Université du Temps Libre Essonne

Codes secrets
Des jeux d'enfants aux affaires d'Etat

Marie-José Durand-Richard

SPHERE (REHSEIS) UMR 7219

CNRS-Université Paris Diderot

UTL Epinay sur Orge : 20/03/2012

UTL Boussy Saint-Antoine : 13/04/2012

Des codes secrets

- Histoire peu connue

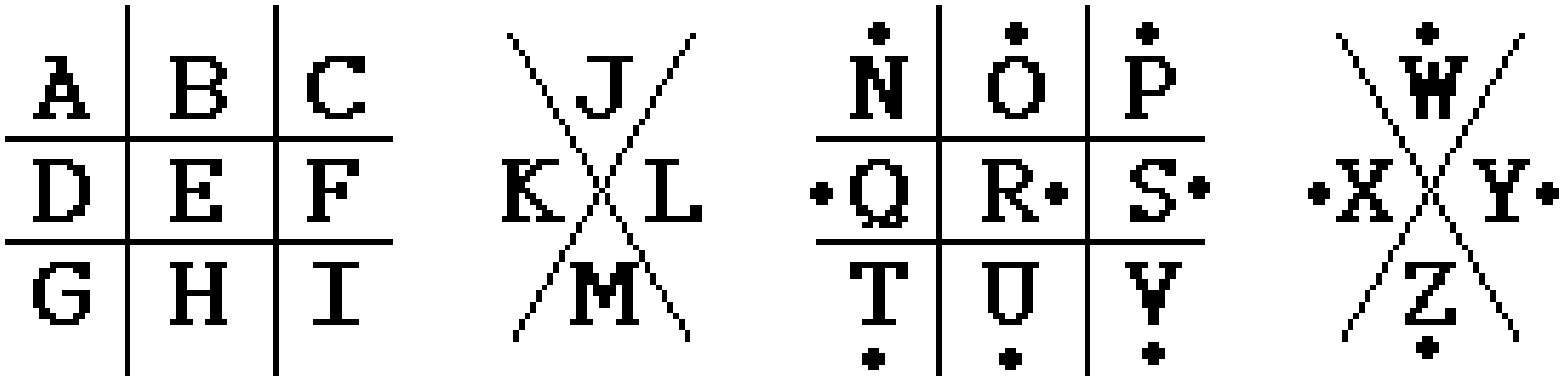
  échange secret de messages
- Pourquoi le secret ?

  Protection : défensive ou offensive ?
- Vulgarisation, popularisation, démocratisation
- Jeu d'enfant, affaires d'Etat, vie quotidienne

  Trois exemples
- Que signifie le secret des communications au 21ème siècle ?

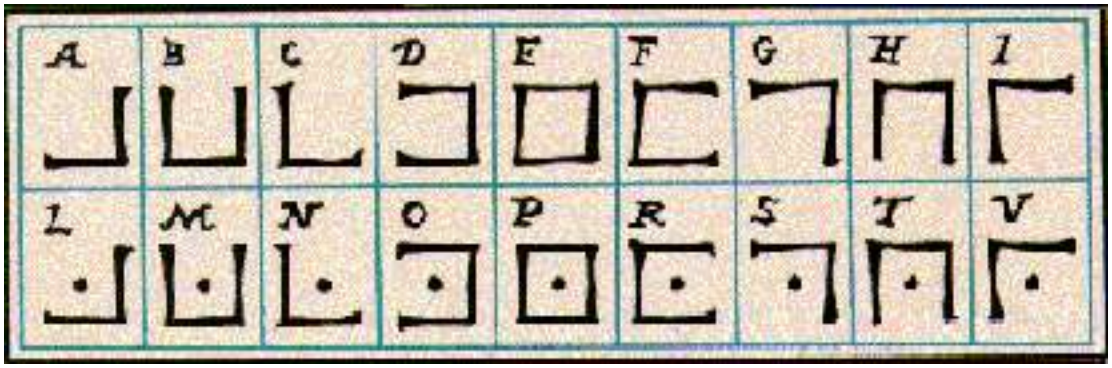
Le secret dans les jeux d'enfant (1)

Repérer chaque lettre de l'alphabet par sa place dans ce système de représentation



Un secret déjà pratiqué

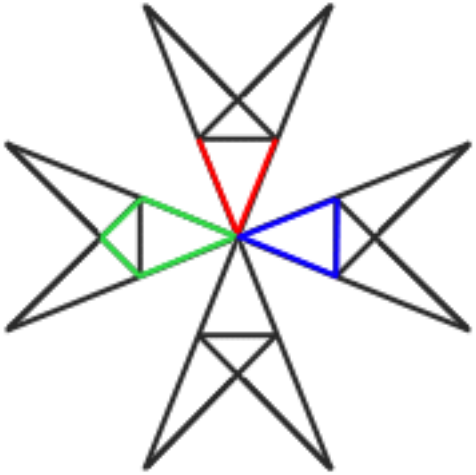
- Heinrich Cornelius Agrippa von Nettelsheim, 1533, *De occulta philosophia*
- Reproduit dans le *Traicté des chiffres, ou secretes manieres d'escrire*, de Blaise de Vigenère en 1586

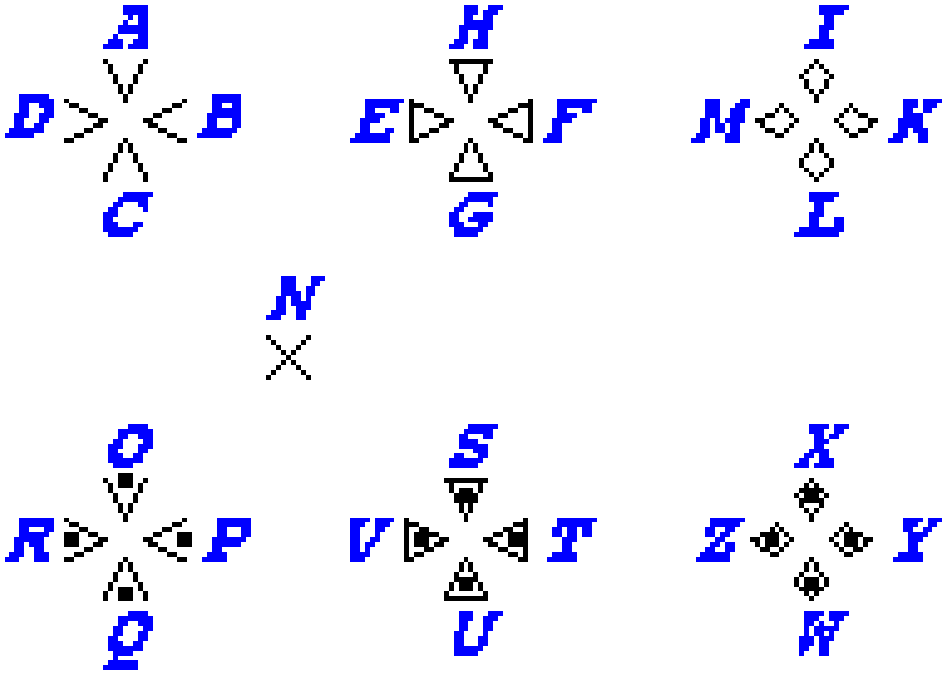


Le secret dans les jeux d'enfant (2)

Souvent appelé le « parc à cochons » [lettres encloses]

Inspiré de l'alphabet des Templiers, XIIème s.





La croix des huit béatitudes était l'emblème de l'ordre

Une affaire d'Etat
Le chiffre de Marie, reine d'Ecosse (1)

- **15 octobre 1586** : Marie Stuart, reine d'Ecosse, emprisonnée depuis 1568, est jugée pour trahison, accusée d'un complot contre la reine d'Angleterre, sa cousine Elizabeth I (1533-58-1603)
- Epoque de l'installation de l'anglicanisme en Angleterre : Elizabeth I excommuniée en 1570

  Marie Stuart catholique
- Complot mis à jour par le décryptement de sa correspondance secrète

La condamnation de Marie Stuart (1542-1587)

- Fille du roi d'Ecosse Jacques V, défait par Henri VIII
- Mariage conclu avec François, dauphin de France (1548) : François II : 1558, veuve en 1560
- Ecosse 1561.
- 2ème mariage : Comte de Darnley 1565, assassiné 1567.
- 3ème mariage. Emprisonnée 1567. S'évade 1568.
- Fuite en Angleterre. Emprisonnée par Elisabeth I (1533-1603)
- Messager Gilbert Gifford / France 1586
- Projet d'évasion d'Antony Babington : chiffrement
- Gifford agent double du premier ministre Sir Francis Walsingham

Une affaire d'Etat
Le chiffre de Marie, reine d'Ecosse (2)

- La correspondance secrète est décryptée par son secrétaire du chiffre, Thomas Phelippes, un linguiste qui parlait français, allemand, italien, espagnol, et latin.

- Ecole du chiffre créée à Londres par Walshingham et placée sous la direction de Thomas Phelippes

Le nomenclateur de Marie Stuart

23 symboles alphabet, 4 nulles, 1 symbole double, 36 mots

Une situation de la vie quotidienne

- Camille demande un rendez-vous sur son téléphone portable
- Elle prend le métro en glissant son sac sur la machine
- Elle entre au bureau en passant son badge devant le tourniquant d'accès
- A midi, elle paie son repas avec sa carte Moneo
- Elle quitte son travail en prenant un vélo en libre service qu'elle paie avec son passe Navigo
- Elle règle son ordonnance avec sa carte Vitale
- Elle regarde Canal + et commande un livre sur Amazon
- Elle boucle sa déclaration de revenus sur Internet

Des codes secrets à la cryptologie

- Histoire peu connue **ou inaperçue**
  circulation limitée de l'information
- Nombreuses interventions aujourd'hui
  carte bancaire, téléphonie mobile,
  carte d'assuré social, monéo, navigo,
  TV à péage
- Accès conditionnel : d'un art à une science
  transparence ou secret ?
  espionnage et démocratie ?

Quelques éléments de vocabulaire

- **cryptographie**, art ou savoir-faire

chiffrer des messages que l'on désire garder secrets,

du grec *Krypto,* secret, caché, et *graphein,* écrire

- chiffrer :

distinguer « code » et « chiffrement »

codes : argot, verlan, « hobos »

chiffrement : lettre à lettre

chiffre-cypher

mot arabe « sifr » : signe pour zéro

- le clair : message d'origine

Quelques éléments de vocabulaire

- Transmission cachée :

  Le chiffré ou le cryptogramme :

- Déchiffrer ou décrypter

  Déchiffrer : on connaît le système

  Décrypter : on ne le connaît pas

- **cryptanalyse**, art du décryptement,

  décrypter les messages chiffrés

Comment parler de l'histoire de la cryptologie ?

- Des affaires d'Etat à la vie quotidienne
- Des jeux d'écriture

  à l'introduction des mathématiques
- Eviter une approche rétro-historique
- Avant les mathématiques : des activités :

  pratiques, instruments, gestes, procédures, théorisation
- Rencontre avec des mathématiques elles aussi marquées historiquement

Quelques procédés matériels de dissimulation de messages

- La scytale de Sparte ou bâton de Plutarque

  (5ème s. avt notre ère)

? Procédé de transposition : redistribution des lettres ?

Ecrire le message en cassant le graphisme des lettres

La scytale (5ème s. avt notre ère)

« Quand on avait à écrire au général quelque chose de secret, on roulait sur ce cylindre une bande de médiocre largeur et de longueur suffisante, en manière de spirale ; les anneaux de la bande, ainsi roulés, devaient être exactement appliqués et unis l'un à l'autre. Puis on traçait les caractères transversalement, les lignes allant de haut en bas. La bande, ainsi chargée d'écriture, était enlevée du cylindre et envoyée au général au fait du stratagème ; après la séparation, elle n'offrait plus que des lettres tronquées et mutilées, des corps et des têtes de lettres, divisés et épars : aussi la dépêche pouvait tomber au pouvoir de l'ennemi sans qu'il lui fût possible d'en deviner le contenu ».

Aulu Gelle, *Nuits attiques*, livre XVII, Ch. 9

Cryptanalyse de la scytale

Edgar Poe, « La cryptographie », *Derniers contes*, 1887.

« [Sur] un cône … dont la circonférence à la base soit au moins égale à la longueur de la bande. … on enroulera [la] bande sur le cône près de la base, bord comme bord. …. On [la] laissera glisser vers le sommet. Il est impossible qu'en suivant ce procédé, quelques-uns des mots, ou quelques-unes des syllabes et des lettres, qui doivent se rejoindre, ne se rencontrent pas au point du cône où son diamètre égale celui de la scytale sur laquelle le chiffre a été écrit…. On a [ainsi] établi… la circonférence de la scytale…… »

Le chiffrement monoaphabétique
Le chiffre de César (–50)

- Signalée dès le 4ème s. en Grèce
- Une lettre de l'alphabet est remplacée par une autre, à partir d'un décalage constant

« On possède enfin de César des lettres à Cicéron, et sa correspondance avec ses amis sur ses affaires domestiques. Il écrivait, pour les choses tout à fait secrètes, à travers des **marques**, c'est-à-dire un ordre arrangé de lettres de sorte qu'aucun mot ne pût être reconnu. Si on veut chercher et s'acharner jusqu'au bout, on change la quatrième lettre, c'est-à-dire un D à la place d'un A et pareillement pour toutes les autres ».

Suétone, *La vie des douze Césars.*

Le chiffrement monoaphabétique
Le chiffre de César (–50)

- ? Procédé de chiffrement par substitution ?

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

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

- Déchiffrement : décalage dans l'autre sens.
- Décryptement :

  Aujourd'hui, on peut dire :

  26 possibilités si on garde l'ordre des lettres

  (26! –1) possibilités si on accepte un ordre quelconque

Environ $4 \cdot 10^{26}$: un essai par seconde, 15 milliards d'années.

Mais c'est un anachronisme.

Le chiffre de César
Utilisations

- Pendant un millénaire
- Officiers sudistes pendant la guerre de Sécession
- Armée russe en 1915

Les cryptanalystes arabes

- Même contexte linguistique que celui de la naissance de l'algèbre, dès le 8ème s.
- Enorme travail de traduction

  Bayt al Hikma, Bagdad
- Langue arabe facteur d'unification
- Importante organisation administrative

  « kuttab » / « diwan »

Les cryptanalystes arabes

- al-Khalil ibn Ahmad (718-786), grammairien

  Kitab al-Mu'amma

  Le livre des messages cryptographiques

- **al Kindi (801-873), *Bayt al Hikma*, Bagdad, *mss***
- ibn Dunaynir (1187– 1229)
- ibn Adlan (1187– 1268), poète, Le Caire
- ibn ad-Duraihim (1312– 1361), émissaire en Egypte

  Miftah al-Kunuz fi Idah al-Marmuz

  le Trésor des clés pour clarifier les chiffres (redécouvert et publié)

- al Qalqashandi, cité par David Kahn

  Subh-al-a sha, 1412

- Ibrahim a. Al-Kahi, 1992, « Origins of Cryptology : the Arab Contributions », *Cryptologia,* vol. VXI, n° 2, pp. 97-126.

al Kindi (801-873)

- Définition de termes / la cryptologie :
  - Chiffrement: *at-ta'miya*
  - Interprétation : *at-tarajma*

    Cryptographie et ses méthodes, parfois cryptanalyse
  - Cryptanalyse : *'ilmu istikhraj al-mu'mamma*

    Science pour extraire l'obscurité
  - Clé : *at-mifta*

    Ensemble de lettres convenues pour retrouver le sens caché

Principes de la cryptanalyse

Méthodes quantitatives :Analyse des fréquences

- Comptage des occurrences des lettres
  - dans la langue [texte long]
  - dans le texte

Méthodes qualitatives : Recherche des mots probables

- Repérage de régularités dans le chiffré
- Connaissance de régularités dans la langue
- Formules convenues
- Combinaisons fréquentes et impossibles

Exemple historique de ce type de cryptanalyse

- Edgar Poe (1809-1849)

  Le scarabée d'or, 1843, Philadelphie
- David A. Conradus

  « Cryptographia Denudata », 1842, *Gentleman's Magazine*

Exemple de décryptement / chiffrement monoalphabétique

BAELXEJ JCKJ ZA JANBH HSXGXWXL XMXPJ LCEEA XK GCP JGCPH DPOH. FKXEL AOOA AKJ JAGNPEA O'SPHJCPGA LA NX'GKD OA HXMAJPAG, AOOA HA OAMX, YXPHX OA HCO LAMXEJ OA HCKMAGXPE AJ OKP LPJ : « IGXEL GCP, LABKPH NPOOA AJ KEA EKPJH RA J'XP GXZCEJA OAH GAZPJH LA O'XEZPAE JANBH AJ OAH OAIAELAH LAH GCPH BXHHAH. BKPH-RA NA BAGNAJJGA LA HCOOPZPJAG KEA DXMAKG LA MCJGA NXRAHJA ? »

ABPOCIKA-ZCEJAH LAH NPOOA AJ KEA EKPJH

Exemple de décryptement / chiffrement monoalphabétique

Lettre	Fréquence		Lettre	Fréquence	
	Occurrences	%		Occurrences	%
A	61	19,5	N	9	2,9
B	8	2,4	O	23	7,3
C	14	4,5	P	26	8,3
D	3	1,0	Q	0	0
E	19	6,1	R	3	1,0
F	1	0,3	S	2	0,6
G	18	5,7	T	0	0
H	28	8,9	U	0	0
I	3	1,0	V	0	0
J	28	8,9	W	1	0,3
K	16	5,1	X	20	6,4
L	15	4,8	Y	3	1,0
M	7	2,2	Z	6	1,9

Tableau 2 Analyse de fréquences du message codé

Exemple de décryptement / chiffrement monoalphabétique

les 3 lettres les plus fréquentes : A, H ou J

a, e ou i

Occurrences avant ou après les autres lettres de l'alphabet

	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	0	4	0	0	8	0	8	10	0	12	3	9	5	4	13	2	0	3	0	0	0	0	0	0	0	1
H	8	2	3	0	0	0	0	1	0	5	0	0	0	0	1	5	0	0	1	0	0	0	0	3	0	0
J	13	0	3	0	4	0	3	5	0	1	2	0	0	0	0	7	0	0	0	0	0	0	0	0	0	0

	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	0	4	0	0	8	0	8	10	0	12	3	9	5	4	13	2	0	3	0	0	0	0	0	0	0	1
H	8	2	3	0	0	0	0	1	0	5	0	0	0	0	1	5	0	0	1	0	0	0	0	3	0	0
J	13	0	3	0	4	0	3	5	0	1	2	0	0	0	0	7	0	0	0	0	0	0	0	0	0	0

- A intervient avec la moitié des lettres

  Sans doute : e
- 13 fois à côté du O et dans des mots courts
- OA
- AOOA
- OAH

  Sans doute « l » pour O et « s » pour H

	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	0	4	0	0	8	0	8	10	0	12	3	9	5	4	13	2	0	3	0	0	0	0	0	0	0	1
H	8	2	3	0	0	0	0	1	0	5	0	0	0	0	1	5	0	0	1	0	0	0	0	3	0	0
J	13	0	3	0	4	0	3	5	0	1	2	0	0	0	0	7	0	0	0	0	0	0	0	0	0	0

- J intervient 13 fois à côté de A
- en particulier AJ : 4 fois : « en » ou « et »
- 1er mot : BAELXEJ, 2ème mot : JCKJ
- J plutôt « t »

BeELXEt tCKt Ze teNBs sSXGXWXL XMXPt LCEEe XK GCP tGCPs DPls. FKXEL elle eKt teGNPEe l'SPstCPGe Le NX'GKD le sXMetPeG elle se leMX, YXPsX le sCl LeMXEt le sCKMeGXPE et lKP LPt.

BeELXEt tCKt Ze teNBs sSXGXWXL XMXPt LCEEe XK GCP tGCPs DPls. FKXEL elle eKt teGNPEe l'SPstCPGe Le NX'GKD le sXMetPeG elle se leMX, YXPsX le sCl LeMXEt le sCKMeGXPE et lKP LPt.

- C est sans doute une voyelle : tCKt, sCl
- Sans doute « o »
- K est sans doute un « u » : tCKt, elle eKt

: « IGXEL GoP, LeBuPs NPlle et uEe EuPts Re t'XP GXZoEte les GeZPts Le l'XEZPeE teNBs et les leIeELes Les GoPs BXsses. BuPs-Re Ne BeGNettGe Le sollPZPteG uEe DXMeuG Le MotGe NXReste ? »

: « IGXEL GoP, LeBuPs NPlle et uEe EuPts Re t'XP GXZoEte les GeZPts Le l'XEZPeE teNBs et les leIeELes Les GoPs BXsses. BuPs-Re Ne BeGNettGe Le sollPZPteG uEe DXMeuG Le MotGe NXReste ? »

- Re t'XP : sans doute un verbe, et R est « j »
- Sans doute « je t'ai ». P est « i »
- Nplle devient Nille
- EuPts devient Euits
- Sans doute N est « m » et E est « n »

  mille et une nuits
- eBiloIue Zontes des mille et une nuits
- Z est « c », B est « p », I est « g »

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	X	–	Z	–	A	–	I	S	P	R	–	O	N	E	C	B	–	–	H	J	K	–	–	–	–	–

- Au début : sans doute XYZ
- A la fin : suite HJK
- Sans doute un mot-clé entre « d » et « o »
- Le début du texte est devenu :

  « penLant tout ce temps, sSaGaWaL aMait Lonne au Goi tGois Dils »
- L est « d », M est « v », G est « r », D est « f »
- « sSaraWad » sans doute « sharazad »

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

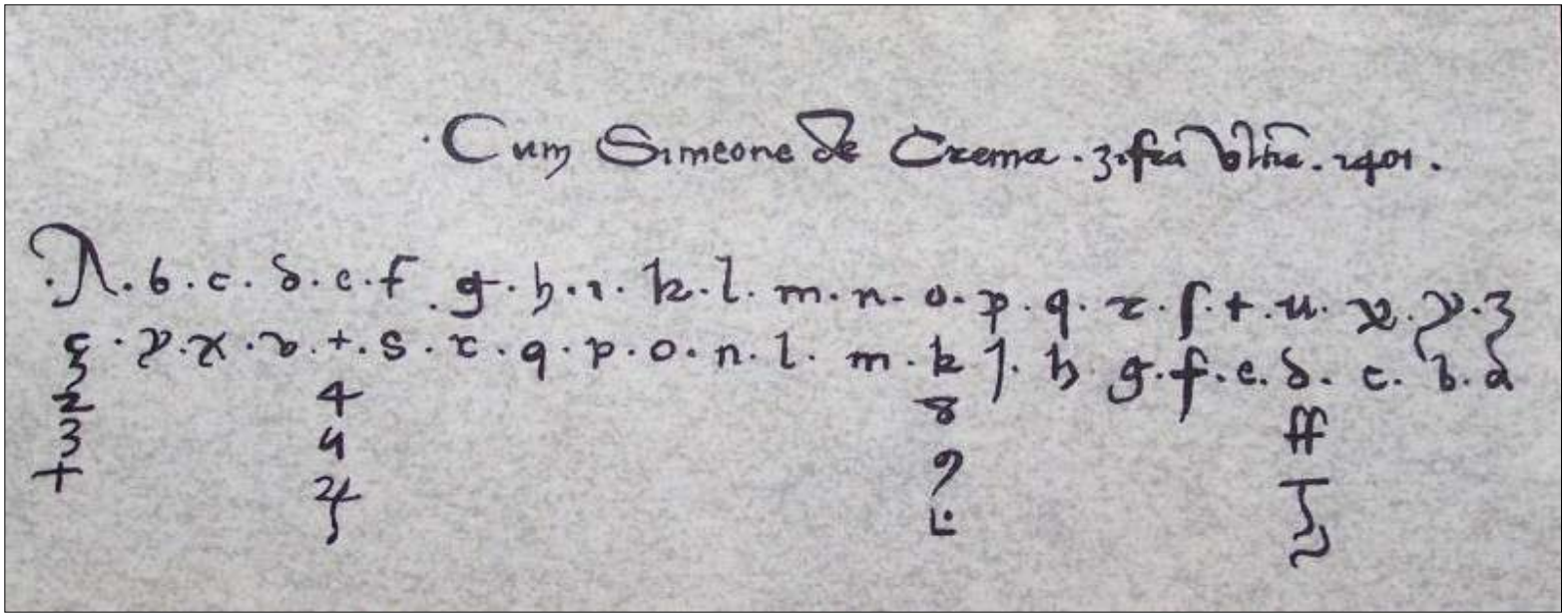
- Mot-clé : **La disparition Perec**. D'où le texte :

Pendant tout ce temps Sharazad avait donné au roi trois fils. Quand elle eut terminé l'histoire de Ma'ruf le savetier, elle se leva, baisa le sol devant le souverain, et lui dit : « Grand roi, depuis mille et une nuits je t'ai raconté les récits de l'ancien temps et les légendes des rois passés. Puis-je me permettre de solliciter une faveur de votre Majesté ? »

Epilogue Contes des mille et une nuits

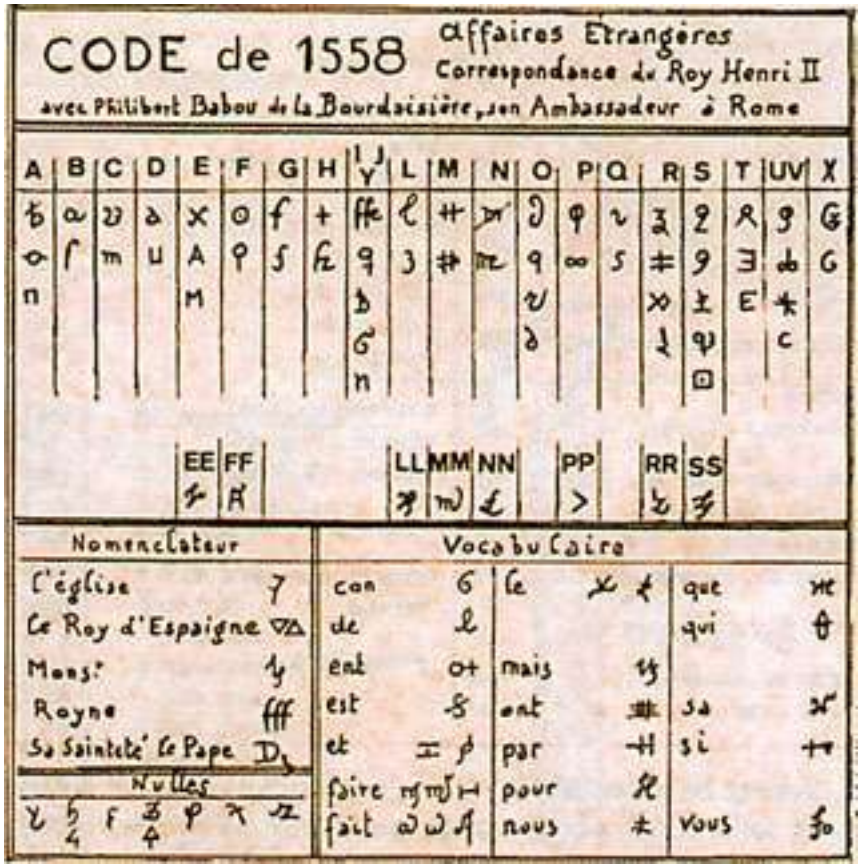
Comment résister à l'analyse des fréquences ?

- Chiffrement sans espace
- Chiffrement des lettres fréquentes par plusieurs lettres, ou avec des alphabets différents : **chiffrement homophone**



Nomenclateurs

- 1372 : Gabriel de Lavinde
  service du pape Clément VII
- 1558 : Philibert Babou
  service de François Ier
- Thomas Phelippes
  service de Walsingham
  cour d'Elizabeth I
- Antoine Rossignol (1600-82)
  le « Grand Chiffre du Roy »
  Louis XIV



Dans le secret des cours royales

Cabinets noirs et secrétaires-chiffreurs

Véritables « services du chiffre »

- La Curie Romaine : Gabriel Lavinde, 14e s.
- François I, Philibert Babou (1500-1569)
- Henri IV, *François Viète (1540-1603)*
- Louis XIII et Louis XIV, Antoine Rossignol (1600-82) : **Cabinet Noir**, ***Gd Chiffre de Louis XIV*** (par des nombres)
- Londres : *John Wallis (1616-1703)*
- Vienne : ***Geheim Kabinets Kanzlei***

Le chiffrement polyalphabétique

- Leon Battista Alberti (1404-1472), architecte, poète
  secrétaire à la chancellerie du Pape
  1466-67 : *De Componendis Cyphris* : **Le disque d'Alberti**
- Jean Trithème (1462-1516), prêtre allemand
  1518 : *Polygraphiae libri sex* : **La « tabula recta »**
  changement à chaque lettre
- 1553, Giovanni Battista Belaso (1505-?), chiffreur/cardinal
  + mot-clé, ou « mot de passe »
- 1563, Giovanni Battista della Porta (1535-1615)
  De Furtivis Literarum Notis : synthèse : table
- Girolamo Cardano (1501-76) : l'autoclé ou autoclave : « clair »

Le cadran d'Alberti
Leon Battista Alberti (1404-1472)

- Disque extérieur fixe

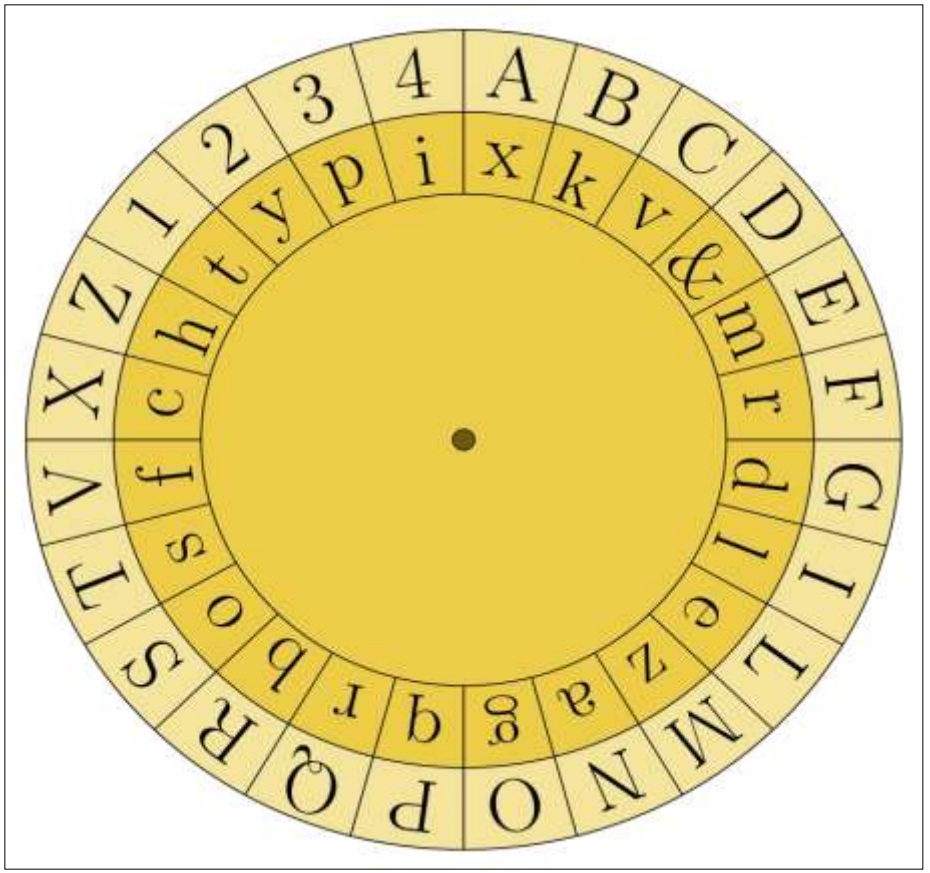
  20 lettres

  Pas de H, K, Y, J, U, W

  1, 2, 3, 4
- Disque mobile

  ordre incohérent

  23 lettres + « & »



- Accord sur une lettre indice : « k »
- Cryptogramme : « B », « D », « N »

La « tabula recta » de Jean Trithème (1462-1516)

- **a b c d e f g h i k l m n o p q r s t u x y z w**
- **b c d e f g h i k l m n o p q r s t u x y z w a**
- **c d e f g h i k l m n o p q r s t u x y z w a b**
- **d e f g h i k l m n o p q r s t u x y z w a b c**
- **e f g h i k l m n o p q r s t u x y z w a b c d**
- **f g h i k l m n o p q r s t u x y z w a b c d e**
- **g h i k l m n o p q r s t u x y z w a b c d e f**
- **h i k l m n o p q r s t u x y z w a b c d e f g**
- **i k l m n o p q r s t u x y z w a b c d e f g h**
- **k l m n o p q r s t u x y z w a b c d e f g h i**
- **l m n o p q r s t u x y z w a b c d e f g h i k**
- **m n o p q r s t u x y z w a b c d e f g h i k l**
- **n o p q r s t u x y z w a b c d e f g h i k l m**
- **o p q r s t u x y z w a b c d e f g h i k l m n**
- **p q r s t u x y z w a b c d e f g h i k l m n o**
- **q r s t u x y z w a b c d e f g h i k l m n o p**
- **r s t u x y z w a b c d e f g h i k l m n o p q**
- **s t u x y z w a b c d e f g h i k l m n o p q r**
- **t u x y z w a b c d e f g h i k l m n o p q r s**
- **u x y z w a b c d e f g h i k l m n o p q r s t**
- **x y z w a b c d e f g h i k l m n o p q r s t u**
- **y z w a b c d e f g h i k l m n o p q r s t u x**
- **z w a b c d e f g h i k l m n o p q r s t u x y**
- **w a b c d e f g h i k l m n o p q r s t u x y z**

Le « mot-clé » de G. B. Belaso (1505-?)

- Chiffrement à partir d'un mot facilement mémorisable

  Le « contresigne »
- On écrit le mot-clé sous le message et on le répète
- Chaque lettre du mot-clé indique l'alphabet grâce auquel la lettre correspondante du message clair sera chiffrée

l e s v a c a n c e s c o m m e n c e n t c e s o i r

b l e u b l e u b l e u b l e u b l e u b l e u b l e

La synthèse de G. B. della Porta (1535-1615)

- Transposition-Substitution
- Réflexion sur la clé

L'autoclave de Girolamo Cardano (1501-1562)

médecin, algébriste

- Le mot-clé n'est autre que le message clair lui-même, en commençant par le premier mot du message clair.

Blaise de Vigenère

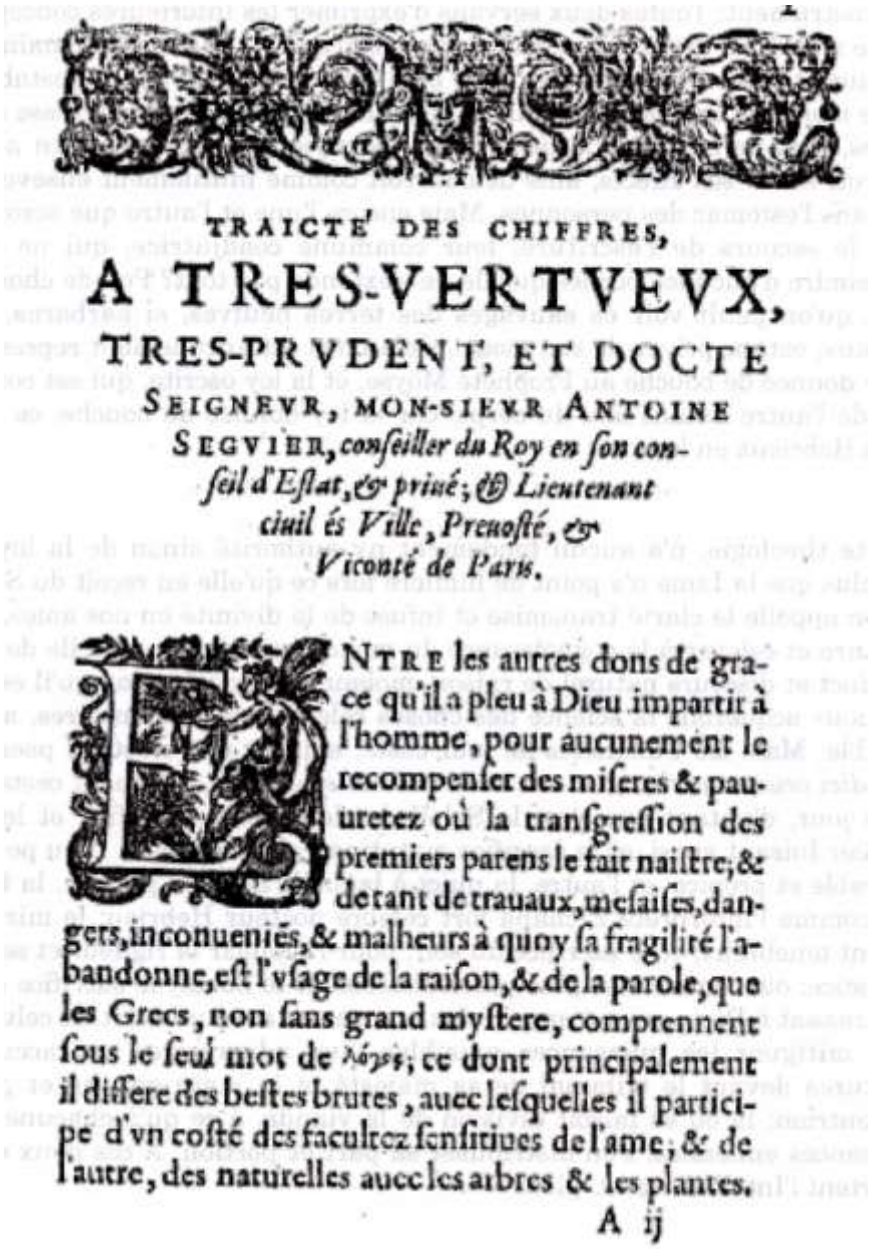
(1523-1596)

diplomate français

secrétaire de Charles IX

1586

Le Traicté des Chiffres



TRAICTE' DES CHIFFRES,

A TRES-VERTVEVX,

TRES-PRVDENT, ET DOCTE

SEIGNEVR, MON-SIEVR ANTOINE

SEGVIER, *conſeiller du Roy en ſon conſeil d'Eſtat, & priué; & Lieutenant ciuil és Ville, Preuoſté, & Viconté de Paris.*

ENTRE les autres dons de grace qu'il a pleu à Dieu impartir à l'homme, pour aucunement le recompenſer des miſeres & pauuretez où la tranſgreſſion des premiers parens le fait naiſtre; & de tant de trauaux, meſaiſes, dangers, inconueniẽs, & malheurs à quoy ſa fragilité l'abandonne, eſt l'vſage de la raiſon, & de la parole, que les Grecs, non ſans grand myſtere, comprennent ſous le ſeul mot de λόγος; ce dont principalement il differe des beſtes brutes, auec leſquelles il participe d'vn coſté des facultez ſenſitiues de l'ame; & de l'autre, des naturelles auec les arbres & les plantes.

A ij

La Renaissance : interrogations sur le langage

- Transition entre l'ancien Monde et le 17ème siècle : comment lire le Nouveau Monde ?
- Tous les « codes » se trouvent réinterrogés
- La Cabale : idée que la Bible est un langage codé qu'il faut déchiffrer
- L'alchimie : importance des rituels
- Puissance des codes : quiconque maîtrise les signes est aussi censé maîtriser la nature
- Manipulation combinatoire des textes
- Marin Mersenne (1588-1648) : prise de distance

  Problèmes de combinatoire

  –

1586 *Le Traicté des Chiffres*
Laïcisation du chiffrement

« L'escriture au surplus est double ; la commune dont on use ordinairement ; et l'occulte secrète, qu'on desguise d'infinies sortes, chacun selon sa fantasie, **pour ne la rendre intelligible qu'entre soy et ses consçachans**. Ce sont les chiffres, comme on les appelle d'un mot corrompu, aujourd'huy non appropriez à autres effects que pour les affaires du monde, et les negociations et practiques, aussi bien des particuliers que des Princes ; là où anciennement les Hebrieux, Chaldees, Egyptiens, Ethiopiens, Indiens, ne s'en servaient que pour voiler les sacrés secrets de leur Théologie, et Philosophie; …. Afin de les **garantir et substraire du prophanement de la multitude**, et en laisser la cognoissance aux gens dignes ; …..

1586 *Le Traicté des Chiffres :* Le carré de Vigenère

Clair : *Au nom de l'eternel soit mon commencement,*
Qui est de tout principe, et parachevement.

Clé : *Le jour obscur; & la nuict claire*

« Cherchez en la colonne des capitales, la lettre *L,* qui est la première de nostre clef, et voyez quelle lettre respond en son alphabet à celle de A, la première aussi du sujet; ce sera *S.* Poursuivez ainsi de lettre en lettre tant que la clef se pourra estendre; Puis estant au bout vous la réitererez de nouveau ……

Vigenère et l'étude des permutations

- Une lettre ne se peut transposer; deux se varient de deux sortes, *a b,* et *b a:* trois de six: quatre de 24. cinq de 120. six de 720. sept de 5040. multipliant tousjours le nombre dernier resulte, par celuy des lettres qui succede apres; comme deux par trois pour trois lettres, et ce seront six: six par quatre que produiront 24. pour quatre: Ces 24. par cinq, 120. pour cinq: cestuy-cy par six, pour les six 720.

Folio 190r-190v

Vigenère et les permutations

- 1 1 folio 191
- 2 2
- 3 6
- 4 24
- 5 120
- 6 720
- 7 5040
- 8 40320
- …….
- 22 1123684719777607680000

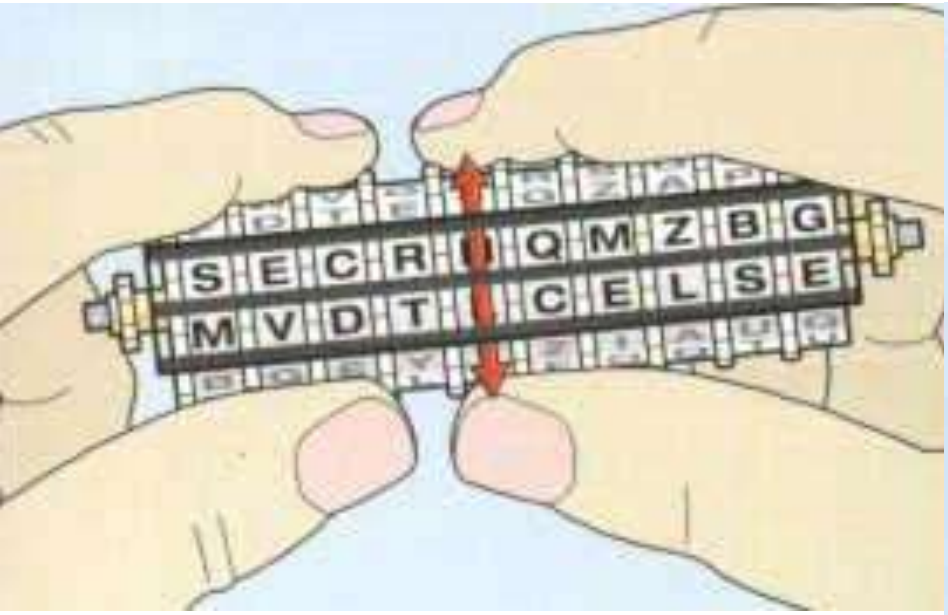
Mais la méthode de Vigenère ne s'impose pas

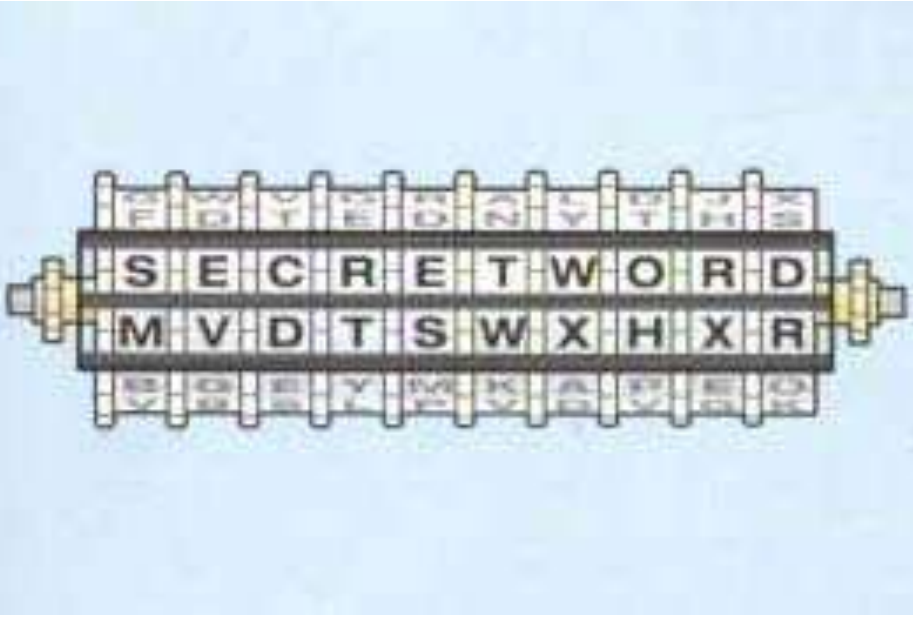
- Longueur et pénibilité du chiffrement
- Méthode complexe : erreurs fatales
- Matérialité des nomenclateurs
- • La mécanisation lui procurera davantage de possibilités d'être utilisée

Le cylindre de Jefferson (1800)

- Thomas Jefferson (1743-1826), secrétaire d'Etat de George Washington, futur président
- • réinventé par Bazeries en 1891 et par le colonel italien Durcos en 1900. Variante du colonel O. Mauborgne aus Etats-Unis entre 1922 et 1942

Le cylindre de Jefferson





Le décryptement du chiffre de Vigenère

- Charles Babbage (1791-1871)

  Casse le code de Vigenère en 1846

  Expert dans un procès 1854

  Journal for the Society of Arts, 1854

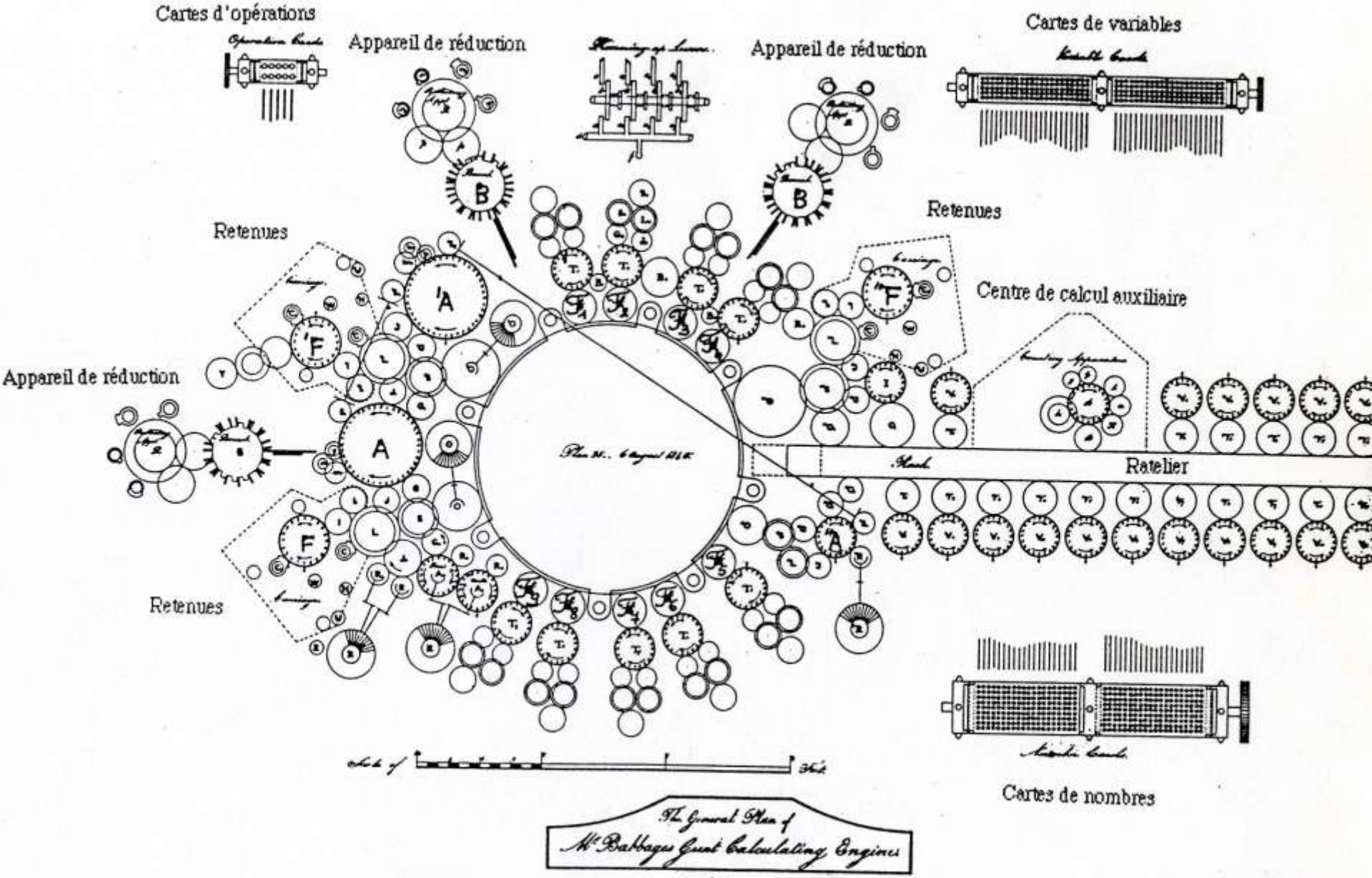
Mss *Philosophy of Deciphering* non publié

- 1863, Friedrich Wilhelm Kasiski (1805-1881)

  Die Geheimschriften und die Dechiffrierkunst
  (l'écriture secrète et l'art du déchiffrement)

Basculement de la situation mi-19ème s.

- Charles Babbage (1791-1871)
  - il casse le chiffre de Vigenère (1586)
- Mathématicien, « gentleman-amateur »
  - La connaissance des codes secrets fait partie de l'éducation des personnes cultivées
  - « agony columns », *The Times*
- Il comprend après coup la relation mathématique entre :
  - l'activité de cryptanalyse
  - le travail de C. Gauss (1777-1855) sur les congruences : *Disquisitiones Arithmeticae* 1801



Machine analytique : Plan général. Science Museum Library, London.

Charles Babbage (1791-1871)

- Manuscrit

The Philosophy of Analysis

British Library, Add. Mss. 37202

- Manuscrit

The Philosophy of Decyphering

Activité constante en cryptologie de 1830 à 1870

British Library, Add. Mss. 37205

Guerre de Crimée (1853-1856) : Sébastopol

France, GB, Emp. Ottoman / Russie

Mac Mahon / Malakoff

Relations persistantes Babbage / Beaufort (Amirauté)

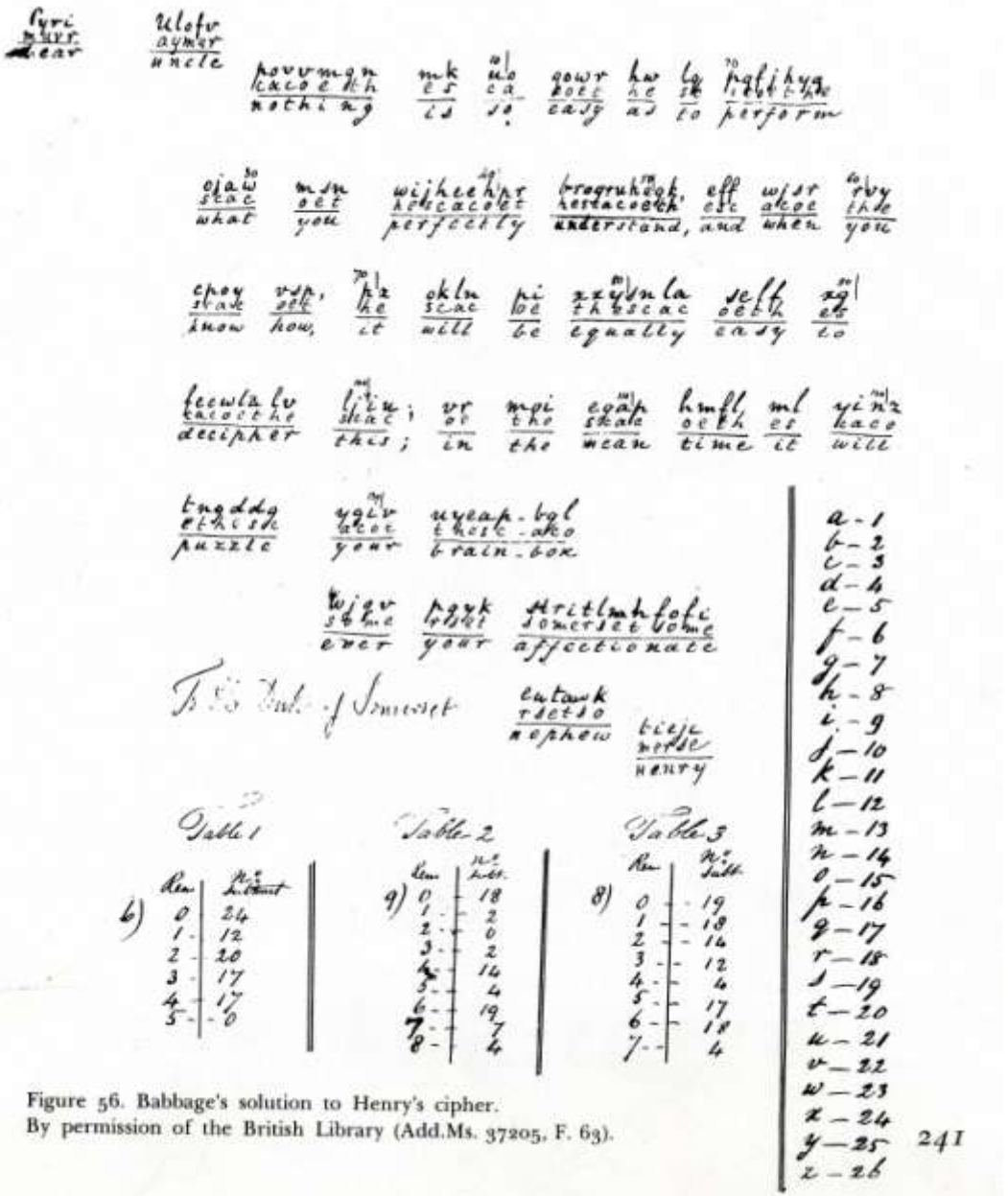


Figure 56. Babbage's solution to Henry's cipher.
By permission of the British Library (Add.Ms. 37205, F. 63).

PYRI ULOFV POVVMGN MK UD GOWR HW LQ PGFJHYQ
murr aymur cacoe th es ca coet h e s c acoethe
dear uncle nothing is so easy as to perform

QJAV MSN WIJHEEHPR BRVGRUHEGK, EFF WJSR RVY
scac oet hescacoet hescacoe th esc acoe the
what you perfectly understand and when you

CPOY VSP, PX OKLN PI XXYSNLA SELF XG
scac oe t he scac oe thescac oeth es
know how it will be equally easy to

FEEWTALV LJIU, VR MOI EGAP HMFL ML YINZ
cacoe the scac oe the scac oeth es caco
decipher this in the mean time it will

TNGDDG YQIV UYEAP – BQL

e t h e sc a c o e t h e s c a c o

p u z z l e y o u r b r a i n b o x

WJQV PGYK ST R IT LMHGOF I

s o m e r s e t s o m e r s e t s o m e

e v e r y o u r a f f e c t i o n a t e

EWTAWK TIEJC

r s e t s o me rse

n e p h e w hen ry

Le travail de Babbage
Lettres repérées par leur rang dans l'alphabet

- **Bl : Add. Mss 37 205 f 58-59 : 24 fév. 1846.**

mot-clé : SOMERSET.

19	20	18	9	20	12	13	8
S	T	R	I	T	L	M	H
S	O	M	E	R	S	E	T
19	15	13	5	18	19	5	20
A	F	F	E	C	T	I	O
1	6	6	5	3	20	9	15

Le travail de Babbage / congruences

- **Bl : Add. Mss 37 205 f 58-59 : 24 fév. 1846.**

  mot-clé : SOMERSET.

  - Cypher = Key + Translation + 1
  - Translation = Cypher – Key + 1

  - Chiffré = Clé + Clair + 1
  - Clair = Chiffré – Clé + 1

Basculement de la situation mi-19ème s

- Frederich Kasiski (1805-1881)
  - Il casse le chiffre de Vigenère
- Officier d'infanterie de l'armée de Prusse, cryptologue et archéologue. Retraite 1852.
- 1863 : *Die Geheiùschriften und die Dechiffrir Kunst*, Berlin [L'écriture secrète et l'art du déchiffrement]
- Sa méthode [« test de Kasiski »]

  – analyser les écarts entre des séquences redondantes dans le texte chiffré

  – donne des indications sur la longueur de la clé

La méthode de Kasiski

XAUNMEESYUEDTLLFGSNBWQUFXPQTYO
RUTYIIN**UMQI**EULSMFAFXGUTYBXXAGB
HMIFIIM**UMQI**DEKRIFRIRZQUHIENOO**OIG**
RMLYETYOVQRYSIXEOKIYPY**OIGR**MLYE
TYOVQRYSIXEOKIYPY**OIGR**FBWPIYRBQ
URJIYEMJ**IGRY**KXYACPPQSPBVESIRZQR
UFREDYJ**IGRY**KXBLOPJARNPUGEFBWMI
LXMZSMZYXPNBPUMYZMEEFBUGENLRD
EPBJXONQEZTMBWOEFIIPAHPPQBFLGDE
MFWFAHQ

Régularités repérées : UMQI, OIGR, IGRY

La périodicité de ces régularités observées estun multiple de la longueur de la clé

Séquence	Distance	Longueur possible de la clé												
		2	3	4	5	6	7	8	9	10	11	12	13	14	15
UMQI	30	x	x		x	x				x					x
OIGR	25				x										
IGRY	30	x	x		x	x				x					x

Si la longueur de la clé est 5, on relève le nombre d'occurrences des lettres 1, 6, 11, … du message

- Elles sont chiffrées avec la même 1ère lettre de la clé : on se ramène à un chiffrement monoalphabétique

- A B C D E F G H **I** J K L M N O P Q R S T….

  0 1 0 0 4 1 2 1 **13** 2 0 0 3 0 0 4 0 3 0 0 …..

- Comparaison avec la fréquence des lettres dans l'aphabet ordinaire : **I** correspond sans doute à « e »

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

A a b c d e f g h i j k l m n o p q r s t u v w x y z

B b c d e f g h i j k l m n o p q r s t u v w x y z a

C c d e f g h i j k l m n o p q r s t u v w x y z a b

D d e f g h i j k l m n o p q r s t u v w x y z a b c

E e f g h i j k l m n o p q r s t u v w x y z a b c d

F f g h i j k l m n o p q r s t u v w x y z a b c d e

G g h i j k l m n o p q r s t u v w x y z a b c d e f

H h i j k l m n o p q r s t u v w x y z a b c d e f g

I i j k l m n o p q r s t u v w x y z a b c d e f g h

J j k l m n o p q r s t u v w x y z a b c d e f g h i

K k l m n o p q r s t u v w x y z a b c d e f g h i j

L l m n o p q r s t u v w x y z a b c d e f g h i j k

La méthode de Kasiski sfin)

- La 1ère lettre de la clé est donc « e »

Même méthode avec des « sous-messages »

- On relève le nombre d'occurrences des lettres 2, 7, 12, … du message pour déterminer la 2ème lettre de la clé.
- On relève le nombre d'occurrences des lettres 3, 8, 13, … du message pour déterminer la 3ème lettre de la clé.
- On relève le nombre d'occurrences des lettres 4, 9, 14, … du message pour déterminer la 4ème lettre de la clé.
- On relève le nombre d'occurrences des lettres 5, 10, 15, … du message pour déterminer la 5ème lettre de la clé.

Mathématisation du chiffrement polyalphabétique

Lester Sanders HILL (1890-1961)

- •Hill, Lester S.., 1929, « Cryptography in an Algebraic Alphabet », *American Mathematical Monthly,* vol 36, 1929, pp. 306-312.

- • Hill, Lester S.., 1931, « Concerning Certain Linear Transformations Apparatus of Cryptography », *American Mathematical Monthly,* vol 38, 1931, pp. 135-154.

Mathématisation du chiffrement polyalphabétique

Lester Sanders HILL (1890-1961)

- Mathématicien Etats-Unis
- 1945-46 : membre de la Faculté de l'US Army University à Biarritz (+ Florence + Shrivenham GB)
- Il fait une lecture numérique du chiffrement polyalphabétique, qui permet de définir des « opérations » de chiffrement

Mathématisation du chiffrement polyalphabétique

Lester Sanders HILL (1890-1961)

Vocabulaire de la théorie des groupes

- Permutation des lettres de l'alphabet anglais
- A chaque lettre de cette permutation, on associe un entier.
- On définit l'addition et la multiplication comme opérations modulaires (mod. 26) sur cet alphabet.
- Le résultat de chaque opération est le reste dans la division par 26.

Le travail de Babbage en calcul modulaire

mot-clé : SOMERSET.

	18	19	17	8	19	11	12	7
•	S	T	R	I	T	L	M	H
	S	O	M	E	R	S	E	T
	18	14	12	4	17	18	4	19
•	A	F	F	E	C	T	I	O
	0	5	5	4	2	19	8	14

Exemples de calcul modulaire

- Le calcul de l'heure en 12 ou 24 heures

- Le calcul en 0 et 1

+	0	1
0	0	1
1	1	0

x	0	1
0	0	0
1	0	1

Basculement : mathématisation et mécanisation

- Une activité liée à l'analyse de la langue écrite :
  - Importance de la laïcisation du texte
- Caractère artisanal et fastidieux du travail

- Evolution / tension constante entre cryptographie et cryptanalyse

- La cryptanalyse a besoin de méthodes :
  - Analyse des fréquences
  - Mots probables

La « thèse » de David Kahn sur les relations entre cryptologie et guerre

- David Kahn, *The Codebreakers, the Story of Secret Writing*. New York. McMillan Pub. Versn abrégée en 1973. London. Sphere Books.
- *La guerre des codes secrets,* Interéditions, 1980.
  - Version expurgée : cryptologie arme de guerre

- Militaires victorieux convaincus de la puissance de leurs services de cryptologie
- Les efforts et les progrès de la cryptologie tendent à venir des puissances vaincues.

Sections de cryptologie créées après des défaites en Europe

- Russie après la guerre de Crimée
- France après la défaite de 1870
- Grande-Bretagne / Inde, menacée par le canal de Suez (France) et la Russie.

- *A contrario,* USA et Allemagne

- Mais la guerre continue de se gagner sur le champ de bataille : cryptologues déconsidérés

Importance de la cryptologie en France

- Jean-Guillaume-Hubert-Victor-François-Alexandre-**Auguste Kerckhoffs** von Nieuwenhof (1835-1901)
  - 1883, *Journal des Sciences Militaires*
- Marquis Gaëtan Henri Viarizio di Lesegno **De Viaris** (1847-1901). EP. Marine.
  - 1888, *Le Génie Civil,* 4 articles
- Paul Louis Eugène Valério
  - 1892-95, 10 arts, *Journal des Scs Militaires* + livre
- Félix-Marie Delastelle (1840-1902). Marine.
  - 1902, *Traité élémentaire de cryptographie*.

Jean-Guillaume-Hubert-Victor-François-Alexandre-Auguste Kerckhoffs von Nieuwenhof (1835-1901)

LOIS DE KERCKHOFFS

Exemple de présentation rétro-historique :

- 1. La sécurité doit reposer sur le secret de la clef et non sur le secret de l'**algorithme**.
- 2. Le déchiffrement sans la clef doit être impossible dans un temps raisonnable.
- 3. Trouver la clef à partir du texte clair et du texte chiffré doit être impossible.
- Par conséquent, toute attaque doit être envisagée en supposant que l'attaquant connaît tous les détails du cryptosystème.

Jean-Guillaume-Hubert-Victor-François-Alexandre-Auguste Kerckhoffs von Nieuwenhof (1835-1901)

- Origine : grande famille flamande (Limbourg)
- Formation littéraire et scientifique
- Grande-Bretagne, Allemagne, France
- Chaire de langues modernes à l'école supérieure de Melun
- Il connaît des difficultés politiques après 1870
- 1873-76 : thèse, Bonn, Tübingen
- 1878 : n'obtient pas la chaire d'allemand à l'EMS
- professeur d'allemand à l'Ecole des Htes Etudes Commerciales et à l'Ecole Arago, Paris.
- 1883 : **« La cryptographie militaire »**
- 1885-91 : propagandiste du **Volapuk (**J. M. Schleyer)

Kerckhoffs ***La Cryptographie Militaire***
Journal des sciences militaires **janv. et fév. 1883**

- DESIDERATA DE LA CRYPTOGRAPHIE MILITAIRE

1. Le **SYSTEME** doit être matériellement, sinon mathématiquement, indéchiffrable
2. Il faut qu'il n'exige pas le secret, et qu'il puisse sans inconvénient tomber entre les mains de l'ennemi
3. La clef doit pouvoir en être communiquée et retenue sans le secours de notes écrites, et être changée ou modifiée au gré des correspondants
4. **Il faut qu'il soit applicable à la correspondance télégraphique,**
5. Il faut qu'il soit portatif, et que son maniement ou son fonctionnement n'exige pas le concours de plusieurs personnes
6. Enfin, il est nécessaire, vu les circonstances qui en commandent l'application, que le système soit d'un usage facile, ne demandant ni tension d'esprit, ni la connaissance d'une longue série de règles à observer.

Les enjeux auxquels Kerckhoffs cherche à faire face

- « Il faut bien distinguer entre un système d'écriture chiffrée, imaginée pour un échange momentané de lettres entre quelques personnes isolées, et **une méthode de cryptographie destinée à régler pour un temps illimité la correspondance des différents chefs d'armée entre eux**. Ceux-ci, en effet, ne peuvent, à leur gré, et à un moment donné, modifier leurs conventions ; de plus, ils ne doivent jamais garder sur eux aucun objet ou écrit qui soit de nature à éclairer l'ennemi sur le sens des dépêches secrètes qui pourraient tomber entre ses mains »

(I. p. 12).

Compatibilité avec la multiplicité des intervenants

« Nos meilleurs généraux sont bien d'avis, aujourd'hui, qu'il est indispensable que les différents commandants d'une armée aient à leur disposition **un système de communications secrètes pour correspondre librement**, non seulement entre eux et avec leur commandant en chef, mais encore avec leurs lieutenants ; […..]

il faudrait pourvoir d'un chiffre en temps de paix comme en temps de guerre, les généraux, les chefs de régiment ou de service, tous les commandants de colonne et de poste…. Et y exercer nos officiers même en temps de paix ». p. 9

Compatibilité avec l'enseignement dans les écoles militaires

« L'Administration doit absolument renoncer aux méthodes secrètes, et établir en principe qu'elle n'acceptera qu'un procédé qui puisse être **enseigné au grand jour dans nos écoles militaires**, que nos élèves seront libres de communiquer à qui leur plaira, et que nos voisins pourront même copier et adopter, si cela leur convient. Je dirai plus : ce ne sera que lorsque nos officiers auront étudié les principes de la cryptographie et appris l'art de déchiffrer, qu'ils seront en état d'**éviter les nombreuses bévues qui compromettent la clef des meilleurs chiffres**, et auxquelles sont nécessairement exposés tous les profanes ».

(I, 14-15).

La Première Guerre Mondiale

- De la commission à la section du chiffre

  Commission 1888, section 1902, officielle 1912

  Marcel Givierge (1871-1931) EP

  Georges-Jean Painvin (1886-1980) EP
- **Le télégramme Zimmermann 1917**

  Entrée en guerre des Etats-Unis
- **Le radiogramme de la victoire 1918**

  ADFGVX décrypté par G.-J. Painvin

  2-3 juin 1918 : offensive allemande annoncée pour le 10

Chiffrement : de ADFGX à ADFGVX

- ADFGX : offensive de mars 1918
- ADFGVX ou GEDEFU 18 (GEheimschrift DEr FUnker 18, chiffre des télégraphistes 18)
- Transfert en code Morse : lettres très différentes

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

Chiffrement ADFGVX

- RENFORT COMPIEGNE 16H10
- DFAXV VFAFD DFGFD DFDFG VAGDA XGGVV AXXAV FDVXA DX
- Clé pour transposition : DEMAIN

D	E	M	A	I	N	
D	F	A	X	V	V	
F	A	F	D	D	F	
G	F	D	D	F	G	
V	A	G	D	A	X	etc

Chiffrement ADFGVX

A	D	E	I	M	N	
X	D	F	V	A	V	
D	F	A	D	F	F	
D	G	F	F	D	G	
D	V	A	A	G	X	etc

Message transmis :

XDFVA VDFAD FFDGF FDGDV AAGXV
GGAVX FXADV VXXAD

1 juin : 3 télégrammes, même heure, ~même lgueur

Décryptés le 3 juin, permettent la contre-attaque

La Seconde Guerre Mondiale
Cryptologie et mécanisation

- Bletchley Park (au nord de Londres)

  GCCS : *Government Code and Cypher School*

  Golf Club and Chess Society

- Alan Turing (1912-1954) et la cryptanalyse
  - **Enigma** : machine à chiffrer allemande 1928
    - Cryptanalyse pour 3 rotors : théorie des groupes, 1931

      Marian Rejewski (1905-1980)

      Jezrzy Rozycki (1909-1942)

      Henryk Zygalski (1907-1978)
    - Machines électro-magnétiques : les « Bombes »

La machine Enigma

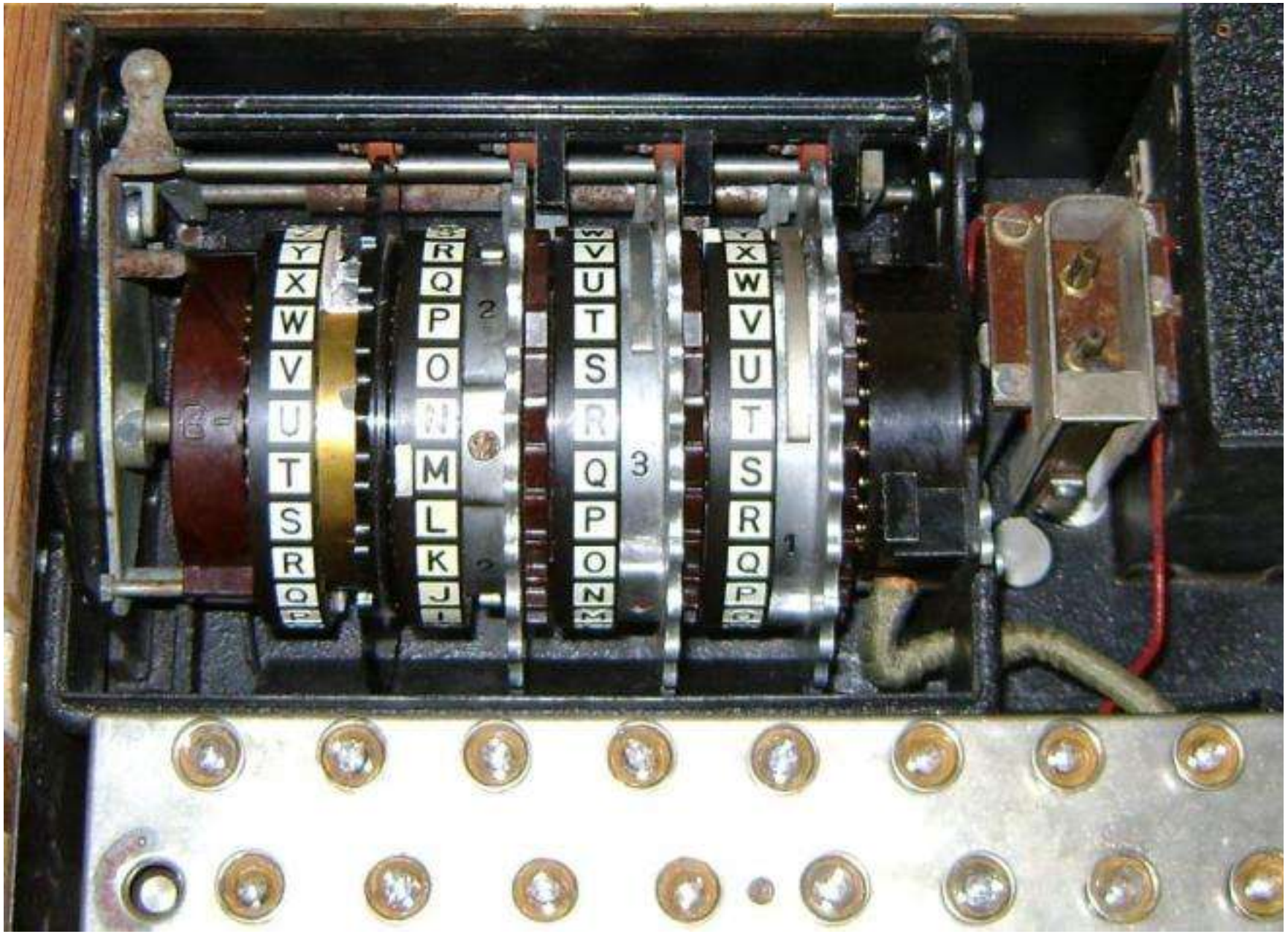
Réflecteur

3 rotors

Tableau de lampes : sortie

Clavier de lettres : entrée

Tableau de connexions


Y X W V U T S R Q
R Q P O N M L K J
2
W V U T S R Q P O N M
3
X W V U T S R Q P
1

Le chiffrement sur Enigma

- Les connexions échangent des paires de lettres
- Chaque rotor effectue une substitution
- L'ordre des rotors peut être changé : 3 ! = 6
- Le 1^{er} tourne d'un cran après le passage d'une lettre, le $2^{ème}$ quand le 1^{er} a fait un tour complet, etc. Soit : $26^3 = 17\,576$ possibilités
- Pour 3 rotors, 6x17 576 = 105 456 possibilités
- Réflecteur : échange de paires de lettres

Nombre de possibilités

- Pour 3 rotors, 6x17 576 = 105 456 possibilités
- Tableau de connexions de 10 fiches

  de l'ordre de 10^{15} possibilités

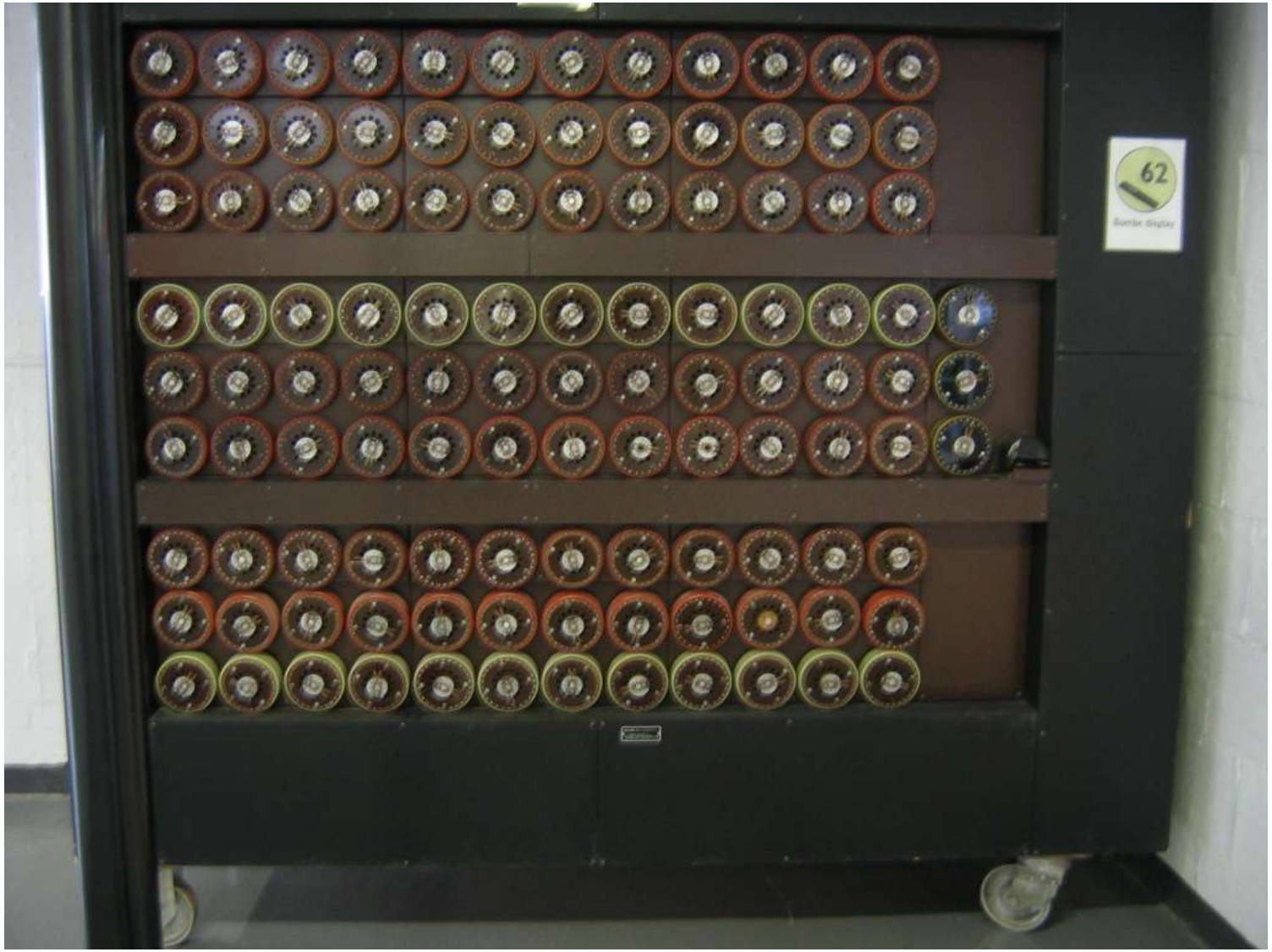
  1 507 382 749 377 250

$$C_{26}^{20} \times \prod_{i=0}^{9} C_{2(10-i)}^{2} \times \frac{1}{10!}$$

Déchiffrement sur Enigma

- Connaître la clé du jour
  - Elle est la même pour toute une armée
- Elle donne l'ordre et le choix des rotors
- Connaître la clé du message
  - Elle donne la position initiale des 3 rotors, et elle est transmise au début du message
- • **Mais ni imprimante, ni transmission automatique (M**orse).
- Déchiffrement : il suffit de taper le message chiffré dans la machine

Les « Bombes »



Les « Bombes »


be to
e is
o
Naval
rom
bes
ich
l Air
ell as
eal
S T U V W X
A B C D E F G
N O P Q R S
X Y Z A

Gilbert Vernam (1890-1960)

- Ingénieur chez AT&T, monopole régulé (1907)
- *American Telephone and Telegraph Company*,

Branche de *Bell Tel. Company* / longues distances

Importance mondiale / Western Electric Company

- Section Télégraphe (1915) du département Recherche et Développement
- Chargé de la sécurité des téléscripteurs « teletype » projet secret

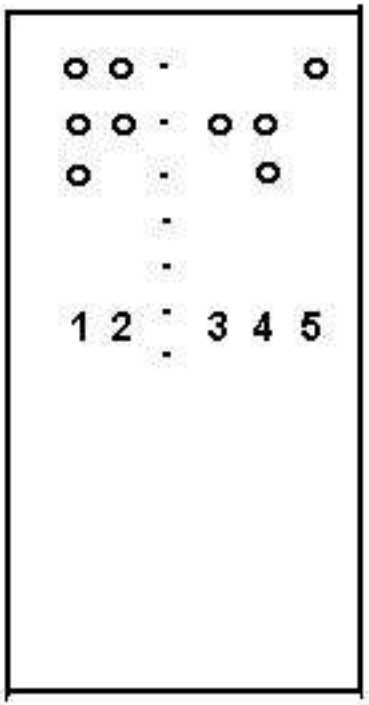
Le code Baudot : Morse / téléscripteurs
Emile Baudot (1845-1903)

- Mis au point en 1911 pour le « telex »
- « Code télégraphique »
- « Alphabet international (AI) n° 2 »
- « Code CCITT n° 2 »
- Code binaire matérialisé par une machine

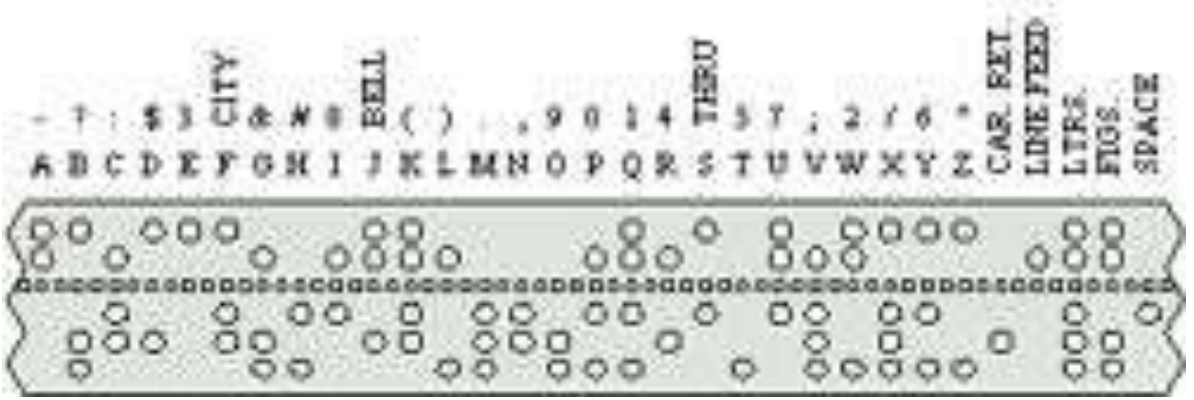
- Années 1960 : code ASCII

  American Standard Code for Information Interchange

Le code Baudot : Morse / téléscripteurs
Emile Baudot (1845-1903)



WKD



Le code Baudot : Morse / téléscripteurs
Emile Baudot (1845-1903)

- Dispositif électrique
- Impulsion : passage du courant
- 5 unités : 32 combinaisons.

  Lower Case & Upper Case
- Exemples :

  a marque marque espace espace espace

  i espace marque marque espace espace

La technique de chiffrement de Vernam

- Vernam double la bande : **message clair**

  par une autre bande : **clé**

formée de marques et espaces aléatoires

- La clé est aussi longue que le message

- Le chiffré transmis est obtenu par combinaison de ces deux bandes selon une certaine règle

La technique de chiffrement de Vernam

- marque / marque espace
- marque / espace marque
- espace / marque marque
- espace / espace espace

OPERATION ou CONNECTEUR « XOR »

1 + 1 = 0

0 + 1 = 1

1 + 0 =

Le déchiffrement est très simple

- Il suffit « d'ajouter » à nouveau la clé au chiffré
- pour obtenir le clair
- puisque 1 + 1 = 0 et 0 + 0 = 0
- Exemple :

Message clair	1	1	0	0	0
Clé	1	0	0	1	1
Chiffré	0	1	0	1	1
Clé	1	0	0	1	1
	1	1	0	0	1

Solidité et fragilité du chiffrement de Vernam

- Solidité et efficacité

  - automatisation du chiffrement et du déchiffrement
  - « one-time pad » ou « masque jetable » : incassable

    la méhode de Kasiski n'est plus possible

    absence de répétition si lgueur clé = lgueur clair

    absence de structure linguistique si clé aléatoire

    impossibilité même de l'analyse exhaustive

- Difficulté et fragilité

  - La production et la distribution des clés
  - et leur suppression

Exigence : ne pas chiffrer 2 fois avec la même clé

- Si on le fait, il suffira d'ajouter les deux chiffrés pour retrouver la somme des 2 clairs.
- En effet, la somme de 2 signes identiques donne 0.
- Et en ajoutant encore un des 2 chiffrés, on retrouve l'autre.
- Système inconditionnellement sûr : utilisé essentiellement dans les cas sensibles
- [téléphone rouge Moscou-Washington]

De la machine de Lorentz au Colossus
M.-H.-A. Newmann (1897-1984)

- Appareil Lorentz LZ ou Tunny
  mécanise le système de Vernam
- Colossus, construit 1943, opérationnel D-day
  10 en opération en 1945
- Code Beaudot
- Colossus détruit sur ordre de Churchill à la fin de la guerre
- Reconstruit à Bletchley Park en 1996

De la machine de Lorentz au Colossus

Claude Shannon (1916-2001) Ingénieur et mathématicien

- 1938, "A Symbolic Analysis of Relay and Swtiching Circuits", *Transactions of the American Institute of Electrical Engineering*, 57, 713-23.
- A parfaitement saisi l'approche symbolique de Boole (1854) et de Huntington (1933) en logique
- Xab = 0 : circuit fermé, Xab = 1 ; circuit ouvert
- + circuits en série, • circuits en parallèle
- **Shannon fournit un langage commun à l'ingénieur et au mathématicien**.

Shannon, 1949 (1946), « Communication Theory of Secrecy Systems »

- Système secret considéré comme ensemble de transformations d'un espace dans un autre, où le chiffrement effectue une opértn fctnelle.
- Si M est le message, et K la clé, si E est le message chiffré, ou cryptogramme,
- $E = f (M, K)$
- c-à-d. que E est fonction de M et de K.
- Ce qu'il préfère écrire :

  $E = T_i M$

  L'indice i correspond à la clé utilisée.
- Une transformation particulière correspond à un chiffrement avec une clé donnée.

Liens structurels avec l'informatique et avec la Défense

- **NSA :** ***National Security Agency***, 1952
  – *No Such Agency* : officielle 1957
  – **assurer la sécurité des communications** (et donc des ordinateurs) du **gouvernement** des USA
  – fournit ENIGMA aux Alliés pendant (x) décennies
  – ECHELON système mondial d'espionnage des communications privées et publiques

- IMB 701 à des fins militaires : Whirlwind et le programme SAGE
- IBM 702 à usage civil de gestion

La pression des milieux économiques

- Sécuriser les échanges commerciaux
- Organiser les relations entre public et privé
  - au plan collectif
  - Dans le code de transmission des messages
- Faire passer ces questions dans le domaine public c-à-d. abandon du secret défense

La question des standards et la distribution des clés

- Coursiers spécialisés des années 1970s
- Appel d'offres *National Bureau of Standards* 1973
  - algorithme public
  - Niveau de sécurité lié à la clé
- LUCIFER de Horst Feistel, 1973, IBM
- DES 1977 *Data Encryption Standard*
  - Niveau de sécurité lié à la clé : secrète
  - Algorithme public : Clair : 64 bits, découpé en 2 blocs, G et D, et un des blocs combiné avec une fonction qui utilise la clé. Itération du procédé.

Du DES à l'AES

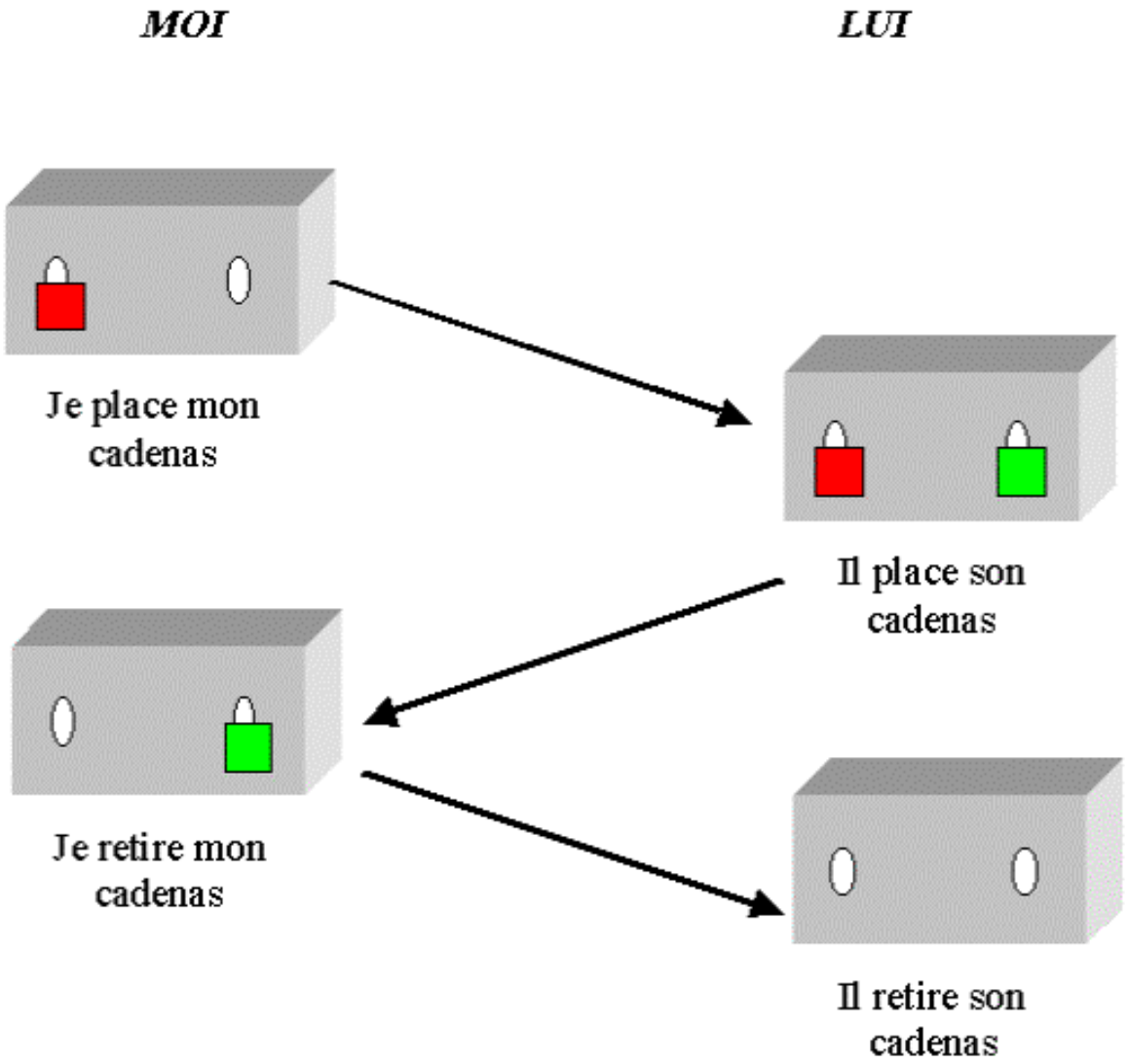
- 1997 : DES cassé en 3 semaines par des ordinateurs effectuant des calculs en parallèle
- Triple DES
- AES *Advanced Encryption Standard*
  - Appel d'offres international. 1997. Clair : 128 bits
  - 2001

La cryptographie à clé publique

- Whitfield Diffle, et Martin E. Hellman
  Université de Stanford
- **Comment éviter l'échange de clés ?**
- **Comment assurer la confidentialité ?**

- 1976 *New Directions in Cryptography*
  - *« Nous nous trouvons aujourd'hui à l'aube d'une révolution en cryptographie »*
- Idée : **Seule l'opération de déchiffrement** doit être contrôlée par une **clé gardée secrète**

La cryptographie à clé publique
Le principe du double cadenas



La cryptographie à clé publique
Le principe du double cadenas

  - La valise : le message
  - Le cadenas et la clé sont des nombres
- Idée : pour permettre un échange sécurisé **en un seul trajet**, A distribue beaucoup d'exemplaires de son cadenas (dont il est le seul à détenir la clé) et que B s'en procure un pour envoyer son message à A.
- **Le principe semble simple, ms il est difficile, de trouver une fonction mathématique permettant un schéma opérationnel similaire.**

La cryptographie à clé publique
Le principe du double cadenas

  - A : Clé de chiffrement : publique
  - B. Clé de déchiffrement : secrète
- Le chiffrement est une fonction à sens unique

Le système à clé publique RSA

- Ronald Rivest (1947-)

  Yale 1969, Stanford 1975, MIT

- Adi Shamir (1952-)

  Tel-Aviv 1973, MIT 1977-1980

- Leonard Adleman (1945-)

  Berkeley 1976

- 1977, *Scientific American*

« A new kind of cryptosystem that would take millions of years to break »

Décrypté en 1994

Le principe du RSA

Théorie des nombres et double échange de clés

- Idée :

Multiplier 2 très grands nombres premiers est une opération facile p = 47, q = 71, module N = 3337.

Retrouver les facteurs à partir du résultat est une opération très difficile.

- Clé de chiffrement : un nombre C premier avec N
- Clé de déchiffrement : son inverse multiplicatif dans un calcul (modulo)

Le principe du RSA

Théorie des nombres et double échange de clés

- Secret : 2 très grands nombres premiers

  p = 47, q = 71, module N = 3337.

- La clé de chiffrement C est un nb premier avec (p-1)(q-1)

  C = 79 Ce qui est public : 3337 et 79

- La clé de déchiffrement, privée, d est telle que

  $d \cdot C = 1 \mod (p-1)(q-1)$ d= 1019

  inverse multiplicatif de C

- Le message est un nombre : 688

  $688^{79} = 1570 \mod N$ $1570^{1019} = 688 \mod N$

Le développement de l'accès conditionnel en France
TV à péage, carte à puce
Louis Guillou

- Rencontres avec :

  Hellman avril 1977et avril 1978

  Rivest en avril 1978

  IBM en avril 1980

- Martin Gardner publie l'invention du RSA dans la rubrique « Jeux mathématiques » du *Scientific American*

Ce qui empêche le MIT de déposer un brevet

- RSA 129 décrypté en 1994 par Arien Lenstra

TV à péage, carte à puce
Louis Guillou et Jean-Jacques Quisquater

- 20 mars 1978, un décret aménage le monopole de la radiodiffusion
- mars 1979 ; création du laboratoire au CCETT
- maquette de carte à puce en 1979
- mise au point en novembre 1980
- Visite programmée du Pr. République
  mais qui n'a pas lieu
- Très mal perçu par les services de la Défense
- 1982 : technologie RSA sur les cartes à puce
- 1984 : cartes bancaires (Lyon, Caen, Blois)
- 1998 : affaire Humpich
- 1998-2002 : la carte à puce est sauvée par la téléphonie mobile

Affaire Humpich 1998

- Dans les cartes à puce françaises, le module public est un nombre connu entre 768 et 1024 bits, produit de 2 nombres premiers. L'exposant C est 3.
- Une valeur de signature est inscrite sur la carte, elle utilise l'information de la carte et une clé secrète
- Quand j'introduis ma carte dans la machine, elle utilise la clé publique
- **Problème en 1998** : ce module était de 320 bits, et n'avait pas changé depuis 1990.
- L'authentification en ligne (pour des achats avec autorisation) utilise maintenant l'AES à la place du DES.

Le logiciel semi-libre PGP, 1991, Philip Zimmermann
Pretty Good Privacy

- Système hybride de sécurisation, utilisé pour les communications en ligne dans certaines entreprises ou institutions où les communications sont « sensibles »
- • Chiffrement symétrique (clé privée)

  et asymétrique (clé publique)