La sécurité des données

Valérie Ménissier-Morain
Laboratoire d'Informatique de Paris 6, UPMC

Principes

Confidentialité
seules des personnes autorisées ont accès à l'information

Intégrité
assurer l'intégrité de données consiste à permettre la détection des modifications de ces données

Authentification
la signature électronique garantit que l'auteur du message ou la source des données est bien ce que l'on croit.

Vocabulaire

Chiffrement
opération pour rendre la compréhension d'un document impossible à toute personne qui n'a pas la clef d'encodage

Déchiffrement
opération inverse du chiffrement, pour obtenir le message qui a été précédemment chiffré, algorithme et clef de chiffrement connus

Cryptosystème algorithne de chiffrement

Cryptographie étude des systèmes de chiffrement

Stéganographie au lieu de rendre le message inintelligible pour tout autre que son destinataire, camoufler le message dans un support de manière à masquer sa présence

Attaquer, casser
cryptanalyser un cryptosystème / *casser un code* : trouver la clef du code ou le moyen d'accéder au message qu'il protégeait

Cryptanalyse étude de la résistance aux attaques d'un cryptosystème, élaboration de nouvelles attaques

Cryptologie = cryptographie + cryptanalyse

Cryptosystème symétrique/asymétrique
symétrique le cryptosystème utilise la même clef pour chiffrer et déchiffrer les messages
asymétrique le cryptosystème utilise une clef publique pour chiffrer et une clef privée (différente) pour déchiffrer les messages

Niveaux d'attaque
force brute ou exhaustive essayer toutes les clés possibles de l'algorithme de chiffrement jusqu'à trouver celle qui donne un message clair qui a un sens à partir d'un message chiffré
attaque à chiffrés connus l'attaquant dispose d'un ou de plusieurs messages chiffrés, sans avoir d'informations sur leur signification en clair
attaque à clairs/chiffrés connus l'attaquant possède une ou plusieurs paires du type message clair/message chiffré
attaque à clairs/chiffrés choisis l'attaquant a accès à un appareil de chiffrement/déchiffrement en boîte noire
attaque par mot probable l'attaquant ne connait pas tout le message clair, mais au moins une partie, par exemple, la signature (exemple *La Jangada* de Jules Verne), ou bien le début (exemple la météo pour Enigma)

Protocole cryptographique
protocole qui effectue des opérations liées à la sécurité, souvent une suite de primitives cryptographiques, qui explique en détail comment elles doivent être utilisées.
Applications : communications sécurisées, échange de clef de session, signature électronique, paiement électronique, vote électronique

Principe de Kerchkoffs
l'ennemi possède tous les détails de l'algorithme, il ne lui manque que la clef spécifique pour le chiffrement. Un cryptosystème qui s'appuie uniquement sur le secret de l'algorithme n'a aucun intérêt.

Références pour les dispositifs physiques

- http://www.nymphomath.ch/crypto/instruments/index.html Dispositifs physiques de chiffrement et déchiffrement à travers les âges
- http://www.cryptomuseum.com/ Musée virtuel de la crytologie : dispositifs physiques de chiffrement et déchiffrement ou d'espionnage
- hhttp://www.apprendre-en-ligne.net/crypto/transpo/scytale.html La scytale spartiate
- http://www.apprendre-en-ligne.net/crypto/jefferson/index.html Le cylindre de Jefferson
- https://en.wikipedia.org/wiki/Cryptanalysis_of_the_Enigma Le cassage d'Enigma

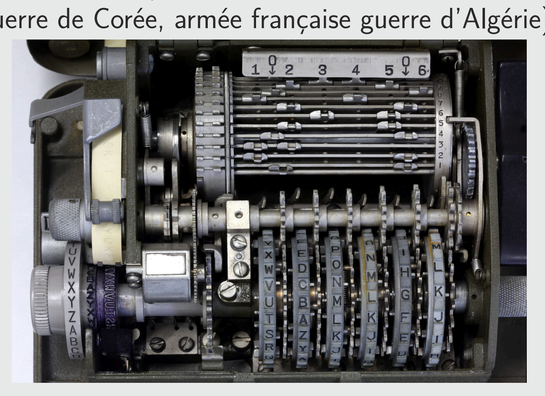
Dispositifs physiques

Scytale spartiate (XXème au VIIème av. JC)

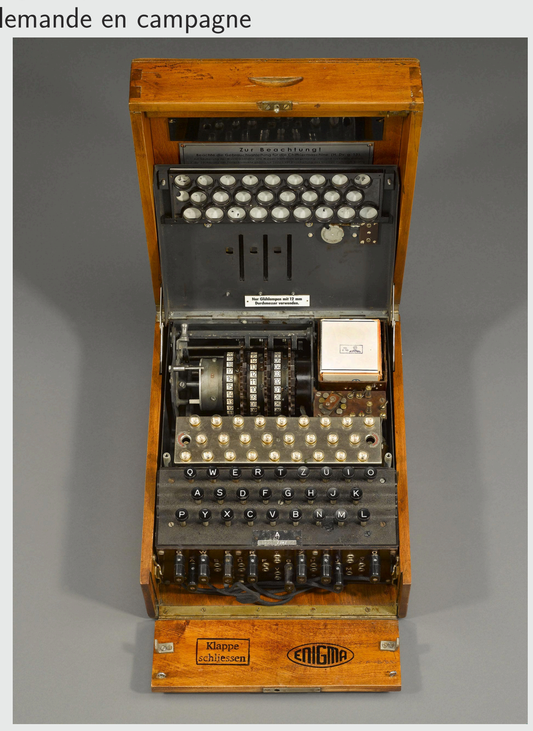
Machines à cylindres
de la version de Jefferson (US, 1793), Bazeries (France, 1891) ou Ducros (Italie, 1900)

à la M-94 (1917-1942 : armée US WWII)

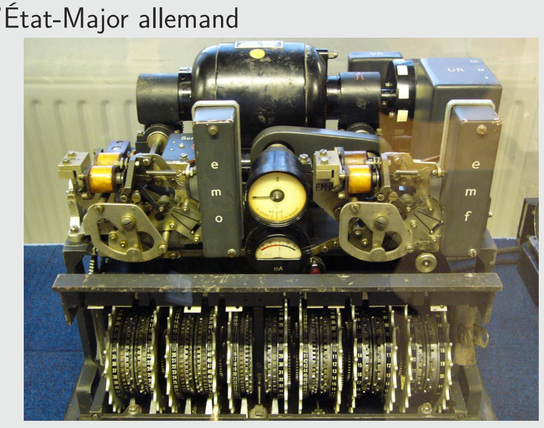
puis la M-209 (1939 - 1962 : armée US WWII, guerre de Corée, armée française guerre d'Algérie)



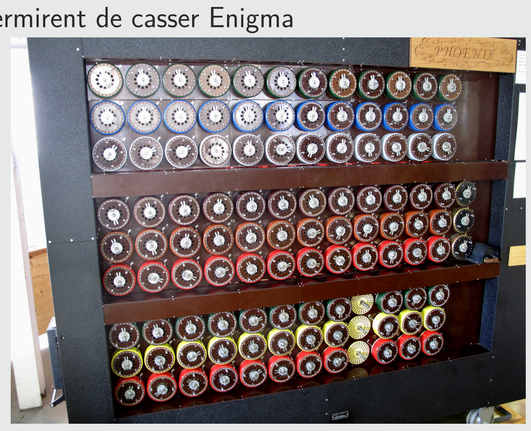
Machines à rotors
Enigma, petite machine portative de l'armée allemande en campagne



et la machine de Lorenz, machine imposante de l'État-Major allemand



Les *bombes* polonaises puis anglaises qui permirent de casser Enigma



Stéganographie : on ne peut pas explorer ce dont on ignore l'existence

Masquages rudimentaires

Nabuchodonosor (-600, Babylone), Histiée de Milet (-500, Grèce ionienne) : écriture sur le crâne rasé d'un esclave qu'on adresse au destinataire après la repousse des cheveux

Demarate (-480) : écriture sur le socle en bois d'une tablette de cire sur laquelle on a retiré la cire puis recouverte à nouveau de cire, le messager semble donc transporter une tablette vierge

Encre sympatique (depuis le Ie siècle av. JC)
L'expéditeur ajoute à un document écrit classique, un message à l'aide de jus de citron, de lait, de produits chimiques, voire d'urine ! En sèchant ce liquide devient invisible à l'oeil, le message voyage sans être détecté. À l'arrivée le destinataire chauffe le document à la flamme d'une bougie ou l'expose à un réactif chimique et le message apparaît.

Chinois, César le message est écrit sur une bandelette roulée en boule puis enrobée de cire et avalée par le messager

Dissimulation d'un texte dans un autre texte : Tritème (chaque caractère est remplacé par une expression religieuse), message composé de caractères, mots ou lignes en position fixe dans le texte (échange de lettres de Georges Sand avec Alfred de Musset)

Grilles de Cardan (XVIè) : l'expéditeur et le destinataire possèdent une plaque opaque percée de trous, l'expéditeur rédige un texte anodin où le texte du message apparaît, le destinataire place la grille sur le texte et lit le message.

Stéganographie moderne

Masquage moderne : on peut cacher un message dans une image, une musique.
Application commerciale : le tatouage électronique ou *watermarking* pour protéger la propriété intellectuelle ou identifier l'exemplaire copié.
Cette technique reste délicate à utiliser.

Systèmes de chiffrement symétriques

Substitution mono-alphabétique

Atbash (VIe av. JC) : inversion de l'alphabet

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

Chiffrement de `BONJOUR`
`BONJOUR`
`YLMQLFI`

Carré de Polybe (IIe av. JC)
Les caractères (25 lettres en confondant deux caractères tels que I et J, 36 avec lettres et chiffres, etc.) sont placés dans un carré avec des chiffres ou des lettres pour les coordonnées des lignes et des colonnnes. Un caractère est remplacé par son abscisse et son ordonnée dans le tableau.

	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

Original

	1	2	3	4	5	6
1	M	O	T	D	E	P
2	A	S	B	C	F	G
3	H	I	J	K	L	N
4	Q	R	U	V	W	X
5	Y	Z	0	1	2	3
6	4	5	6	7	8	9

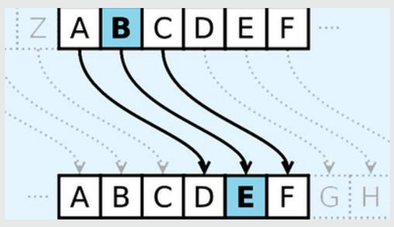
Avec chiffres
et mot de passe `MOTDEPASSE`

	1	2	3	4	5	6	7
1	we	a	ya	ra	yo	chi	i
2	hi	sa	ma	mu	ta	ri	ro
3	mo	ki	ke	u	re	nu	ha
4	se	yu	fu	wi	so	ru	ni
5	su	me	ko	no	tsu	wo	ho
6	n	mi	e	o	ne	wa	he
7	shi	te	ku	na	ka	to	

Variante de Uesugi (XVIè Japon)

Cette variante utilise l'alphabet japonais traditionnel de 48 lettres (tiré du poème iroha-uta).
Si les caractères ne sont pas ordonnés alphabétiquement le carré est la clef du chiffrement sinon c'est un simple code.
Chiffrement de `BONJOUR` avec le carré avec mot de passe `MOTDEPASSE` :
`B O N J O U R`
`23123633124342`

Chiffre de César (Ie av. JC)



Chiffrement de `BONJOUR`
`BONJOUR`
`DQPLQWT`

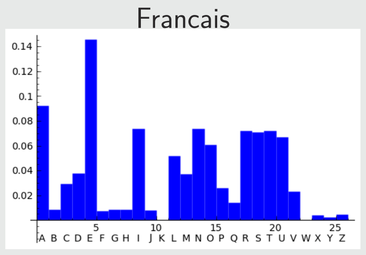
Chiffre des francs-maçons (XVIIIe)

Chiffrement de `BONJOUR` :
`B O N J O U R`

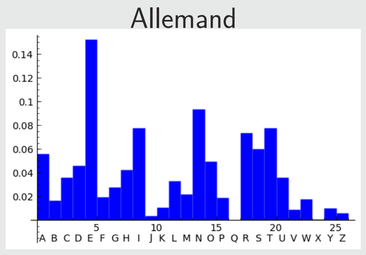
Ce chiffrement est inspiré de celui des Templiers au XIIe siècle, construit à partir de la Croix de Malte symbole de leur ordre.

Cryptanalyse (Al Kindi ≃800) par étude statistique de la fréquence des caractères et des bigrammes (suite de deux caractères) en s'appuyant sur l'hypothèse que la distribution des fréquences dans le texte est représentative de la langue dans laquelle il a été rédigé.

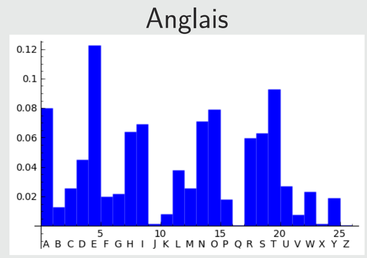
Francais



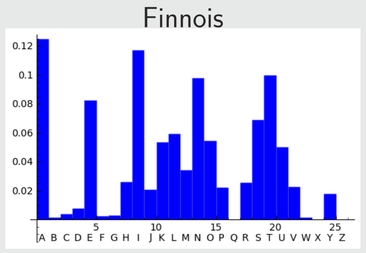
Allemand



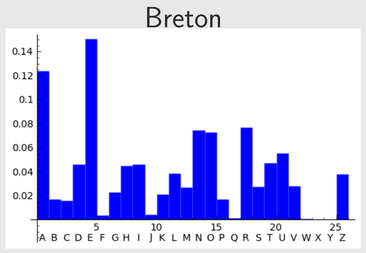
Anglais



Finnois



Breton



Suédois