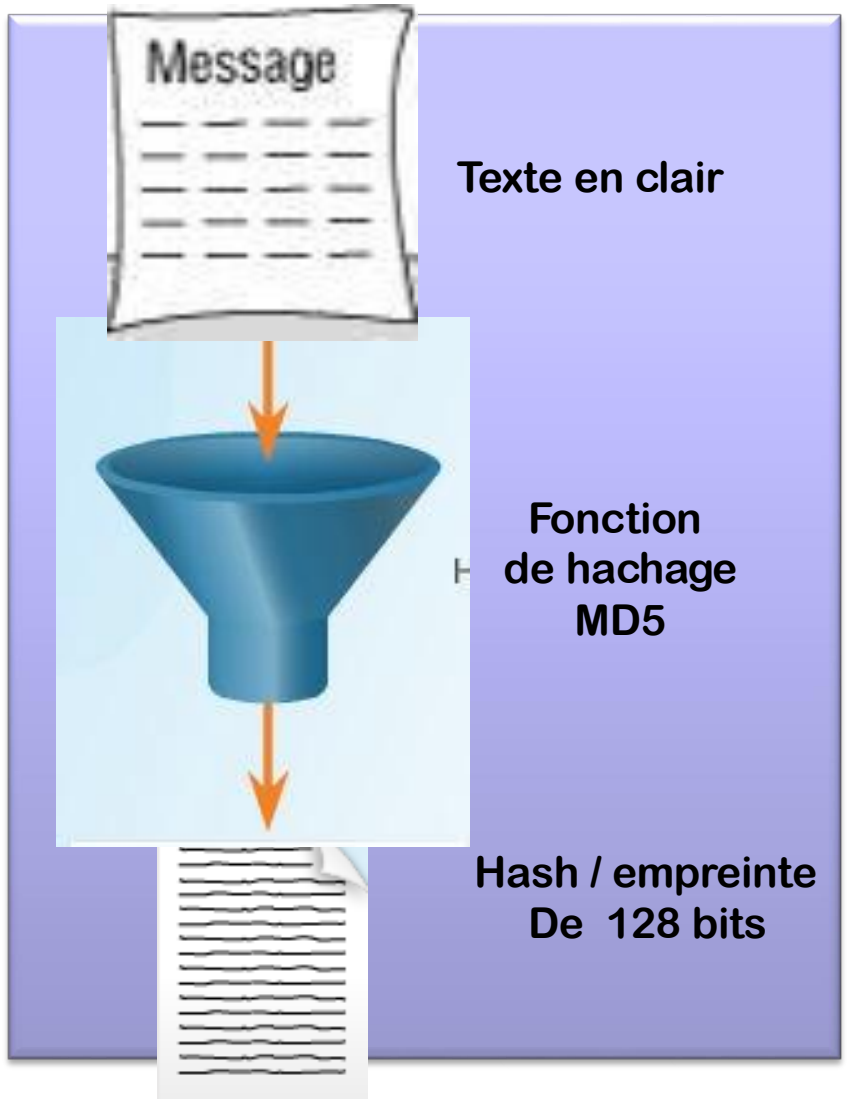


Exemples de hashage en MD5

Données en entrée	Signature
123	202cb962ac59075b964b07152d234b70
124	c8ffe9a587b126f152ed3d89a146b445
1234	81dc9bdb52d04dc20036dbd8313ed055
12345678901234567890123456789O	a46857f0ecc21f0a06ea434b94d9cf1d
abcde	ab56b4d92b40713acc5af89985d4b786
abcdef	e80b5017098950fc58aad83c8c14978e

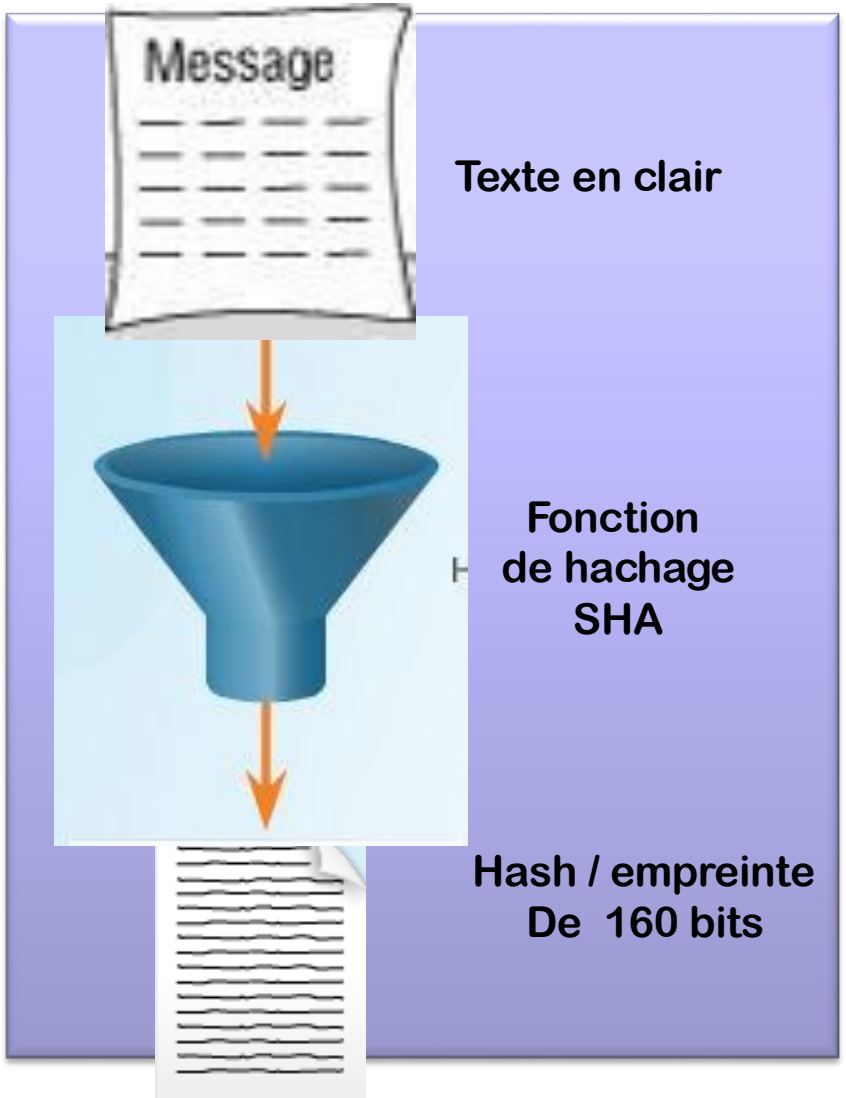
La fonction de hachage MD5

- L'algorithme **MD5**, pour **Message Digest 5**, est une fonction de hachage cryptographique qui permet d'obtenir l'empreinte numérique d'un message.
- Il a été inventé par Ronald Rivest en 1991.
- MD5 est une fonction à sens unique avec une séquence complexe d'opérations binaires; essentiellement de la rotation et du ou exlusif (XOR).
- Cela rend le calcul d'un texte clair à base d'un hash très difficile.
- Le produit est un hach de 128 bits.
- Aujourd'hui, la sécurité du MD5 n'étant plus garantie selon sa définition cryptographique, les spécialistes recommandent d'utiliser des fonctions de hachage plus récentes comme le SHA-256.

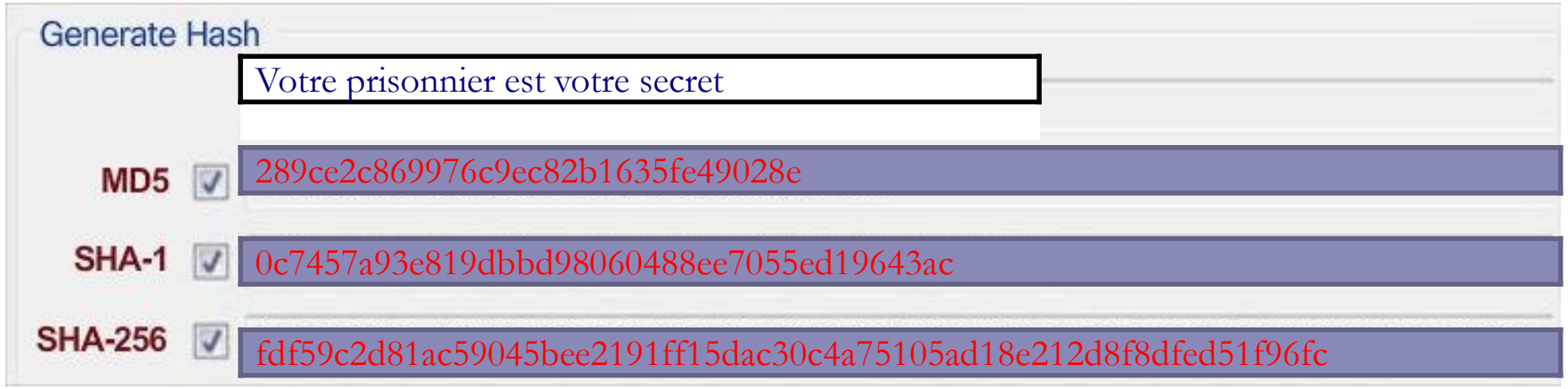


La fonction de hachage SHA

- **SHA-1** (*Secure Hash Algorithm*) est une fonction de hachage cryptographique conçue par la *National Security Agency* des États-Unis (NSA).
- Elle produit un hash (*condensat*) de 160 bits.
- SHA-1 n'est plus considéré comme sûr contre des adversaires disposant de moyens importants.
- En 2005, des cryptanalystes ont découvert des attaques sur SHA-1.
- Depuis 2010, de nombreuses organisations ont recommandé son remplacement par SHA-2.
- SHA2 comporte les fonctions **SHA-256** et **SHA-512** dont les algorithmes sont similaires mais opèrent sur des tailles de mot différentes.
- Le dernier suffixe indique le nombre de bits du haché.



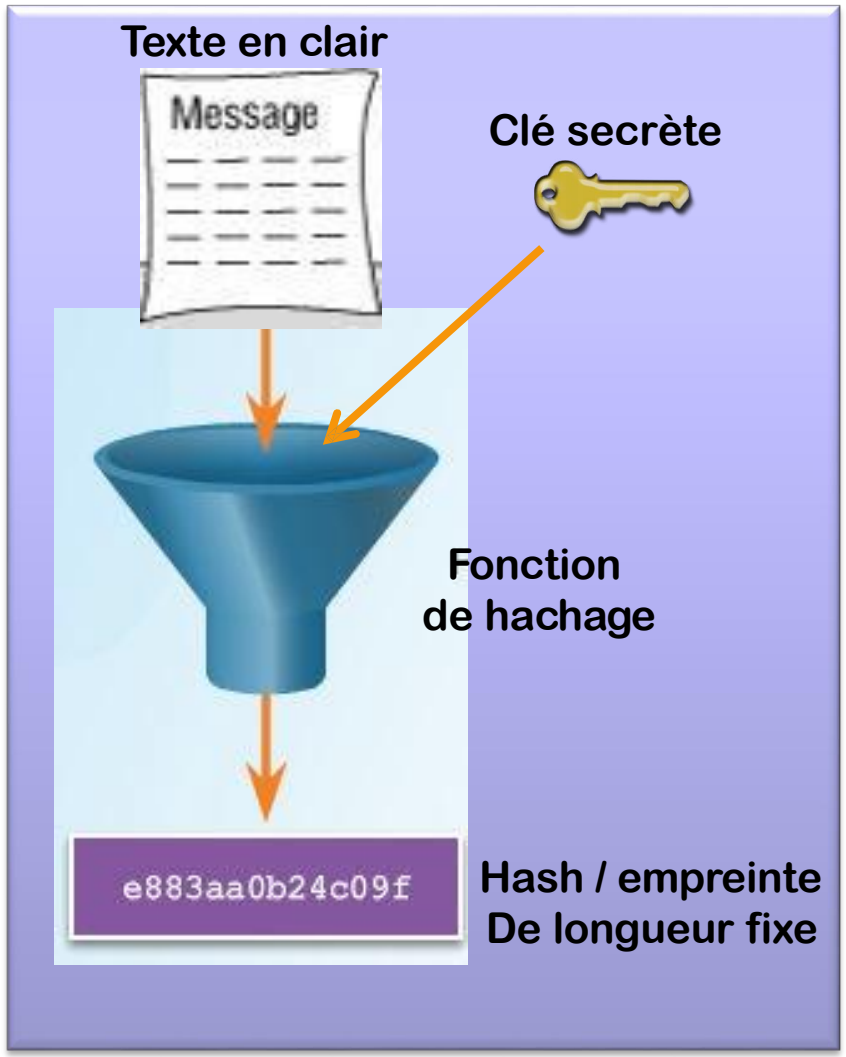
Md5 Vs SHA


Generate Hash
Votre prisonnier est votre secret
MD5
289ce2c869976c9ec82b1635fe49028e
SHA-1
0c7457a93e819dbbd98060488ee7055ed19643ac
SHA-256
fdf59c2d81ac59045bee2191ff15dac30c4a75105ad18e212d8f8dfed51f96fc

Intégrité et/ou authenticité

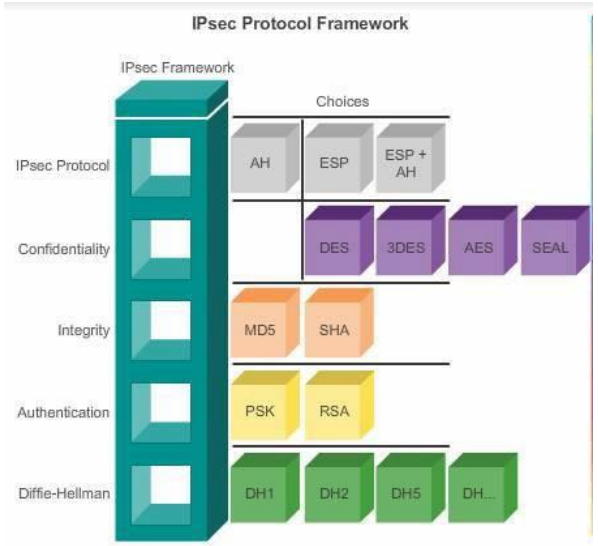
Keyed-Hash Message Authentication Code

- Un code d'authentification de message (MAC, *Message Authentication Code*) est un code accompagnant des données dans le but d'assurer l'intégrité mais aussi l'authenticité.
- Le MAC assure non seulement une fonction de vérification de l'intégrité du message, comme le permettrait une simple fonction de hachage mais de plus authentifie l'expéditeur, détenteur de la clé secrète.
- Le HMAC est calculé en ajoutant aux données en entrée une clé secrète.
- La clé secrète doit être partagée uniquement entre l'émetteur et le récepteur.
- Ces deux technologies utilisées les fonctions de hachage bien connues :
  - Keyed MD5 (HMAC-MD5).
  - Keyed SHA-1 (HMAC-SHA-1).
- HMAC sont parfois appelées signatures numériques.



Utilisations du hachage

- Configuration de l'authentification des protocoles de routage.
- Configuration de l'authentification CHAP entre deux pairs qui communiquent par le protocole PPP.
- Configuration des passerelles et des clients IPsec.
- Téléchargement de fichiers sur Internet.

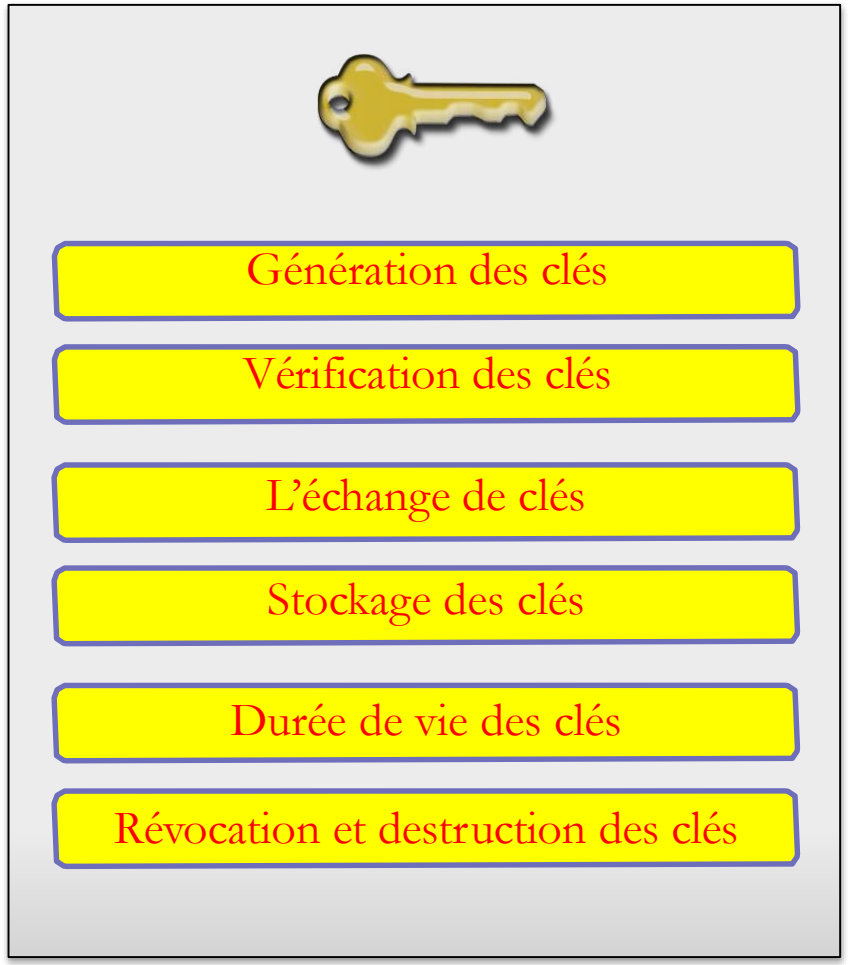


File Name ↓
Parent directory/
MD5SUMS
MD5SUMS.sign
SHA1SUMS
SHA1SUMS.sign
SHA256SUMS
SHA256SUMS.sign
SHA512SUMS
SHA512SUMS.sign
debian-live-8.6.0-i386-cinnamon-desktop.iso
debian-live-8.6.0-i386-cinnamon-desktop.iso.con..>
debian-live-8.6.0-i386-cinnamon-desktop.iso.log
debian-live-8.6.0-i386-cinnamon-desktop.iso.pac..>

Gestion des clés

Caractéristiques de la gestion des clés

- La gestion des clés est la partie la plus délicate dans un cryptosystème.
- Beaucoup de cryptosystèmes ont craqués à cause de faiblesses dans la gestion des clés.
- Pratiquement, la majorité des attaques ciblent le niveau de gestion des clés plutôt que l'algorithme de cryptage lui- même.



Longueur de clé et espace de clés

- Deux termes sont utilisés pour décrire les clés :
  - Longueur de la clé : appelé aussi taille de la clé, c'est une mesure du nombre de clés.
  - Espace de clés : correspond au nombre de possibilités qui peuvent être générées selon une longueur de clé spécifique.
- Autant que la longueur de le clé est incrémentée, l'espace de clés incrémente exponentiellement.

Caractéristiques de AES	
Description	Advanced Encryption Standard
Chronologie	Standard officiel depuis 2001
Type d'algorithme	Symétrique
Vitesse	Élevée
Taille de la clé	128, 192 et 256 bits
Temps pour cracker (ordinateur capable de tester 255 clés par seconde)	149 trillions d'années
Consommation des ressources	Faible

L'espace de clés

- L'espace de clés d'un algorithme est le jeu de toutes valeurs possibles.
- Une clé d'une taille de n bits donne 2^n valeurs possibles.
- L'ajout d'un seul bit double l'espace de clés, et par conséquent un attaquant a besoin d'un temps double pour parcourir l'espace de clés.
- Tout espace de clé possède de faibles clés.

Note : des clés longues sont plus sécurisées mais exigent plus de ressources.

DES Key	Keyspace	# of Possible Keys
56-bit	2^{56} 11111111 11111111 11111111 11111111 11111111 11111111 11111111	72,000,000,000,000,000
57-bit	2^{57} 11111111 11111111 11111111 11111111 11111111 11111111 11111111 1	144,000,000,000,000,000
58-bit	2^{58} 11111111 11111111 11111111 11111111 11111111 11111111 11111111 11	288,000,000,000,000,000
59-bit	2^{59} 11111111 11111111 11111111 11111111 11111111 11111111 11111111 111	576,000,000,000,000,000
60-bit	2^{60} 11111111 11111111 11111111 11111111 11111111 11111111 11111111 1111	1,152,000,000,000,000,000

Types de clés cryptographiques

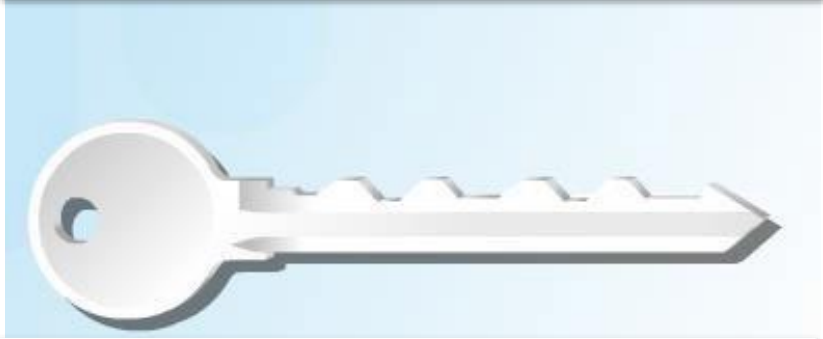
- Différents types de clés peuvent être générées :
  - Clés symétriques.
  - Clés asymétriques.
  - Signatures numériques.
  - Clés hachées.
- Quelque soit le type de clé, certaines caractéristiques sont toujours les mêmes :
  - Définition d'un taille de clé lors de la génération.
  - Lorsqu'il s'agit d'un cryptosystème de confiance, le seul moyen d'attaque possible est l'attaque par force-brute.
  - Ceci nous pousse à chercher à avoir un espace de clés assez large.

	Clé symétrique	Clé asymétrique	Signature numérique	Hash
Protection jusqu'à 3 ans	80	1248	160	160
Protection jusqu'à 10 ans	96	1776	192	192
Protection jusqu'à 20 ans	112	2432	224	224
Protection jusqu'à 30 ans	128	3248	256	256
Protection contre les ordinateurs quantiques	256	15424	512	512

Choix des clés cryptographiques

- Les performances est un des paramètres qui peut influencer le choix de la longueur d'un clé.
- L'administrateur doit chercher un équilibre entre la vitesse du traitement et une longueur de clé assurant la robustesse de l'algorithme.
- Un autre point à évaluer est l'investissement d'un attaquant par rapport au bien visé.
- En moyenne, un attaquant doit parcourir la moitié de l'espace des clés pour retrouver la clé correcte.
- Le temps de recherche demandé dépends de la puissance des ordinateurs utilisés.

Des clés d'une longueur courte :
traitement rapide, mais moins sécurisé



Des clés d'une taille plus grande :
traitement lent, mais plus sécurisé

Contenu du chapitre

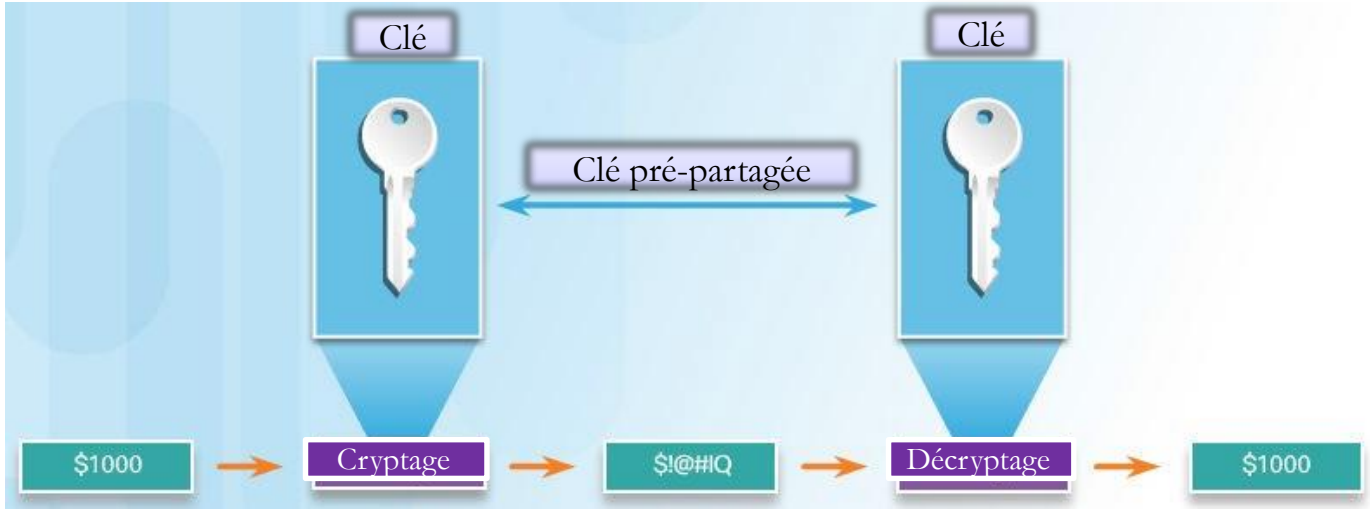
- Introduction
- Services de la cryptographie
- Les bases de l'intégrité et de l'authenticité.
- **La confidentialité**
- La cryptographie à clé publique

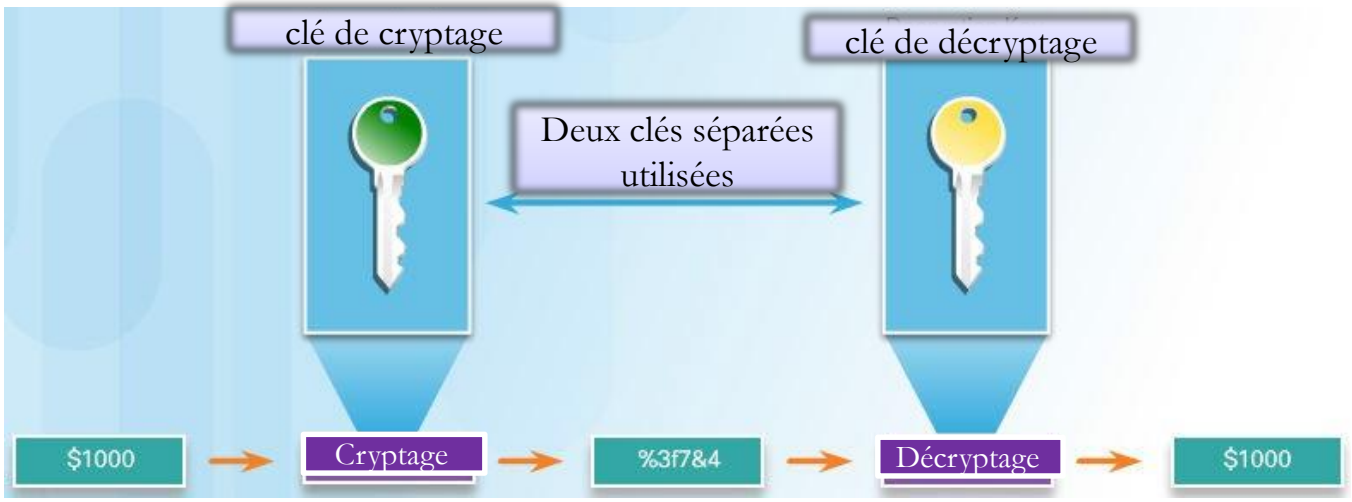
Classification des algorithmes de cryptage

- Dans la cryptographie moderne, tous les algorithmes sont publiques.
- La sécurité des données est donc liée au secret de la clé.
- La clé est donc une séquence de bits qui est introduite dans un algorithme de cryptage à l'image des données elles même.
- Il existe deux classes d'algorithmes de cryptages :
  - Algorithme de cryptage symétrique.
  - Algorithme de cryptage symétrique.

Algorithme de cryptage symétrique	Algorithme de cryptage asymétrique
Connu aussi sous le nom d'algorithme à clé pré-partagée et	Mieux connu sous le nom d'algorithmes à clé publique.
Longueur de clé courante entre 80 et 256 bits.	La longueur de clé courante entre 512 et 4096 bits.
L'émetteur et le récepteur doivent partager la clé secrète	L'émetteur et le récepteur ne partagent pas la clé secrète
Des algorithmes généralement très rapide basé sur de simples opérations mathématiques.	Des algorithmes relativement lents basé sur des calculs complexes.
Exemples : DES, 3DES, AES, IDEA, RC2/4/5/6, blowfish …	Exemples : RSA, ElGamal, Elliptic et Diffie-Hellman

Cryptage sysmétrique et asymétrique





Cryptage symétrique

- Le cryptage symétrique ou cryptage à clé secrété est le type de cryptage les plus utilisé parce que la longueur courte de la clé favorise la rapidité de l'exécution.
- Un autre point, est que le crypatge symétrique est basé sur de simples opérations mathématiques qui peuvent être améliorées par le matériel.
- Le chalenge pour le cryptage symétrique est l'échange de la clé secrète qui doit être connue à la fois par l'émetteur et le récepteur.

Symmetric Encryption Algorithm	Key Length (in bits)
DES	56
3DES	112 and 168
AES	128, 192, and 256
Software Encryption Algorithm (SEAL)	160
The RC series	RC2 (40 and 64) RC4 (1 to 256) RC5 (0 to 2040) RC6 (128, 192, and 256)

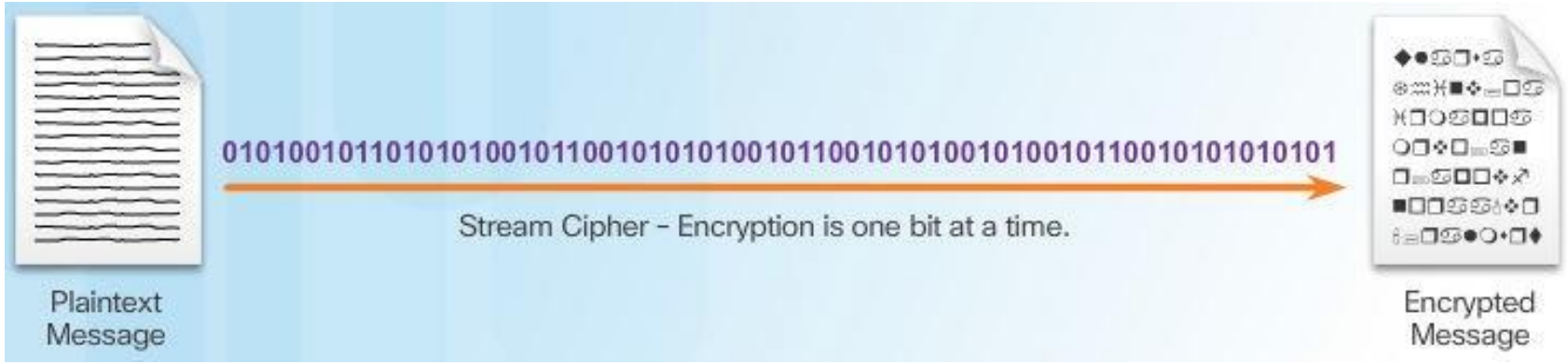
- Le cryptage symétrique utilise principalement deux méthodes différentes : cryptage par bloc et le cryptage de flot.

Cryptage symétrique : cryptage par bloc

- Un algorithme de chiffrement par bloc (Block Cipher) transforme des blocs de données de taille fixe en bloc de données chiffrées de la même taille.
- Il consiste en un découpage des données en blocs de taille généralement fixe.
- Les blocs font généralement 128 bits, mais ils peuvent aller de 32 à 256 bits selon l'algorithme.
- Les blocs sont ensuite chiffrés les uns après les autres.
- L'exemple de DES qui utilise des blocs de 64 bits et AES qui se base sur des blocs de 128 bits.

Cryptage symétrique : Cryptage par flot

- Un algorithme de chiffrement par flux (stream cipher) est un algorithme agissant en continu sur les données.
- Il ne nécessite pas d'avoir toutes les données pour commencer à chiffrer, le chiffrement de flux agit sur chaque bit, l'un après l'autre.
- Ce type de chiffrement est souvent utilisé pour les communications en temps réel telles que le WI-FI (RC4), puisqu'il a la particularité d'être beaucoup plus rapide que n'importe quel algorithme de chiffrement par bloc.
- Un algorithme de flux fonctionne avec ce que l'on appelle un générateur pseudo-aléatoire (keystream en anglais), c'est une séquence de bits précise utilisée en tant que clé. Le chiffrement se fait par la combinaison du keystream et du message, le plus souvent par une opération XOR (OU exclusif).



Choix d'un algorithme de cryptage

- Le choix d'un algorithme de cryptage est une décision cruciale pour un administrateur lors de la mise en œuvre de cryptosystème.
- Les deux éléments principaux suivants sont à prendre en compte :
  - L'algorithme de cryptage est approuvé par la communauté de cryptographie.
  - L'algorithme protège adéquatement contre l'attaque par force-brute.
- Deux autres point peuvent être vérifier :
  - L'algorithme supporte des tailles variables et suffisamment longues pour l'évolutivité.
  - L'algorithme ne possède pas de limites d'importation/exportation dans le cas d'une utilisation internationale.

	DES	3DES	AES
L'algorithme est approuvé par la communauté de cryptographie.	Remplacé par 3DES	Oui	En cours d'évaluation (recommandé)
L'algorithme protège adéquatement contre l'attaque par force-brute.	Non	Oui	Oui

Algorithme DES

- Algorithme de cryptage symétrique par bloc hérité.
- L'algorithme DES transforme un bloc de 64 bits en un autre bloc de 64 bits.
- Il manipule des clés individuelles de 56 bits, représentées par 64 bits (avec un bit de chaque octet servant pour le contrôle de parité).
- Il s'agit essentiellement d'une séquence de permutations et de substitutions sur les bits de données à l'aide de la clé de cryptage.

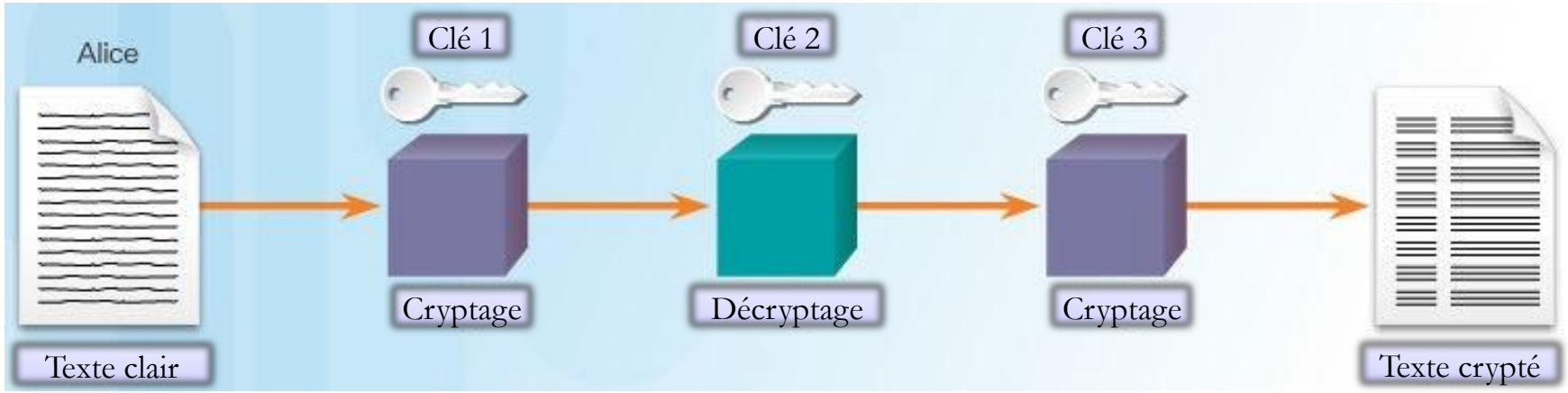
Caractéristiques de DES	
Description	Data Encryption Standard
Chronologie	Standarisé en 1976
Type d'algorithme	Symétrique
Taille de la clé	56 bits
Vitesse	Moyenne
Temps pour cracker (ordinateur capable de tester 255 clés par seconde)	Days (6,4 jours par la machine COPACABANA)
Consommation des ressources	Moyenne

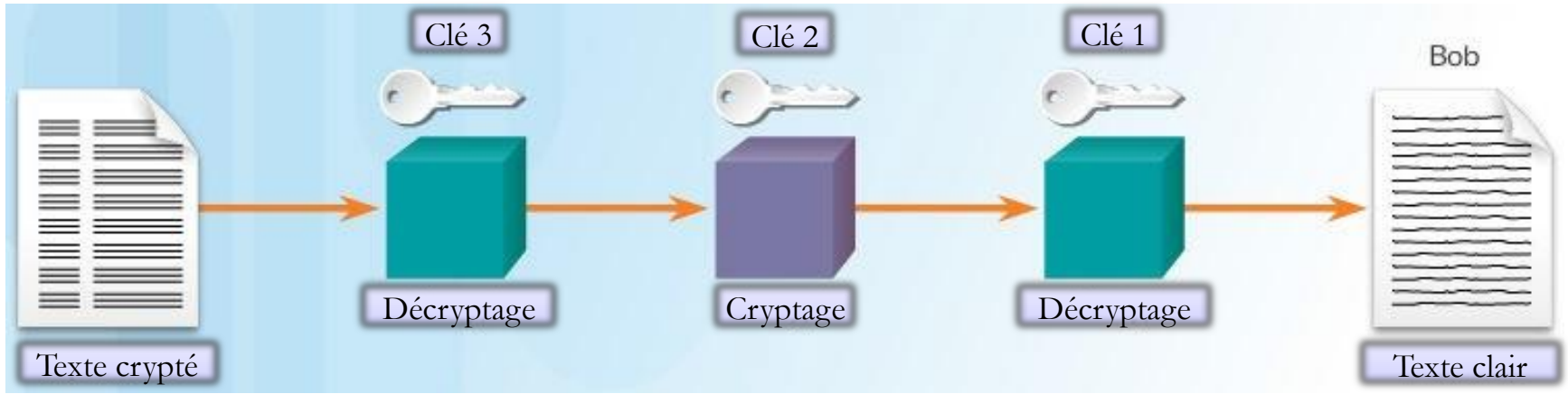
Algorithme 3DES

- Le **Triple DES** (**3DES**) est un algorithme de chiffrement symétrique par bloc, enchaînant 3 applications successives de l'algorithme DES sur le même bloc de données de 64 bits, avec 2 ou 3 clés DES différentes.
- La procédure 3DES-EDE améliore la sécurité du fait qu'elle utilise un chiffrement, suivi d'un déchiffrement pour se conclure à nouveau par un chiffrement.
- 3DES est un algorithme sécurisé mais il consomme des ressources et il est relativement lent, c'est pour ça qu'on a développé AES.

Caractéristiques de 3DES	
Description	Triple Data Encryption Standard
Chronologie	Standarisé en 1977
Type d'algorithme	Symétrique
Vitesse	Lent
Taille de la clé	112 et 168 bits
Temps pour cracker (ordinateur capable de tester 255 clés par seconde)	4,6 billions d'années avec la technologie actuelle
Consommation des ressources	Moyenne

Opérations 3DES





Algorithme AES

- L'AES (Advanced Encryption Standard) est un standard de cryptage symétrique destiné à remplacer le DES qui est devenu trop faible au regard des attaques actuelles.
- Historiquement, le développement de l'AES a été instigué par le NIST (National Institue of Standards and Technology) le 2 janvier 1997.
- L'algorithme a été choisi il y a peu de temps : il s'agit de l'algorithme Rijndael.
- l'AES est un standard, donc libre d'utilisation.
- c'est un algorithme de chiffrement symétrique par blocs.
- il supporte différentes combinaisons [longueur de clé]-[longueur de bloc] : 128-128, 192-128 et 256-128 bits.
- AES est jugé consommant moins de ressources que DES et 3DES.

Algorithme AES

Caractéristiques de AES	
Description	Advanced Encryption Standard
Chronologie	Standard officiel depuis 2001
Type d'algorithme	Symétrique
Vitesse	Élevée
Taille de la clé	128, 192 et 256 bits
Temps pour cracker (ordinateur capable de tester 255 clés par seconde)	149 trillions d'années
Consommation des ressources	Faible

L'échange de clés Diffie-Hellman

- En cryptographie, l'**échange de clés Diffie-Hellman**, du nom de ses auteurs Whitfield Diffie et Martin Hellman, est une méthode automatique d'échange de clés.
- Il ne s'agit pas d'une méthode de cryptage de données.
- Dans un système de cryptage symétrique, les deux extrémités en communication doivent posséder une clé identique.
- Réussir à partager cette clé est un vrai challenge.
- DH est un algorithme mathématique qui permet à deux pairs de générer une clé identique.
- À l'issue de cette génération les deux pairs seront en mesure de crypter les données échangées.
- DH est utilisé dans l'échange de données dans le cas d'un VPN IPSec, et aussi dans le cas d'échange sur Internet à base de SSL ou TLS.

Diffie-Hellman

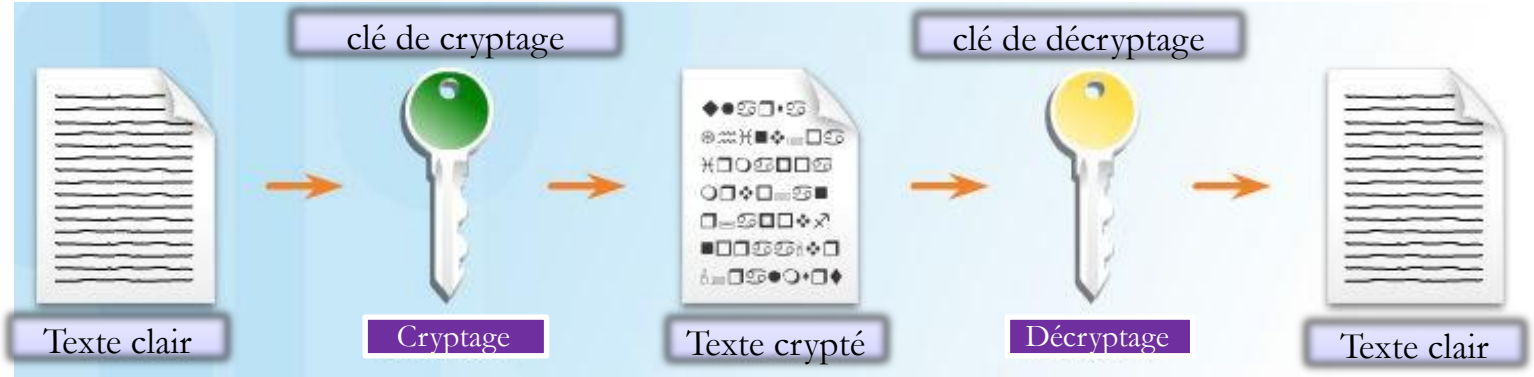
Caractéristiques de DH	
Description	Diffie-Hellman Algorithm
Chronologie	1976
Type d'algorithme	Asymétrique
Vitesse	Lent
Taille de la clé	512, 1024, 2048, 3072 et 4096 bits
Temps pour cracker (ordinateur capable de tester 255 clés par seconde)	Inconnu, mais jugé sécurisé avec l'utilisation de clés de 2048 bits ou plus long.
Consommation des ressources	Moyen

Contenu du chapitre

- Introduction
- Services de la cryptographie
- Les bases de l'intégrité et de l'authenticité.
- La confidentialité
- **La cryptographie à clé publique**

Algorithme à clé asymétrique

- Les algorithmes asymétriques sont conçus de façon à ce que le clé de cryptage soit différente de celle utilisée pour le décryptage.
- La clé de décryptage ne peut à tout moment être calculée depuis la clé de de cryptage et vice-versa.
- Le cryptage asymétrique est utilisé pour échanger des messages secrets sans pour autant avoir un secret pré-partagé.
- Quatre protocoles utilisent des algorithmes à clé asymétrique :
  - Internet Key Exchange (IKE).
  - Secure Socket Layer (SSL).
  - Secure Shell (SSH).
  - Pretty Good Privacy (PGP).

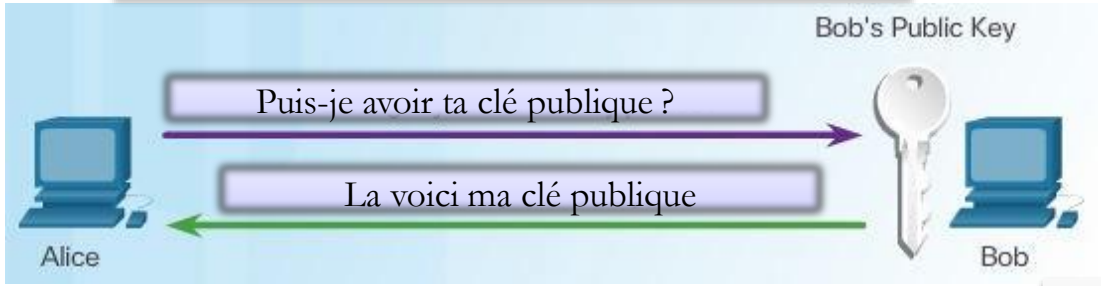


Algorithme à clé asymétrique

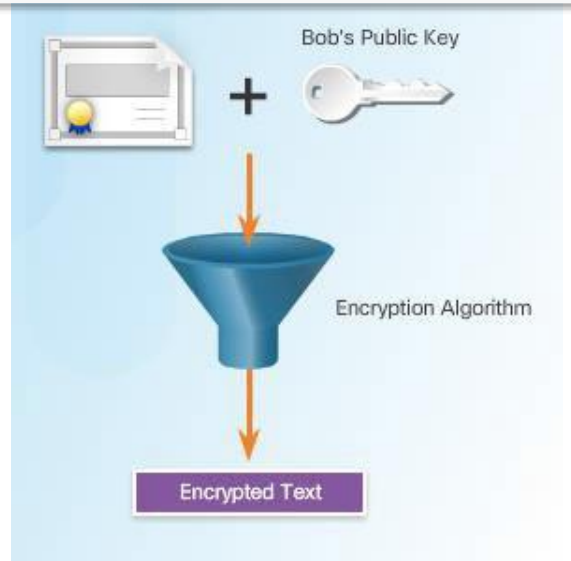
- Les algorithmes asymétriques utilisent deux clés : une clé publique et une autre privée.
- Les deux clés sont capables de cryptage, mais l'autre clé est requise pour le décryptage.
- Si la clé publique est utilisée pour le cryptage, la clé privée doit être utilisée pour le décryptage.
- Le contraire est aussi vrai, si la clé privée a été utilisée pour le cryptage, le clé publique est requise pour le décryptage.
- Grâce à ces fonctionnalités, les algorithmes à clé asymétrique assurent la confidentialité, l'authentification et l'intégrité.

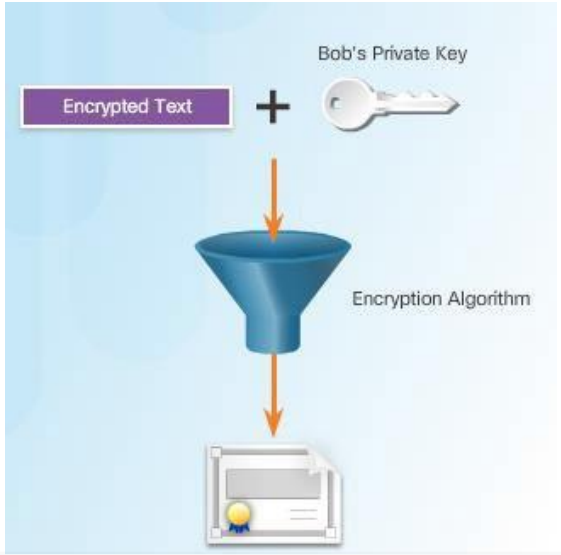
Clé publique (cryptage) + clé privée (décryptage) = confidentialité

1) Alice demande la clé publique de Bob



2) Alice crypte le message à l'aide de la clé publique de Bob

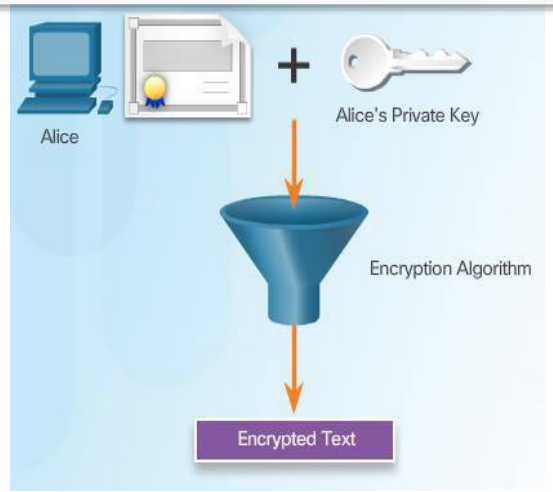


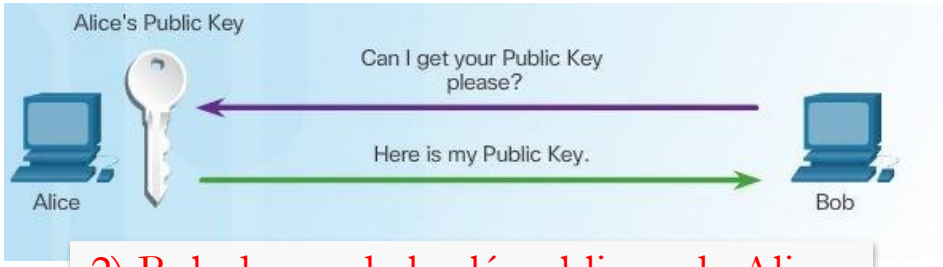


3) Bob utilise sa clé privée pour décrypter le message

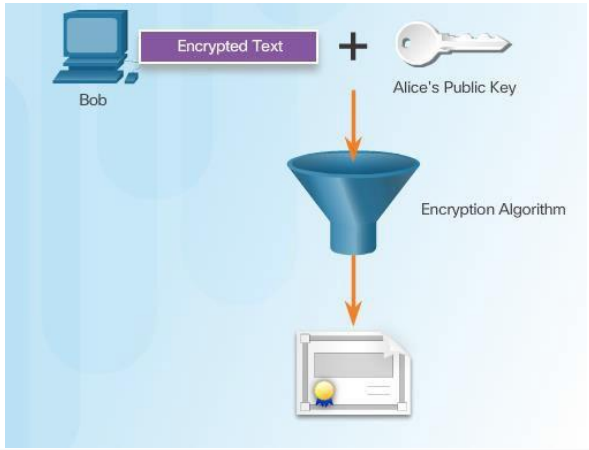
Clé privée (cryptage) + clé publique (décryptage) = authentification

1) Alice crypte un message à l'aide de sa clé privée





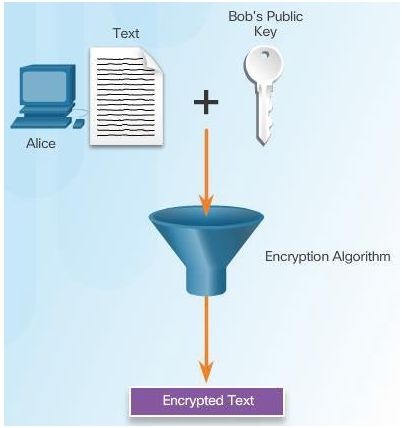
2) Bob demande la clé publique de Alice

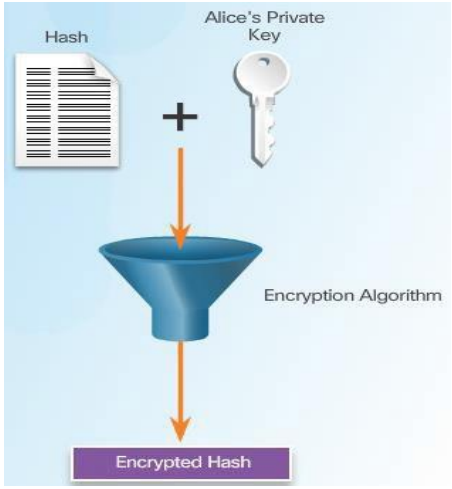


3) Bob déchiffre le message à l'aide de la clé publique de Alice

Algorithmes asymétriques

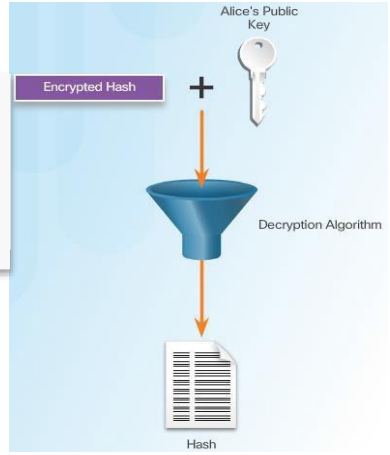
1) Alice crypte le message à l'aide de la clé publique de Bob

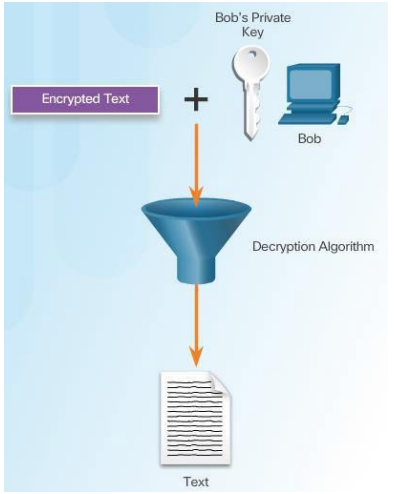




2) Alice crypte un hash à l'aide de De sa clé privée

3) Bob déchiffre le hash à l'aide de la clé publique de Alice





4) Bob utilise sa clé privée pour décrypter le message

Types d'algorithmes asymétriques

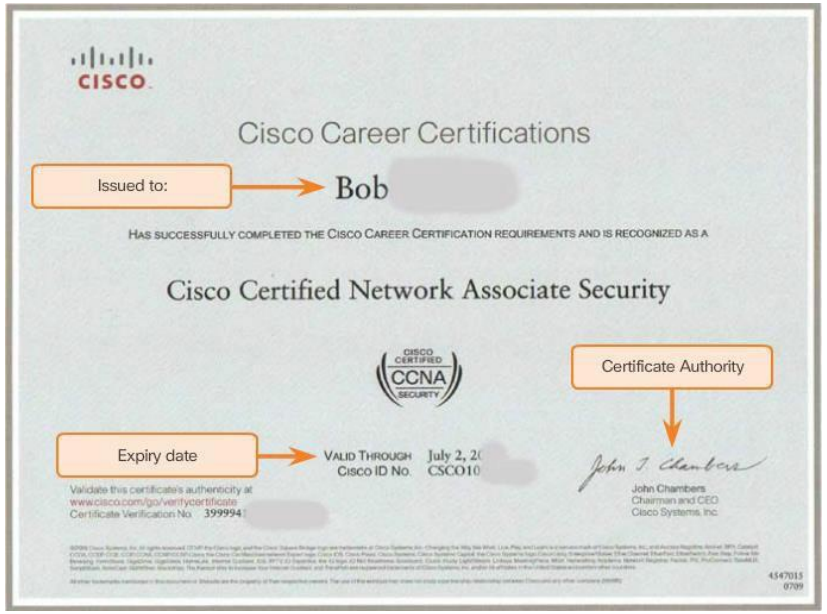
d'algorithmes asymétrique	Taille de la clé
DH	512 à 4096
Digital Signature Standard (DSS) et Digital Signature Algorithm (DSA)	512 - 1024
Algorithme de cryptage RSA	512 à 2048
ElGamal	512 - 1024

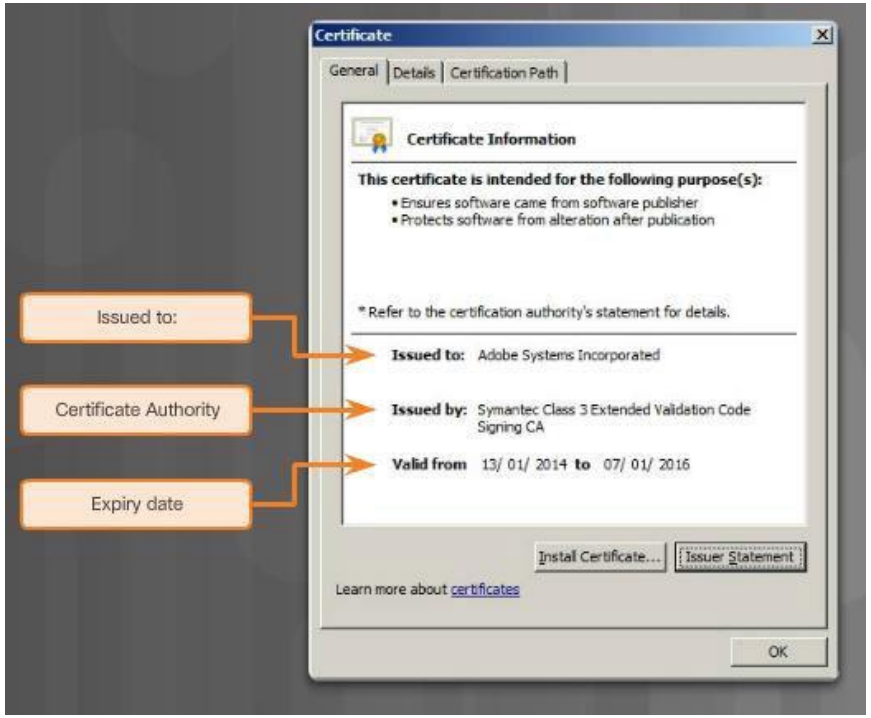
Les signatures numériques

Signature numérique

- La signature numérique (parfois appelée signature électronique) est un mécanisme permettant de garantir l'intégrité d'un document électronique et d'en authentifier l'auteur, par analogie avec la signature manuscrite d'un document papier.
- Les signatures numériques sont utilisées dans deux situations différentes :
  - Signature du code : utilisé pour vérifier l'intégrité des fichiers exécutables téléchargés depuis Internet.
  - Certificats numériques : utilisés pour vérifier l'identité d'un site avant d'établir une connexion cryptée pour l'échange de données confidentielles.

Certificat numérique





Algorithmes de signature numériques

- Il existe trois algorithmes DSS utilisé pour la génération et la vérification des signatures numériques :
  - **Digital Signature Algorithm (DSA)**
  - **Rivest-Shamir Adelman Algorithm (RSA)**
  - **Elliptic Curve Digital Signature Algorithm (ECDSA)**

Algorithmes de signature numériques

Caractéristiques de RSA	
Description	Ron Rivest, Adi Shamir, Len Adleman
Chronologie	1977
Type d'algorithme	Algorithme Asymétrique
Taille de la clé	512 -2048 bits
Avantages	Vérification de la signature rapide
Inconvénients	Génération de la signature lente

Caractéristiques de DSA	
Description	Digital Signature Algorithm
Chronologie	1994
Type d'algorithme	Fournit les signatures numériques
Avantages	Génération de la signature lente
Inconvénients	Vérification de la signature rapide