



PARTIE IV

Cryptographie

- Termes, Définitions, Concepts et Historique
- Types de Chiffrement
- Algorithmes Cryptographiques
- Mise en Œuvre de la Cryptographie
- Types d'Attaques sur la Cryptographie
- Utilisation de la Cryptographie à l'International

Termes, Définitions, Concepts et Historique

- La cryptographie fait partie des mesures (technique préventif) de sécurité mises en œuvre pour renforcer la **confidentialité** et **l'intégrité** du système d'information.
- Le mot **cryptographie** en grec ancien : "*écriture cachée*".
- Le terme cryptographie désigne aujourd'hui "*un procédé permettant de rendre un message inintelligible et de protéger les données*" (définition Robert).
- Il existe bon nombre de termes souvent mal employés, notamment par la presse ou les médias grand public, nous allons donc procéder à la définition des termes corrects.

Termes, Définitions, Concepts et Historique

- **Chiffrement, chiffrer** (en anglais *encipher*) : transformation, au moyen d'une clé et d'un algorithme, d'un message en clair (en anglais *cleartext* message) en un message incompréhensible pour un tiers qui ne possède pas la clé permettant de reconstituer le message en clair.
- **Cryptogramme ou chiffre** (en anglais *ciphertext*) : le message incompréhensible issu de l'opération de chiffrement.
- **Déchiffrement, déchiffrer** (en anglais *decipher*) : transformation inverse du cryptogramme en message en clair, au moyen d'un algorithme **ET AVEC** la clé de déchiffrement.
- **Décryptage, Décrypter** : récupération du message en clair à partir du cryptogramme, **SANS** utiliser la clé de déchiffrement. On dit aussi "**casser**" le chiffre.
- Par contre, les mots **crypter, encrypter, cryptage** ou encore **encryptage** **n'existent pas en cryptographie** (bien qu'employés souvent à tort) car ils signifieraient encoder sans connaître la clé, ce qui n'a pas de sens.
- **Clé** : séquence de valeurs (chiffres, lettres, valeur binaire, etc.) qui détermine les opérations et le comportement de l'algorithme de cryptographie.
- **Espace de clés** : le nombre total de valeurs distinctes que peut prendre la clé d'un algorithme cryptographique.

Termes, Définitions, Concepts et Historique

- **Cryptosystème** : terme mathématique désignant un algorithme et l'ensemble des textes clairs, des cryptogrammes et des clés possibles.
- **Système cryptographique** : ensemble de moyens matériels et logiciels permettant le chiffrement et le déchiffrement de données selon une méthode particulière (algorithme cryptographique).
- **Cryptanalyse** : science ayant pour but l'analyse des cryptosystèmes dans le but de les "casser", donc de pouvoir décrypter les données chiffrées sans posséder la clé de déchiffrement.
- **Cryptologie** : science des messages secrets. Regroupe la cryptographie, art de rendre inintelligible un message et la cryptanalyse, art de trouver le message clair caché.
- **Stéganographie** : art de la dissimulation d'un message à l'intérieur d'un autre message. Un exemple connu durant la guerre froide est l'usage de micro points dans un texte imprimé. Le point d'apparence anodine sur une lettre "i" du texte, dont la position est convenue à l'avance, est en fait un microfilm contenant des informations que l'on souhaite cacher. La stéganographie est encore employée de nos jours, notamment dans les fichiers images ou pour créer un filigrane électronique.

Un peu d'histoire !

- L'histoire de la cryptographie remonte à l'antiquité :
- le premier témoignage de son usage étant une tablette mésopotamienne contenant la formule chiffrée du mélange d'argiles utilisées par un potier afin d'en garder le secret (environ -1500).
- Le plus célèbre reste le "**chiffre de César**" qui utilisait une technique de décalage simple de 3 lettres vers la droite pour protéger ses correspondances secrètes.
- En termes actuels, cette méthode de chiffrement est appelée **substitution** mono-alphabétique par décalage, la clé étant la valeur 3.
- Il va sans dire que ce procédé nous semble aujourd'hui très faible, voire même enfantin.

Un peu d'histoire !

- Chiffre de **César** :

Clair	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
Chiffré	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

- Chiffrement :
VENI VIDI VICI
↓ ↓ ↓
YHQL YLGL YLFL
- Déchiffrement :
RUGLQDWHXU
↓
ORDINATEUR
- Plus tard, au 16ème siècle (1586), le diplomate **Blaise de Vigenère** améliore ce procédé en utilisant une substitution poly-alphabétique et une clé se présentant sous la forme d'un mot ou d'une phrase.
- Cette méthode utilise un décalage différent pour chaque lettre du message.

Un peu d'histoire !

- Tabla de Véginere

	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

- Code de Vigenère :

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

ligne 1 = le message à coder

ligne 2 = la clé (répétée pour couvrir le message)

ligne 3 = le message codé ($S+P=H$; $E+E=I$; $C+R=T$...)

	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

Un peu d'histoire !

- Le code de Viginère résista trois siècles aux cryptanalystes. Puis fut facilement cassée avec l'analyse des répétitions de groupes de lettres et quelques notions simples de mathématiques (les PGCD).
- Vigenère avait également proposé une variante de cette méthode avec une version autoclave : le message à coder fait partie de la clé.

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

- Encore plus difficile à décrypter !

Un peu d'histoire !

- Les armées de Napoléon utilisaient la variante du code de Vigenère pour communiquer.
Le chiffrement permettait de dissimuler des informations aux ennemis, dans une certaine mesure. Mais il faut parfois également dissimuler des informations à des alliés. Il y avait donc plusieurs clés, une pour chaque destinataire ou groupe de destinataire. De plus, pour des raisons de sécurité, les clés changeaient régulièrement. Très vite un problème se posa quand il fallut transmettre les nombreuses clés régulièrement.
- C'est un jeune conseiller de Napoléon qui proposa une méthode pour limiter le nombre de clés à transmettre à chaque changement et augmenter la sécurité en cas d'interception de la clé. Cette prouesse lui valut le surnom de "*le brave*" par Napoléon!

- une clé générale, connue de tous et changée régulièrement : **la clé de la variante de Vigenère** ;
- **une clé spécifique**, connue seulement des destinataires concernés, pour chiffrer le Carré de Vigenère.
- ➔ Une seule clé était alors diffusée à chaque changement, mais cette clé seule est insuffisante pour déchiffrer un message.


		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	1	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
B	2	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
C	3	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
D	4	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
E	1	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
F	2	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
G	3	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
H	4	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
I	1	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
J	2	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
K	3	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
L	4	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
M	1	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
N	2	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
O	3	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
P	4	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
Q	1	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
R	2	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
S	3	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
T	4	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
U	1	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
V	2	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
W	3	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
X	4	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
Y	1	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
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

Un peu d'histoire !

- Ces méthodes de chiffrement dont les origines remontent à près de 2000 ans, fut encore beaucoup utilisé jusqu'au début du siècle dernier.
- Lors de la 1e guerre mondiale par exemple, on retrouve des traces de la variante de Napoléon pour les communications sur le front. (Des 2 côtés)
- Bien que la méthode de décryptage fût connue, les moyens de l'époque étaient insuffisants pour casser rapidement les messages.
- On entre après dans l'ère de la mécanisation et la cryptographie en bénéficie directement. De nombreuses machines à chiffrer sont inventées, la plus célèbre d'entre elles étant la machine **ENIGMA** utilisée par les allemands durant la seconde guerre mondiale.
- Les progrès de la cryptographie sont directement liés à ceux de la cryptanalyse, dont le but est rappelons-le de décrypter les messages chiffrés sans disposer de la clé. Le cas de la machine ENIGMA est pour cela assez emblématique, puisque c'est en cherchant à casser le code de cette machine que l'anglais **Alan Turing** a pu démontrer la supériorité d'une machine programmable, qui deviendra plus tard l'ordinateur.
- C'est d'ailleurs l'informatique qui va faire progresser de manière spectaculaire ces deux disciplines en utilisant la puissance de calcul et de traitement de l'information pour créer des algorithmes de plus en plus complexes et robustes, mais aussi des méthodes de cryptanalyse de plus en plus performantes.
- Filme : imitation game (jeux d'imitation)

- **Exemple - l'analyse en fréquences** : Sur un nombre de textes important on recherche la fréquence d'apparition des différentes lettres ;

lettre	%	lettre	%
A	9,42	N	7,15
B	1,02	O	5,14
C	2,64	P	2,86
D	3,39	Q	1,06
E	15,87	R	6,46
F	0,95	S	7,90
G	1,04	T	7,26
H	0,77	U	6,24
I	8,41	V	2,15
J	0,89	W	0,00
K	0,00	X	0,30
L	5,34	Y	0,24
M	3,24	Z	0,32



lettre	%	lettre	%
E	15,87	C	2,64
A	9,42	V	2,15
I	8,41	Q	1,06
S	7,90	G	1,04
T	7,26	B	1,02
N	7,15	F	0,95
R	6,46	J	0,89
U	6,24	H	0,77
L	5,34	Z	0,32
O	5,14	X	0,30
D	3,39	Y	0,24
M	3,24	K	0,00
P	2,86	W	0,00

Types de chiffrement

- Quel que soit leur type, les systèmes cryptographiques sont composés des éléments suivants :
 - Un **algorithme**, c'est-à-dire un ensemble de fonctions mathématiques et/ou de règles qui vont recevoir en entrée un message et une clé, pour produire un résultat qui sera soit un cryptogramme, soit un texte clair selon l'opération effectuée.
 - Deux opérations dites de **chiffrement** (en général notée E comme *Encipher*) et de **déchiffrement** (en général notée D).
 - Une **clé** ou un **système de clés**
- Comme vu précédemment, l'introduction des machines de calcul a permis l'essor de systèmes cryptographiques dits modernes, que l'on peut différencier des chiffrements classiques qui s'effectuaient aisément à la main ou avec des outils rudimentaires.

Types de chiffrement : Classiques

- **Chiffrement par substitution** : il est possible de substituer un mot complet

mots	code
C	B2
DANS	GH
DE	KL
DIT	C5
DU	ST
ELLE	34
EST	QR
ETAIT	90
FOI	U
FOIE	12
FOIS	UV
FOIX	MN
IL	AB
JE	D6
LA	E7
MA	CD
MARCHANDE	A1
ME	56
PREMIERE	D4
QUE	78
QUI	OP
UNE	EF
VEND	WX
VENDAIT	C3
VILLE	YZ

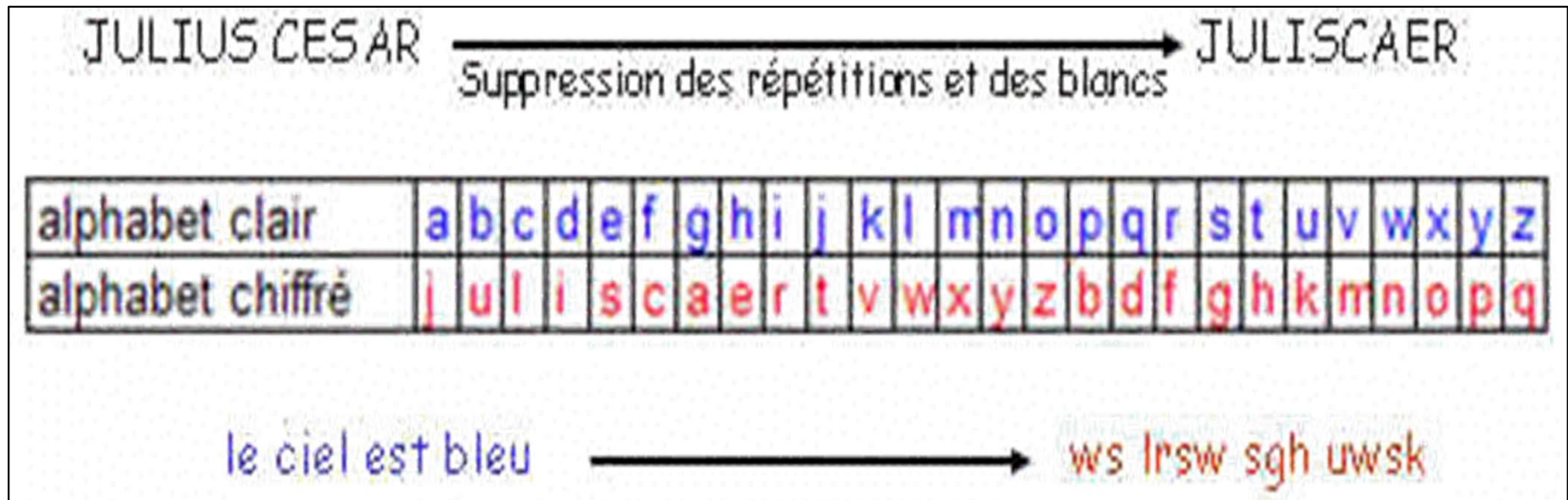
AB 90 EF UV EF A1 KL 12 OP C3 ST 12 GH E7 YZ KL MN.
34 56 C5 CD IJ B2 QR E7 D4 UV 78 D6 WX ST MN GH E7 YZ KL MN

↓

IL ETAIT UNE FOIS UNE MARCHANDE DE FOIE QUI VENDAIT
DU FOIE DANS LA VILLE DE FOIX.
ELLE ME DIT MA FOI C EST LA PREMIERE FOIS QUE JE VEND
DU FOIE DANS LA VILLE DE FOIX.

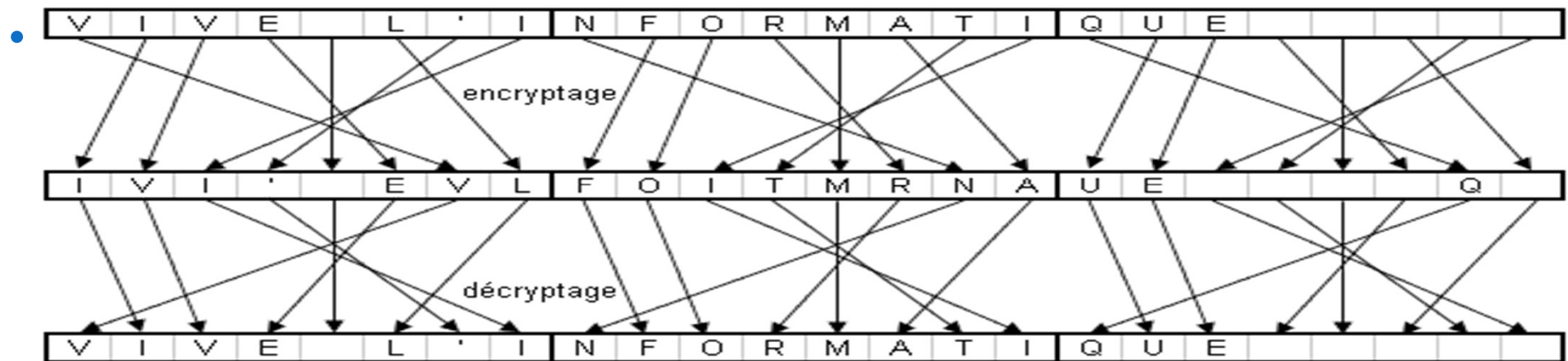
Types de chiffrement : Classiques

- **Chiffrement par substitution** : chaque caractère du message en clair est remplacé (substitué) par un autre, comme dans le chiffre de **César** ou dans **ROT13** sur Unix (choix du chiffre 13?).
- Exemple : construction d'une clé



Types de chiffrement : Classiques

- **Chiffrement par transposition ou permutation** : les caractères du message en clair sont réordonnés selon une règle fixée par l'algorithme et la valeur de la clé.
- **Exemple 1** : Le texte à chiffrer est découpé en blocs (de 8 caractères par exemple).
- Soit **K1 = 71265843** ce qui signifie que le caractère 1 du bloc va en position 7 du bloc encrypté. Ainsi :
- VIVE L'INFORMATIQUE → IVI' EVLFOITMRNAUE Q



- La clé de déchiffrement est **K2 = 23875416**.

Types de chiffrement : Classiques

Chiffrement par transposition ou permutation

- **Exemple 2** : emploi du codage binaire : principe de la méthode Lucifer (IBM ; Feistel)
- Soit à chiffrer la lettre J : $\text{ASCII}(J) = 74 = 01001010$

J 0 1 0 0 1 0 1 0

Mot à coder : J en code ASCII étendu

Partage en deux parties de 4 bits :

Clé : 2143 (clé de permutation)

$$D1 = D'0 + G0$$

G0	D0
0 1 0 0	1 0 1 0

G0	D'0
0 1 0 0	0 1 0 1

$D0 \rightarrow D'0$

G0	D1
0 1 0 0	0 0 0 1

G1	D1
1 0 1 0	0 0 0 1

$G1 = D0$

- Refaire ce traitement 4 fois.

- $J = 01001010$ cle = 3412 (0+0=0 0+1=1 1+1=0)
- 0101
- 10100001
- 0010
- 00011000
- 0100
- 10000101
- 1010
- 01010010 = 2+16+64=82 =R

Types de chiffrement : Classiques

Chiffrement par substitution poly-alphabétique :

- C'est le chiffre de Vigenère, décrit dans son ouvrage « Traicté des chiffres ou secrètes manières d'écrire » publié en 1586 et disponible en ligne à la BNF.
- Vigenère n'est pas l'inventeur de la substitution poly-alphabétique, mais il y a apporté le concept de clé secrète communicable séparément qui en a fait la force et la réputation.

Types de chiffrement : Classiques

Chiffrement par dissimulation : cette méthode est plus proche de la **stéganographie**, car il s'agit de cacher un message à l'intérieur d'un autre message.

- On peut malgré tout parler de cryptographie car cette technique emploie une clé permettant de retrouver le message dissimulé.
- Un exemple classique de cette méthode que vous avez certainement vu dans de vieux films d'espionnage consiste à convenir par exemple du titre d'un livre dans une édition spécifique, qui sera la clé partagée entre l'émetteur et le destinataire.
- Il suffit alors à l'émetteur de constituer son message chiffré au moyen d'une série de paires de nombres donnant la page et la position du mot à chiffrer.
- Le cryptogramme consistera donc en une série de nombre sans signification apparente pour qui ne possède pas la clé, c'est-à-dire le bon livre dans la bonne édition.
- Une variante de cette méthode, encore plus proche de la stéganographie, consiste à transmettre un message de 100 mots, sachant que la clé consiste à ne lire qu'un mot sur 7 par exemple pour retrouver le "vrai" message".

Types de chiffrement : Modernes

- Les chiffrements dits "modernes" sont étroitement liés à l'utilisation des moyens informatiques et/ou électroniques, en ce sens que le concept de message en clair est étendu à toute séquence de bits ou d'octets, qu'ils représentent du texte ou n'importe quelle information binaire.
- Ils utilisent la puissance des moyens de calcul pour enchaîner des opérations de permutation et de substitution en grand nombre sur les bits composant un message, selon des règles déterminées par les bits issus de la clé.
- Jusqu'en juin 1976, les chiffrements étaient tous à **clé symétrique**, c'est-à-dire que la même clé était utilisée pour chiffrer et déchiffrer le message.
- Il était donc crucial que l'émetteur et le destinataire du message chiffré puissent partager cette clé, tout en la gardant secrète vis-à-vis des tiers.
- Selon leur destination principale, ces algorithmes sont conçus pour un chiffrement par blocs (64, 128, 256 ou 512 bits par bloc) ou un chiffrement de flux (octet par octet, très employé pour le chiffrement des transmissions réseau).

Symétrique = mono-clé = à clé secrète

Types de chiffrement : Modernes

- En juin 1976, les universitaires américains **Whitfield Diffie** et **Martin Hellman** ont publié un article démontrant la faisabilité de la cryptographie à clés **asymétriques**, également connue sous le nom de cryptographie à **clé publique**.
- Leur algorithme **Diffie-Hellman** d'échange de clés est d'ailleurs toujours utilisé de nos jours.
- Leurs travaux ont inspiré les chercheurs **Ron Rivest**, **Adi Shamir** et **Leonard Adleman** pour créer l'algorithme **RSA**, le plus employé aujourd'hui dans le domaine de la cryptographie à clé publique.
- Dans le domaine de la sécurité des systèmes d'information, la cryptographie est donc devenue un moyen de choix pour élaborer des mesures de sécurité relatives au critère de la confidentialité, mais nous verrons au chapitre suivant qu'elle est également très utile pour apporter la preuve de l'intégrité d'un message.

Algorithmes Cryptographiques

Cryptographie à Clé Symétrique

- Appelés aussi à **clé secrète**, le principe est d'utiliser une même clé, conservée secrètement par les parties qui échangent un message, à la fois pour chiffrer et déchiffrer ce message.
- Pour chiffrer un texte clair T , on utilise la fonction E avec la clé K pour produire le cryptogramme C et on déchiffre avec la fonction D .
 - **Chiffrement** : $C = E_K(T)$
 - **Déchiffrement** : $T = D_K(C)$
- Le fait que la même clé doive être en possession des deux parties à l'échange implique la mise en place d'un système de distribution et de stockage sécurisé des clés.

Algorithmes Cryptographiques

Cryptographie à Clé Symétrique

- Si l'on considère un nombre **N** d'utilisateurs souhaitant échanger entre eux des messages confidentiels, alors chaque utilisateur doit posséder $N-1$ clés distinctes et le total des clés à gérer est de $N*(N-1)/2$.
- Pour un groupe de 10 utilisateurs, cela représente 45 clés à générer, distribuer et sécuriser, mais pour un groupe de 1000 utilisateurs, on atteint le nombre ingérable de 499.500 clés.
- Cette problématique de gestion des clés est donc un obstacle majeur à surmonter pour mettre en œuvre des échanges sécurisés à base de chiffrement à clé symétrique dès lors que plus de deux parties sont impliquées dans les échanges.
- En effet, si Alice chiffre ses échanges avec Bob au moyen de la clé K_1 et utilise la même clé K_1 pour ses échanges avec Charles, alors Bob peut aussi déchiffrer le message destiné à Charles, ce que ce dernier et Alice ne souhaitent peut-être pas.

Algorithmes Cryptographiques

Cryptographie à Clé Symétrique

- Lorsque le problème de gestion des clés est résolu, les algorithmes à clé symétrique restent les plus **performants** et les **moins coûteux** à mettre en œuvre pour assurer la confidentialité des messages.
- Associés à des **fonctions de hachage**, ils permettent également de fournir des services d'authentification et d'intégrité des messages.
- Les plus répandus de ces algorithmes sont :
- **DES** (*Data Encryption Standard*): le premier standard officiel (1977), remplacé en 2001 car jugé trop faible face à la montée en puissance des moyens de traitement. Chiffrement de blocs de 64 bits, clé sur 64 bits dont 8 de parité soit 56 bits utiles.
- **TDES ou TripleDES** : Afin de combler la faiblesse du DES mais de pouvoir continuer à utiliser les implémentations de l'algorithme, plusieurs modes opératoires ont été élaborés et standardisés par la norme ISO/IEC 18033-3 partie 3.

Algorithmes Cryptographiques

Cryptographie à Clé Symétrique

- **AES** : *Advanced Encryption Standard*, a remplacé DES en 2001. Chiffrement de blocs de 128 bits, trois longueurs de clés possibles, 128, 192 ou 256 bits, d'où les appellations AES-128, AES-192 ou AES-256.
- **Blowfish et Twofish**, algorithmes de chiffrement par blocs, placés dans le domaine public. Ils sont inclus dans de nombreuses suites cryptographiques gratuites et offrent un bon niveau de sécurité. Twofish est le successeur de Blowfish et a été finaliste du concours ayant mené à la sélection de l'AES.
- **RC4** : algorithme de chiffrement de flux, le plus employé des chiffrements par flux, mais a récemment fait l'objet de réserves et est prohibé avec TLS 1.2.
- **eSTREAM** : ce n'est pas un algorithme, mais un projet européen proposant un portfolio d'algorithmes de chiffrement par flux réputés sûrs. On y trouve les algorithmes **HC-128**, **Salsa20**, **Rabbit** ou encore **Trivium**.

Algorithmes Cryptographiques

Cryptographie à Clé Asymétrique

- Appelés aussi à **clé publique**, souvent associés au terme anglais **PKI** (*Public Key Infrastructure*), vont permettre de résoudre le problème crucial de la distribution des clés.
- Le principe permettant cela est que les parties souhaitant communiquer secrètement vont chacune tirer une **paire de clés mathématiquement reliées**, dont une sera **publique** et l'autre restera **privée**.
- Le type de lien mathématique entre les clés privée et publique d'une même paire dépend de l'algorithme choisi :
 - Factorisation de nombres premiers pour **RSA**
 - Logarithmes discrets pour **Diffie-Hellman** et **ElGamal**.
 - Les courbes elliptiques pour la famille des algorithmes **ECC**.

Algorithmes Cryptographiques

Cryptographie à Clé Asymétrique

- La clé publique est dérivée de la clé privée, mais il est matériellement impossible de retrouver la clé privée à partir de la clé publique, en raison de la difficulté mathématique choisie.
- La clé publique d'une entité est librement accessible à tous les partenaires désirant échanger avec elle de façon sécurisée.
- Pour communiquer avec un tiers, il suffit donc simplement de connaître sa clé publique et de lui fournir la nôtre.
- La **propriété la plus intéressante** des algorithmes à clés asymétriques est la suivante :
 - Si on chiffre un message avec la clé publique, il ne peut être déchiffré qu'avec la clé privée
 - Si on chiffre un message avec la clé privée, il ne peut être déchiffré qu'avec la clé publique.
- L'inconvénient majeur des algorithmes à clés asymétriques est leur **lenteur**, essentiellement due à l'utilisation de fonctions mathématiques complexes. Ils seront donc réservés à des **usages non intensifs**.

Algorithmes Cryptographiques

Cryptographie à Clé Asymétrique permettent plusieurs échanges sécurisés grâce à :

1. **Confidentialité** : Alice veut envoyer un message confidentiel à Bob. Elle récupère la clé publique de Bob puis chiffre son message au moyen de cette clé. Désormais, seul Bob est en mesure de déchiffrer ce cryptogramme au moyen de sa clé privée.
2. **Authentification** : Alice veut envoyer un message non confidentiel à Bob, mais veut que Bob soit certain que le message provient bien d'elle. Elle chiffre son message avec sa propre clé privée et envoie le cryptogramme à Bob. Comme n'importe qui ayant accès à la clé publique d'Alice, Bob va utiliser celle-ci pour déchiffrer le cryptogramme et avoir de ce fait la preuve que seule Alice a pu le chiffrer, donc qu'il est authentique.

Algorithmes Cryptographiques

Cryptographie à Clé Asymétrique

3. Intégrité et signature numérique:

- Alice veut signer électroniquement un message.
- Elle va alors utiliser une fonction de hachage convenue avec ses interlocuteurs et générer avec celle-ci une empreinte de son message.
- Elle va ensuite chiffrer cette empreinte au moyen de sa clé privée, et adjoindre le cryptogramme de l'empreinte à son message au titre de signature électronique.
- Dès lors, quiconque veut vérifier à la fois l'intégrité du message d'Alice et avoir la preuve qu'elle seule a pu le signer va simplement régénérer une empreinte du message reçu, puis comparer cette empreinte avec celle attachée au message, qu'il aura préalablement déchiffrée au moyen de la clé publique d'Alice.
- Si les deux empreintes sont identiques, la preuve recherchée est obtenue, sinon c'est que le message a été altéré ou bien n'a pas été signé par Alice.

Algorithmes Cryptographiques

Cryptographie à Clé Asymétrique

4. Non répudiation mutuelle :

- la signature numérique d'un document est théoriquement non répudiable par l'émetteur signataire, sauf à prouver que celui-ci s'est fait dérober sa clé privée.
- Cette non répudiation est appelée NRO (*Non Repudiation of Origin*).
- Mais il est également possible d'établir un protocole de signature entre deux parties et potentiellement un tiers de confiance grâce auquel l'émetteur du message signé recevra un accusé de réception du destinataire également non-répudiable appelé NRR (*Non Repudiation of Receipt*).
- La norme **ISO/IEC 13888-3** décrit les mécanismes à mettre en œuvre pour parvenir à ce résultat.

Algorithmes Cryptographiques

Cryptographie à Clé Asymétrique - RSA

- **Faits de base :**

1) On connaît un algorithme rapide pour déterminer si un nombre entier (grand) est premier

→ théorème de Fermat : si p est premier il existe $n < p$ tel que $n^{p-1} = 1 \pmod{p}$

Nombre de 130 chiffres : temps machine de quelques minutes

2) On ne connaît pas d'algorithme rapide pour déterminer les facteurs premiers d'un nombre entier (grand) non premier.

Pour un produit de 2 nombres entiers premiers de 63 chiffres chacun, le temps de calcul serait de 40 000 000 000 000 000 années avec un ordinateur (1999) !

Algorithmes Cryptographiques

Cryptographie à Clé Asymétrique - RSA

- **Méthode**

a) Choisir aléatoirement 2 différents grands nombres premiers (100 chiffres chacun par exemple) p et q . Calculer $r = p \cdot q$

b) Choisir **aléatoirement** un grand entier e , **premier relativement** à $(p-1) \cdot (q-1)$; e est la clé de chiffrement (publique).

c) Déterminer la clé de déchiffrement (privée) d telle que $d \cdot e = 1 \pmod{(p-1) \cdot (q-1)}$

d) Rendre publics r et e , mais pas d

e) Chiffrement de M : $C = M^e \pmod{r}$

f) Déchiffrement de C : $M = C^d \pmod{r}$

- a) Choisir aléatoirement 2 différents grands nombres premiers
- (100 chiffres chacun par exemple) p et q. Calculer $r = p.q$
- **p=3**
- **q=5**
- **r=3*5=15**
- b) Choisir **aléatoirement** un grand entier e, **premier relativement** à $(p-1).(q-1)$;
- $(p-1).(q-1) = 2*4=8$ (les diviseurs de 8 : 2,4,8)
- e est la clé de chiffrement (publique).
- Exemples e= 7, 9, 11, 13, 15 on choisi **e=11**
- **Clé public de chiffrement : (e,r)=(11,15)**
- e) Chiffrement de message M : $C = M^e \pmod{r}$
- Exemple $M=1101=13$
- $C=13^{11} \pmod{15} = 13^{(8+2+1)} \pmod{15} =$
- $13^8 \pmod{15} * 13^2 \pmod{15} * 13^1 \pmod{15}$
- $4*4*4*4 \pmod{15} * 4 * 13 = 7 = 0111$

c) Déterminer la clé de déchiffrement (privée) d telle que
 $d.e = 1 \pmod{(p-1).(q-1)}$

$$11d = 1 \pmod{8}$$

Il existe x tq $11d = 8x + 1$

$$d = (8x + 1) / 11$$

$$\begin{array}{r|l} 11d & 8 \\ 1 & x \end{array}$$

$x \quad d$

0 $1/11$

1 $9/11$

2 $17/11$

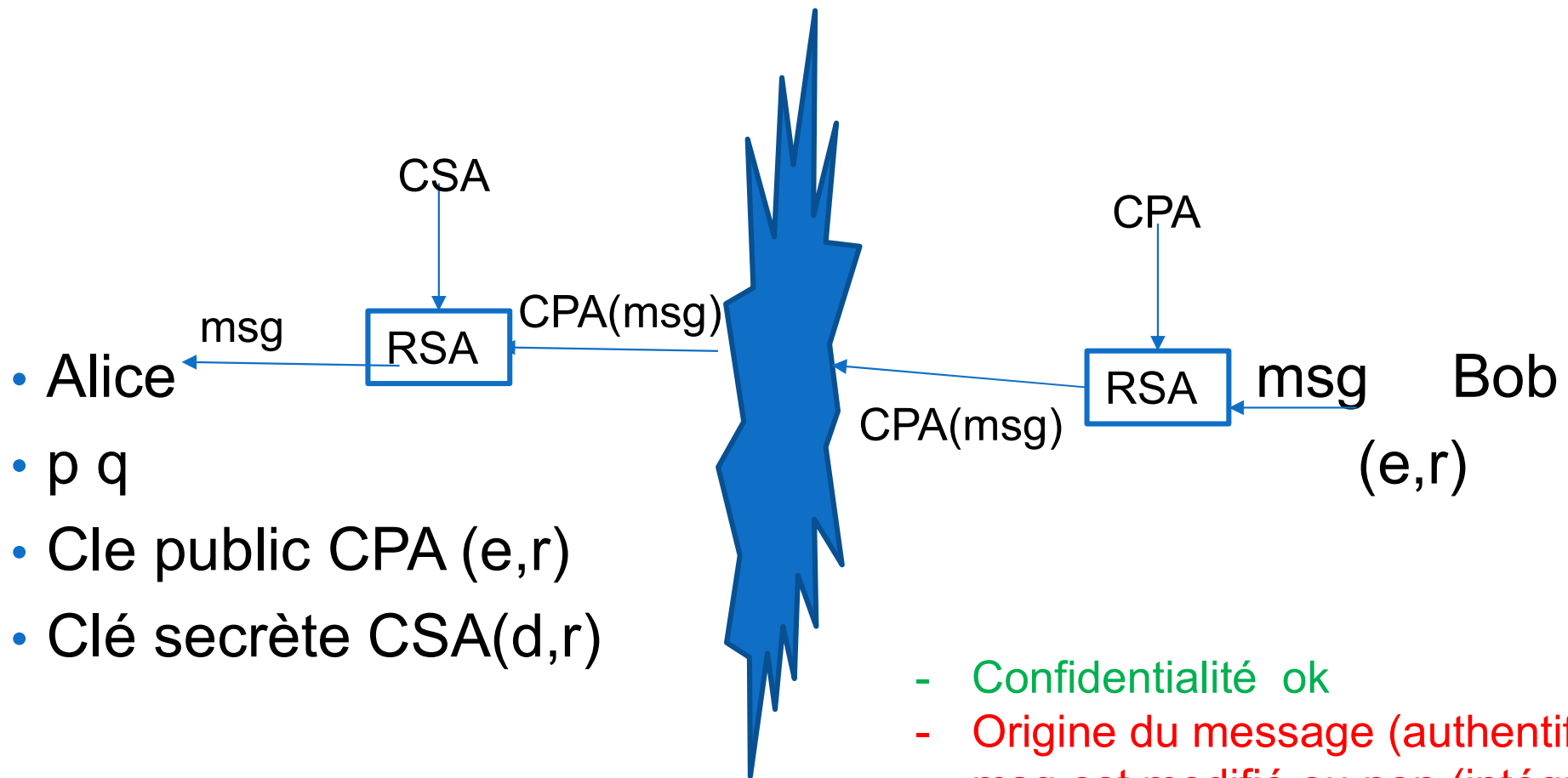
3 $25/11$

4 $33/11 = 3$

Clé privée de déchiffrement $(d, r) = (3, 15)$

f) Déchiffrement de C : **$M = C^d \pmod{r}$**

$$M = 7^3 \pmod{15} = 343 \pmod{15} = 13 = 1101$$



- Alice
- p, q
- Cle public CPA (e,r)
- Clé secrète CSA(d,r)

- Confidentialité ok
- Origine du message (authentification)
- msg est modifié ou non (intégrité)
- Non répudiation
- -----
- Performance
- Gestion des clés publiques

pirate
(e,r)

CPA(msg)

Algorithmes Cryptographiques

Fonction de hachage :

- C'est une fonction qui reçoit en entrée un message de longueur **arbitraire** et produit en sortie une empreinte numérique (*hash* en anglais) de longueur **fixe** (64bits, 128bits, 192bits, 256bits, 512bits ...).
- Si on emploie une fonction cryptographique comme une fonction de hachage, on parle alors d'une **empreinte cryptographique** (*secure hash*).
- Les propriétés recherchées dans une fonction de hachage sont
 - **la non-réversibilité**, c'est-à-dire qu'on ne doit pas pouvoir déduire le message d'entrée à partir de l'empreinte,
 - **la résistance aux collisions**, c'est-à-dire faire en sorte que deux messages distincts ne produisent pas la même empreinte.
 - **effet avalanche** : De plus, il est important qu'un changement même infime dans le message d'entrée provoque un changement important dans l'empreinte qui en résulte.
- Les fonctions cryptographiques de hachage reçoivent, en plus du message d'entrée, une clé cryptographique. Ceci permet d'interdire à quiconque ne connaît pas cette clé de modifier le message et de simplement recalculer une empreinte valide.

Algorithmes Cryptographiques

Fonctions de hachage connues :

- **MD5** (Message-Digest algorithm 5 sur 128 bits), n'est plus sûr !
- **SHA-1** (Secure Hash Algorithm 1 sur 160 bits)
- **SHA-2** (256, 384, 512 bits au choix) : version 2 de SHA-1
- **RIPEMD-160** (RACE Integrity Primitives Evaluation Message Digest)
- **Whirlpool** (512 bits)
- Exemple :
MD5(Wikipedia, l'encycopedie libre et gratuite) = d6aa97d33d459ea3670056e737c99a3d
MD5(Wikipedia, l'encycopedie libre et gratuit**E**) = 5da8aa7126701c9840f99f8e9fa54976
- Les usages principaux de ces fonctions sont le contrôle d'intégrité, l'authentification de messages et la non répudiation (dans le cas d'utilisation d'algorithmes à clé publique).

Algorithmes Cryptographiques

Cryptographie hybride

- C'est la combinaison des types précédents dans le but de tirer parti de leurs avantages respectifs :
 - Facilite de gestion des clés des algorithmes à clés asymétriques.
 - Rapidité des algorithmes à clé symétrique.
 - Intégrité apportée par les fonctions de hachage.
- Par exemple, deux parties qui ne se connaissent pas vont pouvoir tirer aléatoirement une clé secrète éphémère et se l'échanger au moyen d'un algorithme à clé asymétrique grâce à leurs clés publiques mutuelles, puis effectuer des transferts chiffrés par AES et cette clé éphémère.
- C'est ce principe qui est mis en œuvre automatiquement à l'intérieur de certains protocoles de communication sécurisés, comme **HTTPS**.

Algorithmes Cryptographiques

Cryptographie hybride

Exemple :

- Alice veut envoyer un gros fichier confidentiel à Bob.
- Elle va tirer une clé $K1$ aléatoire de 256 bits, puis chiffrer son fichier avec l'algorithme AES.
- Afin de permettre à Bob et à lui seul de retrouver la clé $K1$, elle va retrouver la clé publique de Bob dans un annuaire, puis chiffrer $K1$ au moyen de cette clé publique et de l'algorithme RSA.
- Il ne lui reste plus qu'à transférer le tout à Bob par courrier électronique.

Mise en Œuvre de la Cryptographie

Infrastructure de Clés Publiques ou PKI (Public Key Infrastructure)

- C'est un système cryptographique hybride à base de certificats à la norme **X.509**.
- PKI s'appuie sur un modèle de tiers de confiance, dont le rôle est de vérifier les mentions trouvées dans un certificat (identité du porteur, clé publique, accréditations). Ainsi, lorsqu'un tiers se présente avec un certificat signé par une autorité de confiance, il n'est pas nécessaire de procéder à nouveau à ces vérifications.
- Un système PKI se compose de :
 - Un **service d'annuaire** (*Directory Service*) base sur la norme X.500 et accessible par le protocole LDAP, permettant de stocker et distribuer les certificats, ainsi que de maintenir les listes de révocation (**CRL**).
 - Une ou plusieurs **autorités de certification** (**CA** pour *Certification Authority*), qui signent et valident les certificats.
 - Une ou plusieurs **autorités d'enregistrement** (**RA** pour *Registration Authority*) qui créent les demandes de certificats et procèdent aux vérifications d'identité du demandeur.

Mise en Œuvre de la Cryptographie

Infrastructure de Clés Publiques ou PKI (Public Key Infrastructure)

- Un service de **gestion des clés**, offrant des fonctions de génération de paires de clés, d'échange et de distribution de clés, de sauvegarde et récupération de clés, de révocation de clés, de destruction de clé ou encore de notarisation de clés.
- Un service de **cryptographie**, offrant des algorithmes à clés asymétriques notamment pour les fonctions de gestion des clés, des algorithmes à clé symétrique pour les échanges chiffrés, des fonctions de hachage pour l'intégrité des messages et la signature électronique.
- Une infrastructure PKI peut être **publique** ou **privée**. Si elle est publique, les certificats utilisés par les entités finales (**EE** pour End Entity) doivent être signés par une autorité dont la chaîne de confiance remonte à une CA racine réputée.
- Les composants qui exploitent les certificats, comme les navigateurs Web, effectuent cette vérification avant d'accepter l'usage d'un certificat pour leurs opérations sécurisées.

Mise en Œuvre de la Cryptographie

HTTPS, S-HTTP, SSL/TLS, SSH

- Le plus connu et visible des protocoles sécurisés est le protocole **HTTPS**, que votre navigateur web vous signale en général au minimum par un petit cadenas fermé mais aussi par une indication de couleur verte dans la zone de l'URL.
- A ne pas confondre avec **S-HTTP** (RFC 2660), qui est un protocole de chiffrement au niveau application et qui a quasiment disparu.
- Pour être précis, **HTTPS** n'est pas un protocole à part de HTTP, c'est simplement une codification de l'URI (*Uniform Resource Identifier*, le préfixe https:) qui indique au navigateur que la session HTTP vers le site web indiqué doit se faire en s'appuyant sur une couche de communication sécurisée. Le port de communication sera **443** au lieu de **80** (valeurs par défaut).
- Cette couche de communication sécurisée est fournie par les protocoles **SSL** (*Secure Socket Layer*) ou **TLS** (*Transport Layer Security*).
 - **SSL** a été développé initialement par la société Netscape en 1995 et est considéré comme non sûr depuis 2014.
 - **TLS**, créé en 1999 lui a succédé et la version TLS1.2 est considérée en 2015 comme la plus fiable. Elle est recommandée pour la mise en œuvre de serveurs web sécurisés.

Mise en Œuvre de la Cryptographie

HTTPS, S-HTTP, SSL/TLS, SSH

- Le grand succès de HTTPS vient du fait que ce "protocole" permet d'établir une session sécurisée dès lors que le serveur possède un certificat **X.509** valide et de confiance, sans obliger le client à en posséder un également.
- **SSH** (*Secure Shell*) est un protocole de communication sécurisé qui a remplacé **Telnet** pour l'ouverture de sessions en mode terminal vers les systèmes Unix, mais aussi potentiellement Windows.
Il s'appuie sur des mécanismes de cryptographie hybride pour effectuer l'authentification de l'utilisateur, puis un échange de clés de session permettant de chiffrer tous les échanges, créant de ce fait un tunnel sécurisé entre le client SSH (le plus connu étant le logiciel PuTTY) et le serveur.

Mise en Œuvre de la Cryptographie

Single Sign-On (SSO)

- L'infrastructure PKI a permis le développement d'une architecture dite de **Single Sign-On**, dans laquelle on ne demande à l'utilisateur de s'identifier qu'une seule fois par présentation de son certificat.
- Dans une architecture **Cloud** à multiples niveaux, les requêtes issues d'un utilisateur contiendront son accréditation et les informations en provenance de son certificat, propagées par tous les niveaux au moyen de **SAML** (*Secure Assertion Markup Language*) dans le cadre de flux **SOAP** (*Simple Object Access Protocol*).
- L'identité portée par le certificat sera acceptée par tous les serveurs ciblés dans la mesure où ceux-ci font confiance à l'autorité de certification (CA) ayant délivré le certificat.

Mise en Œuvre de la Cryptographie

E-mail Sécurisé

- La sécurisation des courriers électroniques est un problème difficile à résoudre car c'est par nature une communication de pair à pair (*peer to peer*), ce qui signifie que la mise en œuvre de moyens cryptographiques soit consentie, acceptée et supportée par les deux extrémités.
- On voit ici que seule la cryptographie à clé publique peut permettre de résoudre cette équation. Quelques protocoles sont disponibles pour la sécurisation des E-mails :
 - **S/MIME** (*Secure/Multipurpose Internet Mail Extension*) : décrit par les RFC 2633 et 2311, ce protocole étend MIME pour le support du chiffrement du message et des pièces jointes. Nécessite des certificats X.509.
 - **PGP** (*Pretty Good Privacy*) : basé sur la RFC 4880, PGP est un protocole libre de droits et "open source". Il met en œuvre des techniques cryptographiques hybrides et repose sur un réseau de confiance, contrairement à la hiérarchie de confiance des certificats X.509.

Types d'Attaques sur la Cryptographie

- Les attaques sur les systèmes cryptographiques reposent essentiellement sur la découverte de la clé, puisque les algorithmes sont normalement connus. Il existe deux approches pour y parvenir :
- **Attaques par Cryptanalyse** : ont pour objectif de casser l'algorithme en essayant de rechercher ses faiblesses, afin de pouvoir déduire la clé à partir de l'observation du fonctionnement de l'algorithme dans des conditions connues, par exemple un texte clair et son cryptogramme, le même texte clair chiffré avec des clés différentes (c'est ce type d'approche qui a permis à Alan Turing de casser ENIGMA), etc.
- **Attaques Cryptographiques** : Ces attaques ne cherchent pas à analyser l'algorithme, mais plutôt à trouver la clé par tentatives répétées. On ne soulignera donc jamais assez le soin qu'il faut donc apporter dans la qualité de la clé.
L'attaque par **force brute** consiste à explorer l'ensemble de l'espace de clés pour essayer de déchiffrer un cryptogramme donné, jusqu'à obtention d'un texte clair compréhensible ou connu d'avance.
Cette attaque peut être ciblée sur une partie connue d'un fichier chiffré, par exemple un en-tête toujours présent et constant.
La parade à ce type d'attaque est l'agrandissement de l'espace de clé afin de rendre matériellement improbable le succès de cette attaque dans un temps raisonnable.

Types d'Attaques sur la Cryptographie

- L'attaque par force brute peut-être rendue plus performante si l'attaquant a des indices sur la forme de la clé.
C'est le cas lorsque la clé est un mot de passe, donc que les octets qui la constituent sont obligatoirement des caractères imprimables.
- L'attaquant favorisera alors une attaque par **dictionnaire**, qui est en soi une attaque par force brute limitée à des mots probables afin de réduire le temps d'exploration de l'espace de clés.
- L'encodage des mots de passe dans les bases de données est aussi sujet à un type d'attaque particulier au moyen de tables nommées "***rainbow tables***" qui ciblent une faiblesse démontrée des fonctions de hachage employées généralement pour stocker les mots de passe dans les systèmes.

Utilisation de la Cryptographie à l'International

- Les moyens cryptographiques ont longtemps été considérés comme des **armes de guerre** et de ce fait subissaient de nombreuses restrictions tant pour leur exportation que pour leur importations dans de nombreux pays, dont la France jusqu'en 2000.
- La montée en puissance d'Internet et surtout du commerce électronique, grand consommateur de moyens cryptographiques pour sécuriser les transactions, a forcé les états à assouplir leurs législations en la matière.
- L'**Arrangement de Wassenaar** (2000) portant sur le commerce des armes entre les pays signataires a levé la restriction qui frappait jusque-là les algorithmes utilisant des clés de plus de 64 bits, mais maintient un certain nombre de restrictions dont il est bon de s'enquérir avant tout projet d'utilisation de moyens cryptographiques avancés dans un contexte international.