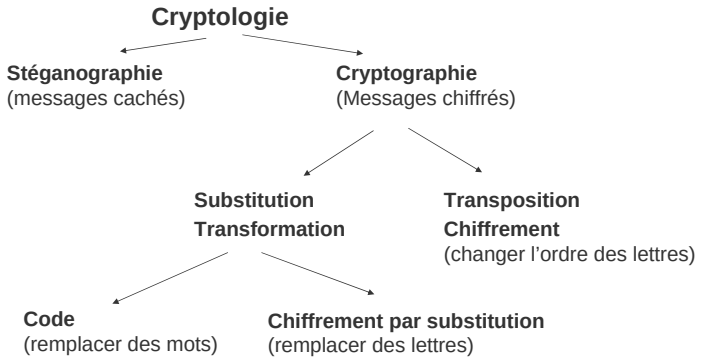
Cryptographie classique

Cryptographie classique



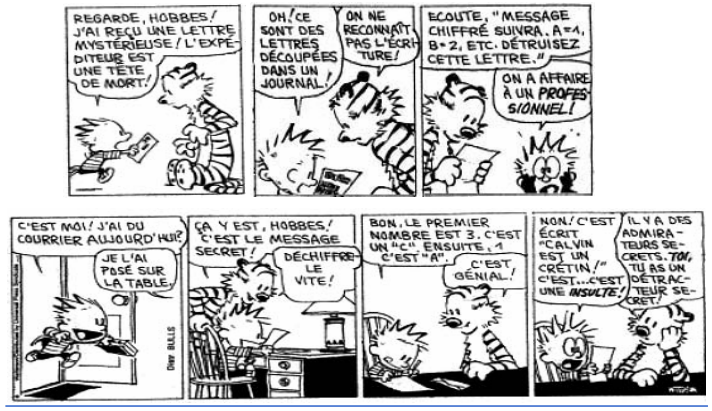
Cryptographie classique

Chiffrement monoalphabétique

Dans les **substitutions simples** (qu'on appelle aussi **monoalphabétiques**), chaque lettre est remplacée par une autre lettre ou un autre symbole. Dans cette catégorie, on peut citer le chiffre de César, les alphabets désordonnés ou encore le chiffre affine. Le message que déchiffre Calvin sur la page suivante est aussi un exemple de substitution simple.

Toutes les substitutions simples sont vulnérables à une **analyse des fréquences** d'apparition des lettres.

Chiffrements par substitution



Chiffrement de César

- Principe : décaler les lettres de l'alphabet.
  - Chiffrement : C = E(p) = (p + k) mod 26
  - Déchiffrement : p = D(C) = (C- k) mod 26
- Si algorithme connu → cryptanalyse par force brute très simple → 25 clés possibles !
- Pourquoi force brute ?
  - Algorithme connu
  - 25 clés à essayer
  - Langage initial connu

→ c'est la longueur de la clé qui rend cette attaque inutilisable

La plupart du temps, les algorithmes et la langue utilisés sont connu → c'est la longueur de la clé qui rend cette attaque inutilisable

De plus,

- une compression ou un langage inconnu rendent l'attaque plus difficile
- une permutation des 26 caractères alphabétiques → 26! clés (ou > $4*10^{26}$ clés). (voir plus loin)

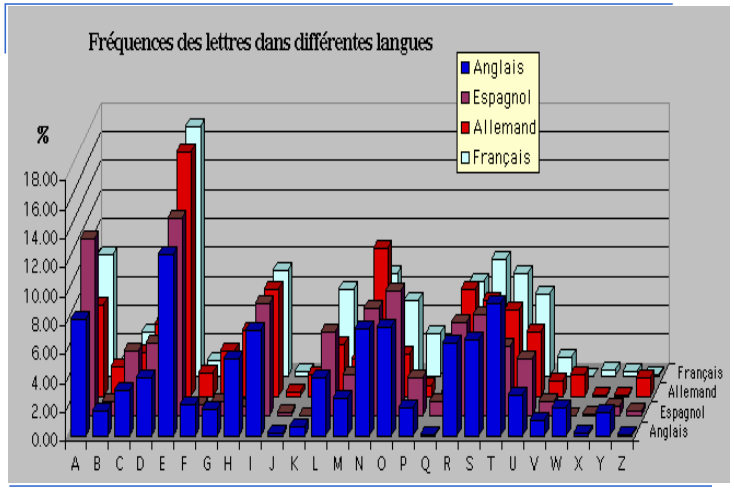
L'attaque par force brute est alors éliminée.

Analyse de fréquence

- Si la langue de départ et la technique de chiffrement sont connus → exploiter les régularités du langage.
- Analyse de la fréquence d'une lettre
- Cette technique ne fonctionne bien que si le message chiffré est suffisamment long pour avoir des moyennes significatives.

Analyse de fréquence

- QTJYCOQTQYVJYIOUOMPEGOJQIOYIUPQPFN
  S E S S E E E ES
  YOUOMGOBJOQSOYJGJQYEWAFOWOYYPHOSTUO
  SE E E E ES S E SS E E
- Fréquences : O = 14, Y = 9, Q = 7, J = 6…
- Fréquences en français : E , A, S, I, T, …
- Dans notre cas : O ?= E, Y ?= A ou Y ?= S, …
- NOUSVENONSJUSTEDEFAIREUNTESTDANALY
  SEDEFREQUENCESURUNSIMPLEMESSAGECODE



Le chiffre affine

- L'idée est d'utiliser comme fonction de chiffrage une fonction affine du type **y = (ax + b) mod 26**, où **a** et **b** sont des constantes, et où **x** et **y** sont des nombres correspondant aux lettres de l'alphabet (A=0,B=1,…)
- On peut remarquer que si **a**=1, alors on retrouve le chiffre de César et **b** est le décalage.
- On remarquera aussi que si **b**=0, alors "a" est toujours chiffré "A".

Le chiffre affine - fonctionnement

- Clé :

  Clé = (k_1, k_2) $k_1,k_2 \in [0,25]$ $\gcd(k_1,26)=1$

- Transformation de chiffrement :

  $c_i = f(m_i) = k_1 * m_i + k_2 \bmod 26$

- Transformation de déchiffrement :

  $m_i = f^{-1}(c_i) = k_1^{-1} * (c_i - k_2) \bmod 26$

- Nombres de clés possibles : 12*26 = 312

Exemple d'utilisation

- Clé = $(k_1, k_2) = (3, 11)$
- Transformation de chiffrement :

  $c_i = f(m_i) = 3 * m_i + 11 \bmod 26$
- Transformation de déchiffrement :

  $k_1^{-1} = 3^{-1} \bmod 26 = 9$ car $3 * 9 \bmod 26 = 1$

  $m_i = f^{-1}(c_i) = 9 * (c_i - 11) \bmod 26$
- Exemple :
  - NSA $\rightarrow$ 13 – 18 – 0 $\rightarrow$ 24 – 13 – 11 $\rightarrow$ YNL

Le chiffre affine - cryptanalyse

1. Établir la fréquence relative de chaque lettre du texte chiffré $\rightarrow$ analyse de fréquence

   ```
   GHUYI DEGRS YTGOR RYOVG EOHGA
   HKEIA AOTDG SBINN TGKGR HENNI
   RGSGH HGNYI ASI
   ```

   ```
   G : 10   H : 6
   ```

   anglais ?

Le chiffre affine – cryptanalyse(2)

2. Sur base de l'analyse de fréquence, dériver les équations correspondantes

- Hypothèse : E et T sont les lettres les plus fréquentes en anglais
- Equations correspondantes :

$E \rightarrow G$	$f(E) = G$
$T \rightarrow H$	$f(T) = H$
$4 \rightarrow 6$	$f(4) = 6$
$19 \rightarrow 7$	$f(19) = 7$

Le chiffre affine – cryptanalyse(3)

3. Résoudre les équations pour k_1 et k_2 inconnus

$f(4) = 6$

$f(19) = 7$

$\Downarrow$

$4*k_1 + k_2 \equiv 6 \pmod{26}$

$19*k_1 + k_2 \equiv 7 \pmod{26}$

$\Downarrow$

$15\ k_1 \equiv 1 \bmod 26$

$\Downarrow$

$K_1 = 7$

Contre-mesures

- Utiliser des homophones
  - remplacer une lettre non pas par un symbole unique, mais par un symbole choisi au hasard parmi plusieurs.
  - Dans sa version la plus sophistiquée, on choisira un nombre des symboles proportionnel à la fréquence d'apparition de la lettre.

  → Renversement des fréquences.
    - faire disparaître complètement les indications fournies par la fréquence
- Contrecarré par les digrammes et les trigrammes

Digrammes et trigrammes

Les 20 bigrammes les plus fréquents

Bigrammes	ES	DE	LE	EN	RE	NT	ON	ER	TE	EL	AN	SE	ET	LA	AI	IT	ME	OU	EM	IE
Nombres	3318	2409	2366	2121	1885	1694	1646	1514	1484	1382	1378	1377	1307	1270	1255	1243	1099	1086	1056	1030

Les 20 trigrammes les plus fréquents

Trigrammes	ENT	LES	EDE	DES	QUE	AIT	LLE	SDE	ION	EME	ELA	RES	MEN	ESE	DEL	ANT	TIO	PAR	ESD	TDE
Nombres	900	801	630	609	607	542	509	508	477	472	437	432	425	416	404	397	383	360	351	350

Cryptographie classique

Chiffrements polygraphiques

Polygrammique : Se dit d'un chiffre où un groupe de *n* lettres est codé par un groupe de *n* symboles.

Dans les **substitutions polygrammiques** (aussi appelées **polygraphiques**), les lettres ne sont pas chiffrées séparément, mais par groupes de plusieurs lettres (deux ou trois généralement).

Exemples: le chiffre de Playfair (avec *n* = 2), le chiffre de Hill et certains systèmes modernes comme le RSA

Le chiffrement de Playfair (1854)

- Chiffrement à lettre multiples (digramme)
- On dispose les 25 lettres de l'alphabet (W exclu car inutile, on utilise V à la place) dans une grille 5x5, ce qui donne la clef. La variante anglaise consiste à garder le W et à fusionner I et J.
- 4 règles à appliquer
- Déchiffrement : appliquer les règles dans l'autre sens.

Playfair - règles

- Si les 2 lettres sont :
  1. sur des « coins » → lettres chiffrées = les 2 autres coins.
  2. sont sur la même ligne → prendre les deux lettres qui les suivent immédiatement à leur droite
  3. la même colonne → prendre les deux lettres qui les suivent immédiatement en dessous
  4. Identiques → insérer une nulle (usuellement le X) entre les deux pour éliminer ce doublon.

Pour former les grilles de chiffrement, on utilise un **mot-clef secret** pour créer un alphabet désordonné avec lequel on remplit la grille ligne par ligne. Les autres lettres de l'alphabet sont alors ajoutées dans l'ordre dans la grille pour la compléter

Playfair – cryptanalyse et critique

- Si le cryptogramme est assez long → analyse de la fréquence des digrammes. Il faut ensuite essayer de reconstituer la grille de chiffrement.
- Avantages :
  - 26 lettres → 26*26 = 676 digrammes
  - Analyse de fréquence difficile
  - Utilisé pendant les 2 guerres mondiales par les alliés
- Inconvénient :
  - Facile à casser car il conserve la structure du texte clair

Chiffrement de Hill (1929)

- **Chiffrement**
  - Les lettres sont d'abord remplacées par leur rang dans l'alphabet. Les lettres P_k et $P_{k+1} \rightarrow C_k$ et C_{k+1}

$$\begin{pmatrix} C_k \\ C_{k+1} \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} P_k \\ P_{k+1} \end{pmatrix} \pmod{26}$$

  - Chaque digramme clair (P_1 et P_2) sera chiffré (C_1 et C_2) selon :

$$C_1 \equiv aP_1 + bP_2 \pmod{26}$$
$$C_2 \equiv cP_1 + dP_2 \pmod{26}$$

Exemple de chiffrement

- **Alice** prend comme clef de cryptage la matrice $\begin{pmatrix} 9 & 4 \\ 5 & 7 \end{pmatrix}$ pour chiffrer le message « je vous aime »
- Après avoir remplacé les lettres par leur rang dans l'alphabet (a=1, b=2, etc.), elle obtiendra

$$C_1 \equiv 9 \cdot 10 + 4 \cdot 5 \pmod{26} = 110 \pmod{26} = 6$$
$$C_2 \equiv 5 \cdot 10 + 7 \cdot 5 \pmod{26} = 85 \pmod{26} = 7$$

- Elle fera de même avec les 3e et 4e lettres, 5e et 6e, etc. Elle obtiendra finalement

Lettres	j	e	v	o	u	s	a	i	m	e
Rangs (P_k)	10	5	22	15	21	19	1	9	13	5
Rangs chiffrés (C_k)	6	7	24	7	5	4	19	16	7	22
Lettres chiffrées	F	G	X	G	E	D	S	P	G	V

Matrice de chiffrement

On ne peut pas prendre n'importe quoi comme matrice de chiffrement. Ses composantes doivent tout d'abord être des **nombres entiers positifs**. Il faut aussi qu'elle ait une matrice inverse dans Z_{26}.

Le chiffre affine peut être vu comme la version unidimensionnelle du chiffrement de Hill.

Chiffre de Hill

- Déchiffrement
  - Pour déchiffrer, le principe est le même que pour le chiffrement: on prend les lettres deux par deux, puis on les multiplie par une matrice

$$\begin{pmatrix} P_1 \\ P_2 \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} \begin{pmatrix} C_1 \\ C_2 \end{pmatrix} \pmod{26}$$

  - **Cette matrice doit être l'inverse de matrice de chiffrement (modulo 26)**. Ordinairement cet inverse est

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \frac{1}{ad - bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

Exemple de déchiffrement

- Pour déchiffrer le message d'**Alice**, **Bob** doit calculer :

$$\begin{pmatrix} 9 & 4 \\ 5 & 7 \end{pmatrix}^{-1} = \frac{1}{43} \begin{pmatrix} 7 & -4 \\ -5 & 9 \end{pmatrix} \pmod{26} = (43)^{-1} \begin{pmatrix} 7 & -4 \\ -5 & 9 \end{pmatrix} \pmod{26}$$

- Comme gcd(43,26) = 1, $(43)^{-1}$ existe dans Z_{26} et $(43)^{-1} = 23$. **Bob** a la matrice de déchiffrement :

$$\begin{pmatrix} 9 & 4 \\ 5 & 7 \end{pmatrix}^{-1} = 23 \begin{pmatrix} 7 & -4 \\ -5 & 9 \end{pmatrix} \pmod{26} = \begin{pmatrix} 161 & -92 \\ -115 & 207 \end{pmatrix} \pmod{26} = \begin{pmatrix} 5 & 12 \\ 15 & 25 \end{pmatrix} \pmod{26}$$

Exemple de déchiffrement

- **Bob** prend donc cette matrice pour déchiffrer le message "FGXGE DSPGV". Après avoir remplacé les lettres par leur rang dans l'alphabet (A=1, B=2, etc.), il obtiendra:

$$P_1 \equiv 5 \cdot 6 + 12 \cdot 7 \pmod{26} = 114 \pmod{26} = 10$$
$$P_2 \equiv 15 \cdot 6 + 25 \cdot 7 \pmod{26} = 265 \pmod{26} = 5$$

- Il fera de même avec les 3e et 4e lettres, 5e et 6e, etc. Il obtiendra finalement:

Lettres chiffrées	F	G	X	G	E	D	S	P	G	V
Rangs chiffrés (C_k)	6	7	24	7	5	4	19	16	7	22
Rangs (P_k)	10	5	22	15	21	19	1	9	13	5
Lettres	j	e	v	o	u	s	a	i	m	e

Cryptographie classique

Substitutions polyalphabétique

Les **substitutions polyalphabétiques** (aussi appelées **à double clef** ou **à alphabets multiples**), utilisent plusieurs "alphabets", ce qui signifie qu'une même lettre peut être remplacée par plusieurs symboles. L'exemple le plus fameux de chiffre polyalphabétique est sans doute le chiffre de Vigenère, qui résista aux cryptanalystes pendant trois siècles.

Chiffre de Vigenère (1568)

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

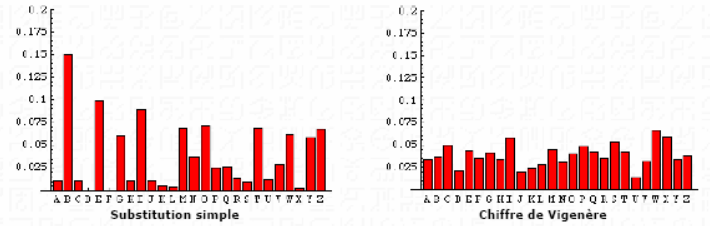
Chiffre de Vigenère (1568)

- **Exemple:** chiffrer le texte "CHIFFRE DE VIGENERE" avec la clef "BACHELIER" (cette clef 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
Clef	B	A	C	H	E	L	I	E	R	B	A	C	H	E	L	I	E
Décalage	1	0	2	7	4	11	8	4	17	1	0	2	7	4	11	8	4
Chiffré	D	H	K	M	J	C	M	H	V	W	I	I	L	R	P	Z	I

- La grande force du chiffre de Vigenère est que la même lettre sera chiffrée de différentes manières **ce qui rend inutilisable l'analyse de fréquence classique**.

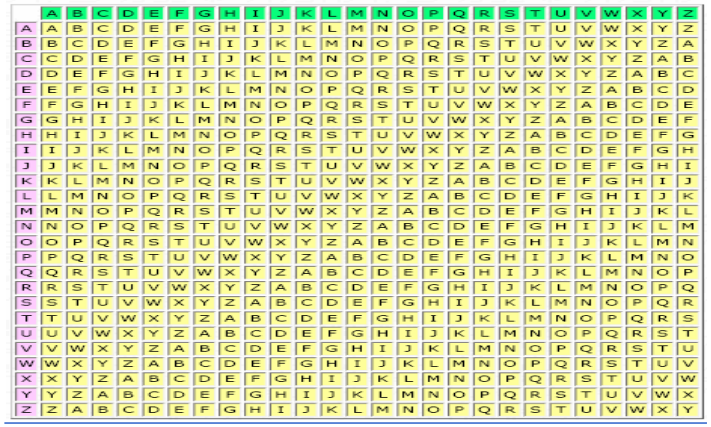
Chiffre de Vigenère (1568)



fréquences des lettres d'une fable de la Fontaine (le chat, la belette et le lapin) chiffrée avec une substitution simple(gauche) et avec le chiffre de Vigenère (droite)

Si la clef est aussi longue que le texte clair, et moyennant quelques précautions d'utilisation, le système est appelé masque jetable.(voir plus loin)

Carré de Vigenère



Carré de vigenère :

> La lettre de la clef est dans la colonne la plus à gauche, la lettre du message clair est dans la ligne tout en haut. La lettre chiffrée est à l'intersection des deux.

L'emploi du carré de Vigenère est souvent sujet à erreurs: la lecture en est pénible et, à la longue, fatigante. Beaucoup de cryptologues préfèrent se servir d'une "réglette", facile à construire, et d'un maniement plus rapide.

Vigenère - notation

- Chiffrement

  $c_i = f_{i \bmod d}(m_i) = m_i + k_{i \bmod d} \bmod 26$

- Déchiffrement

  $M_i = f^{-1}_{i \bmod d}(m_i) = m_i - k_{i \bmod d} \bmod 26$

- Clés

  $k_1, k_2, \ldots, k_{d-1}$

- Nombre de clés

  Pour une longueur de clé d : $(26)^d$

Cryptanalyse – Méthode Kasiski

1. chercher des séquences de lettres qui apparaissent plus d'une fois dans le texte:
   - soit la même séquence de lettres du texte clair a été cryptée avec la même partie de la clef
   - soit deux suites de lettres différentes dans le texte clair auraient (possibilité faible) par pure coïncidence engendré la même suite dans le texte chiffré.
   - Le 1er cas = le plus probable → le nombre de facteurs de la clef
2. méthode de fréquence de distribution des lettres cryptées → les lettres du texte clair.

En prenant par exemple la clef 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. Ainsi le mot *thé* peut être chiffré en DPP, BSS, EVO ou HRM.

K	I	L	O	K	I	L	O	K	I	L	O	K	I	L	O	K	I	L	O	K
t	h	e	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

Dans l'exemple ci-dessus, le mot "thé" est chiffré "DPP" 2 fois et "BSS" 1 fois.
Des répétitions de cette sorte offrent la prise nécessaire pour attaquer Vigenère

Pour attaquer un chiffre de Vigenère, il faut trouver la clef! Cela est possible si la clef est courte et le texte long. Le texte ci-dessus a Le premier pas consiste à deviner la longueur de la clef. On cherche pour cela des séquences de plusieurs lettres consécutives (par exemple 3 ou plus) apparaissant plusieurs fois.

Ce renseignement est capital. Si, par exemple, la longueur de la clef 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 fréquence à ces caractères et trouver la première lettre de la clef. Pour la deuxième lettre de la clef, on analysera les fréquences des caractères de rang 3k+2 et pour le dernière lettre les fréquences des caractères de rang 3k.

Cryptanalyse – test de Friedman

- **Indice de Coïncidence** (IC) $\triangleq$ la probabilité que deux lettres choisies aléatoirement dans un texte soient identiques.
- Soient
  - n le nombre de lettres dans le texte
  - n_1 = nombre de A, …,n_{26} = nombre de Z
- La probabilité de tirer deux A parmi les n lettres du texte est:

$$P(2 \text{ fois } A) = \frac{C_2^{n_1}}{C_2^n} = \frac{\frac{n_1(n_1-1)}{2}}{\frac{n(n-1)}{2}} = \frac{n_1(n_1-1)}{n(n-1)}$$

Le **test de Friedman** (aussi appelé **test kappa**) a pour premier objectif de **déterminer si un texte a été chiffré avec un chiffre monoalphabétique ou polyalphabétique**. Comme second bénéfice, il suggère la longueur du mot-clef si le chiffre est polyalphabétique. Pour réaliser ces buts, le test de Friedman s'appuie sur une métrique appelée **Indice de Coïncidence** (IC), qui est la probabilité que deux lettres choisies aléatoirement dans un texte soient identiques.

Cryptanalyse – test de Friedman

- La probabilité de tirer 2 lettres identiques :

$$IC = \sum_{i=1}^{26} \frac{n_i(n_i-1)}{n(n-1)}$$

- Exemples d'indices calculés sur des textes contemporains dans différentes langues:

Langue	allemand	anglais	espagnol	esperanto	français	italien	norvégien	suédois
IC	0.072	0.065	0.074	0.069	0.074	0.075	0.073	0.071

Cryptanalyse – test de Frieman

- **Remarques importantes**
  - Pour un langage de 26 lettres où chaque lettre a la même fréquence (1/26), IC = 0.038
  - Pour tout chiffre monoalphabétique, la distribution des fréquences est invariante, donc l'IC sera le même que pour le texte clair.
  - Donc, si on applique ce test à un texte chiffré avec un chiffre monoalphabétique, on devrait trouver IC égal environ à 0.074 (en français). Si IC est beaucoup plus petit (p. ex. 0.050), le chiffre est probablement polyalphabétique.

Trouver la longueur de la clé avec l'IC

- Soit le message suivant, chiffré avec Vigenère (369 lettres):
  - PERTQ UDCDJ XESCW MPNLV MIQDI ZTQFV XAKLR PICCP QSHZY
    DNCPW EAJWS ZGCLM QNRDE OHCGE ZTQZY HELEW AUQFR OICWH
    QMYRR UFGBY QSEPV NEQCS EEQWE EAGDS ZDCWE OHYDW QERLM
    FTCCQ UNCPP QSKPY FEQOI OHGPR EERWI EFSDM XSYGE UELEH
    USNLV GPMFV EIVXS USJPW HIEYS NLCDW MCRTZ MICYX MNMFZ
    QASLZ QCJPY DSTTK ZEPZR ECMYW OICYG UESIU GIRCE UTYTI
    ZTJPW HIEYI ETYYH USOFI XESCW HOGDM ZSNLV QSQPY JSCAV
    QSQLM QNRLP QSRLM XLCCG AMKPG QLYLY DAGEH GERCI RAGEI
    ZNMGI YBPP
- On va considérer les sous-chaînes obtenues en prenant les lettres à intervalle donné:
  - Intervalle de 1: PERTQ UDCDJ XESCW MPNLV ... (texte original)
    Intervalle de 2: PRQDD XSWPL ... et ETUCJ ECMNV ...
    Intervalle de 3: PTDJS MLIIQ ..., EQCXC PVQZF... et RUDEW NMDTV
    ...

Trouver la longueur de la clé avec l'IC

- On calcule ensuite les IC pour toutes ces sous-chaînes.

Intervalle	Indice de coïncidence
1	0.0456107
2	0.0476954, 0.0443098
3	0.044249, 0.0494469, 0.0426771
4	0.0465839, 0.0453894, 0.0449116, 0.0425227
5	0.0799704, 0.0925583, 0.0836727, 0.0795282, 0.0684932
6	0.0512956, 0.0407192, 0.0371585, 0.0382514, 0.0661202, 0.0431694

On remarque que quand l'intervalle est de 5, l'IC correspond plus ou moins avec l'IC caractéristique du français (en tout cas, c'est cette ligne qui s'approche le plus de 0.074, les autres lignes étant plutôt proches de 0.038). La longueur de la clef utilisée est donc probablement 5. Pour découvrir la clef elle-même, on peut ensuite procéder comme le faisait kasiski

Trouver la longueur de la clé avec l'IC

- Si un message **en français** de longueur n et d'indice de coïncidence IC est chiffré avec un carré de Vigenère, alors r, la longueur du mot-clef composé de lettres **distinctes**, est donné par la formule

$$r \approx \frac{(0.074 - 0.038)\,n}{(n-1)\mathbf{IC} - 0.038\,n + 0.074} \approx \frac{0.036\,n}{(n-1)\mathbf{IC} - 0.038\,n + 0.074}$$

- En appliquant cette formule au texte précédent, on trouve r = 4.69, ce qui confirme ce que l'on avait trouvé ci-dessus.

http://jf.morreeuw.free.fr/vigenere/vigenere.html

Chiffre de Vernam (One-Time Pad)

- Masque jetable $\triangleq$ chiffre de Vigenère avec comme caractéristique que la clef de chiffrement a la même longueur que le message clair
- Exemple :

Clair	M	A	S	Q	U	E	J	E	T	A	B	L	E
Clef	X	C	A	A	T	E	L	P	R	V	G	Z	C
Décalage	23	2	0	0	19	4	11	15	17	21	6	25	2
Chiffré	J	C	S	Q	N	I	U	T	K	V	H	K	G

Chiffre de Vernam (One-Time Pad)

Méthode du masque jetable

- Il faut :
  1. choisir une clef aussi longue que le texte à chiffrer,
  2. utiliser une clef formée d'une suite de caractères aléatoires,
  3. protéger votre clef,
  4. ne jamais réutiliser une clef,
  5. écrire des textes clairs ne contenant que les lettres (sans ponctuation et sans espaces).

Le système du masque jetable, avec les précautions indiquées ci-dessus, est absolument inviolable si l'on ne connaît pas la clef. Il est couramment utilisé de nos jours par les États. En effet, ceux-ci peuvent communiquer les clefs à leurs ambassades de manière sûre via la valise diplomatique

http://www.pro-technix.com/information/crypto/pages/vernam_base.html

Difficultés

- Le problème de ce système est de communiquer les clefs de chiffrage ou de trouver un algorithme de génération de clef commun aux deux partenaires :
  1. La création de grandes quantités des clefs aléatoires : n'importe quel système fortement utilisé pourrait exiger des millions de caractères aléatoires de façon régulière.
  2. La distribution des clés : une clé de longueur égale est nécessaire pour l'expéditeur et pour le récepteur. Nécessite une bonne organisation.

Cryptographie classique

Transposition

Transposition

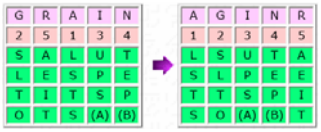
- Consiste à changer l'ordre des lettres
- Pour de très brefs messages : méthode est peu sûre car il y a peu de variantes
- Lorsque le nombre de lettres croît : impossible de retrouver le texte original sans connaître le procédé de brouillage.
- Par exemple, une phrase de 35 lettres peut être disposée de 35! = 10^{40} manières
- Nécessite un procédé rigoureux convenu auparavant entre les parties.

Pour de très brefs messages, comme un simple mot, cette méthode est peu sûre car il n'y a guère de variantes pour redistribuer une poignée de lettres. Par exemple un mot de trois lettres ne peut être tourné quand dans 6 (=3!) positions différentes. Ainsi col ne peut se transformer qu'en col, clo, ocl, olc, lco, loc.

Une transposition au hasard des lettres semble donc offrir un très haut niveau de sécurité, mais il y a un inconvénient: pour que la transposition soit efficace, l'ordonnancement des lettres doit suivre un système rigoureux sur lequel d'expéditeur et l'envoyeur se sont préalablement entendus.

Transposition - exemple

- Une transposition rectangulaire consiste à écrire le message dans une grille rectangulaire, puis à arranger les colonnes de cette grille selon un mot de passe donné (le rang des lettres dans l'alphabet donne l'agencement des colonnes). Dans l'exemple ci- dessous, on a choisi comme clef GRAIN pour chiffrer le message SALUT LES PETITS POTS. En remplissant la grille, on constate qu'il reste deux cases vides, que l'on peut remplir avec des nulles ou pas.



Cryptographie classique

Machines à rotor

Machines à rotor (WWII)

Country	Machine	Period
Germany:	Enigma	d=26·25·26 = 16,900
U.S.A.:	M-325, Hagelin M-209	
Japan:	"Purple"	
UK:	Typex	d=26·(26-k)·26, k=5, 7, 9
Poland:	Lacida	d=24·31·35 = 26,040

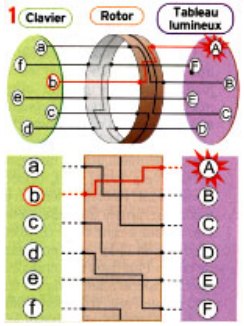
L'entre-deux-guerres voit le début de la mécanisation de la cryptographie. Des outils mécaniques, comme les cylindres chiffrants, sont mis à disposition des opérateurs, et des machines électromécaniques, sont mises au point. Ces machines fonctionnent sur le principe des **rotors** et des **contacts électriques**, afin de réaliser des formes de substitution polyalphabétique dont la clef a une longueur gigantesque de l'ordre de centaines de millions de lettres, au lieu de quelques dizaines dans les méthodes artisanales, comme le chiffre de Vigenère.
Enigma est la machine à chiffrer et déchiffrer qu'utilisèrent les armées allemandes du début des années trente jusqu'à la fin de Seconde Guerre Mondiale. Elle automatise le chiffrement par substitution. Cette machine ressemble à une machine à écrire. Quand on presse sur une touche, deux choses se passent. Premièrement, une lettre s'allume sur un panneau lumineux: c'est la lettre chiffrée. Deuxièmement, un mécanisme fait tourner le rotor de droite d'un cran; toutes les 26 frappes, le deuxième rotor tourne d'un cran, toutes les 676 frappes (26 au carré), c'est le troisième rotor qui tourne d'un cran. Certaines Enigmas avaient 3 rotors, celles de la Kriegsmarine en avaient 4 ou 5 (on peut apercevoir ces 4 cylindres gris sur le dessus de la machine ci-contre). Ces rotors tournants modifient les connexions électriques dans la machine, ce qui fait que la touche "A" allumera peut-être le "B" la première fois, mais le "X" la deuxième, le "E" la troisième, etc. Un "tableau de connexions" et un "réflecteur" complique encore le système. Le côté génial de cette machine est que même si elle tombe entre les mains ennemies, sa sécurité n'est pas compromise. En effet, c'est le nombre faramineux de réglages de la machine qui fait sa force et les réglages changeaient évidement chaque jour. On peut en effet changer l'ordre de rotors, leur orientation initiale et les branchement du tableau de connexions. Par exemple, on pouvait spécifier la clef du jour ainsi:

- Position des rotors : 2 - 3 - 1
- Orientations des rotors : 2 - 23 - 5
- Branchements des connexions : A/L - P/R - T/D - B/W - K/F - O/Y
- Indicateurs : B - W - E

Ainsi, connaître le fonctionnement de la machine n'aide (presque) pas à décrypter les messages qu'elle produit. Tout le problème est de retrouver le bon réglage. C'est dans ce but qu'ont été produites les bombes de Turing.

La machine Enigma – Principe (1)

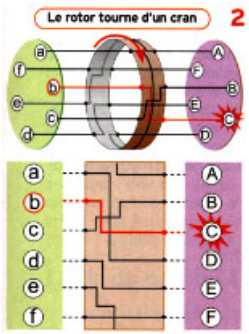
- Si on frappe la lettre **b** sur le clavier, un courant électrique est envoyé dans le rotor, suit la câblage interne, puis ressort à droite pour allumer la lettre **A** sur le tableau lumineux.
- Autre principe de base: chaque fois qu'une lettre est tapée au clavier, le rotor tourne d'un cran. Ainsi, **b** devient **A** la première fois, mais **b** devient **C** la deuxième fois, puis **b** devient **E**, etc.



Le principe de base des machines Enigma conçues par Scherbius repose sur l'utilisation de rotors qui transforment l'alphabet clair (noté en minuscules) en alphabet chiffré (en majuscules). Pour mieux l'illustrer, nous nous limiterons à un alphabet de six lettres. Voici la représentation de l'un de ces fameux rotors, ainsi que le schéma équivalent qui permet de mieux suivre l'opération "avec les doigts".

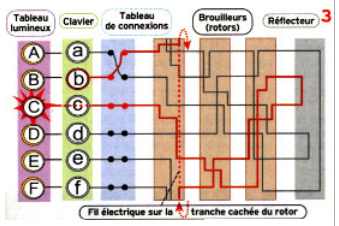
La machine Enigma – Principe (2)

- Dans notre exemple le mot **bac** est chiffré **ADD** (et non **ABD** si le rotor était resté immobile). Pour augmenter le nombre de combinaisons possibles - et déjouer les tentatives des cryptanalystes- , Scherbius a associé plusieurs dispositifs, comme indiqué sur le schéma 3.



La machine Enigma – Principe (3)

- tableau de connexions → brouiller les pistes en reliant deux lettres du clavier entre elles
- Les trois brouilleurs associés multiplient ainsi le nombre de combinaisons.
- Quant au réflecteur, il renvoie le courant dans le dispositif jusqu'au panneau lumineux où la lettre cryptée s'affiche.



Le tableau de connexions permet de brouiller les pistes en reliant deux lettres du clavier entre elles (ici **a** et **b**). Ainsi, quand on tape **b**, le courant prend en fait le circuit prévu pour **a**. Les trois brouilleurs associés multiplient ainsi le nombre de combinaisons. Le deuxième et le troisième avancent respectivement d'un cran quand le premier et le deuxième ont fait un tour complet. Quant au réflecteur, il renvoie le courant dans le dispositif jusqu'au panneau lumineux où la lettre cryptée s'affiche. Son rôle n'est pas d'augmenter le nombre de combinaisons possibles, mais de faciliter considérablement la tâche du destinataire. En effet, si **b** devient **C** dans notre exemple (en rouge), on a aussi **c** devient **B**. Et c'est valable pour toutes les paires de lettres claire/cryptée. Conséquence: si le mot **efface** est chiffré **ACBFEB** par l'émetteur, il suffira à l'opérateur qui reçoit le message crypté de taper **acbfeb** sur son clavier pour voir les lettres **E**, **F**, **F**, **A**, **C**, **E** s'allumer. Seule condition: les deux opérateurs distants doivent avoir réglé leur machine Enigma de la même façon.

La machine Enigma – Principe (4)

- Au final, on a:
  - 26 x 26 x 26 = 17'576 combinaisons liées à l'orientation des chacun des trois brouilleurs,
  - 6 combinaisons possibles liées à l'ordre dans lequel sont disposés les brouilleurs,
  - $\pm 10^{11}$ branchements possibles quand on relie les six paires de lettres dans le tableau de connexions.
- Les machines Enigma peuvent donc chiffrer un texte selon 17'576 x 6 x 100'391'791'500 = 10^{16} combinaisons différentes!

Cryptographie classique

Stéganographie

Contrairement à la cryptographie, qui **chiffre** des messages de manière à les rendre incompréhensibles, la stéganographie (en grec «l'écriture couverte») **cache** les messages dans un support, par exemple des images ou un texte qui semble anodin.

Les premiers emplois attestés de la stéganographie se lisent chez Hérodote vers le Ve siècle avant Jésus-Christ: un certain Histiée, voulant prendre contact avec le tyran Aristagoras de Milet, choisit un esclave dévoué, lui rasa la tête, et y inscrivit le message à transmettre. Il attendit que ses cheveux repoussent pour l'envoyer à Aristagoras avec l'instruction de se faire raser le crâne.

Toujours d'après Hérodote, pour informer les Spartiates de l'attaque imminente des Perses, un certain Démarate utilisa un élégant stratagème: il prit des tablettes, en racla la cire et grava sur le bois le message secret, puis il recouvrit les tablettes de cire. De cette façon, les tablettes, apparemment vierges, n'attirèrent pas l'attention.

En Chine ancienne, on écrivait les messages sur une fine soie dont on faisait une petite boule en l'englobant dans de la cire. Le messager avalait ensuite cette boule.

Au XVIe siècle, le scientifique italien **Giovanni Porta** découvrit comment cacher un message dans un oeuf dur: il suffit d'écrire sur la coquille avec une encre contenant une once d'alun pour une pinte de vinaigre; la solution pénètre la coquille et dépose sur la surface du blanc d'oeuf le message que l'on lira aisément après avoir épluché l'oeuf.

Stéganographie

- La stéganographie (en grec «l'écriture couverte») **cache** les messages dans un support anodin
  - Encre invisible
  - Gammes de musique
  - Lettres de Georges Sand
  - Images
  - …

L'historien de la Grèce Antique Enée le Tacticien imagina d'envoyer un message secret en piquant de minuscules trous sous certaines lettres d'un texte anodin. La succession de ces lettres fournit le texte secret.

Deux mille ans plus tard, les épistoliers anglais employèrent la même méthode, non pour assurer le secret à leurs envois, mais pour éviter de payer des taxes excessives.

En effet, avant la réforme du service postal, dans les années 1850, envoyer une lettre coûtait environ un shilling tous les cent miles, ce qui était hors de portée de la plupart des gens, mais les journaux ne payaient pas de taxe. Grâce aux piqûres d'épingles, les Anglais malins pouvaient envoyer leurs messages gratuitement.

Ce procédé a été aussi utilisé par les Allemands pendant la première guerre mondiale. Au cours de la seconde guerre mondiale, ils améliorèrent le procédé en cochant les lettres de journaux avec de l'encre sympathique.

Lettre de Georges Sand

Cher ami, Je suis toute émue de vous dire que j'ai bien compris l'autre jour 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 une preuve que je puisse être aimée par vous. Je suis prête à montrer mon affection toute désintéressée et sans calcul, et si vous voulez me voir ainsi vous dévoiler, sans artifice, mon âme toute nue, daignez me faire visite, nous causerons et 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 amitié, en un mot : la meilleure épouse dont vous puissiez rêver. Puisque votre âme est libre, pensez que l'abandon où je vis est bien long, bien dur et souvent bien insupportable. Mon chagrin est trop gros. Accourez bien vite et venez me le faire oublier. À vous je veux me soumettre entièrement.

Votre poupée

Réponses

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 coeur
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.

Alfred de Musset

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

George Sand

Un texte apparemment innocent peut aussi révéler un message important. Voici un exemple d'un tel message, envoyé par un espion allemand pendant la seconde guerre mondiale:

Apparently neutral's protest is thoroughly discounted and ignored. Isman hard it. Blockade issue affects pretext for embargo on byproducts, ejecting suets and vegetable oils.

Si l'on prend la deuxième lettre de chaque mot, le message suivant émerge:

Pershing sails from NY June 1.

Les espions allemands de la deuxième guerre mondiale utilisaient aussi des **micropoints** pour faire voyager discrètement leurs informations. C'est une photographie de la taille d'un point de ponctuation, qu'il suffit d'agrandir pour voir apparaître clairement le message (c'est une sorte de microfilm). Ce micropoint pouvait être inséré dans une lettre anodine, parfois sous un timbre, etc.

Ressources

- http://nomis80.org/cryptographie/cryptographie.html
- http://www.01adfm.com/win_xp/hacking/Hacking08.htm
- http://www.01adfm.com/win_xp/hacking/Hacking07.htm
- http://perso.club-internet.fr/guidovdi/codes/lapagecryptologie.htm
- http://www.pro-technix.com/information/crypto/pages/vernam_base.html
- http://www.chez.com/nopb/crypto2.html#transposition

Questions…

Détaillez

- Chiffre de César
- Analyse de fréquence
- Chiffre de Playfair
- Chiffre affine + cryptanalyse
- Chiffre de Hill
- Chiffre de Vigenère + cryptanalyse
- Chiffre de Vernam
- Machine Enigma