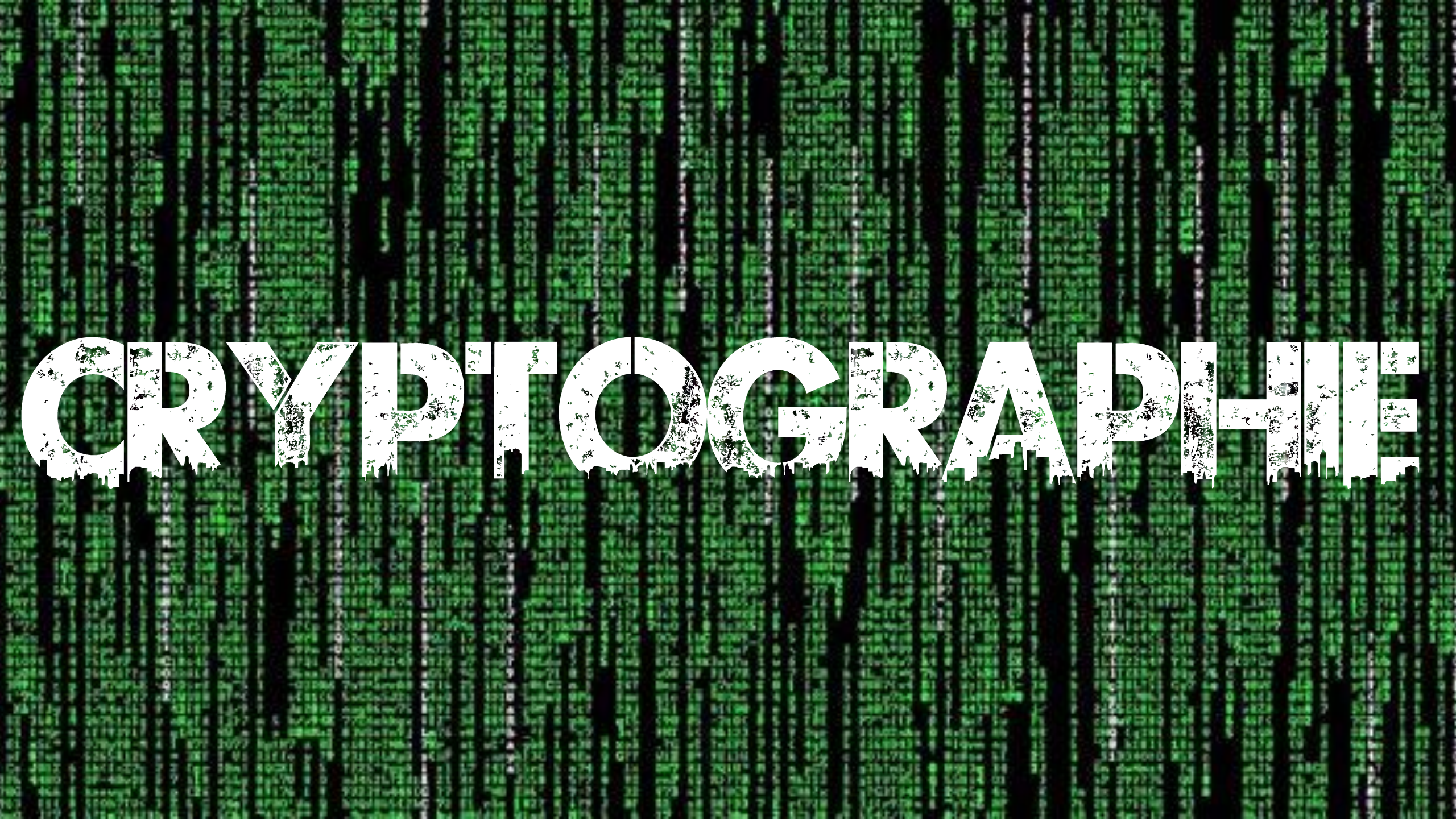
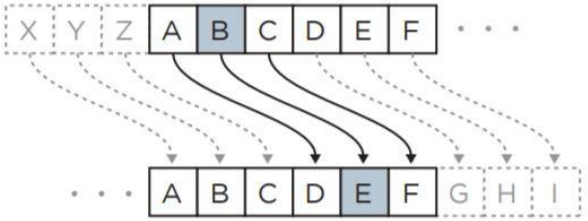

CRYPTOGRAPHIE

La confidentialité des messages a toujours existé. Elle fut surtout utilisé à des fins militaires. A notre époque, elle fait partie intégrante de notre vie. Voici un rapide résumé de son histoire…

La cryptographie a été utilisé par Jules César pour communiquer avec ses généraux. lors de l'envahissement de la Gaule. **Le code César** consistait à changer le rang des lettres. On remplaçait l'alphabet ABCDE… par l'alphabet DEFGH… avec une clé de chiffrement de 3 ce qui transformait, SIMPLON en VLPSORQ ! Le problème était que la clé de chiffrement était toujours de 3 et donc toutes les lettres subissaient le même décalage de 3… Un code facile à casser même à l'époque. Petite aparté… On peut créer un code César avec un programme Java.



Texte clair	MEDAILLEDEBRONZE
Clé	OLYMPIQUEOLYMPIQ
Texte chiffré	APBMXTBYHSMPACHU

	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

Puis la civilisation arabe, très avancée scientifiquement, inventa la **cryptanalyse** en partant du constat que dans toutes langues les lettres de l'alphabet ne se rencontrent pas avec les mêmes fréquences. Par exemple, en français, la lettre la plus utilisée est le e. Pour contrer les attaques des cryptanalystes, on a compliqué durant des siècles la méthode de substitution en compliquant les fréquences.

Chiffres de Vigenères

Blaise de Vigenère, inspiré par les défauts du Code César, a ajouté une algorithme supplémentaire. Il suffisait d'utiliser une clé et un tableau à double entrée. Une même lettre sera remplacée par une autre qui ne sera pas toujours la même. Cf mon image.
Prenons le M de médaille et le O de Olympique. Le M en abcisse et le O en ordonnée convergent vers la lettre A…
En vous appuyant sur ce principe, vous avez 2 solutions :

Première solution :
Utiliser une clef secrète de la même longueur que le texte à chiffrer comme dans mon tableau. On appelle cela le **chiffre de Vernam**. Il fut publié en 1926 par l'ingénieur du même nom. Aujourd'hui on parle du One Time Pad.
C'est le même principe que le chiffre de Vigenère, mais la clé doit répondre à 3 impératifs :

1. elle est aussi longue que le texte à chiffrer
2. elle est parfaitement aléatoire
3. elle n'est utilisée que pour chiffrer un seul message, puis est immédiatement détruite.

Ce code est réputé incassable mais il est très peu pratiqué car il est difficile et complexe de générer des clés aléatoires.

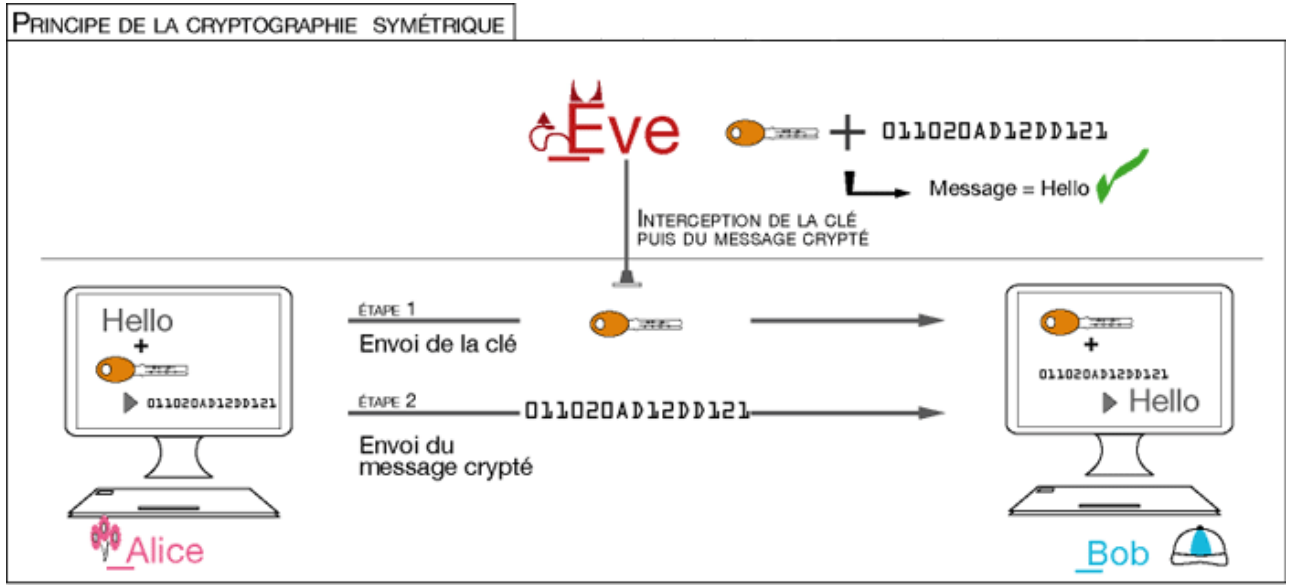
Seconde solution :
Brouiller les lettres qui restent à crypter à l'aide de lettres déjà cryptées. Cela fait aujourd'hui partie du standard de la cryptologie.

1920, la création d'**Enigma**
Enigma intégrait une méthode de chiffrement par substitution polyalphabétique. La machine se composait de multiples rotors comportant les 26 lettres de l'alphabet, un dispositif appelé « brouilleur », ainsi que d'un pupitre de connexions qui effectuait les conversions. C'est cette combinaison qui formait la clé du chiffrement. Une fois le brouilleur configuré, le texte clair était saisi par l'intermédiaire d'un clavier, puis passé à travers le brouilleur pour enfin apparaître crypté sur un tableau lumineux. Pour chaque lettre saisie sur le clavier, le brouilleur tournait d'un cran, changeant ainsi la clé de cryptage à chaque nouvelle frappe. Elle fut utilisée par les allemands durant la Seconde Guerre Mondiale. Son code fut cassé par le cryptologue et mathématicien Alan Turing.

Chiffre de Vernam (II)

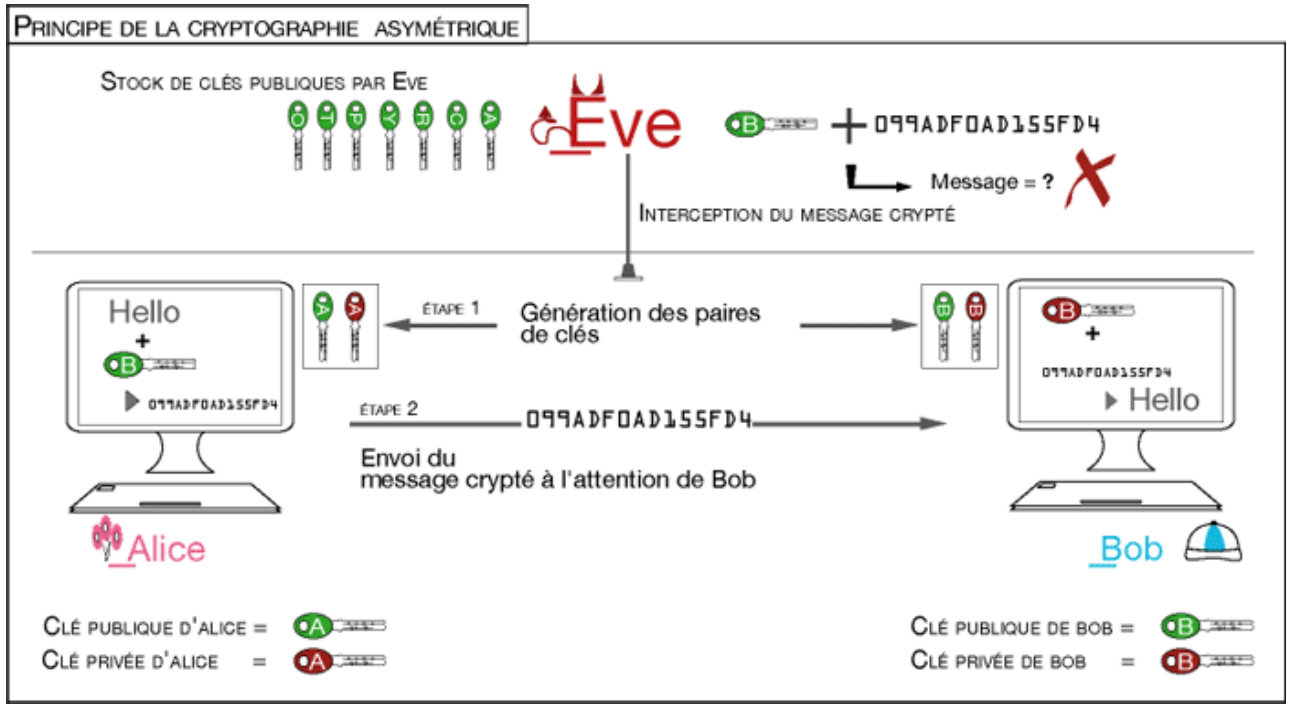
- **Exemple :** *on veut chiffrer le message ≪HELLO≫.*
- On choisit la clé : **X M C K L**
- Puis, on attribue un nombre a chaque lettre, par exemple le rang dans l'alphabet, de **0 a 25**. Ensuite, on additionne la valeur de chaque lettre avec la valeur correspondante dans le masque ; enfin, si le résultat est supérieur à 25 on soustrait 26 (calcul dit "modulo 26") :
- **7 (H) 4 (E) 11 (L) 11 (L) 14 (O) message**
- **+ 23 (X) 12 (M) 2 (C) 10 (K) 11 (L) masque**
- **= 30 16 13 21 25 masque + message**
- **= 4 16 13 21 25 modulo 26**
- **= *E Q N V Z* message codé**
- *Le texte reçu par le destinataire est ≪**EQNVZ**≫.*

En 1973, le National Bureau of Standards lança un appel d'offre pour la création d'un système cryptographique standard. Fut crée **l'algorithme DES** qui devint donc la méthode de chiffrement standard dans le monde entier. Pour transmettre certains messages à leurs clients, les banques faisaient parvenir une clé de cryptage en mains propres !! Nous pouvons considérer que le DES s'apparentait encore au chiffre de César, en ce sens que la même clé servait au cryptage et au décryptage (cf l'image à clé symétrique). La longueur de la clé ne pouvait excéder les 56 bits ce qui était facilement décryptable pour les ordinateurs et leur puissance de calcul.



En 1976, 3 américains ont inventé la cryptographie asymétrique, le RSA.
Elle permet de crypter des communications sans distribution de clés. (Cf Schéma clé asymétrique). Nous avons 2 clés : une clé publique que nous pouvons donner à tout le monde et qui nous permet d'écrire des messages cryptés et une clé privée qui nous sert à déchiffrer les messages codés que l'on reçoit.

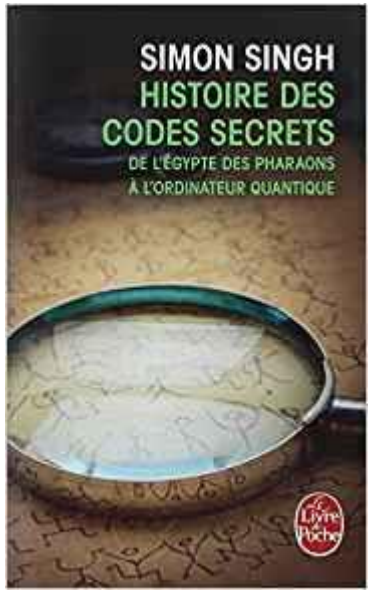
C'est notre protocole SSL. A partir du moment ou vous engager une communication, le SSL émet un certificat électronique qui vérifie l'identité du serveur. Ensuite, la cryptographie à clé publique transmet en toute sécurité la clé symétrique.

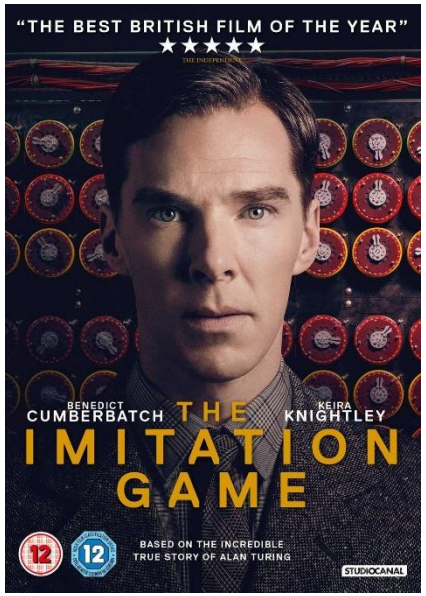


En conclusion…

Les cryptographie n'a eu de cesse d'évoluer depuis des siècles. Elle a su s'inspirer et tirer les leçons de son Histoire. Avec l'apparition des ordinateurs et leur puissance de calcul, la cryptographie est devenue complexe. Mais sommes nous réellement protégés ? Plusieurs cryptographies ont été cassées ces dernières années. A l'heure actuelle, les navigateurs, serveurs et autres travaillent ensemble sur la recherche cryptographique mais nous pouvons nous poser la question de l'efficacité future de la technologie SSL…

Pour en savoir plus





https://www.supinfo.com/cours/1ARI/chapitres/01-introduction-cryptologie

https://www.futura-sciences.com/sciences/dossiers/mathematiques-cryptologie-art-codes-secrets-1817/page/2/

https://www.cnil.fr/fr/comprendre-les-grands-principes-de-la-cryptologie-et-du-chiffrement

Pour les experts Java…
https://jmdoudoux.developpez.com/cours/developpons/java/chap-jce.php

http://objis.com/tutoriel-securite-java-initiation-cryptographie-avec-java-8/