

Cryptographie

Jamal Daafouz



Objectif du cours

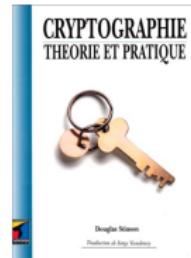
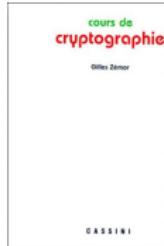
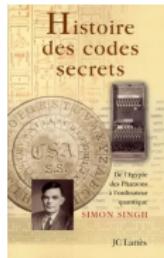
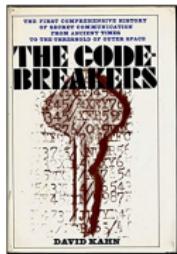
1. Une idée sur l'histoire de la cryptographie
2. Une idée sur les techniques classiques
3. Une idée sur la cryptographie moderne
4. Le principe des techniques les plus utilisées
5. Peu sur la cryptanalyse (manque de temps)

Contenu du cours

- ▶ Introduction, Vocabulaire, Un peu d'histoire
- ▶ Quelques systèmes simples : César, Vigenère.
- ▶ Cryptographie classique
 - Systèmes de cryptage à clé secrète (ou clé symétrique)
 - Standard DES (AES)
- ▶ Cryptographie moderne
 - Systèmes de cryptage à clé publique
 - Chiffrement RSA
- ▶ Quelques éléments de Cryptanalyse
- ▶ Notions sur l'intégrité et l'authentification

Bibliographie

- ▶ Dossier Pour La Science : L'art du secret, Juillet/Octobre 2002 (Vulgarisation)
- ▶ S. Singh : Histoire des codes secrets, Editions JC. Lattès (Histoire)
- ▶ D. Kahn : The Code-Breakers. Editions The Macmillan Company (Histoire)
- ▶ D. Stinson : Cryptographie, Théorie et pratique, Editions Vuibert (Math)
- ▶ G. Zemor: Cours de cryptographie, Editions Cassini (Math)
- ▶ Handbook of applied cryptography (Assez complet, disponible sur le WEB)



Combien de temps faut-il pour former un spécialiste en cryptage ?

Partie 1 : Cryptographie ?

Cryptos ($\chiρυπτοσ$) : caché, dissimulé

Graphein ($\gammaραφειν$) : écrire

Objectifs de la cryptographie :

Confidentialité : transmettre des données de telle sorte que seul le destinataire autorisé puisse les lire.

Intégrité : s'assurer que les données reçues n'ont pas été modifiées durant la transmission.

Authentification : permettre d'identifier des personnes ou des entités et de certifier cette identité.

Cryptographie ?

Cryptographie : marquée par des logiques de guerre, sujet entouré de mystère y compris chez les militaires où il n'était connu que d'un noyau de spécialistes.

Première attitude : statut proche de celui des armes de guerre.

Les gouvernements contraints d'y renoncer : pression des besoins du marché, difficultés d'application des mesures réglementaires, explosion des échanges sur tous les réseaux.

Aujourd'hui, les choses ont bien changé : concurrence économique au lieu de la guerre froide. La cryptographie est devenue de plus en plus fréquente.

Du domaine militaire aux communications par Internet, en passant par les transactions commerciales et bancaires. Il est difficile d'y échapper.

Aujourd'hui, nous sommes tous concernés par la cryptographie.

Vocabulaire

Cryptologie : Science des messages secrets. Elle se décompose en deux disciplines: la cryptographie et la cryptanalyse.

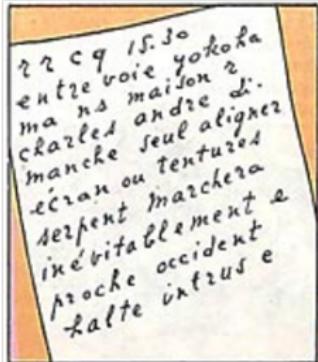
Cryptographie : Art de transformer un message clair en un message inintelligible. Cependant, on utilise souvent le mot cryptographie comme synonyme de cryptologie.

Cryptanalyse : Art d'analyser un message chiffré afin de le décrypter.

Stéganographie : Branche particulière de la cryptographie qui consiste non pas à rendre le message inintelligible, mais à le camoufler dans un support (texte, image, etc.) de manière à masquer sa présence.

Stéganographie

Hergé, le lotus bleu, Casterman, p. 1



Stéganographie



George Sand (1804 - 1876)

George SAND :

Je suis très émue de vous dire que j'ai bien compris l'autre soir que vous aviez toujours une envie folle de me faire danser. Je garde le souvenir de votre baiser et je voudrais bien que ce soit là une preuve que je puisse être aimée par vous. Je suis prête à vous montrer mon affection toute désintéressée et sans calcul, et si vous voulez me voir aussi vous dévoiler sans artifice mon âme toute nue, venez me faire une visite. Nous causerons en amis, franchement. Je vous prouverai que je suis la femme sincère, capable de vous offrir l'affection la plus profonde comme la plus étroite en amitié, en un mot la meilleure preuve que vous puissiez rêver, puisque votre âme est libre. Pensez que la solitude où j'habite est bien longue, bien dure et souvent difficile. Ainsi en y songeant j'ai l'âme grosse. Accourez donc vite et venez me la faire oublier par l'amour où je veux me mettre.

Réponse d' Alfred de MUSSET :

*Quand je mets à vos pieds un éternel hommage
Voulez-vous qu'un instant je change de visage ?
Vous avez capturé les sentiments d'un cœur
Que pour vous adorer forma le Créateur.
Je vous chéris, amour, et ma plume en délire
Couche sur le papier ce que je n'ose dire.
Avec soin, de mes vers lisez les premiers mots
Vous saurez quel remède apporter à mes maux.*

Réponse finale de George SAND :

*Cette insigne faveur que votre cœur réclame
Nuit à ma renommée et répugne mon âme.*

Vocabulaire (suite)

Chiffre : Ensemble de procédés et ensemble de symboles (lettres, nombres, etc.) employés pour remplacer les lettres du message à chiffrer.

Chiffrement : Procédé grâce auquel on peut rendre la compréhension d'un document impossible à toute personne qui n'a pas la clé.

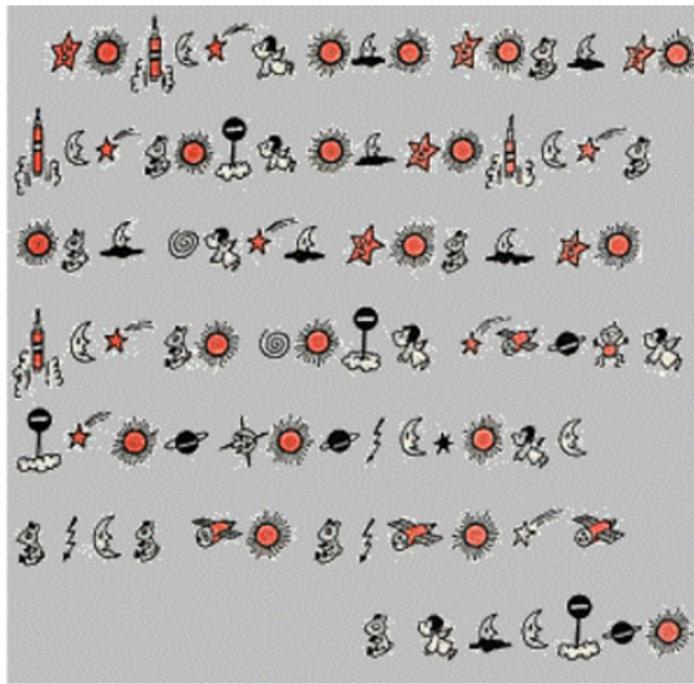
Chiffrer : Transformer un message afin qu'il ne soit lisible qu'à l'aide d'une clé.

Déchiffrer : Opération inverse du chiffrement, i.e. obtenir la version originale d'un message qui a été précédemment chiffré en connaissant la méthode de chiffrement et les clés (contrairement à décrypter).

Décrypter : Restauration des données qui avaient été chiffrées à leur état premier ("en clair"), sans disposer des clés théoriquement nécessaires.

Exemple

Un des moyens les plus simples de chiffrer un message est de remplacer chaque lettre par une autre (ou un autre symbole).



Exemple

Par sa simplicité et par sa force, ce système a dominé la technique des écritures secrètes pendant tout le premier millénaire.

Il a résisté aux cryptanalystes jusqu'à ce que le savant arabe **Abu Yusuf Ya'qub ibn Is-haq ibn as-Sabbah Oòmran ibn Ismaïl Al-Kindi** mette au point, au IXème siècle, une technique appelée **analyse des fréquences**.

Concours Alkindi : compétition de cryptographie pour les classes de 4e, 3e et 2de.
<https://www.concours-alkindi.fr>



Analyse des fréquences : Al-Kindi (801-873)

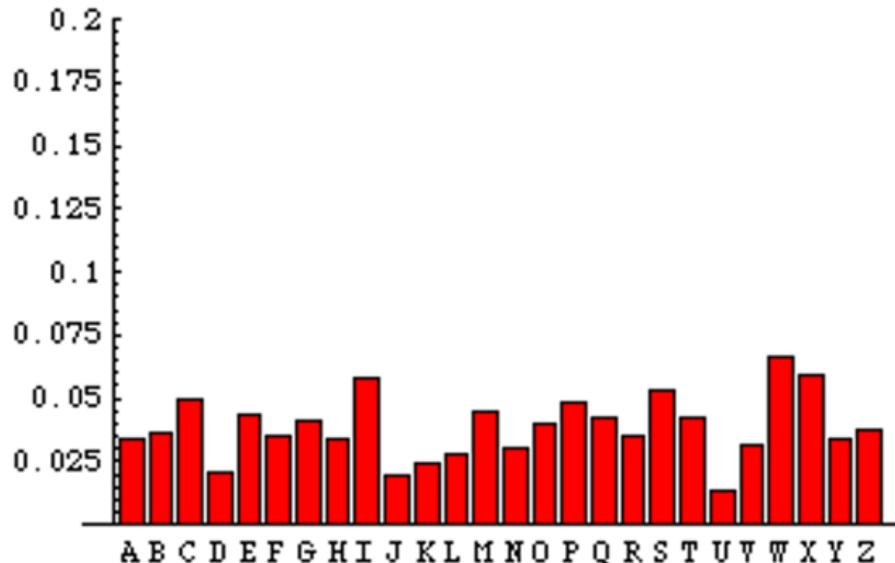
"Manuscrit sur le déchiffrement des messages cryptographiques"

Premier manuscrit mentionnant la fréquence d'apparition des lettres.
La plus ancienne description de la cryptanalyse par analyse des fréquences.

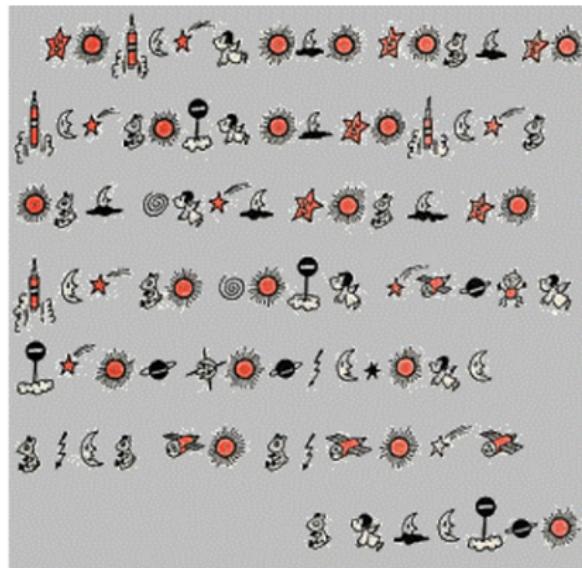
Al-Kindi explique : "la façon d'élucider un message crypté, si on sait dans quelle langue il est écrit, est de **se procurer un autre texte en clair** dans la même langue, de la longueur d'un feuillet environ, et de **compter alors les apparitions de chaque lettre**. Ensuite, on **se reporte au texte chiffré** qu'on veut éclaircir et on relève de même ses symboles. On **remplace le symbole le plus fréquent par la lettre première (la plus fréquente du texte clair)**, le suivant par la deuxième, le suivant par la troisième, et ainsi de suite jusqu'à ce qu'on soit venus à bout de tous les symboles du cryptogramme à résoudre."

Analyse des fréquences

Cette technique ne fonctionne bien que si le message chiffré est suffisamment long pour avoir des moyennes significatives.



Exemple



Réponse : ce qui a été, c'est ce qui sera et ce qui s'est fait, c'est ce qui se fera, il n'y a rien de nouveau sous le soleil. Saturne.

Vocabulaire

Code : ensemble de procédés et de symboles (lettres, nombres, signes, etc.) employés pour remplacer les mots du message à coder.



- | | |
|---|--|
| <input checked="" type="checkbox"/> SOUS | <input type="checkbox"/> PENSER AUX |
| <input type="checkbox"/> LAISSE | <input type="checkbox"/> ENTERRE |
| <input checked="" type="checkbox"/> IL FAUT | <input type="checkbox"/> NOËL |
| <input checked="" type="checkbox"/> LES | <input type="checkbox"/> APRÈS |
| <input type="checkbox"/> ILS ÉTAIENT | <input type="checkbox"/> ON SAIT |
| <input type="checkbox"/> LE JARDIN | <input checked="" type="checkbox"/> ONC'DONALD |
| <input type="checkbox"/> MERCI | <input checked="" type="checkbox"/> LE CHARBON |
| <input type="checkbox"/> DESSUS | <input checked="" type="checkbox"/> BOÎTES |
| <input type="checkbox"/> PETITS | <input type="checkbox"/> CADEAUX |
| <input checked="" type="checkbox"/> DES | <input type="checkbox"/> LA PENDERIE |
| <input type="checkbox"/> DÉJÀ | <input type="checkbox"/> UN ARBRE |
| <input type="checkbox"/> ET PLANTER | <input checked="" type="checkbox"/> FOUINEURS |
| <input type="checkbox"/> DIX MINUTES | <input type="checkbox"/> AURA POUR |
| <input type="checkbox"/> DE | <input type="checkbox"/> CE QU'ON |
| <input type="checkbox"/> JE VAIS | <input checked="" type="checkbox"/> TROUVERONT PAS |
| <input checked="" type="checkbox"/> DANS | <input type="checkbox"/> EN AOÛT |
| <input type="checkbox"/> ILS NE | <input checked="" type="checkbox"/> PATINS |
| <input type="checkbox"/> REGARDE | <input type="checkbox"/> TU AS |

Cryptogramme : Le message chiffré.

Cryptosystème : L'algorithme de chiffrement.

Vocabulaire (fin)

Mono-alphabétique : Se dit d'un chiffre où une lettre du message clair est toujours remplacée par le même symbole. On a donc une bijection entre les lettres claires et les symboles de l'alphabet de chiffrage.

Exemple: le chiffre de César.

Poly-alphabétique : Se dit d'un chiffre où plusieurs alphabets de chiffrement sont utilisés en même temps. Exemples: le chiffre de Vigenère.

Substitution : Un chiffre à substitution remplace les caractères du message en clair par des symboles (caractères, nombres, signes, etc.) définis à l'avance.

Transposition : Un chiffre de transposition ne modifie pas le contenu du message mais mélange les caractères selon une méthode prédéfinie.

Substitution / Transposition

Le chiffrement d'un message repose sur la substitution et/ou la transposition.

Substitution : changement des lettres du « clair » par d'autres lettres ou symboles.

Clair : M E S S A G E S E C R E T.

Chiffré : N F T T B H F T F D S D U.

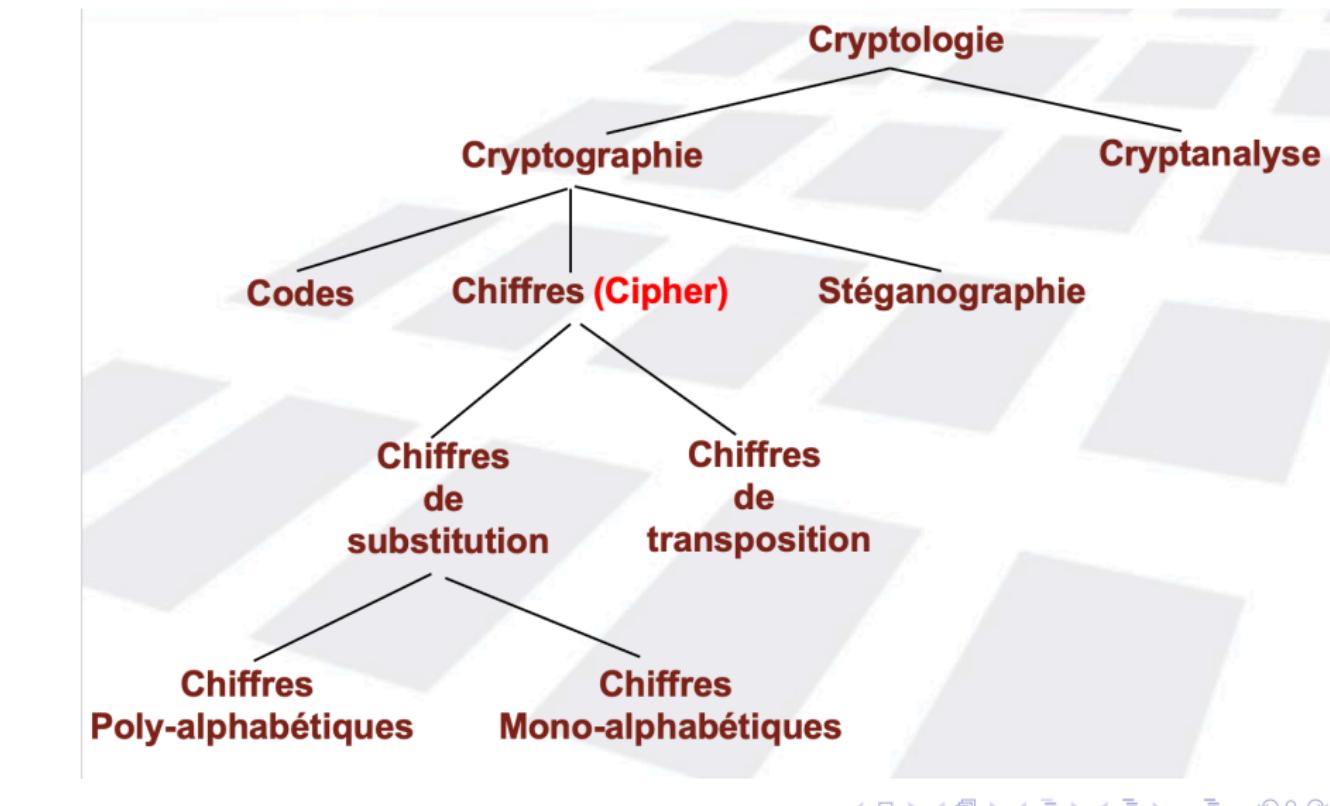
Transposition : consiste à changer l'ordre des lettres.

Clair : M E S S A G E S E C R E T.

Chiffré : E M S S G A E E S R C T E.

Ce sont les deux grands principes de la cryptologie, principes connus dès l'antiquité.

Classification



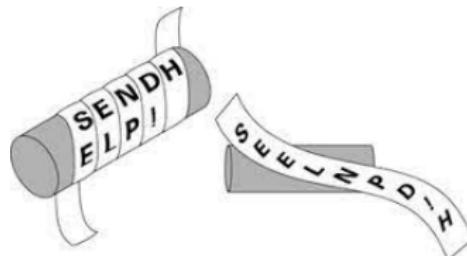
Petite histoire de la cryptologie

Les 3000 premières années (2000 av. J.C. 1000) :

1900 avant J.C. : Un **scribe égyptien** a employé des hiéroglyphes non conformes à la langue correcte dans une inscription. On le qualifie de premier exemple documenté de cryptographie écrite.

1500 avant J.C. : Une tablette d'argile est retrouvée sur les bords du Tigre, en Irak, sur laquelle un **potier babylonien** a gravé un texte codé pour dissimuler la recette de son succès (un vernis).

487 avant J.C. : Les grecs emploient un dispositif appelé la **scytale**, un bâton autour duquel une bande longue et mince de cuir (ceinture) était enveloppée et sur laquelle on écrivait le message.



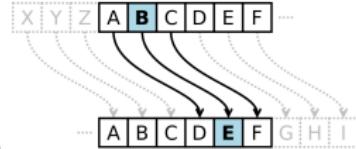
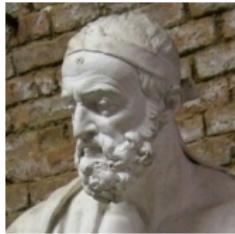
Petite histoire de la cryptologie

Les 3000 premières années (2000 av. J.C. 1000) :

205 - 126 avant J.C. :

Le Grec Polybe a inventé un moyen simple de crypter les messages : **le Carré de Polybe**. Pour chiffrer une lettre, on la remplaçait par ses coordonnées. Ainsi, F donne (2, 1), X donne (5, 3), etc.

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I/J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z



50 avant J.C : Sacré Jules !

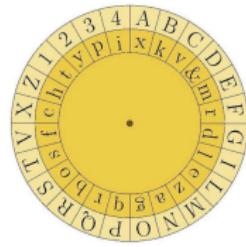
Un des premiers personnages connus pour avoir utilisé des chiffres mathématiques. Il a mis au point un algorithme de chiffrement très simple : **le chiffrement par décalage**.

Moyen Age et Renaissance

1379 : Gabriel de Lavinde, secrétaire du pape Clément VII, inaugure, au XIV^e siècle, le système de code secret le plus employé en occident jusqu'à la Première Guerre mondiale : **Nomenclateur**. C'est un dictionnaire qui permet de transcrire en chiffres ou en signes des mots et des syllabes courantes.

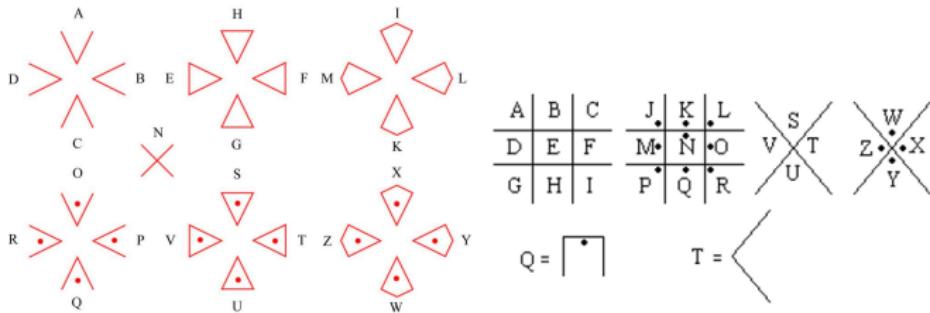
1466 : Les 25 pages manuscrites de Leon Battista Alberti constituent le plus ancien manuel de cryptologie occidental.

Méthode de chiffrement : **le disque à chiffrer** où l'alphabet du petit disque mobile, dans le désordre, constituait un alphabet de substitution. Longtemps oublié, il ne réapparut qu'en 1867, à l'exposition universelle de Paris où il passa pour l'invention de l'Anglais Charles Wheatstone.



XVI^{ème} siècle

Chiffre des templiers : correspondance entre l'alphabet et une suite de figures géométriques issues de la Croix de Malte. La franc-maçonnerie s'en inspira pour créer le système du "case-cochon".



A la même époque, **Blaise de Vigénère (1523 - 1596)** met au point un nouveau système. Il remplit une grille de 26 rangées sur 26 colonnes avec toutes les lettres de l'alphabet. Ce mode de chiffrement est devenu célèbre car c'était l'un des premiers à ne pas associer toujours les deux mêmes lettres comme le disque à chiffrer.



Marie-Antoinette (1755 - 1793)

Chiffre polyalphabétique (Vigénère) pour communiquer avec le comte Axel de Fersen.

Tableau de 22 lettres : les lettres manquantes sont J, K, U et W. Usage venant du latin où I et J d'un côté, U et V de l'autre sont confondues. K peut être remplacé par C et W par V.



Exemple : Chiffrer "Je vous aime" avec la clé "SEL".

TABLEAU DE 22 LETTRES		
A	B C D E F G H I L M	
O P Q R S T V X Y Z N		
C D	M A B C D E F G H I L	
Z N O P Q R S T V X Y Z		
E F	L M A B C D E F G H I	
N O P Q R S T V X Y Z		
G H	I L M A B C D E F G H	
N O P Q R S T V X Y Z		
I L	H I L M A B C D E F G	
N O P Q R S T V X Y Z		
M N	G H I L M A B C D E F	
N O P Q R S T V X Y Z		
O P	F G H I L M A B C D E	
S T	N O P Q R S T V X Y Z	
Q R	E F G H I L M A B C D	
S T	N O P Q R S T V X Y Z	
S T	D E F G H I L M A B C	
V X	N O P Q R S T V X Y Z	
Y Z	B C D E F G H I L M A	
N O P Q R S T V X Y Z		

J	E	V	O	U	S	A	I	M	E
S	E	L	S	E	L	S	E	L	S
S	T	D	E	F	B	X	Z	Q	O

En réalité :

J	E	V	O	U	S	A	I	M	E
S									
J	O	V	M	U	B	A	S	M	T



CHIFFRE
DE S. M. MARIE ANTOINETTE,

Histoire (suite)

Jerome Cardan (1501 – 1576) : Principe de la grille trouée.

Grille trouée en place, l'expéditeur écrit son message. En retirant la grille, il complète les trous par des lettres au hasard. Le destinataire applique la même grille pour lire le message.



J	A	R		I	V	E		R
A		I	D		B	M		A
N	A		C	I	N		Q	H
	E		U	R		E	S	

JSIAR VHR NIMVNE BGDKIRT
HIAJFGIEIDDFSJE DM JHNIA DI
LNHO AASC CJI HNHGFSQGCH
JMBESDGDUI RJRU EFIS VDFCN



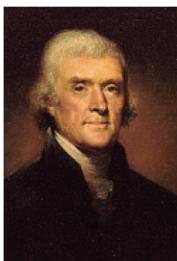
Benedict Arnold (1741 - 1801) : directeur de l'académie militaire américaine de West Point vendait aux Anglais des renseignements importants. Il codait chaque mot en le remplaçant par trois nombres : le numéro de la page du dictionnaire sur laquelle il figurait, le numéro de la ligne sur laquelle il se trouvait, et enfin le numéro du mot dans la ligne.

Histoire (suite)

Thomas Jefferson (1743 - 1826) : a mis au point une machine à chiffrer.

Un cylindre constitué de quelques roues fixées sur un axe. Sur chaque roue se trouvait l'alphabet complet mais dans des ordres différents.

Le président écrivait alors son message sur une ligne. Il choisissait ensuite une autre ligne au hasard où les lettres ne voulaient plus rien dire. Le correspondant écrivait alors ce message sur son propre cylindre et le faisait tourner pour trouver une ligne intelligible qui correspond au message.



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

< Message en clair

< Message codé

XIX^{ème} et début du XX^{ème} siècle

L'essor des communications (1800 - 1970) : moyens de transports rapides, journaux, télégraphe ... Une nouvelle impulsion à la cryptologie.

Les guerres modernes utilisent abondamment les télécommunications; l'interception devient simple et décrypter les informations devient vital.
L'ère industrielle de la cryptologie.

La Première Guerre mondiale : l'essentiel des télécommunications est transmis par radio. **Avantage à la cryptanalyse !**

Le chiffre ADFGVX est constitué d'une substitution de type carré de Polybe, suivie d'une transposition.

Georges Painvin : polytechnicien, paléontologue et un des génies de la cryptologie a déchiffré un des messages envoyés par les allemands avec le chiffre ADFGVX et contribua à la victoire en 1918.



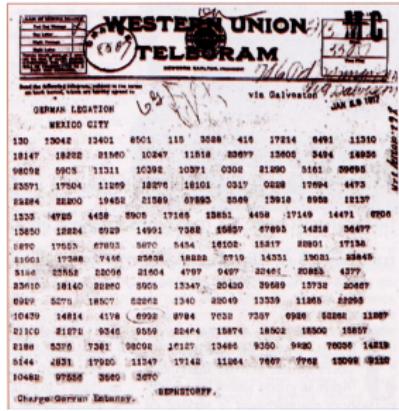
L'affaire du télégramme de Zimmermann

Comment la cryptanalyse d'un message chiffré a fait basculer les Etats-Unis dans la guerre en 1917 et changé le cours de l'histoire !

Arthur Zimmermann, ministre allemand des affaires étrangères, voulait retarder l'envoi de renforts américains en les occupant sur d'autres fronts, créés par le Mexique et le Japon.

Les anglais ont intercepté, déchiffré et transmis aux USA le message envoyé par Zimmermann, en janvier 1917, à Bernstoff, ambassadeur d'Allemagne aux États-Unis, pour lui faire part de son projet.

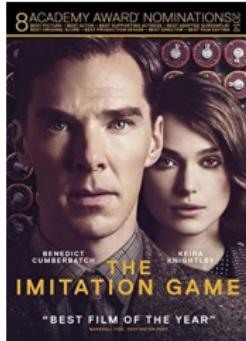
<https://www.bibmath.net/crypto/index.php?action=affiche&quoi=debvingt/zimmermann>



XIX^{ème} et début du XX^{ème} siècle

La Seconde Guerre mondiale : Pendant la seconde guerre mondiale, les Allemands utilisaient une machine pour crypter leurs messages : **Enigma**.

Réputé inviolable, le secret céda devant des mathématiciens de génie : **Marian Rejewski (1905 - 1980)**, Mathématicien Polonais à l'origine de la première attaque au début des années 1930, **Alan Turing (1912 - 1954)** leader du service de décryptage anglais, baptisé Ultra.



XIX^{ème} et début du XX^{ème} siècle

Vers 1960 : l'arrivée de l'informatique a supplanté les machines de chiffrement électromécanique (type Enigma).

DES (pour Data Encryption Standard), l'inviolable ?

Début 1960, IBM lance un programme de recherche sur le chiffrement.

Début 1970, Horst Feistel développe le chiffre Lucifer, qui inspira plus tard le chiffre DES et d'autres chiffres.

En 1975, le résultat est proposé aux banques (initiative qui n'a pas plu au NSA : National Security Agency). Jugé difficile à percer, le ministère de la défense des Etats-Unis l'a adopté et a contrôlé son exportation.

Mis à jour tous les cinq ans environ et n'étant plus limité, les ordinateurs modernes ont remis en cause son inviolabilité.

Nécessité de le changer (AES : pour Advanced Encryption Standard).

La révolution : la cryptographie à clé publique

Jusque là, tous les systèmes proposés avaient un **talon d'Achille : la clé**.

C'est bien joli de chiffrer ses messages, mais encore faut-il que le destinataire ait la clé. La clé circule, et peut être interceptée.

1976 : Whitfield Diffie et Martin Hellman publient New Directions in Cryptography, introduisant l'idée de **cryptographie à clé publique**.

Solution entièrement nouvelle au problème de l'échange de clés.

"L'habileté dans la cryptanalyse a toujours été lourdement du côté des professionnels, mais l'innovation, en particulier dans la conception des nouveaux types de systèmes cryptographiques, est venue principalement d'amateurs."



Le RSA

1979 : Naissance du RSA, au Weizmann Institute en Israël.



A. **S**hamir

(1952 - ...)

R. **R**ivest

(1947 - ...)

L. **A**dleman

(1945 - ...)

Il permet de distribuer librement la clé publique, mais sans que personne ne puisse décrypter les messages ainsi chiffrés.

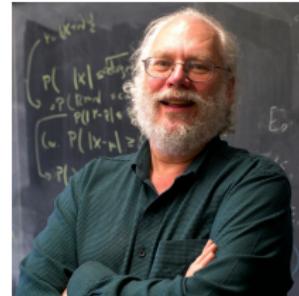
Le futur ?

L'informatique fait entrer la cryptologie dans son ère moderne. La grande invention fut la **cryptographie à clé publique**.

Le futur sera peut-être la **cryptographie quantique** (les bits sont remplacés par les qbits).

David Deutsch (1953 - ...) : physicien israélo-britannique qualifié de "Père de l'informatique quantique" par "The Economist".

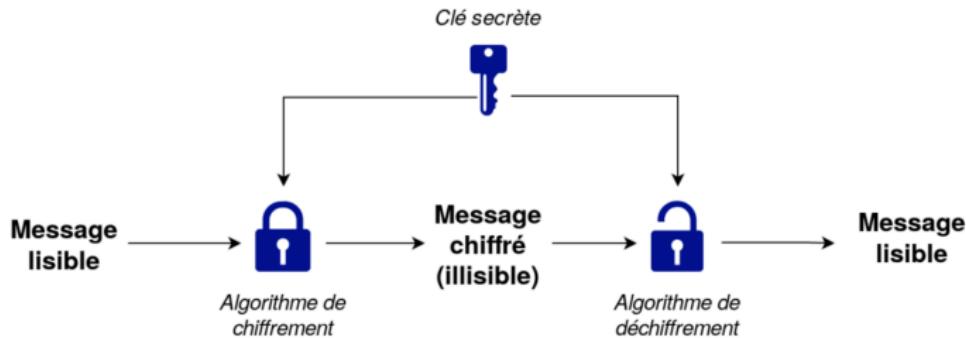
Peter Shor (1959 - ...) : mathématicien américain, a inventé un algorithme quantique de factorisation (implanté en 2001 par IBM sur le premier ordinateur quantique 7qbits, résultat : factoriser $15 = 3 \times 5$!).



Cryptographie classique

Cryptographie conventionnelle, également appelée cryptographie à clé secrète ou à clé symétrique : une seule clé suffit pour le chiffrement et le déchiffrement.

Le DES est un exemple de système de **chiffrement symétrique**.



Chiffre de César (60-50 avant J.C.)

C'est un **chiffrement symétrique mono-alphabétique**. Consiste simplement à remplacer une lettre par une autre, en utilisant un alphabet désordonné. L'alphabet désordonné est obtenu par **décalage** des lettres.
Ex : 3 rangs vers la gauche pour Jules César (d'où le nom).

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

"Ave Caesar morituri te salutant"

devient

DYH FDHVDU PRULWXUL WH VDOXWDQW

Par exemple, on pourrait utiliser la grille de chiffrement ci-dessous:

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

Pb : difficile de se souvenir de la grille de chiffrement

Chiffre de Vigenère (1585)

Blaise de Vigenère (1523-1596) : diplomate français à Rome.

Vers 1560, Vigenère considéra qu'il avait mis de côté assez d'argent pour abandonner sa carrière et se consacrer à l'étude en détail des idées de ses prédécesseurs Alberti, Trithème, Bellaso et Porta. C'est du nom de Vigenère que ce nouveau chiffre fut baptisé, en l'honneur de l'homme qui lui donna sa forme finale.

Blaise de Vigenère écrit son "Traité des chiffres" ou "Secrètes manières d'écrire" paru pour la première fois en 1586. Il présente entre autres un tableau que l'on dénomme aujourd'hui **carré de Vigenère**.

Amélioration décisive du chiffre de César, sa force réside dans l'utilisation non pas d'un mais de **26 alphabets décalés pour chiffrer un message**. On peut résumer ces décalages avec le carré de Vigenère.

Chiffre de Vigenère (1585)

Ce chiffre utilise une clé qui définit le décalage pour chaque lettre du message (A: décalage de 0 cran, B: 1 cran, C: 2 crans, ..., Z: 25 crans).

Chiffrer "CHIFFRE DE VIGENERE" avec la clé "BACHELIER"

La clé est éventuellement répétée plusieurs fois pour être aussi longue que le texte clair.



Clair	:	C H I F F R E D E V I G E N E R E
Clé	:	B A C H E L I E R B A C H E L I E
Décalage	:	1 0 2 7 4 1 1 8 4 1 7 1 0 2 7 4 1 1 8 4
Chiffré	:	D H K M J C M H V W I I L R P Z I

Carré de Vigenère

Comment utiliser le carré de Vigenère ?

Vigenère (chiffré = clair + clé)



Exemple :

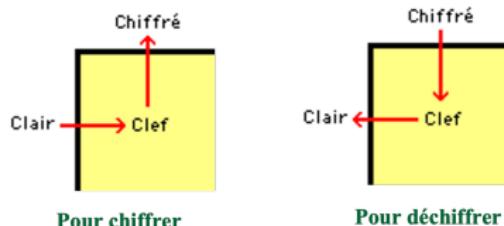
clair : HELLOWORLD
clé : ECSECSECSE
chiffré : LGDPQOSTDH

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	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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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

Carré de Vigenère

Autre possibilité :

Beaufort (chiffré = clé - 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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	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

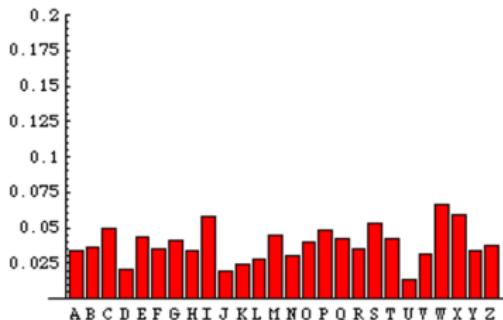
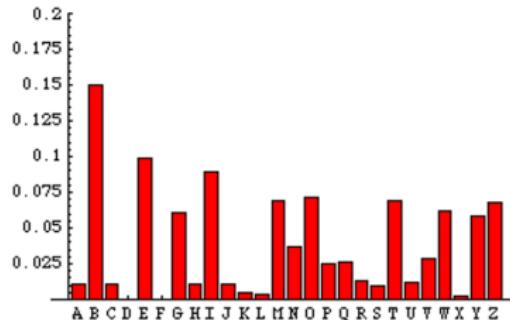
Exemple :

clair : HELLOWORLD
clé : ECSECSECSE
chiffré : XYHTOWQLHB

Fréquence d'apparition des lettres

Force de Vigenère : une même lettre sera chiffrée de différentes manières. L'analyse des fréquences classique est inutilisable.

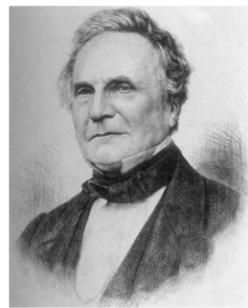
Fréquences des lettres d'une fable de la Fontaine (Le chat, la belette et le petit lapin) chiffrée avec une substitution simple et celles de la même fable chiffrée avec le chiffre de Vigenère.



Chiffre de Vigenère (1585)

Longtemps considéré comme indécryptable, légende si tenace que même en 1917, plus de 50 ans après avoir été cassé, il était donné pour "impossible à décrypter" par la très sérieuse revue Scientific American.

En 1854, **Charles Babbage (1792-1871)** casse le chiffre de Vigenère, mais sa découverte resta ignorée, car il ne la publia pas. Ce travail ne fut mis en lumière qu'au 20e siècle, lors de recherches effectuées sur l'ensemble des papiers de Babbage.



Il a aussi été trouvé et publié par Kasiski en 1863 qui rédigea "Die Geheimschriften und die Dechiffrierkunst" où il présentait le test qui allait porter son nom : le **test de Kasiski**.

Casser le chiffre de Vigenère

En prenant par exemple la clé KILO, la lettre E peut être chiffrée en O, M, P ou S selon que K, I, L ou O sont utilisés pour la chiffrer.

Le mot "thé" est chiffré "DPP" 2 fois et "BSS" 1 fois.

K	I	L	O	K	I	L	O	K	I	L	O	K	I	L	O	K								
the	r	u	s	s	e	t	h	e	j	a	s	m	i	n	t	h	e	c	h	i	n	e		
D	P	P	F	E	A	D	S	D	P	P	X	K	A	X	W	X	B	S	S	M	P	T	B	O

Babbage comprit que ces **répétitions** permettent d'attaquer Vigenère.

Chercher des séquences de lettres qui apparaissent plus d'une fois.

Soit la même séquence de lettres du texte clair a été chiffrée avec la même partie de la clé

Soit deux suites de lettres différentes dans le texte clair auraient par pure coïncidence engendré la même suite dans le texte chiffré (peu probable).

Méthode : déduire le nombre de facteurs de la clé puis par une méthode de fréquence de distribution des lettres cryptées déduire les lettres du texte clair.

Décrypter un texte chiffré avec Vigenère

Pour attaquer un chiffre de Vigenère, il faut trouver la clé ! Si la clé est courte et le texte long, c'est possible.

Commencer par deviner la longueur de la clé. Chercher des séquences de plusieurs lettres consécutives qui apparaissent plusieurs fois.

XAUNM EESYI EDTLL FGSNB WQUFX PQTYO RUTYI IN**UMQ** IEULS MFAFX
GUTYB XXAGB HMIFI IM**UMQ** IDEKR IFRIR ZQUHI ENOO**O** **IGRML** YETYO
VQRYS IXEOK IYPY**O** **IGRFB** WPIYR BQURJ IYEMJ **IGRYK** XYACP PQSPB
VESIR ZQRUF REDY**J** **IGRYK** XBLOP JARNP UGEFB WMILX MZSMZ YXPNB
PUMYZ MEEFB UGENL RDEPB JXONQ EZTMB WOEFI IPAHP PQBFL GDEM**F**
WFAHQ

Déchiffrer un texte chiffré avec Vigenère

D'après l'emplacement de ces groupes, déduire la longueur de la clé.

Ce renseignement est capital. Si, par exemple, la longueur de la clé est 3, cela signifie que les caractères de rang 1, 4, 7, 10, ..., $3k + 1$, sont simplement décalés à la manière du chiffre de César.

On peut donc appliquer maintenant l'analyse de fréquences à ces caractères et trouver la première lettre de la clé.

Pour la deuxième lettre de la clé, on analysera les fréquences des caractères de rang $3k + 2$ et pour la dernière lettre les fréquences des caractères de rang $3k$.

Exemple complet

KQOWE FVJPU JUUNU KGLME KJINM WUXFQ MKJBG WRLFN
FGHUD **WUU**MB SVLPS NCMUE KQCTE SWREE **KOYSS** IWCTU
AXYOT APXPL WPNTC GOJBG FQHTD **WXIZA YGFFN** SXCSE
YNCTS SPNTU JNYTG GWZGR **WUU**NE JUUQE APYME KQHUI
DUXFP GUYTS MTFFS **HNUOC ZGM** RU WEYTR GKMEC DCTVR
ECFBP JQCUS WVBNP LGOYL SKMTE FVJJT WWMFM WPNME
MTMHR SPXFS SKFFS **TNUOC ZGM DO EOYEE KCPJRG** PMURS
KHFRS EIUEV GOYC**W XIZAY** GOSAA NYDOE OYJLW UNHAM
EBFEL XYVLW NOJNS IOFRW UCCES WKVID **GMUCG** OCRUW
GNMAA FFVNS IUDKE QHCEU CPFCM PVSUD GAVEM NYMAM
VLFMA OYFNT QCUAF VFJNX KLNEI WCWOD CCULW RIFTW
GMUSW OVMAT NYBUH TCOCW FYTNM GYTQM KBBNL GFBTW
OJFTW GNTEJK NEEDC LDHWT VBUVG FBIJG

Il faut d'abord chercher des séquences de lettres qui apparaissent plus d'une fois dans le texte.

Exemple complet

Séquence répétée	Espace de répétition	Longueurs de clef possibles			
		2	3	5	19
WUU	95			x	x
FEK	200	x		x	
WXIZAYG	190	x		x	x
NUOCZGM	80	x		x	
DOEOY	45		x	x	
GMU	90	x	x	x	

Les facteurs premiers du nombre de caractères entre deux débuts de séquences figurent dans le tableau (ex. $95 = 5 \times 19$).

Toutes les périodes sont divisibles par 5. Tout se cale parfaitement sur un mot-clé de 5 lettres.

Il va falloir découvrir les lettres qui composent la clé: L1-L2-L3-L4-L5.

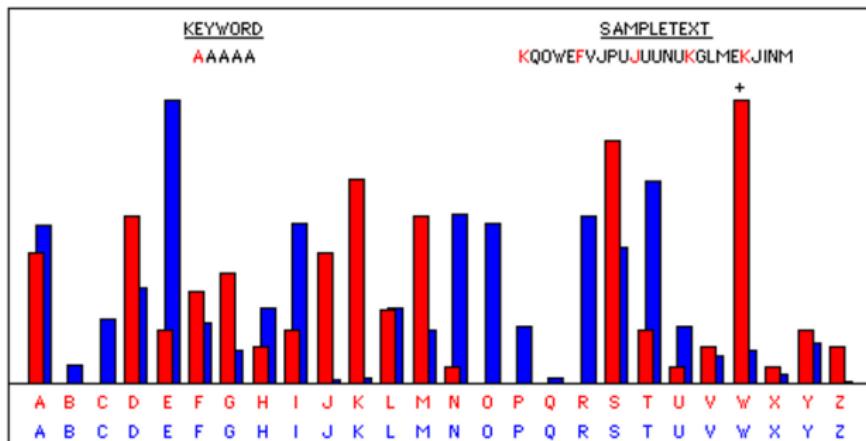
Exemple complet

Déterminer L1 : La ligne du carré de Vigenère, définie par L1, pilote l'alphabet chiffré pour la 1^{ère}, la 6^{ème}, la 11^{ème} ... lettres du message.

En regardant la 1^{ère}, la 6^{ème}, la 11^{ème} ... lettres du texte chiffré on peut utiliser l'analyse des fréquences.

Tracer le graphique montrant la distribution des lettres qui apparaissent à la 1^{ère}, la 6^{ème}, la 11^{ème} ... dans le texte chiffré

KQOWEFVJPUJUUNUKG ... , soit K, F, J, ...

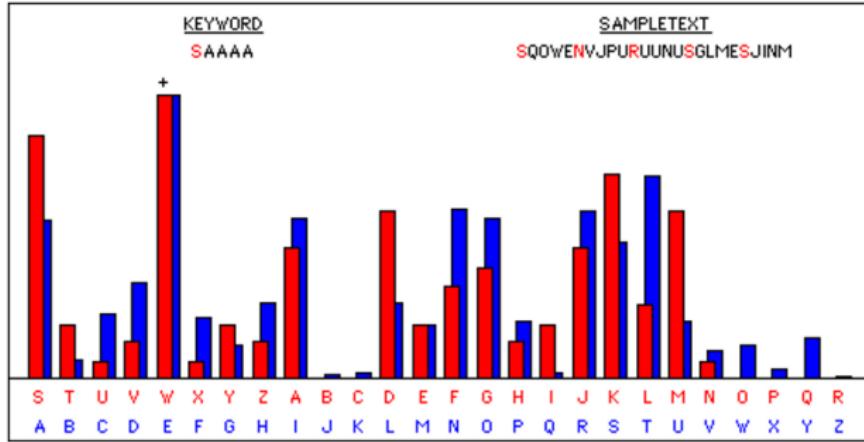


Exemple complet

La répétition ci-dessus (en rouge) présente des traits communs avec celle de l'alphabet courant (en bleu) décalée de 18 crans. Le pic bleu le plus important se trouve sur le E et le pic rouge sur le W.

En superposant les deux graphiques pour qu'ils aient la même silhouette générale, on constate que la 1^{ère} lettre de la clé L1 est S.

L1	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	
S	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



Exemple complet

On recommence la même démarche pour identifier L2-L3-L4-L5.

L2	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
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	
L3	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
U	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
L4	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
L5	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	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

La clé est : S C U B A

Souvent pour s'amuser les hommes d'équipage prennent des albatros, vastes oiseaux des mers, qui suivent, indolents compagnons de voyage, le navire glissant sur les gouffres amers. A peine les ont-ils déposés sur les planches que ces rois de l'azur, maladroits et honteux, laissent piteusement leurs grandes ailes blanches, comme des avirons, traîner à côté d'eux. Ce voyageur ailé, comme il est gauche et veule, lui naguère si beau, qu'il est comique et laid. L'un agace son bec avec un brûle-gueule, l'autre mime en boitant l'infirme qui volait. Le poète est semblable au prince des nuées, qui hante la tempête et se rit de l'archer. Baudelaire

ENIGMA

Inventée en 1920 par un ingénieur allemand
Arthur Scherbius (1878-1929).



Deux claviers : un pour le texte en clair,
l'autre pour le texte chiffré.

Le cryptage d'Enigma repose sur plusieurs roues : sur chacune d'entre elles se trouve l'alphabet dans un ordre différent.

3 rotors arrangés dans un ordre connu de l'opérateur et du destinataire pour une période donnée (3 mois jusqu'à fin 1935, tous les mois jusqu'à septembre 1936, et tous les jours à partir d'octobre 1936).



Fonctionnement d'ENIGMA

Chiffrer : on tape la lettre sur le premier clavier. La lettre chiffrée s'allume sur le deuxième clavier.

Déchiffrer : on tape la lettre chiffrée sur le deuxième clavier, la lettre du message déchiffré s'allume sur le premier clavier.

La clé est composé de trois lettres : les **positions initiales des 3 rotors**.

Lorsque le premier caractère est tapé, la machine repère le caractère correspondant sur le premier rotor grâce à des connections entre les rotors, fait de même pour le rotor suivant... Elle affiche enfin le caractère correspondant sur le dernier rotor. Ce dernier tourne alors d'un cran.

On recommence ensuite pour la deuxième lettre et ainsi de suite jusqu'à ce que le rotor ait fait un tour complet. Le second rotor avance alors d'un cran. Et on recommence...

Pour chaque rotor, **on multiplie par 26 le nombre d'alphabets de substitution**. Enigma avait jusqu'à 4 rotors !

Fonctionnement d'ENIGMA

Clé : 3 lettres (positions initiales des rotors).

Tableau de connexions avec six câbles.

Mise à clé : brancher les 6 câbles du tableau de connexions, placer les trois rotors dans l'ordre indiqué par le tableau des clés (position secrète).

Choisir une clé de message : QWE.

Saisir 2 fois : QWEQWE WTRBAZ

Rotors sur : QWE

Saisir le texte et noter le résultat : JOZNXPSU

On transmet : WTRBAZJOZNXPSU



En réception : rotors sur position secrète, on déchiffre WTRBAZ : QWEQWE

On positionne les trois rotors sur QWE et on déchiffre le reste du texte JOZNXPSU

Fonctionnement d'ENIGMA

Chacun des rotors peut être réglé sur 1 des 26 positions.

Il y a donc $26 \times 26 \times 26$ dispositions $\Rightarrow \mathbf{17\,576}$

Les trois rotors (1,2,3) peuvent être placés selon les 6 dispositions suivantes : 123, 132, 213, 231, 312, 321 $\Rightarrow \mathbf{6}$

Tableau de connexions à fiches :

Le nombre de branchements possibles en appariant 6 fois 2 lettres prises parmi les 26 de l'alphabet est énorme $\Rightarrow \mathbf{100\,391\,791\,500}$

D'où le nombre total de clés, produit de ces trois facteurs :

$$\mathbf{17576 \times 6 \times 100391791500 = 1.05869e16 \approx 10\,000\,000\,000\,000\,000}$$

La cryptographie

D'abord un art, la cryptographie est devenue une science lorsque l'apport des **mathématiques** est devenu capital notamment avec l'introduction du concept de clé publique.

Pourtant, aujourd'hui encore, la **sécurité** n'est pas fondée sur des preuves formelles, mais sur la **difficulté à résoudre un problème mathématique** par le calcul **en temps raisonnable**, comme celui de la factorisation des grandes entiers (chiffre RSA).

Système de chiffrement théoriquement indécryptable ?



Réponse : "one time pad" démontré par Claude Shannon en 1949 (Communication theory of secrecy system).

Clé aléatoire, de longueur égale au message et n'est utilisée qu'une fois.

Utilisé au haut niveau (téléphone rouge).

Partie 2

Cryptographie

Le vocabulaire stabilisé en français est le suivant :

On **chiffre** des messages ;

On **déchiffre** des messages si on a la clé ;

On **décrypte** des messages si on n'a pas la clé.

On distingue deux types d'algorithmes cryptographiques : les **algorithmes symétriques** qui utilisent la même clé pour chiffrer et déchiffrer les messages et les **algorithmes asymétriques** qui utilisent deux clé, une clé servant à chiffrer et l'autre à déchiffrer.

Les algorithmes symétriques sont rapides et performants au niveau de la qualité de la cryptographie.

Défaut majeur : les deux parties doivent partager une clé secrète pour pouvoir communiquer.

Exemple d'algorithme symétrique : **DES**.

Cryptographie

Les algorithmes asymétriques : chaque utilisateur dispose d'une paire de clés (une clé de chiffrement, dite **clé privée**, et une clé de déchiffrement, dite **clé publique**).

Il est impossible de recalculer une clé à partir de l'autre.

Pour chiffrer un message, on utilise la clé publique. Seul le possesseur de la clé privée peut alors déchiffrer le message.

Les algorithmes asymétriques sont basés sur des **propriétés mathématiques complexes**. L'inconvénient de ces protocoles est qu'ils sont très coûteux en ressources et donc très lents.

Exemple d'algorithme asymétrique : **RSA**.

Les solutions performantes sont donc des solutions hybrides où la communication est chiffrée par une clé dite de session basée sur un protocole symétrique. Cette clé est générée aléatoirement et transmise via un protocole asymétrique.

Cryptographie

Le protocole entre A et B a donc la forme suivante :

A tire une clé de session k.

B envoie sa clé publique à A.

A chiffre k avec la clé publique de B et envoie le résultat à B.

B le déchiffre avec sa clé privée.

A et B communiquent en utilisant un protocole symétrique (clé k).

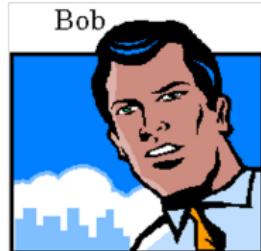
Le problème de cette méthode est que rien ne garantit à A que c'est bien la clé publique de B qu'il reçoit.

Imaginons qu'un pirate se place au milieu de cette communication, s'il envoie sa clé publique à la place de B, il prend sa place dans toute la suite de la communication : ce problème est appelé "**man in the middle**".

Il faut donc utiliser la **signature numérique** pour garantir que la clé publique de B est bien celle de B (**authentification**), et n'a pas été modifiée (**intégrité**). On se base alors sur des protocoles de signatures.

Personnages

Les personnages récurrents les plus célèbres de la cryptographie: **Alice** et **Bob** (ou **Bernard** en français) d'un coté et le méchant (l'escroc) **oscar** ou l'espion **Eve**.



Objectifs d'Eve

1. **Lire** le message
2. **Trouver la clé** utilisée par Alice et lire tous les messages chiffrés avec cette clé.
3. **Modifier le contenu** du message de telle sorte que Bob pense que c'est Alice qui a envoyé ce message .
4. **Prendre la place d'Alice** et communiquer avec Bob persuadé être entrain de communiquer avec Alice.

Oscar est un observateur passif qui essaye de faire (1) et (2).

Mallory est plus active et essaye de faire (3) et (4).

Du téléphone rouge aux systèmes à clé réduite

Un seul algorithme de chiffrement sûr (prouvé Shannon en 1949) : aucune corrélation entre le message de départ et sa version chiffrée;

Utilisé pour les communications au plus haut niveau (ex: le téléphone rouge entre Moscou et Washington)



Méthode de chiffrement mise au point par Gilbert Vernam en 1917 : tout simplement un chiffre de Vigenère, mais la clé est de la taille du message à envoyer, utilisable une seule fois (**Masque jetable**), et les lettres de cette clé sont choisies aléatoirement. (**One time pad de Vernam**)

Inconvénients : génération et transport des clés, taille des clés incompatible avec le chiffrement de grandes masses de données !

Comment fait-on ?

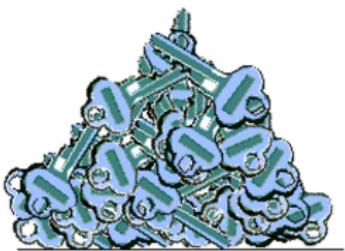
Approcher ce fonctionnement avec des clés de taille réduite.

Par exemple, le chiffrement symétrique (AES) avec une clé de 128 bits offre une protection suffisante pour une attaque exhaustive.

Essayer toutes les clés exige 2^{128} opérations.

Le supercalculateur le plus puissant au monde : **Fugaku** (développé par Fujitsu, Japon).

Il peut effectuer 2^{59} opérations par seconde. Pour faire 2^{128} opérations, il lui faut **20 mille milliards d'années** (âge de l'univers 13 à 14 milliards d'années).



Retrouvez la bonne clé parmi 2^{128} !

On découpe le message à chiffrer en blocs et on effectue des **transformations toujours réversibles**, mais suffisamment compliquées (chiffré non corrélé au message clair).

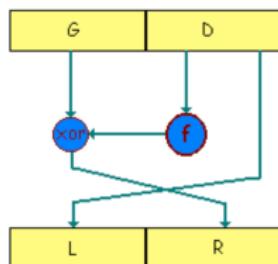
Les schémas de Feistel

Avant les travaux de Feistel, on ne savait pas construire des bijections aléatoires.

Solution de Feistel : on suppose qu'on a une fonction f "presque aléatoire" qui prend comme argument un mot de n bits, et renvoie un mot de n bits.

L'algorithme de chiffrement va procéder en chiffrant des blocs de $2n$ bits, qu'on partage en 2, partie gauche G , partie droite D . L'image du bloc (G,D) par le schéma de Feistel est le bloc (L,R) , avec :

$L=D$, et $R= G \text{ xor } f(D)$.



On a toujours $b \text{ xor } b = 0$ donc $a \text{ xor } b \text{ xor } b = a$ d'où la reseversibilité du schéma de Festel.

Les schémas de Feistel

Cette transformation est cette fois bijective, car si on a un tel couple (L, R) , on retrouve (G, D) par $D=L$ et $G=R \text{ xor } f(L)$.

Bien sûr, la partie droite n'a pas été transformée (juste envoyée à gauche). C'est pourquoi **on répète le schéma de Feistel** un certain nombre de fois (on parle de tours - le DES en comporte 16).

La plupart des algorithmes à clé secrète de la fin du XX^{ème} siècle étaient des schémas de Feistel.

L'avènement de l'AES, qui n'en est plus un, marque la fin de la prédominance de tels algorithmes.

La saga du DES

Jusque dans les années 1970, seuls les militaires possédaient des algorithmes à clé secrète fiables.

Devant l'émergence de besoins civils, le NBS (National Bureau of Standards) lança le 15 mai 1973 un **appel d'offres** dans le Federal Register (l'équivalent du Journal Officiel américain) pour la création d'un système cryptographique.



Le **cahier des charges** était le suivant :

L'algo repose sur une **clé relativement petite**, qui sert au chiffrement et au déchiffrement.

L'algo doit être **facile à implémenter** et très **rapide**.

le chiffrement doit avoir un **haut niveau de sûreté**, uniquement lié à la clé, et non à la confidentialité de l'algorithme.

IBM, qui propose **Lucifer fin 1974**, et la NSA (National Security Agency) élaborent le **DES (Data Encryption Standard)**.

La clé du DES : une chaîne de 64 bits (succession de 0 et de 1), mais seuls 56 bits servent réellement à définir la clé. Les bits 8, 16, 24, 32, 40, 48, 56, 64 sont des bits de parité (détection d'erreur).

Le 8^{ème} bit est fait en sorte que sur les 8 premiers bits, il y ait un nombre impair de 1. Par exemple, si les 7 premiers bits sont 1010001, le 8^{ème} bit est 0. Ceci permet d'éviter les erreurs de transmission.

2⁵⁶ clés possibles, environ ... 72 millions de milliards possibilités.

Les grandes lignes de l'algorithme sont :

Phase 1 : Préparation - Diversification de la clé.

Le texte est découpé en blocs de 64 bits. On diversifie aussi la clé K , c'est-à-dire qu'on fabrique à partir de K 16 sous-clés K_1, \dots, K_{16} à 48 bits. Les K_i sont composés de 48 bits de K , pris dans un certain ordre.

Phase 2 : Permutation initiale.

Pour chaque bloc de 64 bits x du texte, on calcule une permutation finie $y = P(x)$. y est représenté sous la forme $y = G_0 D_0$, G_0 étant les 32 bits à gauche de y , D_0 les 32 bits à droite.

Phase 3 : Itération

On applique 16 rondes d'une même fonction. A partir de $G_{i-1} D_{i-1}$ (pour i de 1 à 16), on calcule $G_i D_i$ en posant :

$$\begin{aligned}G_i &= D_{i-1} \\D_i &= G_{i-1} \text{ XOR } f(D_{i-1}, K_i)\end{aligned}$$

XOR est le ou exclusif bit à bit, et f est une fonction de confusion (suite de substitutions et de permutations).

Phase 4 : Permutation finale.

On applique à $G_{16} D_{16}$ l'inverse de la permutation initiale.

$Z = P^{-1}(G_{16} D_{16})$ est le bloc de 64 bits chiffré à partir de x .

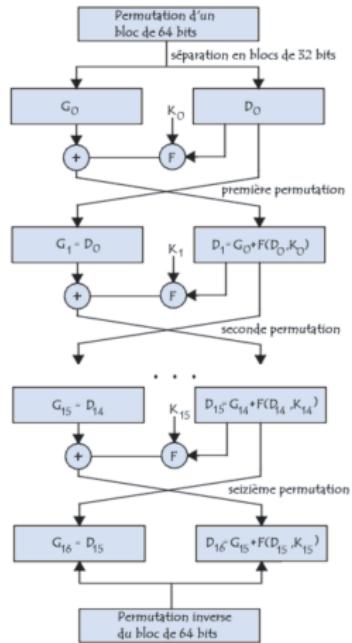
DES : Objet de polémiques

Toute sa sécurité repose sur la **fonction de confusion f** . C'est la seule opération non-linéaire.

Permutations initiale et finales : aucun rôle.
Les autres opérations sont toutes linéaires :
facile à cryptanalyser

Certains ont affirmé que la NSA, qui a finalisé l'algo, a placé des **trappes** qui permettaient de tout décrypter, tout en affirmant que l'algo est sûr.

Toutefois, rien n'a objectivement étayé cela.
En particulier, le **DES a toujours résisté aux travaux des cryptanalystes** non basés sur la force brute.



Fin du DES

17 juin 1997 : le DES est cassé en 3 semaines par une fédération de petites machines sur Internet.

A cette date, on estime à quelques secondes le temps nécessaire à un Etat pour percer les secrets d'un message chiffré avec le DES (rapport présenté au Sénat Américain).

Solution temporaire : le triple DES, trois applications de DES à la suite avec 2 clés différentes (d'où une clé de 112 bits) :



Le TDES suffit mais il est trois fois plus lent que le DES. C'est pourquoi, le NIST (National Institute of Standards and Technologies) a lancé en 1997 un nouvel appel pour créer un successeur au DES.

Une nouvelle saga commence : l'**AES (Advanced Encryption Standard)**.

Un nouveau standard de chiffrement symétrique

Cahier des charges :

1. Grande **sécurité**.
2. Large **portabilité** : l'algorithme devant remplacer le DES, il est destiné à servir aussi bien dans les cartes à puces, aux processeurs peu puissants, que dans des processeurs spécialisés pour chiffrer des milliers de télécommunications à la volée.
3. **Rapidité**.
4. **Lecture facile** de l'algorithme (destiné à être rendu public).
5. Techniquement, le **chiffrement doit se faire par blocs de 128 bits**, les clés comportant 128,192 ou 256 bits.

15 juin 1998 : fin des candidatures, 21 projets ont été déposés.

Evaluation des algorithmes pendant deux ans (experts, forum de discussion sur Internet, et organisation de conférences).

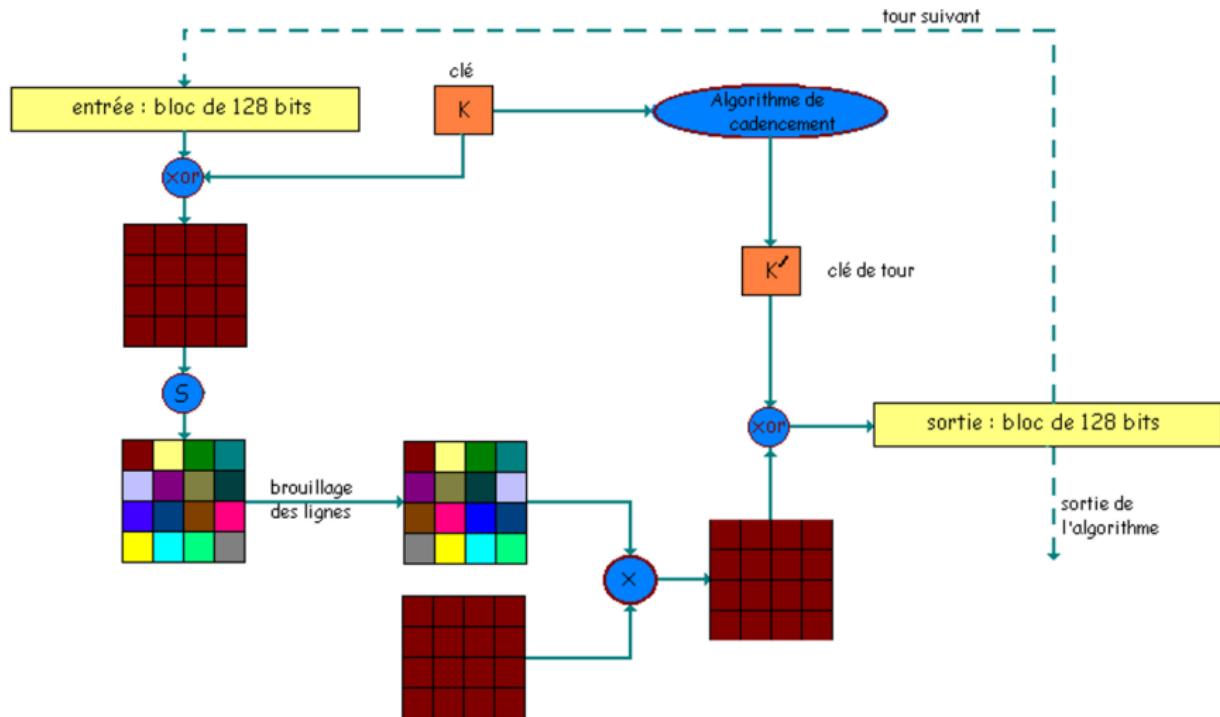
Le gagnant est :

2 octobre 2000 : le NIST donne sa réponse; C'est le **Rijndael** qui est choisi, un algorithme mis au point par 2 belges, J. Daemen et V. Rijmen.

Le Rijndael procède par **blocs de 128 bits**, avec une **clé de 128 bits**. Chaque bloc subit une séquence de **5 transformations répétées 10 fois**

1. **Addition de la clé secrète** : par un ou exclusif.
2. **Transformation non linéaire d'octets** : les 128 bits sont répartis en 16 blocs de 8 bits, eux-même dispatchés dans un tableau 4×4 . Chaque octet est transformé par une fonction non linéaire S .
3. **Décalage de lignes** : les 3 dernières lignes sont décalées cycliquement vers la gauche : la 2^{ème} ligne est décalée d'une colonne, la 3^{ème} ligne de 2 colonnes, et la 4^{ème} ligne de 3 colonnes.
4. **Brouillage des colonnes** : chaque colonne est transformée par combinaisons linéaires des différents éléments de la colonne (ce qui revient à multiplier la matrice 4×4 par une autre matrice 4×4).
5. **Addition de la clé de tour** : à chaque tour, une clé de tour est générée à partir de la clé secrète par un algorithme (dit de cadencement). Cette clé de tour est ajoutée par un ou exclusif au dernier bloc obtenu.

Le Rijndael



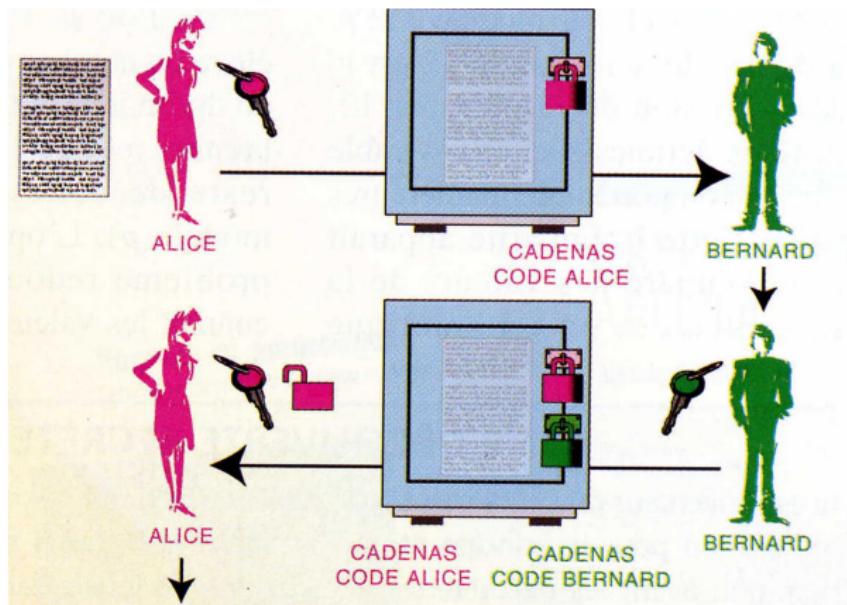
Cryptographie symétrique, oui mais ...



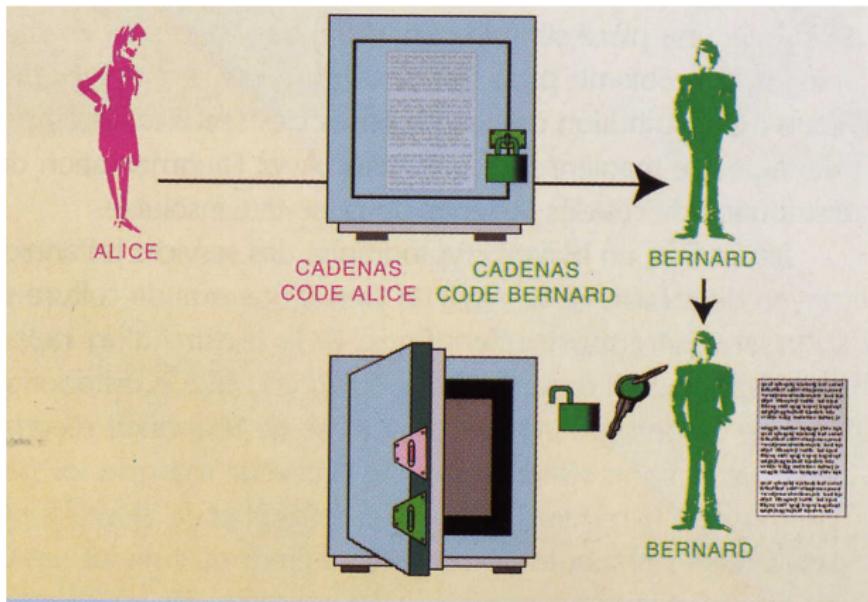
Cryptographie à clé publique (ou asymétrique)

1976 : Whitfield Diffie et Martin Hellman proposent une nouvelle façon de chiffrer qui contourne le problème d'échange des clés.

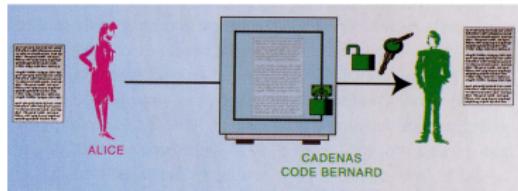
L'illumination :



Cryptographie à clé publique (ou asymétrique)



Problème



Clé d'Alice :

HFSUGTAKVDEOYJBPNXWCQRIMZL

Clé de Bernard :

CPMGATNOJ EFWIQBURYHXSDZKLV

Message : **vois moi à midi**

Chiffré avec la clé d'Alice : RBVW YBV H YVUV

Chiffré avec la clé de Bernard : YPDZ LPD O LDSD

Déchiffré avec la clé d'Alice : MPJY ZPJ L ZJCJ

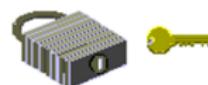
Déchiffré avec la clé de Bernard : **cbir wbi y wiai**

En réalité

Cryptographie à clé publique :



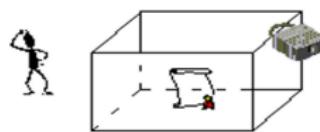
Etape 1 : Fabrication des clés. Bob fabrique une clé publique qui permet de sceller le message codé dans la boîte (ici : le cadenas), et une clé privée qui permet d'ouvrir le cadenas.



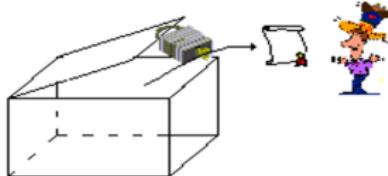
Etape 2 : Distribution des clés. Bob fait parvenir à Alice le cadenas, mais garde la clé pour lui.



Etape 3 : Envoi du message. Alice met son message dans une boîte qu'elle ferme à l'aide du cadenas.



Etape 4 : Réception du message. Bob ouvre la boîte à l'aide de sa clé, et récupère le message. Personne n'a pu l'intercepter puisque lui seul pouvait ouvrir la boîte.



En pratique comment ça marche ?

On dispose d'une **fonction P** sur les entiers, **et son inverse S** .

On suppose qu'on peut fabriquer un tel couple (P, S) , mais que connaissant uniquement P , il est impossible (ou au moins très difficile) de retrouver S .

P est la clé publique, que vous pouvez révéler à quiconque. Si Louis veut vous envoyer un message, il vous transmet **$P(\text{message})$** .

S est la clé secrète, elle reste en votre unique possession. Vous décodez le message en calculant **$S(P(\text{message})) = \text{message}$** .

La connaissance de P par un tiers ne compromet pas la sécurité de l'envoi des messages codés, puisqu'elle ne permet pas de retrouver S . Il est possible de donner librement P , qui mérite bien son nom de clé publique.

Difficulté : comment trouver de telles fonctions P et S ?

RSA

Diffie et Hellman n'ont pas eux-même proposé de fonctions satisfaisantes, mais dès 1977, D.Rivest, A.Shamir et L.Adleman trouvent une solution possible, la meilleure et la plus utilisée à ce jour, le RSA.

Le RSA repose sur les faits suivants :

1. On peut générer de grands nombres premiers p et q .
2. Etant donné un nombre entier $n = pq$ produit de 2 grands nombres premiers, il est très difficile de retrouver les facteurs p et q .

La clé publique utilise n et elle suffit pour chiffrer. La clé privée utilise p et q et il faut connaître p et q pour déchiffrer..

Défaut : algorithme beaucoup plus lent qu'un algorithme symétrique. Inutilisables pour échanger beaucoup de données en.

Cryptosystèmes hybrides : échanger les clés grâce à la cryptographie à clé publique, et utiliser ensuite un algorithme de chiffrement symétrique. Le célèbre PGP, notamment utilisé pour chiffrer le courrier électronique, fonctionne sur ce principe.

Cryptographie à clé publique : le RSA

RSA : algorithme à clé publique le plus utilisé de nos jours. Invention fortuite : au départ, R, S et A voulaient prouver que tout système à clé publique possède une faille.



Adi Shamir

Ron Rivest

Len Adleman

Principe de fonctionnement : Si Bob souhaite recevoir des messages en utilisant le RSA, il procède de la façon suivante :

1. **Création des clés :** Bob crée 4 nombres p , q , e et d :

p et q sont deux grands nombres premiers générés au hasard, en utilisant un algorithme de **test de primalité probabiliste**.

e est un entier premier avec le produit $(p - 1)(q - 1)$.

d est tel que $ed = 1$ modulo $(p - 1)(q - 1)$. Autrement dit, $ed - 1$ est un multiple de $(p - 1)(q - 1)$.

On peut fabriquer d à partir de e , p et q , en utilisant l'**algorithme d'Euclide**.

Générer des nombres premiers

Nombres de Mersenne : $M_p = 2p - 1$, où p est premier.

Ils ne sont pas tous premiers, mais on dispose d'un test particulièrement efficace (le test de Lucas-Lehmer) pour tester s'ils le sont :

On construit en effet une suite S_n en posant $S_1 = 4$, et par la formule de récurrence : $S_n = (S_{n-1})^2 - 2$.

Pour $p > 2$, M_p est premier si et seulement si M_p divise S_p .

Les records des plus grands nombres premiers sont depuis des années réalisés à partir des nombres de Mersenne.

M₁₃₄₆₆₉₁₇ possède 4 053 946 chiffres décimaux !

Pourtant, ces nombres de Mersenne ne sont **jamais utilisés** pour la cryptographie : ils sont bien trop particuliers, et l'algorithme serait beaucoup plus facile à casser.

Test de primalité

Un premier aléatoire, sur lequel on n'a a priori pas d'information.

Prendre un entier de 500 chiffres au hasard, de tester s'il est premier : si c'est le cas, on le garde, sinon on choisit un autre nombre au hasard, jusqu'à finir par tomber sur un premier. Cela pose deux problèmes :

- 1) Trouver un premier au bout d'un nombre raisonnable de tirages.
- 2) Déterminer rapidement si un nombre n est premier ou non.

Pour 1), un théorème conjecturé par Gauss, et démontré par de la Vallée Poussin, affirme que si $P(n)$ désigne le nombre de nombres premiers plus petits que n , alors :

$$P(n) \approx \int_2^n \frac{dx}{\ln n} \approx \frac{n}{\ln n} + \frac{n}{(\ln n)^2} + \frac{2n}{(\ln n)^3} + \dots$$

En pratique, le nombre de premiers inférieurs à n est de l'ordre de $n / \ln n$.

Test de primalité

En conclusion : il y a environ 2^{1014} nombres premiers de 1024 bits. La probabilité qu'un nombre x soit premier est proche de $1/\ln n$, probabilité de $1/710$ pour un entier de 1024 bits. C'est très raisonnable !

Pour 2), le plus rudimentaire est de prendre tour à tour tous les nombres entre 2 et racine de n , et vérifier s'ils divisent ou non n .

Mais cet algorithme est bien trop naïf, car il nécessite 10250 calculs environ pour un nombre de 500 chiffres !

On a recours aux **tests probabilistes** : Solovay-Strassen et Miller-Rabin.

"n est probablement premier", avec une probabilité très grande (et que l'on peut ajuster).

En général, en cryptographie, on se contente de nombres dont on sait qu'ils sont premiers avec une probabilité supérieure à $1 - 1/2100$.

Algorithme d'Euclide étendu

Quel est le plus grand diviseur commun (pgcd) de 126 et 462 ?

On apprend au collège à calculer ce pgcd en décomposant les 2 nombres en produits de facteurs premiers, et en réunissant les facteurs en commun.

Cette méthode n'est plus envisageable quand les entiers deviennent grands (plusieurs centaines de chiffres décimaux), car la factorisation est un problème difficile.

On calcule le pgcd en appliquant l'algorithme d'Euclide, qui repose sur la constatation suivante :

Si a et b sont deux entiers avec $a > b$, si r est le reste de la division de a par b , alors le pgcd de a et b est égale au pgcd de b et r .

On effectue donc des divisions euclidiennes, jusqu'à ce qu'on trouve un reste nul. Le dernier reste non nul est le pgcd de a et b .

Algorithme d'Euclide étendu

Algorithme de calcul des coefficients (u, v) tels que

$$au + bv = d = \text{pgcd}(a, b)$$

(u, v) sont les coefficients de Bézout pour les deux entiers naturels a et b

a	b	q
546738492	6754024	
6754024	6416572	80
6416572	337452	1
337452	4984	19
4984	3524	67
3524	1460	1
1460	604	2
604	252	2
252	100	2
100	52	2
52	48	1
48	4	1
4	0	12

a	u	v	q
4864	1	0	
3458	0	1	1
1406	1	-1	2
646	-2	3	2
114	5	-7	5
76	-27	38	1
38	32	-45	2
0	

$$38 = 32a - 45b = \\ 32 \times 4864 - 45 \times 3458$$

RSA

Bob souhaite recevoir des messages en utilisant le RSA

1. **Création des clés :** Bob crée 4 nombres p , q , e et d (p et q grands nombres premiers distincts générés au hasard, e est un entier premier avec le produit $(p - 1)(q - 1)$ et d est tel que $ed = 1$ modulo $(p - 1)(q - 1)$).
2. **Distribution des clés :** Le couple (n, e) constitue la **clé publique** de Bob. Il la rend disponible. Le nombre d constitue sa **clé privée**. Il le garde secret.
3. **Envoi du message :** Alice veut envoyer un message à Bob. Elle le représente sous la forme d'un ou plusieurs entiers M compris entre 0 et $n - 1$. Alice possède la clé publique (n, e) de Bob. Elle calcule $C = M^e \pmod{n}$. C'est ce dernier nombre qu'elle envoie à Bob.
4. **Réception du message :** Bob reçoit C , et il calcule $D = C^d \pmod{n}$ grâce à sa clé privée. On démontre que $D = M^{de} = M \pmod{n}$. Il a donc reconstitué le message initial.

RSA

Les attaques actuelles du RSA se font essentiellement en factorisant l'entier n de la clé publique.

La sécurité du RSA repose sur la difficulté de factoriser de grands entiers.

Le nombre **RSA-250**, qui fait partie du "**RSA Factoring Challenge**", a été factorisé le **28 février 2020**. C'est le produit de deux nombres premiers de 125 chiffres chacun.

2140324650240744961264423072839333563008614715144755017797754920881418023447
1401366433455190958046796109928518724709145876873962619215573630474547705208
0511905649310668769159001975940569345745223058932597669747168173806936489469
9871578494975937497937

=

64135289477071580278790190170577389084825014742943447208116859632024532344630
238623598752668347708737661925585694639798853367

*

33372027594978156556226010605355114227940760344767554666784520987023841729210
037080257448673296881877565718986258036932062711

RSA-250

2140324650240744961264423072839333563008614715144755017797754920881418023447
1401366433455190958046796109928518724709145876873962619215573630474547705208
0511905649310668769159001975940569345745223058932597669747168173806936489469
9871578494975937497937

=
64135289477071580278790190170577389084825014742943447208116859632024532344630
238623598752668347708737661925585694639798853367

*

33372027594978156556226010605355114227940760344767554666784520987023841729210
037080257448673296881877565718986258036932062711

Résultat obtenu avec un algorithme spécifique appelé le crible algébrique, et un logiciel open-source (**CADO-NFS**) que les chercheurs du **LORIA** et leurs collègues développent depuis 2007, et qui comporte de l'ordre de 400 000 lignes de code.

Pour établir ce nouveau record, il aurait fallu faire travailler **un ordinateur** pendant **2700 années** !

À la place, ce sont environ **10000 ordinateurs** qui ont calculé pendant **quelques mois**, dans plusieurs universités et centres de calcul en France, en Allemagne, et aux États-Unis.

RSA sûr ?

Pour garantir la sécurité, il faut choisir des clés suffisamment grandes.

Concernant le RSA, le record est la factorisation d'un entier de 768 bits.

L'usage des clés de 1024 bits, répandu entre 2000 et 2010, est désormais fortement déconseillé, et il est **recommandé de choisir une clé de 2048 bits, voire 4096 bits pour un usage sensible.**



Recommandations de l'agence nationale de la sécurité des systèmes d'information (ANSSI). Il représente l'expression du gouvernement français en termes de qualité cryptographique.

Date	Symétrique	Factorisation Module	Logarithme discret Clef	Groupe	Courbe elliptique GF(p)	GF(2^n)	Hash
2014 - 2020	100	2048	200	2048	200	200	200
2021 - 2030	128	2048	200	2048	256	256	256
> 2030	128	3072	200	3072	256	256	256

La signature électronique

La cryptographie à clé publique s'affranchit du problème de l'échange de clés. Mais comment s'assurer de l'authenticité de l'envoi ? Comment être sûr que personne n'usurpe l'identité d'Alice pour envoyer un message ? Comment être sûr qu'Alice ne va pas nier avoir envoyé ce message ?

Alice veut donc envoyer un message crypté à Bob, mais Bob veut s'assurer que ce message provient bien d'Alice.

Alice possède le couple clé publique/clé privée (**PA, SA**), et Bob le couple (**PB, SB**). Alice veut envoyer M.

Phase d'envoi : Alice calcule **SA(M)**, avec sa clé secrète, puis **PB(SA(M))**, à l'aide de la clé publique de Bob.



Phase de réception : A l'aide de sa clé privée, Bob calcule **SB(PB(SA(M))) = SA(M)**. Seul lui peut effectuer ce calcul (=sécurité de l'envoi). Puis il calcule **PA(SA(M)) = M**. Il est alors sûr que c'est Alice qui lui a envoyé ce message, car elle-seule a pu calculer **SA(M)**.

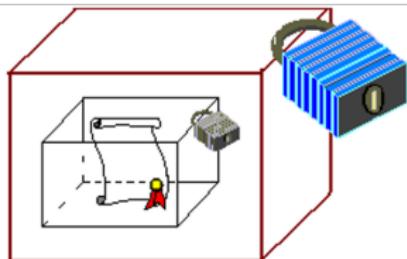
La signature électronique



Alice



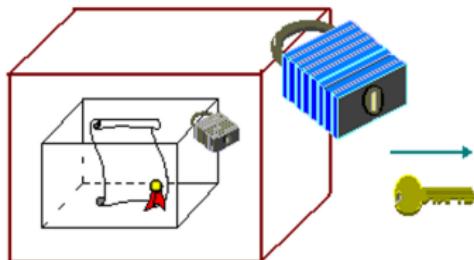
enferme le message dans une boîte à l'aide de sa clé privée (authentification de l'expéditeur)



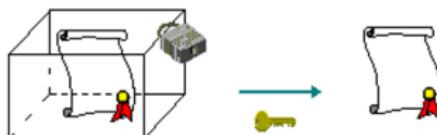
enferme cette boîte dans une autre boîte avec la clé publique de Bob (chiffrement, seul Bob peut ouvrir)



Bob



reçoit le message chiffré et authentifié



ouvre la première boîte avec sa clé privée (déchiffrement)

ouvre la deuxième boîte avec la clé publique d'Alice (authentification)

Intégrité : Fonctions de hachage

Fonction de hachage : fonction qui, à partir d'une donnée arbitraire, calcule une empreinte servant à condenser et identifier rapidement la donnée initiale. L'empreinte est également appelée résumé.

En expédiant un message accompagné de son résumé (on dit aussi son haché), on peut s'assurer de l'intégrité du message, en recalculant le résumé à l'arrivée.

Mais il y a mieux : la fonction de hachage, couplée à la cryptographie à clé publique;

Phase d'envoi : Alice calcule $h(M)$, le résumé, et envoie à Bob **PB(M)** (calculé à l'aide de la clé publique de Bob) accompagné de **SA(h(M))**.

Phase de réception : Bob calcule **SB(PB(M)) = M'**. Puis il calcule **PA(SA(h(M)))**, qu'il compare à $h(M')$. Si les quantités sont égales, il est sûr que c'est bien Alice qui a envoyé le message, et que celui-ci a été correctement transmis.

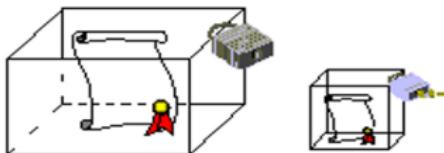
Intégrité : Fonctions de hachage



Alice



Calcule le résumé du message

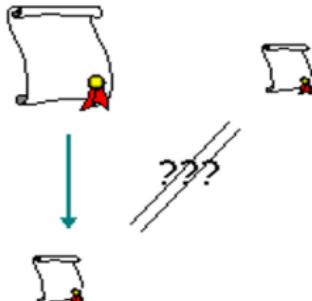


Met le message dans une boîte que seul Bob peut ouvrir.

Met le résumé dans une boîte que elle seule peut fermer.



Bob



Ouvre les 2 boîtes.

Calcule le résumé du message reçu.

Le compare avec le résumé envoyé.

S'ils sont égaux, le message a été envoyé correctement, et il est sûr que c'est Alice l'expéditeur.

Le certificat numérique

Le problème des certificats numériques est à l'opposé de celui de la signature électronique.

Cette fois, c'est donc du Destinataire que l'on veut être sûr, et non de l'Expéditeur.

Alice veut certifier que sa clé publique lui appartient. Elle envoie sa clé à un organisme de certification, ainsi que différentes informations la concernant (nom, émail, etc...).

Cet organisme vérifie les informations fournies par Alice, et ajoute au certificat son propre nom, une date limite de validité, et surtout une signature numérique.

Cette signature est calculée de la façon suivante : à partir des informations du certificat, l'organisme calcule un résumé en appliquant une fonction de hachage connue. Puis il signe ce résumé en lui appliquant sa clé secrète.

Le certificat numérique

Si Bob veut envoyer son message à Alice, il télécharge le certificat d'Alice sur un serveur de certificat (on parle de PKI, Public Key Infrastructure).



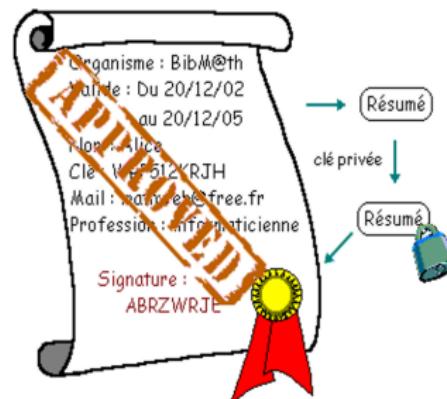
Alice

Nom : Alice
Clé : WRP512KRJH
Mail : mathweb@free.fr
Profession : informaticienne

Alice fournit une fiche d'identité à l'organisme de certification.



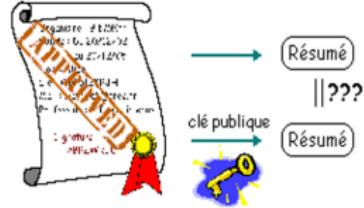
Organisme de certification



- * Vérifie les informations d'Alice
- * Ajoute ses propres informations
- * Calcule un résumé, le chiffre avec sa clé privée
- * Signe le certificat avec ce résumé



Bob



- * Télécharge le certificat
- * Calcule son résumé
- * "Ouvre" la signature avec la clé publique de l'organisme
- * Compare les 2 résumés

Le certificat numérique

Un site Web qui utilise le protocole HTTPS (destiné à assurer la sécurité de la connexion), son serveur présente un certificat pour prouver l'identité du site aux navigateurs, tels que Chrome, Firefox, etc.

N'importe qui peut émettre un certificat en se faisant passer pour un autre site Web.

Pour préserver votre sécurité sur le Web, utiliser des navigateurs qui exigent que les sites utilisent des certificats provenant d'organismes approuvés !

Problème ...

Vrai site

Faux site

The image shows a comparison between a legitimate CAF website and a fraudulent one. On the left, the 'Vrai site' (real site) is displayed with a URL ending in '.fr'. It features a blue header with the CAF logo and 'Mon compte'. Below it is a login form with fields for 'Code postal', 'Numéro d'allocation', 'Code confidentiel', 'Jour et mois de naissance', and 'Mot de passe'. A red arrow points from the URL bar of the 'Faux site' to this form. On the right, the 'Faux site' is shown with a URL ending in '.mss.middleeastvisa.com'. It has a similar layout but includes additional fields for 'Numéro de carte bancaire', 'Cryptogramme visuel', and 'Date d'expiration'. Both sites feature a background image of a woman and a child.

Le certificat de l'UL

univ-lorraine.fr

JO
**UNIVERSITÉ DE LORRAINE**

ASSOCIATION INITIATIVES ÉTUDIANTS

| INFORMATION

univ-lorraine.fr

USERTrust RSA Certification Authority

GEANT OV RSA CA 4

*.univ-lorraine.fr

***.univ-lorraine.fr**
Délivré par: GEANT OV RSA CA 4
Expire le vendredi 25 février 2022 à 00:59:59 heure normale d'Europe centrale
 Ce certificat est valide

Se fier
Lors de l'utilisation de ce certificat : [Réglages par défaut](#)  

Règles de base X.509 [aucune valeur spécifiée](#) 

Détails

Sujet

Pays ou région FR
Code postal 54000
Région/Province Grand-Est
Localité NANCY
Rue 34 cours Léopold
Organisation Université de Lorraine
Nom *.univ-lorraine.fr

Nom de l'émetteur

Pays ou région NL
Organisation GEANT Vereniging
Nom GEANT OV RSA CA 4

Numéro de série 00 87 93 8C B2 3A F5 FF A0 DE 96 A4 70 E3 D6 4B 21
Version 3

Algorithme de signature SHA-384 avec chiffrement RSA (1.2.840.113549.1.1.12)
Paramètres Aucun

Non valide avant mercredi 24 février 2021 à 01:00:00 heure normale d'Europe centrale
Non valide après vendredi 25 février 2022 à 00:59:59 heure normale d'Europe centrale

Infos de clé publique

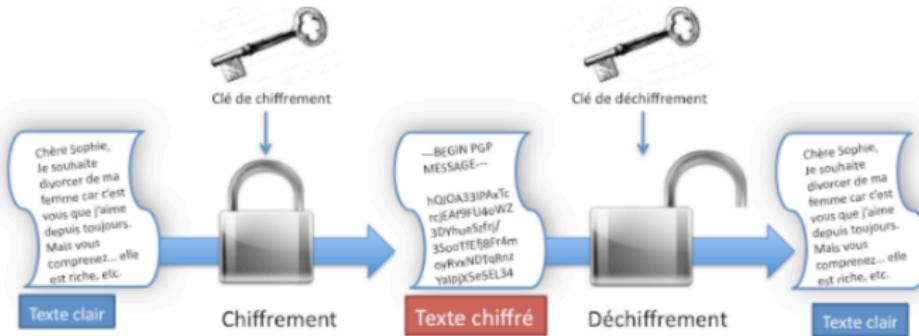
Algorithme Chiffrement RSA (1.2.840.113549.1.1.1)
Paramètres Aucun
Clé publique 256 octets : E8 88 F6 27 74 6D 68 49 ...
Exposant 65537
Dimension de clé 2048 bits
Utilisation de la clé Chiffrer, Vérifier, Ajuster, Dériver

Signature 512 octets : 58 25 C9 25 89 52 AC BC ...

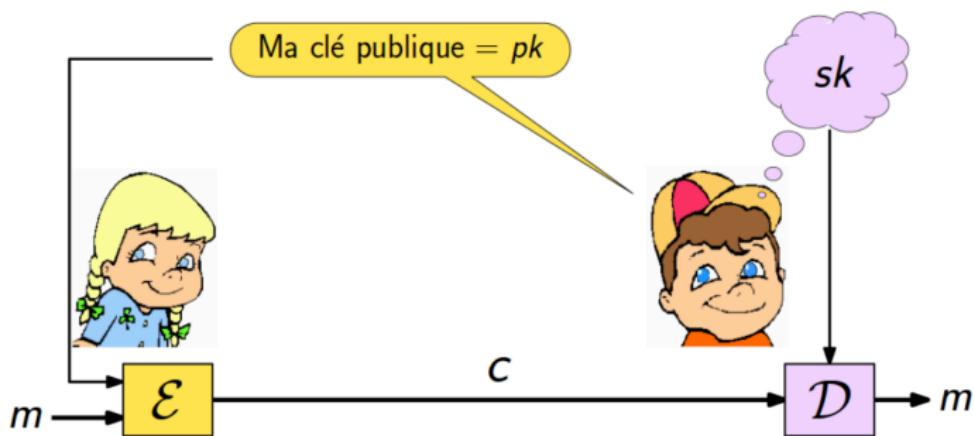
    

Partie 3

Chiffrement symétrique



Chiffrement à clé publique



Chiffrement à clé publique

RSA (Rivest-Shamir-Adleman, 1978) :

basé sur les racines modulaires et la décomposition en facteurs premiers

ElGamal (1984) :

basé sur le logarithme discret

McEliece (1978) :

basé sur les codes correcteurs

Merkle-Hellman (1978) :

basé sur des problèmes combinatoires (sac-à-dos)

Hidden Field Equation (Patarin, 1996) :

basé sur les systèmes multivariables

Comparatif : symétrique /asymétrique

Cryptographie Symétrique	Cryptographie Asymétrique
Problème majeur d'échange de clés	Pas de clés à échanger
Relative simplicité d'implémentation	Relative complexité d'implémentation
Sécurité heuristique	Sécurité prouvée
Clés (pseudo-)aléatoires	Clés avec structure mathématique
Taille des clés réduite *	Taille des clés grande *
Relativement rapide	Très lent

* Pour le même niveau de sécurité : la sécurité disponible avec RSA avec une clé de 1024 bits , est considérée égale à la sécurité d'un cryptosystème symétrique avec une clé de 80 bits (keylength.com)

Système cryptographique : Formalisation

Un quintuplet $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ satisfaisant :

1. \mathcal{P} est un ensemble fini de bloc de textes **clairs** possibles.
2. \mathcal{C} est un ensemble fini de bloc de textes **chiffrés** possibles.
3. \mathcal{K} , appelé **espace des clés**, est un ensemble fini de **clés** possibles.
4. Pour tout $K \in \mathcal{K}$, il existe une **règle de chiffrement** $e_K \in \mathcal{E}$ et une **règle de déchiffrement** correspondante $d_K \in \mathcal{D}$. Chaque $e_K : \mathcal{P} \rightarrow \mathcal{C}$ et $d_K : \mathcal{C} \rightarrow \mathcal{P}$ sont des fonctions telles que $d_K(e_K(x)) = x$ pour tout texte clair $x \in \mathcal{P}$.

Système cryptographique

Alice veut envoyer à Bob le message :

$$\mathbf{x} = x_1 x_2 \dots x_n, \quad n \geq 1, \quad x_i \in \mathcal{P}, \quad 1 \leq i \leq n$$

Elle choisie une clé K et chiffre chaque x_i en utilisant une règle de chiffrement e_K :

$$y_i = e_K(x_i), \quad 1 \leq i \leq n$$

Le texte chiffré et envoyé à Bob est :

$$\mathbf{y} = y_1 y_2 \dots y_n$$

Bob le déchiffre en utilisant la fonction de déchiffrement d_K et récupere le texte clair original $\mathbf{x} = x_1 x_2 \dots x_n$.

Système cryptographique

Chaque fonction de chiffrement e_K doit être injective (ne pas chiffrer deux blocs différents en deux valeurs égales).

- ▶ Si :

$$y = e_K(x_1) = e_K(x_2), \text{ avec } x_1 \neq x_2$$

Bob ne peut pas savoir si y doit être déchiffré en x_1 ou en x_2 .

- ▶ Si :

$$\mathcal{P} = \mathcal{C}$$

chaque fonction de chiffrement doit être une permutation (elle réarrange les éléments de cet espace).

$\mathbb{Z}/n\mathbb{Z}$

a	01100001	b	01100010	c	01100011
d	01100100	e	01100101	f	01100110
g	01100111	h	01101000	i	01101001
j	01101010	k	01101011	l	01101100
m	01101101	n	01101110	o	01101111
p	01110000	q	01110001	r	01110010
s	01110011	t	01110100	u	01110101
v	01110110	w	01110111	x	01111000
y	01111001	z	01111010		

Chiffrement par décalage (Shift cipher)

Le chiffrement par décalage est basé sur l'arithmétique modulaire.

Définition

Si a , b , et m sont des entiers, et si $m > 0$, on écrit $a \equiv b \pmod{m}$ si m divise $b - a$ (que l'on note $m|(b - a)$).

*La phrase $a \equiv b \pmod{m}$ est une **congruence** et elle se lit "a est congru à b modulo m". L'entier m est appelé **module**.*

Si l'on divise a et b par m , on obtient :

$$a = q_1m + r_1, \quad 0 \leq r_1 \leq m - 1$$

$$b = q_2m + r_2, \quad 0 \leq r_2 \leq m - 1$$

Ainsi, $a \equiv b \pmod{m}$ si et seulement si $r_1 = r_2$.

Chiffrement par décalage (Shift cipher)

Quelques remarques :

- ▶ $a \bmod m$ désigne le reste dans la division de a par m , donc :
 $a \equiv b \pmod{m}$ si et seulement si $a \bmod m = b \bmod m$.
- ▶ Remplacer a par $a \bmod m$, revient à **réduire** a modulo m .
- ▶ Pour calculer $101 \bmod 7$, on a $101 = 7 \times 14 + 3$. Comme $0 \leq 3 \leq 6$, on obtient $101 \bmod 7 = 3$.
- ▶ Pour calculer $(-101) \bmod 7$, on écrit $-101 = 7 \times (-15) + 4$. Comme $0 \leq 4 \leq 6$, on obtient $(-101) \bmod 7 = 4$.
- ▶ Plusieurs langages de programmation définissent $a \bmod m$ comme l'entier congru à a compris entre $-m + 1$ et $m - 1$ et de même signe que a . Dans ce cas, $(-101) \bmod 7$ est -3 au lieu de 4 . Dans ce cours, le reste est considéré comme étant toujours positif.

Chiffrement par décalage (Shift cipher)

Arithmétique modulo m :

- ▶ \mathbb{Z}_m désigne l'ensemble $\{0, \dots, m-1\}$ muni des opérations + et \times . Pour ces opérations, les résultats sont réduits modulo m .

Calculer 11×13 dans \mathbb{Z}_{16} :

On a $11 \times 13 = 143$ et $143 = 8 \times 16 + 15$. Donc, $143 \bmod 16 = 15$ et par conséquent $11 \times 13 = 15$ dans \mathbb{Z}_{16} .

- ▶ \mathbb{Z}_m est un groupe abélien vis-à-vis de l'addition.
- ▶ \mathbb{Z}_m est également un anneau.
- ▶ Les opposés existent dans \mathbb{Z}_m , on peut faire des soustractions :

$a - b$ dans \mathbb{Z}_m est défini comme $a + m - b \bmod m$

On peut aussi calculer $a - b$ et le réduire modulo m .

$11 - 18$ dans \mathbb{Z}_{31} : $11 + 13 \bmod 31 = (11 - 18) \bmod 31 = 24$.

Chiffrement par décalage (Shift cipher)

Le chiffrement par décalage peut être défini sur \mathbb{Z}_m avec n'importe quel m . Il est défini sur \mathbb{Z}_{26} pour l'alphabet français.

C'est un système qui vérifie : $d_K(e_k(x)) = x$ pour tout $x \in \mathbb{Z}_{26}$.

Soit $\mathcal{P} = \mathcal{C} = \mathbb{Z}_{26}$. Pour $0 \leq K \leq 25$, on définit :

$$e_K(x) = (x + K) \bmod 26$$

et

$$d_K(y) = (y - K) \bmod 26$$

avec $(x, y \in \mathbb{Z}_{26})$.

Le chiffrement de César correspond à $K = 3$.

Pour chiffrer un texte avec le chiffrement par décalage (modulo 26), on utilise la correspondance : $A \leftrightarrow 0, B \leftrightarrow 1, \dots, Z \leftrightarrow 25$.

Chiffrement par décalage : un exemple

Chiffrement par décalage avec la clé K = 11.

Le texte clair est :

wewillmeetatmidnight

Conversion en une suite d'entiers :

22 4 22 8 11 11 12 4 4 19 0 19 12 8 3 13 8 6 7 19

On ajoute 11 et on réduit modulo 26 :

7 15 7 19 22 22 23 15 15 4 11 4 23 19 14 24 19 17 18 4

Cela donne :

HPHTWWXPPELEXTOYTRSE

Pour déchiffrer ce texte, il faut le convertir en nombres, soustraire 11 à chaque valeur (en réduisant modulo 26) et convertir le résultat en caractères alphabétiques.

Chiffrement par décalage

- ▶ Chaque fonction de chiffrement e_K et chaque fonction de déchiffrement d_K doit être calculable efficacement.
- ▶ Ni la clé K , ni le texte clair x ne doivent être déterminés par un pirate à partir du texte chiffré y . Cela définit de manière informelle la notion de "sécurité".

L'opération qui consiste à déterminer la clé K à partir du texte chiffré y est appelée **cryptanalyse**. Le chiffrement par décalage (modulo 26) n'est pas sûr. Il peut être cryptanalysé par la méthode dite de **recherche exhaustive de clé**. Il suffit de tester les 26 clés possibles.

Exemple : JBCRCLQRWCRVNBJENBWRWN

On essaye de déchiffrer avec d_0 , d_1 , ..., et on obtient avec d_9 le texte clair ($K = 9$) : "a stitch in time saves time".

Chiffrement par substitution

Soit $\mathcal{P} = \mathcal{P} = \mathbb{Z}_{26}$. \mathcal{K} est l'ensemble des permutations sur l'ensemble des 26 nombres 0, 1, ..., 25. Pour chaque permutation $\pi \in \mathcal{K}$, on définit :

$$\mathbf{e}_\pi(\mathbf{x}) = \pi(\mathbf{x})$$

et

$$\mathbf{d}_\pi(\mathbf{y}) = \pi^{-1}(\mathbf{y})$$

où π^{-1} est la permutation inverse de π .

Dans le chiffrement par substitution, il est plus commode de penser au chiffrement et au déchiffrement comme à des permutations sur l'ensemble des caractères alphabétiques.

La clé est la permutation des 26 caractères alphabétiques. Il y $26!$ clés possibles ce qui est supérieur à 4×10^{26} . Une recherche exhaustive est impossible mais on peut casser ce chiffrement à l'aide de **l'analyse des fréquences**.

Chiffrement par substitution : Exemple

Exemple de permutation π :

a	b	c	d	e	f	g	h	i	j	k	l	m
X	N	Y	A	H	P	O	G	Z	Q	W	B	T

n	o	p	q	r	s	t	u	v	w	x	y	z
S	F	L	R	C	V	M	U	E	K	J	D	I

Cela donne : $e_\pi(a) = X$, $e_\pi(b) = N$, ...

L'opération de déchiffrement correspond à :

A	B	C	D	E	F	G	H	I	J	K	L	M
d	l	r	y	v	o	h	e	z	x	w	p	t

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
b	g	f	j	q	n	m	u	s	k	a	c	i

Ainsi, $d_\pi(A) = d$, $d_\pi(B) = l$, ...

Le système de Vernam (one-time pad, 1926)

Les messages s'écrivent sur \mathbb{Z}_m . Un message de n symboles $M = (x_1, x_2, \dots, x_n)$ se chiffre par la transformation f_K :

$$\begin{aligned} f_K : \quad \mathcal{M} = \mathbb{Z}_m^n &\rightarrow \quad \mathcal{C} = \mathbb{Z}_m^n \\ (x_1, x_2, \dots, x_n) &\mapsto (y_1, y_2, \dots, y_n) \end{aligned}$$

où

$$y_i = x_i + k_i \bmod m.$$

$K = (k_1, \dots, k_n)$ constitue la clé de la transformation et elle est **choisie aléatoirement** dans \mathbb{Z}_m^n .

A chaque nouveau message, une nouvelle clé K est utilisée, d'où l'appellation "one-time".

Il faut générer des clés aléatoires très longues et les mettre simultanément à disposition de l'émetteur et du récepteur !
(Kremlin-Maison Blanche)

Le système de Vernam (one-time pad, 1926)

En 1949, Shannon démontre que le "one-time pad" garantit une confidentialité parfaite au sens de la théorie de l'information.

Un système est parfait si l'information approtée par le cryptogramme sur le message en clair ou sur la clé est nulle.

Le "one-time pad" assure une sécurité inconditionnelle par opposition à la sécurité calculatoire.

Sécurité inconditionnelle : ne préjuge pas de la puissance de calcul du cryptanalyste qui peut être illimitée.

Sécurité calculatoire : utilise des clés courtes et le cryptanalyste aura tous les éléments pour calculer clé ou message en clair mais s'il n'a pas la puissance de calcul pour le faire, il n'aboutira pas.

Théorie de Shannon pour la cryptographie

Théorie fondée sur l'étude de l'information qu'apporte le cryptogramme sur le message en clair.

Notions : information, information moyenne, entropie.

X : une variable aléatoire qui prend un nombre fini de valeurs.

On définit **l'information** associée à l'événement $X = x$ par :

$$-\log P(X = x) \tag{1}$$

Les informations associées à des événements indépendants s'ajoutent.

L'**incertitude** ou **entropie** de X est l'information moyenne apportée par X :

$$H(X) = - \sum_x P(X = x) \log P(X = x) \tag{2}$$

La base du logarithme est souvent choisie égale à 2, et dans ce cas l'entropie est mesurée en bits (binary information unit).

Théorie de Shannon pour la cryptographie

Si X est une variable à n valeurs, $H(X)$ est maximale lorsque X est équidistribuée $P(X = x) = 1/n$ pour tout x . Dans ce cas :

$$H(X) = -n \times \frac{1}{n} \log \frac{1}{n} = \log n$$

Si X est une variable binaire, son entropie vaut, lorsqu'elle est équidistribuée, 1 bit.

Entropie conditionnelle : incertitude résiduelle associée à X connaissant Y

$$H(X|Y) = - \sum_{x,y} P(X=x, Y=y) \log P(X=x|Y=y) \quad (3)$$

Règle intuitive : l'entropie de la variable (X, Y) vérifie

$$H(X, Y) = H(X) + H(Y|X) \quad (4)$$

Théorie de Shannon pour la cryptographie

Le modèle de Shannon :

- \mathcal{M} : ensemble des messages possibles
- \mathcal{C} : ensemble des cryptogrammes possibles
- \mathcal{K} : ensemble des clés possibles

Chaque clé $K \in \mathcal{K}$ définit une transformation $M \mapsto C$ avec $M \in \mathcal{M}$ et $C \in \mathcal{C}$.

Originalité : traiter M , K et C comme des variables aléatoires.

Le cryptanalyste connaît le système $(\mathcal{M}, \mathcal{C}, \mathcal{K})$ mais il ne connaît ni M ni K . Le paramètre pertinent est :

$$H(M|C)$$

C'est la mesure de l'**incertitude** qu'il reste **sur** le message en clair **M si on connaît** le cryptogramme **C**.

Théorie de Shannon pour la cryptographie

Shannon définit le **système cryptographique** $(\mathcal{M}, \mathcal{K}, \mathcal{C})$ comme étant **parfait si** :

$$H(\mathbf{M}|\mathbf{C}) = H(\mathbf{M})$$

Cela signifie que la connaissance d'un cryptogramme n'apporte aucune information sur le message en clair.

Le "one-time pad" est un système parfait.

Exemple : $\mathcal{M} = \mathcal{C} = \mathcal{K} = \mathbb{Z}_m^n$ et $C = M + K$ où K est une variable équidistribuée, pour tout $k \in \mathbb{Z}_m^n$

$$P(K = k) = \frac{1}{\#\mathcal{K}}$$

Intercepter $y \in \mathbb{Z}_m^n$, toutes les valeurs x du message M restent possibles puisque toutes les valeurs $y - x$ de la clé sont possibles.

$$P(M = x | C = y) = \frac{P(M = x, C = y)}{P(C = y)}$$

Théorie de Shannon pour la cryptographie

Or d'une part,

$$\begin{aligned} P(C = y) &= \sum_x P(C = y | M = x)P(M = x) \\ &= \sum_x P(K = y - x)P(M = x) \\ &= \frac{1}{\#\mathcal{K}} \end{aligned}$$

et d'autre part,

$$P(M = x, C = y) = P(M = x, K = y - x) = P(M = x)P(K = y - x)$$

car K est une variable indépendante de M . On en déduit

$$P(M = x | C = y) = P(M = x)$$

ce qui implique

$$\mathbf{H}(\mathbf{M} | \mathbf{C}) = \mathbf{H}(\mathbf{M})$$

Théorie de Shannon pour la cryptographie

Pour n'importe quel système cryptographique, on a :

$$H(M|C) \leq H((M, K)|C) \quad (5)$$

$$= H(K|C) + H(M|(C, K)) \quad (6)$$

$$= H(K|C) \quad (7)$$

$$\leq H(K) \quad (8)$$

(5) et (8) \implies rajouter de l'incertitude augmente l'entropie

(6) est l'application de (4)

(7), i.e. $H(\mathbf{M}|(\mathbf{C}, \mathbf{K})) = 0$, traduit le fait qu'une clé et un cryptogramme donnés déterminent complètement le message en clair.

Théorie de Shannon pour la cryptographie

La conséquence suivante de l'inégalité (8) est un résultat fondamental de la théorie de Shannon.

Théorème

Si le système cryptographique $(\mathcal{M}, \mathcal{K}, \mathcal{C})$ est parfait, alors

$$H(K) \geq H(M)$$

Cela veut dire que l'information que révèle la connaissance de la clé secrète K doit être au moins aussi grande que l'information associée au message en clair M .

Si tous les messages en clair sont équiprobables, cela implique que la **taille de la clé est au moins aussi grande que la taille des messages en clair**.

⇒ On ne ferait pas mieux que le "one-time pad".

Théorie de Shannon pour la cryptographie

Shannon a aussi considéré le cas des systèmes imparfaits, à clé courte.
Quelle quantité d'information est nécessaire au cryptanalyste pour
recouvrir la clé à partir du texte chiffré ?

Chiffrement par substitution :

$$\mathcal{M} = \mathcal{C} = \Sigma = \{A, B, \dots, Z\}$$

avec \mathcal{K} l'ensemble des permutations de 26 éléments.

Combien de lettres intercepter pour trouver la clé ?

Hypothèse : une même clé K , de longueur fixe, est utilisée pour chiffrer un texte constitué de n messages M_1, \dots, M_n auxquels sont associés les cryptogrammes C_1, \dots, C_n .

Théorie de Shannon pour la cryptographie

Distance d'unicité d : le plus petit entier n tel que :

$$H(K|(C_1, \dots, C_n)) = 0$$

Il s'agit du plus petit nombre moyen de cryptogrammes C_1, \dots, C_n tel que, connaissant C_1, \dots, C_n , il n'y ait plus aucune incertitude résiduelle sur la clé. On a :

$$\begin{aligned} H(K|(C_1, \dots, C_n)) &= H(K, C_1, \dots, C_n) - H(C_1, \dots, C_n) \\ &= H(M_1, \dots, M_n, K, C_1, \dots, C_n) - H(C_1, \dots, C_n) \\ &= H(M_1, \dots, M_n, K) - H(C_1, \dots, C_n) \\ &= H(M_1, \dots, M_n) + H(K) - H(C_1, \dots, C_n) \end{aligned}$$

car les M_i sont indépendants de K . On vient de montrer que

$$H(M_1, \dots, M_d) + H(K) - H(C_1, \dots, C_d) = 0 \quad (9)$$

Comment trouver d ?

Théorie de Shannon pour la cryptographie

Comment trouver d ? On pourra faire l'hypothèse que

$$H(C_1, \dots, C_d) = d \log(\#\mathcal{C})$$

Cela signifie que tous les cryptogrammes possibles sont équiprobables.

On pose :

$$H = \frac{1}{d} H(M_1, \dots, M_d)$$

Si les messages M_i sont indépendants, alors

$$H = H(M_1)$$

L'hypothèse d'indépendance est inexacte si les M_i sont des lettres d'un texte écrit dans une langue naturelle.

Théorie de Shannon pour la cryptographie

On pourra prendre un échantillon de texte, calculer la fréquence p_L d'apparition de chaque i -uple L de lettres et poser

$$H \approx -\frac{1}{i} \sum_{L \in \Sigma^i} p_L \log p_L$$

Dans ce cas, l'inégalité (9) devient

$$dH + H(K) - d \log(\#\mathcal{C}) = 0$$

Autrement dit :

$$d = \frac{H(K)}{\log(\#\mathcal{C}) - H}$$

Cas du chiffrement par substitution :

$$H(K) = \log(26!) \text{ et } \log(\#\mathcal{C}) = \log(\#\Sigma) = \log 26.$$

Textes écrits en anglais ou en français : i de l'ordre de 8 permet d'estimer l'entropie par lettre $H \approx 2$ bits.

⇒ $d \approx 30$. On doit savoir retrouver la clé dès que le texte chiffré dépasse une trentaine de lettres.

Théorie de Shannon pour la cryptographie

En conclusion :

- ▶ Chiffrer des messages qui contiennent une certaine redondance (langues naturelles) avec des clés de longueur fixée



avec suffisamment de cryptogrammes interceptés, le cryptanalyste aura à sa disposition assez d'information pour retrouver la clé **quel que soit le système de chiffrement utilisé**. Cela ne préjuge pas de l'effort de calcul qui lui sera nécessaire.

- ▶ Pour augmenter la distance d'unicité, il est souhaitable de réduire la redondance des messages en clair avant de les chiffrer (par exemple, par un algorithme de compression)

Partie 4

Cryptographie "moderne"

Principe de Kerckhoffs (1883) :

La sécurité d'un système de chiffrement ne doit reposer que sur le secret de la clé.



L'ennemi peut avoir connaissance du système de chiffrement. Il sera testé, attaqué, étudié et ne sera utilisé que s'il est robuste.

Outils mathématiques capables de répondre au principe de Kerckhoffs :
la complexité !

Calculer $p \times q$ est plus facile que de factoriser $n = pq$.

- ▶ Somme de deux entiers à n chiffres : complexité n .
- ▶ Multiplication de deux entiers à n chiffres : complexité n^2 .
- ▶ **Factorisation** : complexité en $\exp(4n^{1/3})$

Fonctions à sens unique

Fonctions difficilement inversibles (one-way functions).

Définition

Une fonction f :

$$\begin{array}{ccc} \mathcal{E} & \rightarrow & \mathcal{F} \\ x & \mapsto & f(x) \end{array}$$

est dite à sens unique si :

1. Il est **facile** de calculer $f(x)$ pour tout x .
2. Pour un $y \in f(\mathcal{E})$, trouver x tel que $f(x) = y$ est **difficile**.

- ▶ "Facile" : il existe un algorithme qui pour tout x calcule $f(x)$ en un temps polynomial en la longueur de x .
- ▶ "Difficile" : le calcul nécessite un nombre prohibitif d'opérations ou avoir une chance sur laquelle il est déraisonnable de compter.

Fonctions à sens unique

Fonctions à sens unique à **trappe**.

Exemple :

$$f : \quad x \mapsto x^3 \pmod{100}$$

Trouver x tel que $x^3 \equiv 11 \pmod{100}$.

- ▶ Recherche exhaustive, tester 0, 1, 2, 3, ..., 99

$$71^3 = 357911 \equiv 11 \pmod{100}$$

- ▶ Trappe secrète :

$$y \mapsto y^7 \pmod{100}$$

donne directement le résultat !

$$11^7 = 19487171 \equiv 71 \pmod{100}$$

Chiffrement à clé publique

Paramètres d'un **chiffrement à clé publique**

1. Les fonctions de chiffrement et de déchiffrement \mathcal{C} et \mathcal{D}
2. La clé publique du destinataire qui paramètre la fonction \mathcal{C}
3. La clé privée du destinataire qui paramètre la fonction \mathcal{D}

Trouver x tel que $x^3 \equiv 11 \pmod{100}$

1. $\mathcal{C} : x \mapsto x^7 \pmod{100}$ et $\mathcal{D} : y \mapsto y^3 \pmod{100}$
2. La clé publique est 3 :

$$\mathcal{C} : x \mapsto x^3 \pmod{100}$$

3. La clé privée est 7 :

$$\mathcal{D} : y \mapsto y^7 \pmod{100}$$

Chiffrement à clé publique

Petit théorème de Fermat :

Théorème

Si p est un nombre premier et $a \in \mathbb{Z}$ alors :

$$a^p \equiv a \pmod{p}$$

Corollaire : si p ne divise pas a alors

$$a^{p-1} \equiv 1 \pmod{p}$$

Chiffrement à clé publique

Petit théorème de Fermat amélioré:

Théorème

Soient p et q deux nombres premiers distincts et soit $n = pq$. Pour tout $a \in \mathbb{Z}$ tel que $\text{pgcd}(a, n) = 1$ alors :

$$a^{(p-1)(q-1)} \equiv 1 \pmod{n}$$

- ▶ $\text{pgcd}(a, n) = 1 \iff p$ et q ne divisent pas a .
- ▶ Exemple : $p = 5, q = 7$
 - ▶ $n = p \times q = 35$
 - ▶ $(p - 1) \times (q - 1) = 4 \times 6 = 24$
 - ▶ Pour $a = 1, 2, 3, 4, 6, 8, 9, 11, 12, 13, 16, 17, 18, \dots$ on a

$$a^{24} \equiv 1 \pmod{35}$$

Chiffrement à clé publique

Preuve du petit théorème de Fermat amélioré:

Soit $c = a^{(p-1)(q-1)}$

- ▶ c modulo p : $c \equiv (a^{(p-1)})^{(q-1)} \equiv 1^{(q-1)} \equiv 1 \pmod{p}$
- ▶ c modulo q : $c \equiv (a^{(q-1)})^{(p-1)} \equiv 1^{(p-1)} \equiv 1 \pmod{q}$
- ▶ On va en déduire que $c \equiv 1 \pmod{pq}$:
 - $c \equiv 1 \pmod{p}$ donc $\exists \alpha \in \mathbb{Z}$ tel que $c = 1 + \alpha p$
 - $c \equiv 1 \pmod{q}$ donc $\exists \beta \in \mathbb{Z}$ tel que $c = 1 + \beta q$
 - $c - 1 = \alpha p = \beta q$ donc $p|\beta q$
 - comme p et q sont premiers entre eux $p|\beta$
 - il existe donc $\beta' \in \mathbb{Z}$ tel que $\beta = \beta' p$
 - ainsi $c = 1 + \beta q = 1 + \beta' p q$
 - d'où $c \equiv 1 \pmod{pq}$

Chiffrement à clé publique

Algorithme d'Euclide :

$$\text{pgcd}(a, b) = \text{pgcd}(b, a \bmod b)$$

$$a_0 = a, b_0 = b \quad \text{puis} \quad \begin{cases} a_{i+1} = b_i \\ b_{i+1} = a_i \pmod{b_i} \end{cases}$$

Algorithme d'Euclide étendu : pour obtenir les coefficients de Bézout u, v tels que $\mathbf{au} + \mathbf{bv} = \text{pgcd}(a, b)$

$$x_0 = 1, \quad x_1 = 0, \quad y_0 = 0, \quad y_1 = 1$$

Puis pour $i \geq 1$

$$x_{i+1} = x_{i-1} - q_i x_i \quad y_{i+1} = y_{i-1} - q_i y_i$$

où q_i est le quotient de la division euclidienne de a_i par b_i .

Chiffrement à clé publique

Inverse de a modulo n : Soit $a \in \mathbb{Z}$, on dit que $x \in \mathbb{Z}$ est un inverse de a modulo n si

$$ax \equiv 1 \pmod{n}$$

Proposition

1. *a admet un inverse modulo n si et seulement si $\text{pgcd}(a, n) = 1$*
2. *Si $au + nv = 1$ alors u est un inverse de a modulo n*

Preuve :

$$\begin{aligned} \text{pgcd}(a, n) = 1 &\iff \exists u, v \in \mathbb{Z} \quad au + nv = 1 \\ &\iff \exists u \in \mathbb{Z} \quad au \equiv 1 \pmod{n} \end{aligned}$$

Chiffrement à clé publique

Calcul efficace de a^k :

Exemple : calcul de $5^{11} \pmod{14}$

1. On remarque que $11 = 8 + 2 + 1$ donc

$$5^{11} = 5^8 + 5^2 + 5^1$$

2. Calculer les $5^{2^i} \pmod{14}$

$$5 \equiv 5 \pmod{14}$$

$$5^2 \equiv 25 \equiv 11 \pmod{14}$$

$$5^4 \equiv 5^2 \times 5^2 \equiv 11 \times 11 \equiv 121 \equiv 9 \pmod{14}$$

$$5^8 \equiv 5^4 \times 5^4 \equiv 9 \times 9 \equiv 81 \equiv 11 \pmod{14}$$

3. Résultat

$$5^{11} \equiv 11 \times 11 \times 5 \equiv 11 \times 55 \equiv 11 \times 13 \equiv 143 \equiv 3 \pmod{14}$$

Chiffrement à clé publique

Méthode générale

1. Développer k en base 2 : $(k_l, \dots, k_2, k_1, k_0)$, $k_i \in \{0, 1\}$

$$k = \sum_{i=0}^l k_i 2^i.$$

2. Calculer les x^{2^i} modulo n sachant

$$x^{2^{i+1}} = x^{2^i} \times x^{2^i}$$

3. Calculer

$$x^k = x^{\sum_{i=0}^l k_i 2^i} = \prod_{i=0}^l (x^{2^i})^{k_i}$$

Exemple : 11 en base 2 s'écrit (1, 0, 1, 1).

On calcule 5^{2^0} , 5^{2^1} , 5^{2^2} , 5^{2^3} et on a

$$5^{11} = (5^{2^3})^1 \times (5^{2^2})^0 \times (5^{2^1})^1 \times (5^{2^0})^1$$

Chiffrement à clé publique

Calculer $17^{154} \pmod{100}$:

1. $k = 154$ en base 2 correspond à $(1, 0, 0, 1, 1, 0, 1, 0)$ car

$$154 = 128 + 16 + 8 + 2 = 2^7 + 2^4 + 2^3 + 2^1$$

2. Calculer $17, 17^2, 17^4, 17^8, \dots, 17^{128}$ modulo 100.

$$17 \equiv 17 \pmod{100}$$

$$17^2 \equiv 289 \equiv 89 \pmod{100}$$

$$17^4 \equiv 17^2 \times 17^2 \equiv 89 \times 89 \equiv 7921 \equiv 21 \pmod{100}$$

$$17^8 \equiv 17^4 \times 17^4 \equiv 21 \times 21 \equiv 441 \equiv 41 \pmod{100}$$

$$17^{16} \equiv 17^8 \times 17^8 \equiv 41 \times 41 \equiv 1681 \equiv 81 \pmod{100}$$

$$17^{32} \equiv 17^{16} \times 17^{16} \equiv 81 \times 81 \equiv 6561 \equiv 61 \pmod{100}$$

$$17^{64} \equiv 17^{32} \times 17^{32} \equiv 61 \times 61 \equiv 3721 \equiv 21 \pmod{100}$$

$$17^{128} \equiv 17^{64} \times 17^{64} \equiv 21 \times 21 \equiv 441 \equiv 41 \pmod{100}$$

3. Résultat

$$\begin{aligned} 17^{154} &\equiv 17^{128} \times 17^{16} \times 17^8 \times 17^2 \equiv 41 \times 81 \times 41 \times 89 \\ &\equiv 3321 \times 3649 \equiv 21 \times 49 \equiv 1029 \equiv 29 \pmod{100} \end{aligned}$$

Chiffrement à clé publique

Principe :

1. Alice prépare une clé publique et une clé privée
2. Bob utilise la clé publique d'Alice pour chiffrer son message
3. Alice reçoit le message chiffré et le déchiffre avec sa clé privée.

Méthode :

- ▶ Problème difficile : factoriser un entier produit de deux grands nombres premiers
- ▶ Clé publique et clé secrète : calculées à l'aide de l'algorithme d'Euclide et des coefficients de Bézout
- ▶ Calcul modulo un entier
- ▶ Déchiffrement : fonctionne grâce au petit théorème de Fermat

Chiffrement à clé publique

Préparation des clés :

- ▶ Choix de deux nombres premiers distincts p et q
- ▶ Calcul de $n = p \times q$
- ▶ Calcul de $\phi(n) = (p - 1) \times (q - 1)$

Exemple :

- ▶ $p = 5$ et $q = 17$
- ▶ $n = p \times q = 85$
- ▶ $\phi(n) = (p - 1) \times (q - 1) = 64$

Chiffrement à clé publique

Préparation des clés :

- ▶ Choisir un exposant e tel que $\text{pgcd}(e, \phi(n)) = 1$
- ▶ Calculer l'inverse d de e modulo $\phi(n)$ par l'algorithme d'Euclide étendu

$$d \times e \equiv 1 \pmod{\phi(n)}$$

- ▶ La clé publique est constituée de n et e
- ▶ La clé privée est d

Exemple :

- ▶ $e = 5$ et on a bien $\text{pgcd}(e, \phi(n)) = \text{pgcd}(5, 64) = 1$
- ▶ $5 \times 13 + 64 \times (-1) = 1$, donc $5 \times 13 \equiv 1 \pmod{64}$
L'inverse de e modulo $\phi(n)$ est $d = 13$.
- ▶ $n = 85$ et $e = 5$
- ▶ $d = 13$

Chiffrement à clé publique

Chiffrement du message :

- ▶ Transformer le message en un (ou plusieurs) entier m . L'entier m vérifie $0 \leq m < n$.
- ▶ Récupérer la clé publique et calculer le message chiffré

$$x \equiv m^e \pmod{n}$$

- ▶ Transmettre le message chiffré x

Exemple :

- ▶ $m = 10$
- ▶ $n = 85$ et $e = 5$
- ▶ $x \equiv m^e \pmod{n} \equiv 10^5 \pmod{85}$

$$10^2 = 100 \equiv 15 \pmod{85}$$

$$10^4 = (10^2)^2 \equiv 15^2 \equiv 225 \equiv 55 \pmod{85}$$

$$10^5 = (10^4) \times 10 \equiv 55 \times 10 \equiv 550 \equiv 40 \pmod{85}$$

- ▶ Le message chiffré est $x = 40$.

Chiffrement à clé publique

Déchiffrement du message :

- ▶ Déchiffrer le message reçu à l'aide de la clé privée d

$$m \equiv x^d \pmod{n}$$

Exemple :

- ▶ $x = 40$
- ▶ $d = 13$ et $n = 85$
- ▶ Calculer $40^{13} \pmod{85}$. On a $40^{13} = 40^{8+4+1}$

$$40^2 = 1600 \equiv 70 \pmod{85}$$

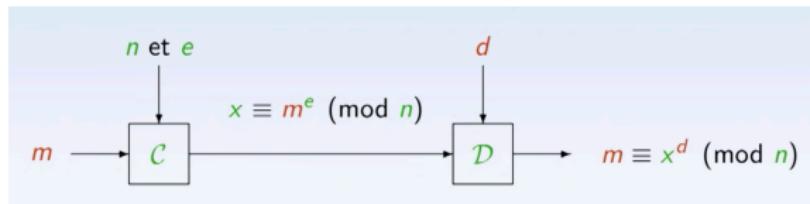
$$40^4 = (40^2)^2 \equiv 70^2 \equiv 4900 \equiv 55 \pmod{85}$$

$$40^8 = (40^4)^2 \equiv 55^2 \equiv 3025 \equiv 50 \pmod{85}$$

- ▶ $40^{13} \equiv 40^8 \times 40^4 \times 40^1 \equiv 50 \times 55 \times 40 \equiv 10 \pmod{85}$
- ▶ On retrouve bien $m = 10$.

Déchiffrement du message

En résumé :



Le principe du déchiffrement du RSA repose sur le petit théorème de Fermat amélioré. Le résultat peut être énoncé sous la forme d'un lemme de déchiffrement.

Lemme

Soit d l'inverse de e modulo $\phi(n)$ avec $n = p \times q$ et $p \neq q$.

Si $x \equiv m^e \pmod{n}$ alors $m \equiv x^d \pmod{n}$

Déchiffrement du message

Preuve:

- ▶ d est l'inverse de e modulo $\phi(n)$ donc $d \times e \equiv 1 \pmod{\phi(n)}$.
Il existe $k \in \mathbb{Z}$ tel que $d \times e = 1 + k \times \phi(n)$.
- ▶ Petit théorème de Fermat amélioré :

Si $\text{pgcd}(m, n) = 1$ alors $m^{\phi(n)} = m^{(p-1)(q-1)} \equiv 1 \pmod{n}$

- ▶ Si $\text{pgcd}(m, n) = 1$ alors modulo n :

$$\begin{aligned} (m^e)^d &\equiv m^{1+k \times \phi(n)} \equiv m \times m^{k \times \phi(n)} \\ &\equiv m \times (m^{\phi(n)})^k \equiv m \times (1)^k \\ &\equiv m \pmod{n} \end{aligned}$$

Déchiffrement du message

Preuve:

Si $\text{pgcd}(m, n) \neq 1$, par exemple $\text{pgcd}(m, n) = p$ et $\text{pgcd}(m, q) = 1$ alors

- ▶ modulo p : $m \equiv 0$ et $(m^e)^d \equiv 0$ donc $(m^e)^d \equiv m \pmod{p}$
- ▶ modulo q :
$$(m^e)^d \equiv m \times (m^{\phi(n)})^k \equiv m \times (m^{q-1})^{(p-1)k} \equiv m \pmod{q}$$
- ▶ $\text{pgcd}(p, q) = 1$
$$(m^e)^d \equiv m \pmod{n}$$