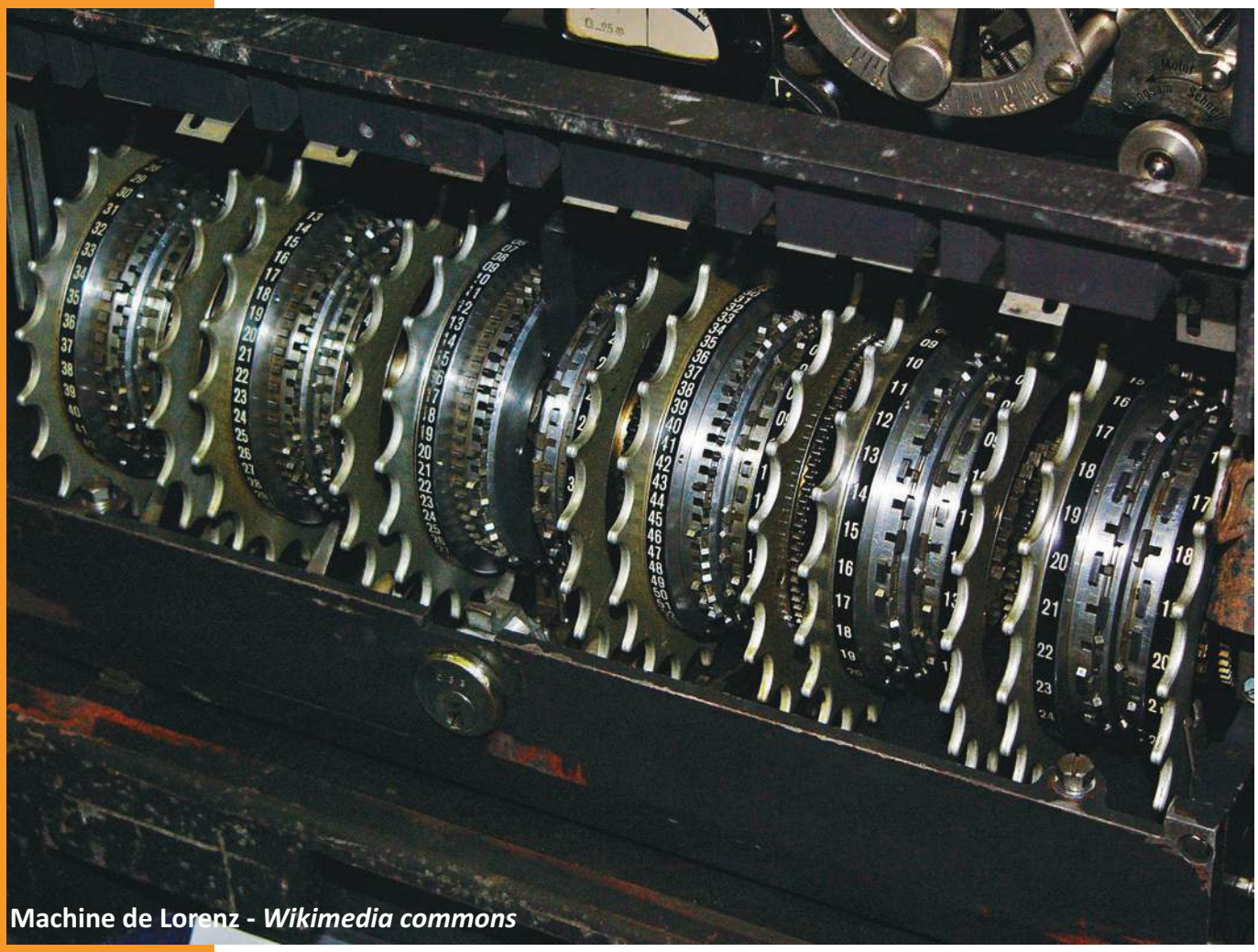
Livret pédagogique
Exposition Cryptographie



Machine de Lorenz - *Wikimedia commons*

Réalisation
Comité International
des Jeux Mathématiques
Association nationale de jeunesse
et d'éducation populaire
Association agrée par
l'Éducation Nationale

CIJM - Institut Henri Poincaré
11 rue Pierre et Marie Curie
75231 PARIS Cedex 05
cijm@cijm.org N° SIRET : 433 879 343 00047
APE 927 C

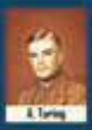
www.cijm.org

L'exposition
Cryptographie et Codages
dont est issu ce livret
a été réalisée grâce
au partenariat du

Crédit CME Mutuel
Enseignant
www.cme.creditmutuel.fr











Cryptographie et codages

Avant Jésus-Christ

La stéganographie est l'art de dissimuler des messages.
(stéganos : cacher ; graphie : écriture)

Hérodote retrace dans ses *Histoires* (V^e siècle av JC) les conflits entre la Grèce et la Perse et rapporte plusieurs exemples de stéganographie.

Il conte l'histoire d'Histaïacus qui voulait encourager Aristagoras de Milet à se soulever contre le roi des Perses. Il rasa la tête de son messager, écrivit le message, attendit que les cheveux repoussent...

Les spartiates écrivaient le message sur une bandelette enroulée autour d'un «scytale» (ou bâton codé). Une fois la bandelette déroulée, ne subsiste qu'un hâchis incompréhensible. Un bâton de même diamètre est indispensable pour retrouver le sens caché.

Au I^er siècle ap JC, Pline l'Ancien explique comment on fait de l'encre invisible avec le lait de l'euphorbe *tithymallus*.

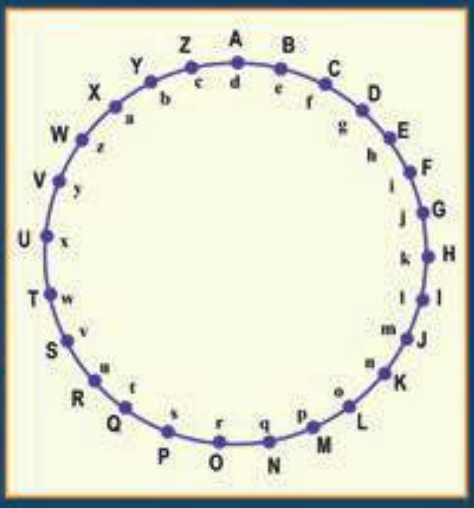
La cryptographie est l'art de transformer un message

Jules César - I^er siècle av. JC - a l'idée simple et efficace de transmettre des messages en décalant chaque lettre de trois crans dans l'alphabet.

Ainsi **A** devient ***d***, **B** devient ***e***, etc, et le message clair
Rendez vous vendredi soir devient,
uhqghc yrxv yhqguhgl vrlu

Depuis, tout système de cryptage de ce type, quelque soit le décalage choisi, est appelé :

Alphabet de César



Au cours des siècles, cryptographie et stéganographie se sont souvent conjuguées pour mieux transmettre en secret !

Pour mieux comprendre la cryptographie

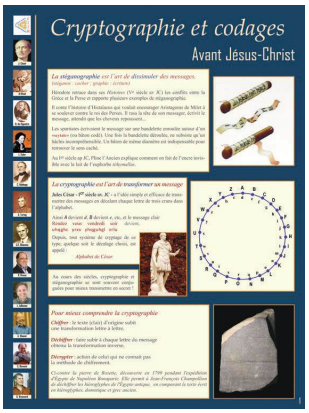
Chiffrer : le texte (clair) d'origine subit une transformation lettre à lettre.

Déchiffrer : faire subir à chaque lettre du message obtenu la transformation inverse.

Décrypter : action de celui qui ne connait pas la méthode de chiffrement.

Ci-contre la pierre de Rosette, découverte en 1799 pendant l'expédition d'Égypte de Napoléon Bonaparte. Elle permit à Jean-François Champollion de déchiffrer les hiéroglyphes de l'Égypte antique, en comparant le texte écrit en hiéroglyphes, domotique et grec ancien.

Panneau 1
Avant Jésus-Christ



Pour mieux comprendre

Un peu de vocabulaire propre à la cryptographie :

Chiffrer : appliquer au message une transformation qui le rend incompréhensible à ceux qui ne connaissent pas la méthode de chiffrement.

Coder : écrire un message dans un autre alphabet, littéral ou numérique, en utilisant une technique connue de tous. Donc tout le monde peut décoder.
Le chiffreur transforme le clair en un cryptogramme.

Déchiffrer : transformer le cryptogramme en « clair» quand on connaît la méthode de chiffrement.
On peut penser que lorsqu'on sait chiffrer, on sait déchiffrer. C'était vrai jusqu'en 1976. Depuis, ce n'est pas toujours vrai (voir le panneau 5).

Décrypter : transformer le cryptogramme en « clair » quand on ne connaît pas la méthode de chiffrement.

Pour en savoir un peu plus sur la stéganographie

La stéganographie, c'est l'art de cacher des messages et de rendre leur présence insoupçonnable pour toute autre personne que le destinataire. Vous pouvez vous y essayer entre amis !

Acrostiches, contrepèteries, jeux de césure, sauts de mots ou de lettres ou de lignes… les procédés stéganographiques sont multiples et la littérature regorge de textes à double lecture.

En dehors des subtilités linguistiques, un message peut être caché par des moyens techniques : de l'esclave dévoué à la tête rasée aux microfilms et fichiers électroniques en passant par les encres sympathiques, l'imagination humaine est infinie.. .

Quelques encres sympathiques :

Première catégorie avec les liquides organiques : lait, citron, sève, urine …. Ils apparaissent souvent au chauffage.

Deuxième catégorie aves les liquides chimiques :
ils sont invisibles une fois secs ; des caractères colorés apparaissent après avoir été en contact avec un produit chimique appelé réactif.

Des liens importants existent entre la télématique et la stéganographie et l'usage de cette dernière sur Internet semble promis à un bel avenir …

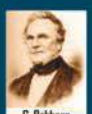
Voir manipulations autour de l'Alphabet de César et autres méthodes de cryptographie en fin de dossier .


J. César


Al-Kindi


B. de Vigenère


L. Euler


C. Babbage


A. Turing


C.E. Shannon


R. Rivest


L. Adleman


A. Shamir


C. Bennett


G. Brassard

Cryptographie et codages

De César au XXe siècle

La cryptanalyse

Les érudits et les savants du monde arabe inventent au IXe siècle, la cryptanalyse, l'art de décrypter les messages sans en connaître la *clé*. Le philosophe mathématicien Al-Kindi propose une méthode de cryptanalyse basée sur les fréquences de lettres dans le texte.

En même temps que se développent des méthodes de cryptanalyse, la cryptographie par substitution progresse en complexité.


Al- Kindi
800- 873

Qu'est-ce qu'une *Clé* en cryptographie ?

Une clé de chiffrement est un paramètre utilisé en entrée d'une opération cryptographique.

Elle peut se présenter sous différentes formes : mots, phrases, nombres...

Elle peut être symétrique (elle sert alors au chiffrement comme au déchiffrement)

ou asymétrique (il y a alors des clés différentes pour le chiffrement et le déchiffrement)

Le chiffre de Vigenère : premier exemple de cryptographie à «clé».

L'idée d'utiliser plusieurs décalages de l'alphabet pour crypter revient au florentin *Léon Alberti* au XVe siècle mais Blaise de Vigenère lui donna sa forme finale.

Pour chiffrer un message on utilise un mot clé, ROUGE par exemple. Pour encrypter la première lettre du message, on utilise le décalage alphabétique A ⟶ R, pour la deuxième lettre on utilise le décalage A ⟶ O,... ainsi de suite ; à la sixième lettre on recommence le décalage A ⟶ R, ... Dans ce chiffrement la lettre E peut-être codée soit I, K, S, V ou Y.

Ainsi le message clair

RENDEZ-VOUS VENDREDI SOIR

devient, crypté, en employant le mot clé ROUGE :

ISHJIA JOYW MSHJVVRC ZSZF

Le chiffre de Vigenère ne fut réellement utilisé que deux siècles plus tard. Pourtant il résista plus de trois siècles à la cryptanalyse.
En s'appuyant sur certaines occurences obligatoires de séquences de lettres dans le chiffrement de Vigenère, Charles Babbage au XIXe siècle réussit à faire céder *«le chiffre indéchiffrable»* de Vigenère, mais là aussi sa découverte resta longtemps ignorée.

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

Le carré de Vigenère permet de donner les vingt- cinq décalages de l'alphabet.

Seconde Guerre Mondiale

Enigma, machine à crypter de l'armée allemande, a affolé les Alliés pendant une partie de la guerre.
Son système, à base de plusieurs disques entraînés mécaniquement, permettait des combinaisons extrêmement complexes.
Il a fallu toute l'intelligence d'un petit groupe de mathématiciens dirigés par le grand Alan Turing pour casser les codes d'Enigma.

Machine à crypter Enigma.
A droite les disques permettant de multiples combinaisons.

Panneau 2
De César au XX^{ème} siècle

« Au temps de César, changer A en D, B en E, C en F, etc. dans un message suffit pour le rendre incompréhensible à un éventuel intercepteur. Il faudra un millénaire pour qu'un savant arabe Al-Kindi trouve une méthode pour décrypter les chiffres obtenus par simple substitution alphabétique : la méthode des fréquences. Elle consiste à comparer les fréquences des lettres des messages avec les fréquences usuelles dans la langue utilisée. Ainsi est né la cryptanalyse, l'art de décrypter les messages.
La cryptographie dite Alphabet de César va être perfectionnée à la Renaissance par un diplomate Blaise de Vigenère, en modifiant la substitution en fonction d'une clef. Ce code n'est brisé qu'au XIX^{e} siècle par Babbage. Il ne survit aujourd'hui dans la réalité qu'à la condition que la clef soit aussi longue que le message, pour le téléphone rouge et la cryptographie quantique »
Bibliothèque TangenteHS n°26 Cryptographie et Codes Secrets

Le Chiffre de Vigenère
Utilisez le carré de Vigenère du panneau ou fabriquez-vous votre propre carré.

Changez de mot clé : Prenez AMIE par exemple qui fournit le décalage suivant (1, l3, 9, 5) obtenu à partir de la position des lettres dans l'alphabet.
Transformez le message RENDEZ VOUS VENDREDI SOIR (ou celui que vous voulez …)
On transforme le message en décalant d'une place la première lettre, de 13 places la seconde, etc, puis on réapplique la clé à la cinquième lettre du « clair» et ainsi de suite, ...

Le cassage de Babbage
Le mathématicien anglais et précurseur de l'informatique Charles Babbage eut l'idée de chercher des répétitions dans les messages cryptés pour en déduire des informations sur la longueur de la clé. Il définit ainsi des groupes de mots auxquels il applique la méthode des fréquences de El Kindi et retrouve la clé lettre par lettre.

La ruse de Gilbert Vernam
Le cryptographe américain Gilbert Vernam (1890 – 1960) eut l'idée, pour éviter le décryptage par la méthode de Babbage d'utiliser une clé aussi longue que le message, clé qui doit être jetée après usage. Shannon a montré ensuite que si l'on choisit la clé au hasard ce code est inviolable : la raison est simple en codant un texte avec une clé aléatoire le texte lui-même devient aléatoire. Les faiblesses de ce code « parfait» sont la taille et la transmission des clés. Pour l'instant il n'est utilisé qu'en diplomatie, par exemple il est au cœur du téléphone rouge reliant Washington à Moscou.

La machine ENIGMA

La machine ENIGMA utilise une méthode de chiffrement qui est en fait une version plus compliquée de l'alphabet de Jules César. Son système à base de plusieurs disques entrainés mécaniquement permettait des combinaisons extrêmement compliquées.

Quelques mots sur la Machine de Lorenz

Les machines de Lorenz *SZ 40 et SZ 42 (SZ pour « Schlüsselzusatz », qu'on peut traduire par « pièce jointe chiffrée ») sont des machines de chiffrement ayant été utilisées pendant la Seconde Guerre mondiale par les Allemands pour les communications par téléscripteur. Les cryptographes britanniques, qui se référaient de façon générale au flux des messages chiffrés allemands envoyés par téléscripteur sous l'appellation Fish (« fish » peut se traduire par « poisson »), ont nommé la machine et ses messages « Tunny » (qu'on peut traduire par « Thon »).*

Tandis que la renommée Enigma servait à l'armée, la machine de Lorenz était destinée aux communications de haut niveau entre le quartier-général du Führer et les quartiers-généraux des groupes d'armées, qui pouvaient s'appuyer sur cet appareil lourd, son opérateur et des circuits dédiés.

La machine elle-même mesurait 51 cm × 46 cm × 46 cm et accompagnait les téléscripteurs Lorenz standards. Ces machines appliquaient une méthode de chiffrement de flux. Les cryptanalystes de Bletchley Park ont compris le fonctionnement de la machine en janvier 1942 sans jamais en avoir vu un seul exemplaire. Cela fut possible à cause d'une erreur commise par un opérateur allemand. Le 30 août 1941, un message de 4 000 caractères fut transmis ; cependant, le message n'ayant pas été reçu correctement à l'autre bout, celui-ci fut retransmis avec la même clé (une pratique formellement interdite par la procédure). De plus, la seconde fois le message fut transmis avec quelques modifications, comme l'utilisation de certaines abréviations. À partir de ces deux textes chiffrés, John Tiltman a été en mesure de reconstituer à la fois le texte en clair et le chiffrement.

D'après Wikipédia

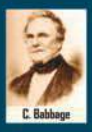
Utilisation d'une machine Enigma dans le comand-car du Général Heinz Guderian.


J. César


Al-Kindi


B. de Vigenère


L. Euler


C. Babbage


A. Turing


C.E. Shannon


R. Rivest


L. Adleman


A. Shamir


C. Bennett

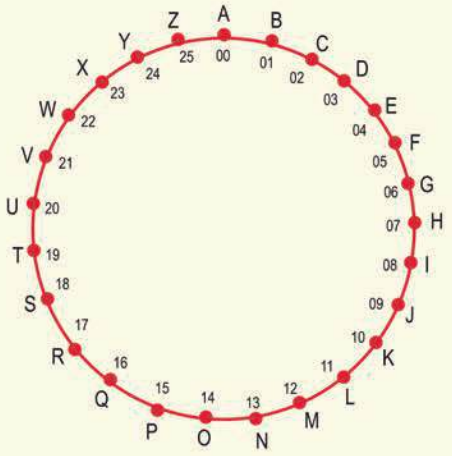

G. Brassard

Cryptographie et codages

Arithmétique pour chiffrer

En 1976, l'**arithmétique** fait son entrée dans la cryptographie et lui fournit de nouveaux outils.

Les lettres sont codées par des nombres. On obtient alors un clair numérique.



Le message :

Rendez-vous vendredi soir

a pour «clair» numérique :

17 04 13 03 04 25 21 14 20 18 21 04 13 03 17 04 03 08 18 14 08 17

Le clair est ensuite chiffré ***mathématiquement****.*

Les **nombres premiers** *vont jouer un rôle fondamental*

Quelques définitions

$a \equiv b \pmod{n}$

se lit *a congru à b modulo n*

et veut dire *a et b ont même reste dans la division par n.*

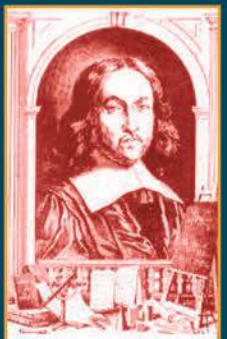
Dans le cas particulier où b est le reste de la division de a par n,

on peut écrire $a \bmod n = b$ et lire *a modulo n égal b.*

Quelques exemples :

$18 \equiv 13 \pmod{5}$; $18 \equiv 8 \pmod{5}$;

et $18 \equiv 3 \pmod{5}$ peut s'écrire $18 \bmod 5 = 3$.



Pierre de Fermat
1601 - 1655

Un théorème dû à Fermat et Euler

Quand p et q sont deux nombres premiers distincts
pour tous les entiers k et M, on a

$M^{k\,(p-1)(q-1)+1}$ congru à M modulo pq
ce qui s'écrit

$$\mathbf{M^{k\,(p-1)(q-1)+1} \equiv M \pmod{pq}}$$

Un exemple simple :

Avec $p = 3$ et $q = 5$, on a $pq = 15$ et $(p-1)(q-1)+1 = 9$

donc $2^9 \equiv 2 \pmod{15}$.

Léohnard Euler
1707 - 1783

3

Panneau 3
Arithmétique pour chiffrer

Les mots deviennent des nombres ...

On code les lettres par un nombre de deux chiffres, par exemple :
A devient 00 ; B devient 01 ; ..... ; Z devient 25.
Les messages deviennent ainsi une suite de chiffres que 1' on regroupe en blocs de *n* chiffres (souvent *n* est imposé par la méthode de chiffrement choisie).

Le message B R A V O devient 01 17 00 21 14

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

Le carré de Polybe :

Une autre façon de numériser les messages.

L'historien grec Polybe vécu de 205 à 125 av J.C. et est connu pour être l'inventeur d'un système de chiffrage connu sous le nom de Carré de Polybe .

Chaque lettre du message est remplacée par un nombre de deux chiffres notant pour les dizaines le numéro de la ligne et pour les unités le numéro de la colonne.

Le message B R A V O devient 12 43 11 52 35

Le Chiffre des nihilistes

double le carré de Polybe du code de Vigenère

Les nihilistes, prisonniers politiques du Tsar, communiquaient en frappant le nombre de coups correspondant au chiffre qu'ils voulaient transmettre, deux chiffres consécutifs correspondant à une lettre de l'alphabet.

Le message B R A V O devient X-XX—XXXX-XXX—X-X—XXXXX-XX—XXX-XXXXX
(X signifiant un coup ...)

Il est bien sûr possible d'utiliser une clé pour crypter d'abord le message ...

Un mot sur l'arithmétique modulaire

L'idée de répartir les nombres entiers en p classes selon leur reste dans la division par p, on dit, en classes modulo p, revient à **Gauss** qui exposa, dans son célèbre ouvrage *Disquisitiones Arithmétiques* publié en 1801, ses travaux en arithmétique.

Ainsi est née l'**arithmétique modulaire** qui permet de calculer sur des nombres très, très grands en travaillant sur leur classe (donc leur reste dans la division par p).
Pratique pour les calculs en astronomie ou pour les besoins actuels de la cryptographie

Apprenons à compter dans le monde des multiples de 5, c'est à dire «modulo CINQ ».

Les tables d'addition et de multiplication « modulo CINQ »

$\overline{0}$ représente l'ensemble de tous les multiples de 5
$\overline{1}$ représente l'ensemble de tous les multiples de 5 plus 1
$\overline{2}$ représente l'ensemble de tous les multiples de 5 plus 2
$\overline{3}$ représente l'ensemble de tous les multiples de 5 plus 3
$\overline{4}$ représente l'ensemble de tous les multiples de 5 plus 4

+	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$

x	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{1}$	$\overline{3}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{1}$	$\overline{4}$	$\overline{2}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Remarquons que l'on a, quel que soient les nombres entiers a et b,
$(a + b)^5 \equiv a^5 + b^5 \pmod 5$ ce qui permet de montrer un cas particulier du Petit Théorème de Fermat : $a^5 \equiv a \pmod 5$.

Le Petit Théorème de Fermat, clé de voute de la cryptographie moderne, dit que :
pour p premier, quelque soit l'entier a, on a : $a^p \equiv a \pmod p$.

Pierre de Fermat, énonça pour la première fois en 1640, ce résultat.

Le théorème de Fermat Euler

La démonstration du théorème de Fermat Euler dépasse le niveau des programmes des lycées ; il est en fait un corollaire du « Petit Théorème de Fermat».

On peut trouver toutes ces démonstrations, en particulier, dans le livre de Guy Robin *Apprenons l'arithmétique élémentaire pour comprendre la cryptographie moderne*, édité par l'IREM de Limoges.

On peut« vérifier» ce théorème sur l'exemple simple du panneau :

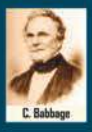
Soit p=3, q=5. Pour M=2, on a: $2^9 = 512 = 34 \times 15 + 2$ donc $2^9 \equiv 2 \pmod{15}$
et pour M=7, on a aussi: $7^9 = 40\,353\,607 = 2\,690\,240 \times 15 + 7$
donc $7^9 \equiv 7 \pmod{15}$.

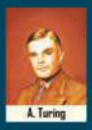

J. César


Al-Kindi


B. de Vigenère


L. Euler


C. Babbage


A. Turing


C.E. Shannon


R. Rivest


L. Adleman


A. Shamir


C. Bennett


G. Brassard

Cryptographie et codages

Nombres Premiers

*Un **nombre premier** est un nombre entier ayant exactement deux diviseurs, 1 et lui-même.*

Les premiers nombres premiers sont :
2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53...

Euclide, (325-265 avant JC), dans ses *Eléments*, prouve qu'il y a une infinité de nombres premiers.

Eratosthène, mathématicien grec de l'école d'Alexandrie (274 -194 avant JC) a mis au point un algorithme permettant de dresser une table des premiers nombres premiers.

Mais un nombre premier étant donné on ne sait toujours pas trouver systématiquement le suivant et
la répartition des nombres premiers est un problème au coeur de l'arithmétique moderne.

Les grands nombres premiers, une recherche difficile

Les nombres de Mersenne, nombres qui s'écrivent $2^p - 1$ avec p nombre premier, sont candidats pour être des nombres premiers.

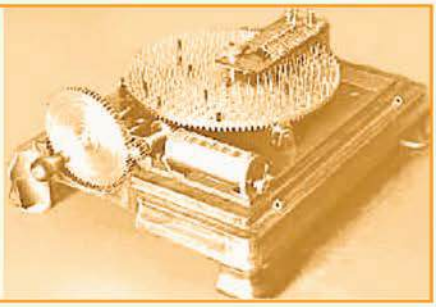
Le plus grand nombre de Mersenne premier connu depuis 2008 est $2^{43112609} - 1$.
Il s'écrit sous forme développée avec 12 978 189 chiffres.

Le plus grand nombre dont la primalité a été prouvée en 2011 est :
60336838787923722145...(26602 autres chiffres)...97795227069490003443
Ce nombre premier est un nombre de 26 642 chiffres.

Trouver la factorisation d'un grand nombre, en deux nombres premiers, est encore plus difficile.

La machine à factoriser des frères Carissan

En 1912, Eugène et Pierre Carissan, construisent une machine à factoriser les grands nombres, mais ce premier prototype ne donne pas de résultats intéressants.
Eugène reprend après la guerre la construction de cette machine dite machine à congruences. Elle sera achevée en 1919 par la maison Château Frères spécialisée dans la fabrication d'instruments scientifiques. La machine factorise des nombres de 13 chiffres en moins de 18 minutes.
Elle permettra la résolution de plusieurs problèmes de la théorie des nombres jusqu'au décès d'Eugène Carissan en 1925.



En décembre 2009, une équipe internationale de mathématiciens a obtenu la factorisation d'un nombre de 232 chiffres en deux grands nombres premiers de 116 chiffres. C'est un vrai record qui aura demandé deux ans de travaux et l'exécution d'environ 10^{20} opérations.

123018668453011775513049495838496272077285356959533479219732245215172640050726365751874520219978646938995647494277406384592519255732630345373154826850791702612214291346167042921431160222124047927473779408066535141959745985690214341336

=

334780716989568987860441698482126908177047949837137685689124313889828837938780022876147116525317430877378144679994893674604366679959042824463379962795263227915816434308764267603228381573966651127923337341714339681027009279873630891 7

x

367460436667995904282446337996279526322791581643430876426760322838157396665112792333734171433968102700927987363089177

Panneau 4
Nombres Premiers

Nombre premier : nombre entier qui admet exactement deux diviseurs, **1** et **lui même**.

On écarte 1 pour des raisons théoriques : ce nombre joue un rôle très particulier (c'est l'élément unitaire de la multiplication) et il intervient trop souvent comme un cas particulier (par exemple l'unicité de la décomposition d'un nombre en facteurs premiers serait en défaut si 1 était premier).

Remarquez que 2 a raison d'être fier d'être premier ; il est le seul nombre pair à avoir le titre de nombre premier.

Les nombres premiers fascinent depuis toujours.

Euclide a prouvé le premier, dans ses « Eléments », qu' il y a une infinité de nombres premiers.

Euler proposa une autre démonstration de ce résultat en utilisant les suites géométriques

Eratosthène vivant vers 250 av J.C, fut le premier géographe d'Alexandrie et on lui doit, en particulier, le calcul du rayon terrestre. Il a mis au point un algorithme, le crible d'Eratosthène, qui permet d'établir la liste des nombres premiers inférieurs à 100 (ou 1000 si la taille de la table ne fait pas peur …)

Nicomaque de Gérase, au premier siècle de notre ère, a exposé pour la première fois une méthode de recherche des nombres premiers dans un ouvrage «*Introduction Arithmétique*». Il dit avoir trouvé cette idée chez Eratosthène.

Autour des nombres premiers

2013 est-il premier ? non
Celui d'avant est **2011** : il est même somme de 11 nombres premiers consécutifs 157, 163, 167, 173, 179, 181, 191, 193, 197, 199, 211.

Le suivant est **2027** : c'est un **nombre premier sûr** , car 2027 = 2 x 1013 + 1 et 1013 est un nombre premier.

2039 est à la fois **un nombre prmier sûr**
mais aussi un **nombre premier de Sophie Germain,**
car 2 x 2039 + 1 = 4079 et 4079 est premier.

Construction du crible d'Eratosthène des nombres jusqu'à 100 Voir manipulations en fin de brochure

A la recherche des grands nombres premiers

Les nombres de Mersenne

En mathématiques un **nombre premier de Mersenne** est un nombre premier pouvant s'écrire sous la forme 2^p-1 , avec p lui-même entier premier..

Plus généralement, les **nombres de Mersenne** (pas nécessairement premiers, mais candidats à l'être) constituent la suite des nombres :

$$M_p = 2^p - 1$$

Ces nombres premiers doivent leur nom à un érudit et mathématicien français du XVII^e siècle, Marin Mersenne.

En effet, on démontre qu'un entier de la forme $2^n - 1$ ne peut pas être premier si *n* n'est pas premier

- Si n n'est pas premier (par exemple le produit $n = qp$ où ni q, ni p n'est égal à 1) alors le nombre $2^{qp} - 1$ n'est pas premier.

En effet, en remarquant que la suite des q premiers termes de la suite géométrique de raison 2^p est égale à :

$$1 + 2^p + (2^p)^2 + \ldots + (2^p)^{q-1} = \frac{2^{qp} - 1}{2^p - 1}$$

on prouve que $2^{qp} - 1$ est divisible par $2^p - 1$ qui est différent de 1 dès que p est également distinct de 1. (On peut, dans ce raisonnement, intervertir les rôles de p et q.)

Mais si n est premier , $2^n - 1$ n'est pas nécessairement premier

Les plus petits nombres premiers de Mersenne sont donc :

- M1 = $M_2 = 2^2 - 1 = 3$;
- M2 = $M_3 = 2^3 - 1 = 7$;
- M3 = $M_5 = 2^5 - 1 = 31$;
- M4 = $M_7 = 2^7 - 1 = 127$;
- Mais, $M_{11} = 2^{11} - 1 = 2047 = 23 \times 89$, est un nombre de Mersenne non premier .

Ainsi, lorsque l'on cherche des nombres premiers via les nombres de Mersenne, on sait déjà qu'il faut éviter les candidats comme $2^4 - 1$ (i.e. 15), $2^6 - 1$(i.e. 63) ou $2^9 - 1$ (i.e. $511 = 7 \times 73$)

Les nombres premiers de Mersenne sont liés aux **nombres parfaits**, qui sont les nombres égaux à la somme de leurs diviseurs propres. C'est cette connexion qui a motivé historiquement l'étude des nombres premiers de Mersenne. Dès le IV^e siècle av. J.-C., Euclide démontrait que si $M = 2^p - 1$ est un nombre premier, alors $M(M + 1) / 2 = 2^{p-1}(2^p - 1)$ est un nombre parfait. Deux millénaires plus tard, au XVIII^e siècle, Euler prouvait que tous les nombres parfaits *pairs* ont cette forme. Aucun nombre parfait impair n'est connu.

Pour les nombres de Mersenne, il existe une méthode (comparativement) très rapide pour déterminer s'ils sont premiers, développée à l'origine par Édouard Lucas en 1878 et améliorée par Derrick Lehmer dans les années 1930.

A la recherche des nombres premiers de Mersenne

Mersenne n'a pas inventé les nombres de Mersenne, mais il a fourni une liste de nombres premiers de Mersenne jusqu'à l'exposant 257. Malheureusement cette liste était fausse : elle incluait par erreur 67 et 257, et omettait 61, 89 et 107.
Les quatre premiers nombres premiers de Mersenne étaient connus dès l'Antiquité. Le cinquième (2^{13}-1) a été découvert avant 1461 par un inconnu. Les deux suivants ont été trouvés par Pietro Cataldi en 1588. Plus d'un siècle plus tard, en 1750, Euler en trouva encore un. Le suivant dans l'ordre chronologique (mais non numérique) a été trouvé par Lucas en 1876, puis un par Ivan Pervushin en 1883. Deux autres ont été trouvés au début du XX^{e} siècle par R. E. Powers en1911 et en 1914.
La recherche pour les nombres premiers de Mersenne fut révolutionnée par l'introduction des calculateurs électroniques. La première identification d'un nombre de Mersenne par ce moyen eut lieu à 22 heures le 30 janvier 1952 par un ordinateur SWAC à l'Institut d'Analyse Numérique *(Institute for Numerical Analysis)* du campus de l'université de Californie à Los Angeles, sous la direction de Derrick Lehmer, avec un programme écrit par Raphael Robinson.
C'était le premier nombre premier de Mersenne identifié depuis 38 ans. Le suivant fut trouvé moins de deux heures plus tard par le même ordinateur, qui en trouva trois de plus dans les mois suivants.
En juin 2011, 47 nombres premiers de Mersenne étaient connus, le plus grand étant $2^{43\,112\,609}$-1. Comme plusieurs de ses prédécesseurs, il a été découvert par un *calcul distribué* sous l'égide du projet GIMPS, *Great Internet Mersenne Prime Search* (qui signifie « grande recherche par Internet de nombres premiers de Mersenne »).
Le *calcul distribué* ou *réparti* ou encore *partagé*, est l'action de répartir un calcul ou un traitement sur plusieurs microprocesseurs et plus généralement toute unité centrale informatique. Le calcul distribué est souvent réalisé sur des clusters de calcul spécialisés, mais peut aussi être réalisé sur des stations informatiques individuelles à plusieurs cœurs. La distribution d'un calcul est un domaine de recherche des sciences mathématiques et informatiques.

Cependant on ne sait toujours pas, un nombre premier étant connu, prévoir le suivant.

Que sait-on de la répartition des nombres premiers ?

En 1997, il existait des tables de nombres premiers allant jusqu 'à N = 5.10^{8}.

Les nombres premiers se raréfient à mesure que N croît. On note π (N) le nombre de nombres premiers compris entre 2 et N.

Entre 1 et 10, on trouve 4 nombres premiers
Entre 1 et 100, on en trouve 25 ;
Entre 1 et 1 000, on en trouve 168 ;
Entre 1 et 10 000, on en trouve 1 229 ;
Entre 1 et 100 000, on en trouve 9 592 ;
Entre 1 et 1 000 000, on en trouve 78 498. Etc.

Gauss et Legendre énoncèrent le théorème suivant : « Plus N est grand, plus π (N) est proche de N/lnN ». Ce résultat fut démontré en 1896, séparément par Hadamard et de la Vallée Poussin.

Pour N = 1 000 000, par exemple, la différence entre N/lnN et π (N) vaut à peu près 6116. On a $\pi(10^{6})$ = 78 498.

Sur les nombres premiers, il y a de nombreux problèmes non résolus, de nombreuses conjectures.

Ces conjectures sont d'autant plus fascinantes qu'elles sont faciles à énoncer et à comprendre. Un bel exemple est la conjecture de Goldbach (1690- 1764) :
« *Tout nombre pair, strictement supérieur à 2, est somme de 2 nombres premiers et tout nombre impair strictement supérieur à 5, est somme de 3 nombres premiers* »

Les **nombres premiers jumeaux**, ceux qui diffèrent de 2, (comme 3 et 5 ; 5 et 7; ...) se raréfient mais on ne sait pas s'il y a une infinité de nombres premiers ...

Pourquoi a-t-on besoin de grands nombres premiers ?
La sécurité des systèmes de chiffrement qui protègent notre carte bleue et de nombreux moyens de transactions bancaires est basée sur la factorisation d'un nombre en deux très grands facteurs premiers.

La machine des frères Carissan

Texte intégral
PRÉSENCE DE L'HISTOIRE
François MORAIN

À la recherche des machines qui décomposaient les grands nombres en facteurs premiers.

Pourquoi est-il facile de multiplier deux nombres entiers et si ardu de trouver deux entiers dont le produit est donné?

Le problème de la factorisation occupe les mathématiciens depuis longtemps ; dès le XIX^{ème} siècle, ils ont cherché à construire des machines facilitant les calculs répétitifs et fastidieux de la factorisation.
Dans certaines branches de la théorie des nombres, les calculs peuvent être assez aisément automatisés. C'est le cas des cribles. Le plus connu d'entre eux est *le crible d'Ératosthène* qui permet de trouver tous les nombres premiers dans un intervalle donné (on écrit tous les nombres de 0 à 100. par exemple ; on élimine ensuite tous les multiples de 2, puis tous les multiples de 3, puis de 5, etc; après avoir passé tous les nombres «au crible», on ne conserve ainsi que 2, 3, 5, 7, 11, 13, etc. qui sont premiers). Une extension de cette notion de crible permet de résoudre les équations en nombres entiers du type $N = x^2 - y^2$: c'est le cas de la méthode de Fermat. La méthode est efficace quand les diviseurs ont des valeurs voisines et elle est adaptable à des dispositifs mécaniques.
Le mathématicien anglais Frederick Lawrence semble avoir été le premier à préconiser la construction d'un crible pour factoriser des entiers, en 1896. Bien qu'il ait écrit comment fabriquer une telle machine, elle ne vit pas le jour. L'idée de Lawrence fut oubliée jusqu'en 191 0, quand André Gérard publia une traduction française de son article dans sa revue de «mathématiques amusantes», *Sphinx-OEdipe*. Cet article semble avoir inspiré à l'ingénieur Maurice Kraitchik, l'idée de construire un prototype d'une telle machine, en 1912.

Pierre Carissan, professeur de mathématiques, est aussi rédacteur à la revue Sphinx-OEdipe. Il s'intéresse à la fabrication d'une telle machine. Après avoir occupé différents postes de professeur de mathématiques, il est nommé, en 1914, au Collège Dumont-d'Urville, près de Caen. Certains de ses proches le considèrent comme un «original fini». Son frère, Eugène Olivier, entre à l'École spéciale militaire, en 1900. En 1912, les deux

frères construisent une machine à factoriser les grands nombres, mais ni leur prototype, ni celui de Kraitchik ne donne de résultats intéressants. Eugène entreprend la fabrication d'un nouveau prototype en 1913 mais le projet est interrompu par la guerre.

Héroïque, il est blessé trois fois durant la guerre (en juillet 1915, il refuse même d'être évacué et continue à se battre). Après la guerre, il est nommé professeur à l'École militaire de Saint-Maixent, et reprend la construction de la machine, dite *machine à congruences.* Elle sera achevée en 1919 par la maison Château Frères, spécialisée dans la fabrication d'instruments scientifiques. Elle permettra la résolution de plusieurs problèmes de la théorie des nombres. Eugène Carissan meurt en 1925 sans avoir eu le temps de faire exécuter les modifications qu'il jugeait nécessaires. Il voulait notamment entraîner la machine par un petit moteur électrique et non plus à la main. Aucune modification n'est entreprise, et la machine disparaît.

À la recherche de la machine de Carissan

Avec mes collègues Jeffrey Shallit à l'Université canadienne de Waterloo et Hugh Williams à l'Université du Manitoba, nous apprenons l'existence de la machine des frères Carissan à l'automne 1989. Sherlock Holmes des mathématiques, nous cherchons la machine dans toute la France : nous enquêtons pour retrouver la maison *Chateau Frères*, et visitons les musées techniques français. La première piste aboutit rapidement à une impasse : la maison *Chateau Frères* n'existe plus. Les pistes du Conservatoire National des Arts et Métiers, de l'École Normale Supérieure, de l'Institut Henri Poincaré ou encore de la Bibliothèque Nationale échouent.

Après une année de recherches infructueuses, J. Shallit décide d'employer les grands moyens : avec l'aide de Jean-Paul Allouche, de l'unité CNRS URA 410, il écrit à tous les Carissan de France et de Navarre pour leur demander s'ils connaissent la machine que nous recherchons. Au cours de l'été 1991, les 85 Carissan référencés sur notre liste reçoivent une lettre, où on leur demande tous les renseignements possibles sur cette machine et sur ses inventeurs.

Les premières réponses ne tardent pas à arriver, mais elles sont toutes décevantes. Enfin, nous recevons un appel téléphonique d'une des filles d'Eugène Carissan : la machine existe toujours et elle est entreposée près de Bordeaux. Apparemment, la machine est restée en possession de la famille jusque vers 1940, quand Jean Dubois, astronome et ami de la famille Carissan, la fit transférer à l'Observatoire de Floirac, près de Bordeaux. Elle y a été entreposée jusqu'en 1992.

Elle fonctionne parfaitement bien. La famille de l'inventeur, étonnée de voir trois chercheurs remuer ciel et terre pour retrouver la machine due au génie paternel a donné la machine au Conservatoire national des arts et métiers, où elle est désormais installée.

La machine à congruences des frères Carissan.

Quelques précisions

Une manivelle fait tourner la roue dentée qui entraîne d'une part un compteur et d'autre part 14 couronnes de laiton, chacune avançant d'un picot à l'autre pour la rotation d'une dent de pignon (le compteur avance d'une unité à chaque rotation d'une dent). Avant de tourner la roue, toutes les couronnes sont en position «0». À chaque couronne est associé un nombre (19, 21, 23, 26, 29, 31, 34, 37, 41, 43, 47, 53, 55 et 59) matérialisé par autant de picots. Soit N le nombre à factoriser. On utilise la relation $N = x^2 - y^2$ et l'on cherche les conditions que doit remplir x pour que y^2 soit un carré parfait. Si des valeurs permises de x sont 1, 7, 8, 13, 14 et 20 modulo 21, on place un capuchon métallique sur les picots n° 1, 7, 8, etc. de la couronne 21. De même pour les autres couronnes utilisées. On tourne

la manivelle et quand les capuchons métalliques (les plots noirs) des différentes couronnes sont alignés, un contact électrique s'établit sous la barrette métallique, et un signal retentit. Le nombre indiqué sur le cadran a alors des chances d'être un carré parfait. La machine factorise des nombres de treize chiffres en moins de 18 minutes, tâche qui demanderait plusieurs jours à la main.

Cette machine a permis à Carissan, en tournant la manivelle pendant dix minutes, de prouver que 708 158 977 est un nombre premier.

Documentation Arts et Métiers (Pour la Science Janvier 1998)

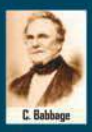
Machine à résoudre les congruences des frères Carissan (en cours de remontage).
Construite entre 1913 et 1919 en laiton, fer et bois, de dimension 31 x38 cm par la société Chateau Frères, Horlogers, Constructeurs Machines à calculer, France Paris rue Montmartre, sur les plans d'Eugène et Pierre Carissan, cette machine a rejoint la collection des instruments scientifiques du Musée des Arts et Métiers.


J. César


Al-Kindi


B. de Vigenère


L. Euler


C. Babbage


A. Turing


C.E. Shannon


R. Rivest


L. Adleman


A. Shamir


C. Bennett


G. Brassard

Cryptographie et codages

Chiffrement RSA

Trois mathématiciens, Rivest, Shamir et Adleman ont proposé en 1978 un algorithme de chiffrement asymétrique à clés publiques performant.

Principe du chiffrement RSA

Alice choisit deux nombres premiers p, q et un nombre entier quelconque d ;
p, q et d sont ses clés secrètes.

Elle publie dans un annuaire accessible à tous deux entiers n et e ;
n et e sont les clés publiques.

n et e sont calculées ainsi :
$n = pq$ et $ed \equiv 1 \pmod{(p-1)(q-1)}$

Bob veut envoyer un message à Alice, il le code sous la forme d'un entier M

M est le clair numérique

Pour chiffrer M, Bob consulte l'annuaire pour connaître n et e.
A l'aide de son logiciel, il calcule $M^e \bmod n = C$
et envoie C.

A la réception, pour déchiffrer C, Alice utilise la clé secrète d
elle calcule M ainsi $C^d \bmod n = M$

car $C^d \equiv M^{ed} \equiv M^{k(e-1)(q-1)+1} \equiv M \pmod{n}$

Alice choisit $p = 971$, $q = 977$ et $d = 841\,529$ et publie les données $n = pq$ et $e = 9$
Bob code le message *rendez-vous vendredi soir* en remplaçant les lettres par les nombres correspondants a=00, ..., z=25, il obtient :

REN	DEZ	VOU	SVE	NDR	EDI	SOI	R
170413	030425	211420	182104	130117	040308	181408	17

il calcule :
$170413^9 \bmod 948667 = 947481$
$030425^9 \bmod 948667 = 909875$
$211420^9 \bmod 946667 = 535838$ . . .

Le message chiffré transmis à Alice est :
947481 909875 535838 573617 905809 658606 032768 890073

A la réception Alice retrouve les nombres de départ
$947841^{841529} \bmod 948667 = 170413$
$909875^{841529} \bmod 948667 = 030425$
$535838^{841529} \bmod 948\,667 = 211420$ . . .

En remplaçant les lettres par les chiffres correspondants elle découvre le message de Bob.

La sécurité du chiffrement RSA repose sur la difficulté à déterminer la factorisation d'un grand nombre en deux nombres premiers.

5

Panneau 5
Chiffrement RSA

Principe du Chiffrement RSA

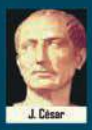
R S A pour Rivest, Shamir et Adelman est une méthode de chiffrement inventée en 1978 aux Etats-Unis, par trois mathématiciens Ronald Rivest, Adi Shamir et Léonard Adleman.
La méthode de chiffrement RSA permet à Alice de recevoir des messages chiffrés qu'elle seule pourra déchiffrer grâce à une clé secrète (p, q, d).
Pour envoyer des messages chiffrés à Alice, on, c'est-à-dire tout le monde, dispose d'une clé publique (n et e).

Le RSA en « termes simples » :
Celui qui veut mettre en place un chiffrement RSA (Alice par exemple) choisit:
deux grands nombres premiers p et q et calcule les trois entiers n, e, d ainsi :
n = pq et (ed-1) multiple de (p-l)(q-1).
p, q et d sont les clés secrètes que seule Alice connaît.
Tout le monde (Bob par exemple) peut crypter avec n et e ; **n et e sont les clés publiques.**
Le message M devient C ; C est le reste dans la division de M par n
Pour décrypter (Alice, seule, peut le faire) il faut connaître d qui dépend de p et q.
Le message crypté C devient M' : M' est le reste dans la division de C^e par n
Or M'= M d'après le théorème de Fermat-Euler
En fait, seul d est important, mais si on ne connaît pas p et q facteurs premiers intervenant dans la décomposition de n, on ne peut pas calculer d. **Donc plus on choisit p et q grands, plus la méthode de chiffrement est inviolable.**

On peut essayer sur un exemple numérique simple :
p = 3; q = 5; n = 15; (p - 1)(q - 1) = 8; Alice choisit d premier avec 8, par exemple d = 3.
Elle calcule e = 11 car 3 x 11 ≡ 1 (mod 8) clé secrète : (p = 3, q = 5, d = 3);
clé publique (n = 15, e = 11).
Bob veut envoyer M = 2 à Alice; en fait Bob envoie C = 8 car 2^{11} (mod 15) = 8.
Alice calcule $c^3 = 8^3 = 512 = 34 \times 15 + 2$ et on obtient $2 = 8^3$ mod 15 : M est bien 2.
Sur l'exemple«rendez-vous vendredi soir», le dernier bloc ne comporte que les chiffres 1 et 7. En pratique, on le complète par des chiffres quelconques : on dit qu'on «pacte». Après déchiffrement, le lecteur délaisse de lui-même les lettres ainsi introduites.

Pour décrypter ...
On explique ici la difficulté de décrypter liée à celle de trouver la décomposition en facteurs premiers d'un grand nombre, **l'entier n** ci-dessus qui **est appelé nombre RSA.**

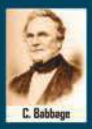
Pour en savoir davantage, vous pouvez vous reporter au dossier de Pour la Science intitulé« L'art du secret» de juillet-octobre 2002 et consulter, entre autres, les sites Internet ci-dessous :
http://rsasecurity.cm/rsalabs/challenges
http://parodie.com/monetique/revuepresse.htm


J. César


Al-Kindi


B. de Vigenère


L. Euler


C. Babbage


A. Turing


C.E. Shannon


R. Rivest


L. Adleman


A. Shamir


C. Bennett


G. Brassard

Cryptographie et codages

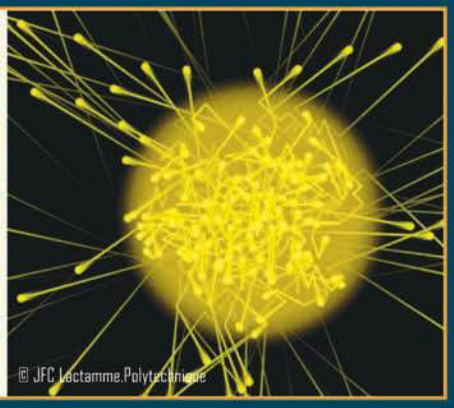
L'aventure quantique

En 1984, deux chercheurs canadiens, Charles Bennett et Gilles Brassard eurent l'idée d'utiliser les propriétés de la décomposition de la lumière en particules élémentaires, les photons (*fos* en grec veut dire *lumière*).

La cryptographie quantique ou distribution quantique de clés désigne un ensemble de procédures qui permet de transmettre en toute sécurité une clé secrète de chiffrement.

Il s'agirait de trouver un procédé cryptographique permettant de résister au futur et encore improbable ordinateur quantique

Cette clé peut être ensuite utilisée dans un autre type de chiffrement hautement sécurisé.



Principe de la cryptographie quantique

Un photon se propage dans l'air dans des directions de vibration - ou polarisation - différentes que l'on réduit à quatre pour simplifier 0°, 45°, 90° et 135°.

Bennett et Brassard attribuent aux polarisations 0° et 45° le bit 0 et aux deux autres, 90° et 135° le bit 1.

L'émetteur envoie une suite de photons polarisés aléatoirement.
Le récepteur les fait passer soit par un filtre polarisant rectiligne orienté à 0°
soit par un filtre polarisant diagonal orienté à 45°.

Si le filtre est rectiligne, les photons orientés à 0° le traversent, ceux à 90° sont stoppés
mais les photons orientés à 45° ou 135° sont stoppés une fois sur deux.

Si le filtre est diagonal, les photons orientés à 45° le traversent et ceux à 135° sont stoppés
mais les photons orientés à 0° ou à 90° sont stoppés une fois sur deux.

Le récepteur derrière le filtre note 0 si le photon traverse et 1 si ce n'est pas le cas.
Pour éliminer les cas d'incertitude, le récepteur donne l'orientation de son filtre à l'émetteur ;
s'il diffère de l'orientation à l'émission le bit envoyé est incertain donc supprimé.

La clé transmise est la suite des bits conservés.

Une interception malhonnête du flux de photons ne permet donc pas de reconstituer l'intégralité de la clé.

Emission	0°	45°	90°	45°	0°	135°	90°	0°
Bit envoyé	0	0	1	0	0	1	1	0
Filtre de réception	diagonal	diagonal	rectiligne	diagonal	rectiligne	rectiligne	rectiligne	diagonal
Traversé ?	non	oui	non	oui	oui	non	non	non
Bit reçu	1	0	1	0	0	1	1	1
Clef	X	0	1	0	0	X	1	X

Exemple d'émission de photons, de réception et de clé obtenue

La cryptographie quantique a quitté le domaine de la recherche pour atteindre celui du développement et de la commercialisation. Les difficultés restent nombreuses ; vitesse et distance de transfert restent limitées et dans le monde sensible de la cryptanalyse, le secret reste toujours de rigueur !

6

Panneau 6
L'aventure quantique

En 1900, Max Planck suggère que les ondes électromagnétiques évoluent par paquets ou quanta. On parle dès lors de mécanique quantique. Dans les années trente, Werner Heisenberg découvre que l'observation de ces corpuscules est difficile car toute mesure exige de leur fournir une énergie et cette énergie modifie leurs propriétés. Autrement dit, l'observation modifie l'objet observé !

L'idée essentielle de la cryptographie quantique est de créer un canal de communication au sein duquel toute interception fausse le message. Ce canal est utilisé pour transmettre la clef de codage qui est aussitôt essayée sur un message convenu d'avance.
Pour réaliser cette idée, on utilise une propriété des photons polarisés. Chaque photon peut être polarisé, c'est-à-dire que l'on peut imposer une direction à son champ électrique. La polarisation est mesurée par un angle qui varie de 0° à 180°. Dans le protocole de cryptographie que nous décrivons dans le panneau, la polarisation prend quatre directions : 0°, 45°, 90°, 135°. Pour détecter la polarisation des photons, on prend un filtre polarisant suivi d'un détecteur de photons…

Historiquement, le premier succès réel du prototype qui implante toutes ces idées a eu lieu le 27 février 1991. Ce jour là, environ 715 000 impulsions d'intensité moyenne (0,12 photon par impulsion) ont été transmises entre deux interlocuteurs. Cet essai est certes encourageant mais limité en distance – sur 32cm- et en vitesse -1bit par seconde- ! *

Une des propriétés les plus prometteuses de l'information quantique est qu'elle peut être simultanément en deux états différents. C'est ce qu'on appelle le principe de superposition. Sous certaines conditions, un électron, par exemple, peut être simultanément sur deux « orbitres » différentes du même atome. On dit alors qu'il est dans un état superposé…
Ce phénomène de superposition pourrait avoir des conséquences révolutionnaires dans la conception des ordinateurs quantiques. En utilisant des particules dans des superpositions de plusieurs états simultanément, un tel ordinateur pourrait parvenir à trouver la réponse à des problèmes extrêmement complexes dans un temps record ; d'autant plus vite que le problème est difficile !
Mais l'avenir de l'ordinateur quantique est encore incertain, laissons donc la conclusion (provisoire) à Gilles Branssard : « *Mais si l'on découvre un jour que l'ordinateur quantique n'est pas faisable, cela nous aura tout de même permis d'apprendre de nouvelles lois physiques* »

Extraits d'un article de Chérif Zananiri
Bibliothèque Tangente n°26 Cryptographie et Codages

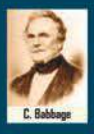
*En Février 2002, Nicolas Gisin et ses collègues, chercheurs à l'Université de Genève ont réussi à transmettre un message sur un canal entièrement sécurisé entre Genève et Lausanne (67 km)

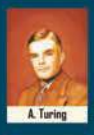

J. César


Al-Kindi


B. de Vigenère


L. Euler


C. Babbage


A. Turing


C.E. Shannon


R. Rivest


L. Adleman


A. Shamir


C. Bennett


G. Brassard

Cryptographie et codages

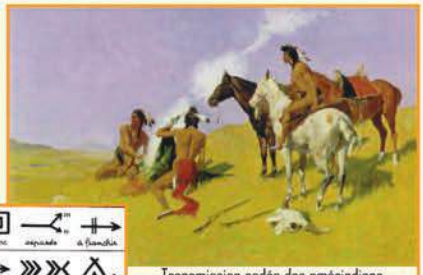
Codes d'hier et d'aujourd'hui

Théoriquement la cryptographie utilise la substitution au niveau des lettres avec la volonté de cacher le message alors que le codage utilise la substitution au niveau des mots ou des phrases et un «livre des codes» en donne en principe la signification.

En pratique il arrive que le langage courant confonde ces deux mots car la différence est parfois subtile. La confusion entre chiffre et code n'est pas bien grave…

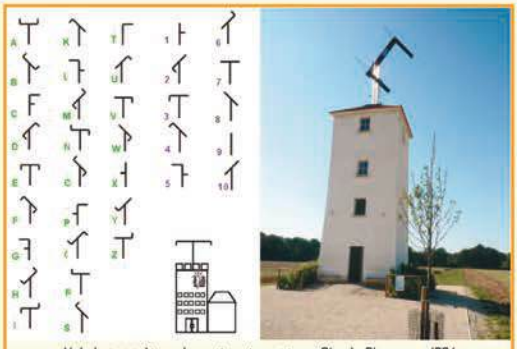

Le code de l'éventail
XVIII[e] et XIX[e] siècles
Peinture de P.A. Renoir

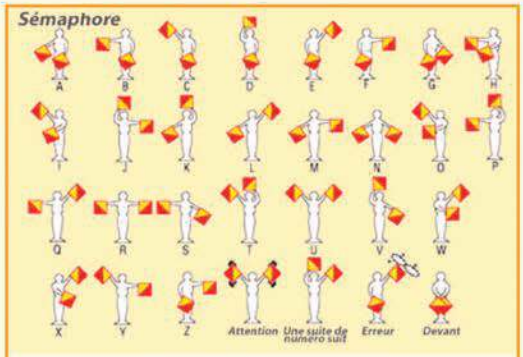
Quelques signaux du code de la route


Transmission codée des amérindiens
Peinture de Frederic Remington


Quelques signaux du code
maritime international


Signes de piste Scouts
Mouvement fondé par Baden Powell en 1907


Alphabet et télégraphe optique inventé par Claude Chappe en 1794
La France fut pourvue en quelques années d' un réseau de 5 000 km.
Ci-contre une tour du télégraphe à Marly-le-Roi



Signaux à bras utilisés dans la marine
avant l'apparition de la radio

Alphabet international Morse.
Ci-dessous Samuel Morse, peintre américain, développeur en 1837
de l'alphabet qui porte son nom et du télégraphe électrique.

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

Exemple de code QR (Quick Reponse), inventé en 1999, contenant plus d'informations qu'un code barre.

Destiné à être lu par un lecteur de code-barres, un téléphone mobile, un smartphone, ou une webcam, ses données sont directement reconnues par des applications : internet, commande, paiement, etc.

Ensemble nous sommes plus fort pour faire aimer les mathématiques est ainsi codé :

Panneau 7
Codes d'hier et d'aujourd'hui

Dans le langage courant on confond souvent cryptographie et codage. Ce n'est pas bien grave mais pour plus de clarté dans le développement de cette exposition et pour justifier ce panneau nous distinguons ainsi cryptographie et codages.

En cryptographie on transforme un message M, **avec la volonté de le cache**r, en un message M' que l'on transmet sans qu'il soit possible en théorie à quiconque qui n'a pas la « clé » de comprendre M à travers M'.

En codage, le message M est transformé en M' selon un système connu, M' étant supposé plus facile à transmettre que M.

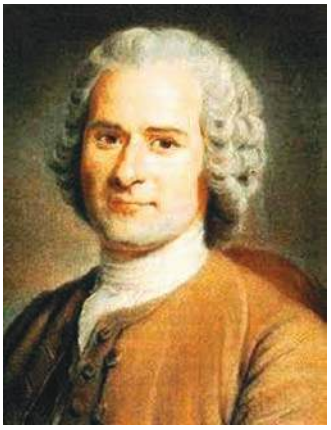
Les systèmes de signalisation optique :
Le phare d'Alexandrie projetait ses feux en mer jusqu'à 55 km environ pour signaler le port !

Le télégraphe Chappe : En 1793, le français Claude Chappe inventa, un système de signalisation optique qui permettait d'envoyer des messages de tour en tour. Les frères Chappe réalisèrent le 3 mars 1791 une première expérience publique de télégraphe aérien de Brûlon à Parcé sur une distance de 14 km. Les télégraphes aériens furent adoptés le 26 juillet 1793 par la Convention Nationale. Le 16 juillet 1794 la première ligne officielle Paris-Lille fût mise en service. En quelques années, 5000 km de réseau et près de 533 stations étaient mis en place, couvrant une partie importante du territoire français.

Le système Sémaphore (sêma : signe et phoros : qui porte) s' utilise avec un drapeau dans chaque main. Il est encore utilisé sur les voies ferrées, dans les aéroports et … chez les scouts !

Le code Morse est un précurseur des communications numériques. Ce langage code chaque lettre de l'alphabet par des signaux brefs (les points) et des signaux longs (les traits). Les signaux peuvent être transmis par des signaux lumineux, sonores ou radio. En 1838, nait l'alphabet Morse.
Le premier signal de détresse SOS fut utilisé par le Titanic en détresse le 15 avril 1912.
Le réseau télégraphie Morse tissa les « routes de l'information » du XIX^{ème} siècle.
Pourtant dès mars 1876, Alexandre Bell inventait le téléphone et dès 1927 Marconi réalisait la première transmission radiotéléphonique transatlantique. A partir de là , la phonie concurrence la télégraphie.
Aujourd'hui le Morse n'est plus guère en vogue que chez les radioamateurs.

Un code pour noter la musique, bien peu connu…



On connait l'œuvre de Rousseau, philosophe et écrivain mais on ignore souvent qu'il fut d'abord un musicien autodidacte. Autodidacte est sûrement le mot qui caractérise le mieux Rousseau. Jean-Jacques est réfractaire, depuis ses premières années d'apprentissage, à toute forme d'enseignement autoritaire ; il a un rapport au savoir très personnel. Rousseau veut donner à l'homme le moyen de retrouver sa liberté. Il a la farouche volonté de diffuser tous ces savoirs qu'il a du mal à appréhender et il cherche des moyens pédagogiques efficaces pour y parvenir.

L'exemple de la musique est au regard de tout cela très significatif.

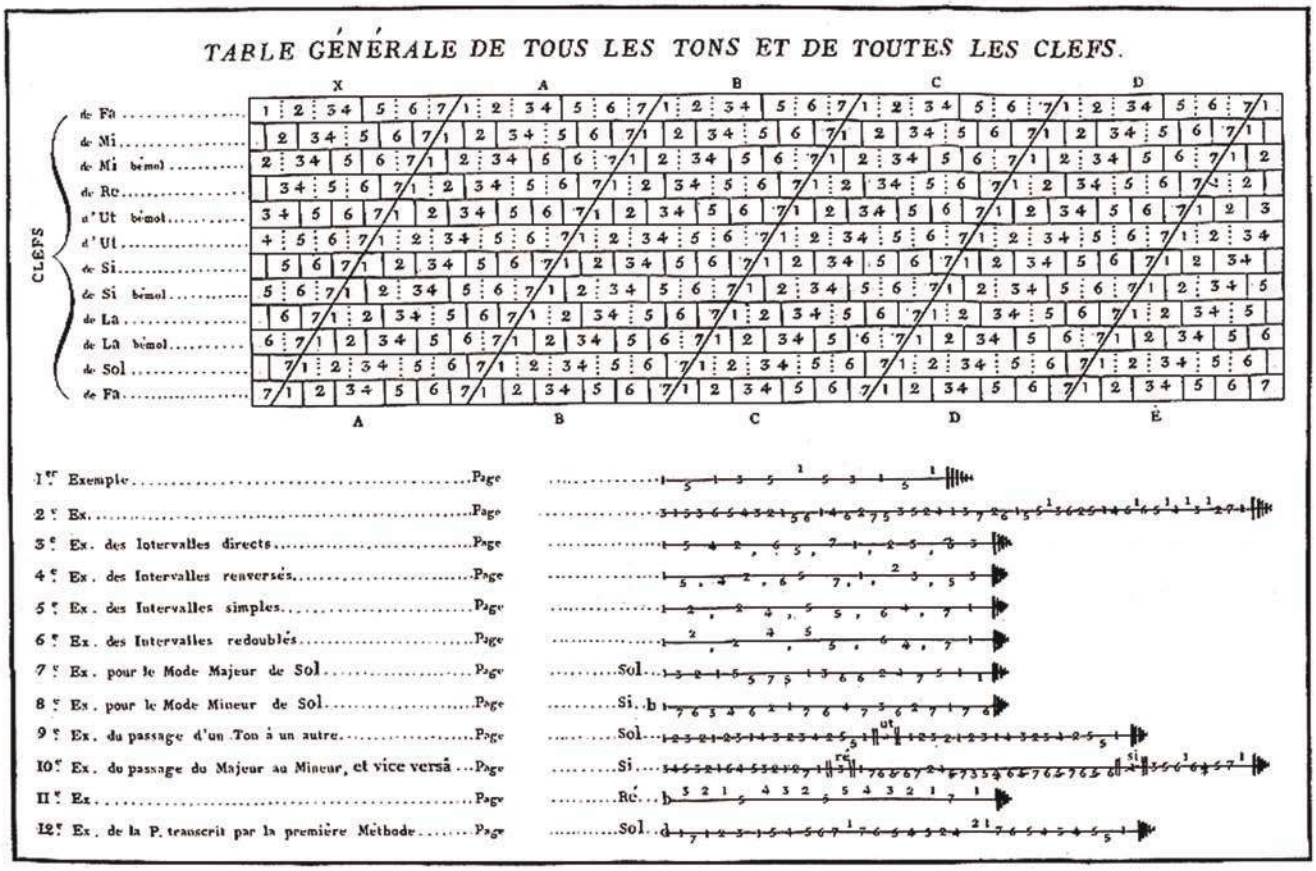
Jean Jacques n'est pas d'une famille de musiciens et il aura « *le plus grand mal à apprendre à déchiffrer la note* ». Pourtant son premier travail de copiste en musique va l'inciter à composer des mélodies. Et quand, installé chez madame de Warrens, il veut lui venir en aide pour l'aider à « briller dans la république », il pense en savoir assez pour mettre au point un système de notation chiffrée pour noter la musique.

Il propose à l'Académie des sciences à Paris le 22 aout 1742, à l'âge de 30 ans , un projet concernant de nouveaux signes pour la musique.

Le système est présenté dans

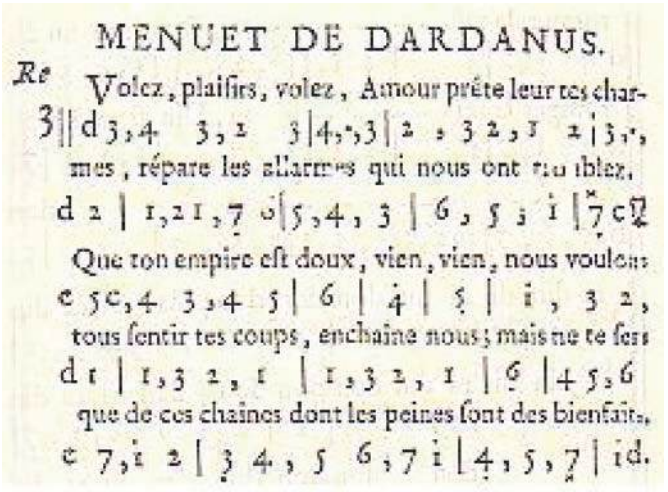
la Table générale de tous les tons et de toutes les clefs.

Rousseau, Dissertation, 140



Il peut se résumer ainsi : 7 chiffres 1, 2, 3, 4, 5, 6 et 7 correspondent aux 7 notes ut, ré, mi, fa, sol, la , si. Quand il faut sortir de l'octave, un point est placé au dessus de la note qui monte hors de l'octave (on y reste jusqu'au point suivant) , comme un point inférieur placé sous la note permet de descendre à l'octave inférieure. Les octaves sont marquées par des lettres et le ton du morceau par des chiffres, le tout placé dans la marge. Ainsi d3 signifie le mi de la 4ème octave …

Ce système de notation chiffrée reçoit un accueil très mitigé. Rameau par exemple tout en reconnaissant « vos signes sont très bons en ce qu'ils déterminent simplement et clairement les valeurs… » mais dit-il « ils sont mauvais en ce qu'ils exigent une opération de l'esprit qui ne peut toujours suivre la rapidité de l'exécution ».


MENUET DE DARDANUS.

Re Volez, plaiſirs, volez, Amour prête leur tes charmes, répare les allarmes qui nous ont troublez,
Que ton empire eſt doux, vien, vien, nous voulons tous ſentir tes coups, enchaine nous; mais ne te ſers que de ces chaines dont les peines ſont des bienfaits.

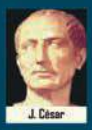
Il semble en effet que ce codage soit mal adapté à cette musique savante, en orchestre symphonique, que du reste Rousseau n'appréciait pas.
Cette méthode fut utilisée en France, sous le nom de méthode Rousseau- Julien Chevet, à la fin du 19ème siècle , à la même période au Japon et encore de nos jours, semble-t-il, en Chine …

Sources :
Tome V des œuvres de Rousseau dans la collection de la Pléiade « Ecrits sur le musique, la langue et le théâtre »
Bibliothèque d'études rousseauistes Montmorency (95160)

Extrait du code de l'éventail du XVIIIe et XIXe siècle

…
Ouvrir complètement l'éventail : *j'y songe.*
Bailler derrière son éventail : *va-t-en, tu m'ennuies !*
Effleurer son oeil droit de son éventail fermé : *quand te verrai-je ?*
Menacer de l'éventail fermé : *ne sois pas trop audacieux.*
Cacher ses yeux derrière son éventail : *je t'aime.*
Poser l'extrémité de l'éventail sur sa bouche : *attention, on nous écoute.*
Appuyer son menton sur son éventail fermé : *je boude.*
Agiter vers soi son éventail ouvert : *danse avec moi.*
Suspendre son éventail fermé à sa main droite : *au revoir.*

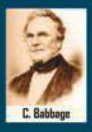
…


J. César


Al-Kindi


B. de Vigenère


L. Euler


C. Babbage


A. Turing


C.E. Shannon


R. Rivest


L. Adleman


A. Shamir


C. Bennett


G. Brassard

Cryptographie et codages

Principe des codes correcteurs d'erreurs

Comment être sûr de l'exactitude d'un message reçu ?

L'émetteur envoie un signal S sans erreur.

Le signal S est transmis par un canal générateur de *bruit*. S peut être déformé.

Le récepteur reçoit le message S déformé c'est à dire un autre message S'

Pour retrouver le message S à partir de S'
on envoie des informations supplémentaires.

L'enjeu est de retrouver l'information contenue dans le message émis en ajoutant le minimum d'informations supplémentaires dans un mot de longueur donnée, tout en corrigeant, ou au moins en détectant, un maximum d'erreurs.

Exemples de codes utilisés dans la vie courante

Numéro INSEE (Institut National de la Statistique et des Etudes Economiques)

1	42	09	36	233	066	96
1 pour un homme 2 pour une femme	Année de naissance	Mois de naissance	Département de naissance	commune de naissance	numéro sur le registre d'état civil	clé

Pour déterminer la clé, on divise par 97 le nombre formé par les treize premiers chiffres, on obtient un reste r. La clé vaut $97- r$

Identité Bancaire

10071	87000	00000021616	44
code de la banque (5 chiffres)	Editeur (un bloc de chiffres)	Numéro de compte (11 chiffres)	clé

Pour déterminer la clé, on divise par 97 le nombre formé par les vingt et un premiers chiffres, on obtient un reste r. La clé vaut $97- r$

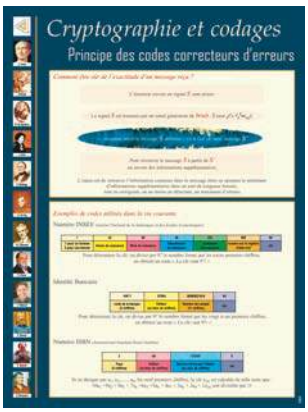
Numéro ISBN (International Standard Book Number)

2	09	172187	5
Pays (5 chiffres)	Editeur (un bloc de chiffres)	Numéro donné par l'éditeur (un bloc de chiffres)	clé

Si on désigne par a_1, a_2,.....a_9, les neuf premiers chiffres, la clé a_{10} est calculée de telle sorte que :
$10a_1 + 9a_2 + 8a_3 + 7a_4 + 6a_5 + 5a_6 + 4a_7 + 3a_8 + 2a_9 + 1a_{10}$ soit divisible par 11

Panneau 8

Principes des codes correcteurs d'erreurs



Quand on envoie un message, on met une information supplémentaire (encore appelée clé, sans rapport avec les clés de chiffrement en cryptographie) ; on dit encore qu'on encode le message.

L'ensemble des mots encodés constitue le **«code correcteur d'erreurs»**.

Grâce à cette information, on peut vérifier si le message (généralement numérique) est correct : elle permet en effet de détecter et éventuellement de corriger une erreur dans le message émis.

On montre dans ce panneau comment sont utilisés quelques codes correcteurs d'erreurs.

Dans les trois exemples décrits dans ce panneau, on calcule des clés (qui n'ont rien à voir avec les clés utilisées en cryptographie). Ces clés sont des ***«détecteurs»*** d'erreurs. Cependant, quand il n'y a pas d'erreur détectée, il peut malgré tout y en avoir une (et même au moins deux, un peu comme pour la preuve par 9).

Pour le numéro d'ISBN, on peut apporter quelques précisions:
L'ISBN-International Standard Book Number est le **numéro d'identification international normalisé des livres**.
Il est composé de 10 chiffres répartis en 4 zones.
- zone 1 : un ou deux chiffres. Cette première série de chiffres est le numéro d'identification du groupe national, géographique ou linguistique où le livre est publié. Les publications du groupe francophone commencent toujours par le chiffre 2.
- zone 2 : groupe de deux à sept chiffres. Cette série représente le numéro d'identification de l'éditeur qui a publié le livre, le numéro est « inversement proportionnel» à l'importance de l'éditeur. Ce numéro est attribué par une agence du groupe : pour les pays francophones, 1 'AFNIL (Agence Francophone pour la Numérotation Internationale du Livre).
- zone 3 : groupe de deux à sept chiffres. Cette série représente le numéro d'identification du titre dans la production de 1' éditeur : ce numéro comporte d'autant plus de chiffres que l'éditeur est important, il est attribué par l'éditeur.
- zone 4 : un chiffre de contrôle (la clé) destiné à tenter de vérifier 1' exactitude des indicatifs précédents. Quand le reste est 10, on le représente par le « chiffre » X.

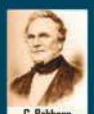
Voici un exemple non traité sur le panneau : il s'agit du **numéro d'affiliation à la Fédération Française de Bridge.**
Le numéro est composé de 7 chiffres « abcdefg », le septième, g, étant la clé, calculée de telle sorte que le nombre a+2b+c+2d+e+2f+g soit divisible par 10. Si on permute deux chiffres consécutifs, on décèle 1 'erreur. Bien sûr, si on permute par exemple a et c, l'erreur n'est pas détectée, mais ce type de permutation est moins probable.


J. César


Al-Kindi


B. de Vigenère


L. Euler


C. Babbage


A. Turing


C.E. Shannon


R. Rivest


L. Adleman


A. Shamir


C. Bennett


G. Brassard

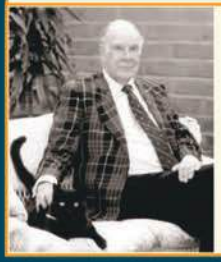
Cryptographie et codages

Codes correcteurs d'erreurs numériques

Comment détecter, éviter et même corriger des erreurs dans la transmission des données ?

A l'heure du numérique, la transmission d'informations se fait par l'envoi successif de bits égaux à 0 ou à 1. Rien ne semble plus simple …pourtant les sources d'erreurs de transmission sont nombreuses.

Dès 1950, Richard Wesley Hamming, propose une solution à ces problèmes et sa méthode est toujours d'actualité.



Richard Hamming reçoit sa licence à l'université de Chicago en 1937, sa maîtrise à l'université du Nebraska en 1939 et enfin son doctorat à l'université de l'Illinois en 1942. Il enseigne à l'Université de Louisville lorsque la Seconde Guerre mondiale débute. Il est appellé à rejoindre le projet Manhattan en 1945. Il programme l'un des premiers calculateurs digitaux qui permettra aux physiciens nucléaires du projet de calculer les solutions de leurs équations.

Après la guerre il travaillera avec Shannon chez Bell et proposera des systèmes de codes correcteurs d'erreur qui sont encore utilisés aujourd'hui pour restituer au mieux images et sons numériques.

Le principe de base

Pour détecter et éventuellement corriger l'information transmise sous forme d'une succession de bits, on y introduit une information de contrôle calculée sur la parité du nombre de bits 1 envoyés

Bit de parité

On sectionne l'information à transmettre en paquets de n bits. A chaque paquet de n bits constituant un morceau de notre message, on ajoute un $n+1^{ème}$ bit (le bit de parité) de sorte qu'il y ait en tout un nombre pair de bit 1.

Par exemple **0101110** devient 0101110 **0** et 0101100 devient 0101100 **1**

Tableau de parité

On sectionne l'information à transmettre en paquets de n^2 bits en faisant un tableau de n lignes et n colonnes. On complète ce tableau constituant donc un morceau de notre message d'une $n+1^{ème}$ ligne et d'une $n+1^{ème}$ colonne de sorte que chaque ligne et chaque colonne présentent un nombre pair de 1

Par exemple

1	0	1		1	0	1	0
1	1	1	devient	1	1	1	1
0	1	1		0	1	1	0
				0	0	1	1

Codage de Hamming

On sectionne l'information à transmettre en paquets de 2^{n-1} bits et le message contrôlé comportera des paquets de 2^n bits .
Exemple : transmettons des octets en choisissant n = 3. Pour chaque octet nous allons numéroter les bits de 0 à 7 en allant de droite à gauche.

- Le bit 0 va contrôler la parité de l'octet
- Les bits 1, 2 et 4 (correspondant aux puissances de 2) sont des bits de contrôle du message
- Les bits 3, 5, 6 et 7 seront les bits contenant l'information à transmettre. Comment calculer les bits 1, 2 et 4 ?

Ils doivent contrôler les bits 3, 5, 6 et 7 et on a 3 = 2 + 1 ; 5 = 4 + 1 ; 6 = 4 + 2 ; 7 = 4 + 2 + 1
Pour trouver la valeur du bit 1, on regarde les bits 3, 5 et 7 ; le bit 1 contrôle la parité de ces trois bits
Pour trouver la valeur du bit 2, on regarde les bits 3, 6 et 7 ; le bit 2 contrôle la parité de ces trois bits
Pour trouver la valeur du bit 4, on regarde les bits 5, 6 et 7 ; le bit 4 contrôle la parité de ces trois bits

Bits de l'octet	7	6	5	4	3	2	1	0
Message		**1**	**1**	**0**		**1**		

Bits de l'octet	7	6	5	4	3	2	1	0
Message envoyé	**1**	**1**	**0**	**0**	**1**	**1**	**0**	**0**

Le **code de Hamming** est plus efficace que le **tableau de parité** lorsqu'on travaille avec un grand nombre de bits à transmettre. Cependant les démarches utilisées pour contrôler les transmissions des données numériques sont plus sophistiquées et utilisent des outils d'algèbre linéaire difficiles….

9

Panneau 9

Codes correcteurs d'erreurs numériques

Codes correcteurs d'erreurs en transmission de données numériques.

Les codes correcteurs sont utilisés dans les transmissions de données.
Dans les réseaux informatiques, le code correcteur utilisé est facile à comprendre.

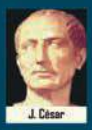
Dans la norme ASCII, les lettres sont codées sur 7 bits.
Par exemple : pour A : 1000001 - Pour a : 1100001
Mais on envoie des blocs de 8 bits. Le 8ème bit est alors calculé pour que le bloc contienne un nombre pair de 1, c'est un « bit de parité pair ».
Par exemple : pour A : 1000001 **0** - pour a : 1100001 **1**

La transmission des clés secrètes en cryptographie.

Pour transmettre les clés secrètes, on commence par les chiffrer avec des algorithmes à clés publiques. Les messages numériques ainsi obtenus sont ensuite« encodés», avec un code correcteur d'erreur, pour être transmis.
Dans tous les exemples traités, on a surtout vu comment on détecte les erreurs ; pour les corriger, c'est plus difficile mais on peut essayer d'expliquer sur un exemple simple comment on détecte et on corrige une erreur.

On code le mot 0 par 000 et le mot 1 par 111. On construit ainsi un code comportant les deux mots 000 et 111. Supposons que lors de la transmission d'un code, on fasse au plus une erreur. Alors, lors de la transmission du mot 000, on peut recevoir un des mots de l'ensemble A_0 *= {000, 100, 010, 001}*
Et lors de la transmission du mot 111, on peut recevoir l'un des mots de l'ensemble A_1 *= { 111, 011, 101, 110}.*
Les deux ensembles A_0 *et* A_1 *forment une partition de l'ensemble des mots de trois chiffres écrits avec 0 et 1. Ainsi quand on reçoit l'un quelconque des mots de* A_0 *, on le corrige si nécessaire en 000 ; de même pour* A_1 *en 111.*

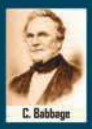
On peut aussi construire un exemple simple de code permettant de corriger une erreur et aussi d'en détecter deux sans pouvoir cependant les corriger.
On souhaite transmettre les mots 00, 01, 10 et 11 en les encodant :
00 par 1111 1111
01 par 0000 0000
10 par 0000 1111
11 par 1111 0000
Il est clair qu'on peut détecter et corriger une erreur sur un seul bit (exemple : dans le nombre 1011 1111 le 0 est faux, on devrait lire 1).
Supposons que lors de la transmission, deux erreurs soient commises, par exemple:
on reçoit 0011 0000 alors que 0000 0000 a été envoyé.
On détecte qu'il y a deux erreurs (en effet on suppose toujours que le nombre d'erreurs est petit ...). Mais pour corriger, on a deux candidats : 0000 0000 mais aussi 1111 0000.
Donc on ne peut pas corriger...


J. César


Al-Kindi


B. de Vigenère


L. Euler


C. Babbage


A. Turing


C.E. Shannon


R. Rivest


L. Adleman

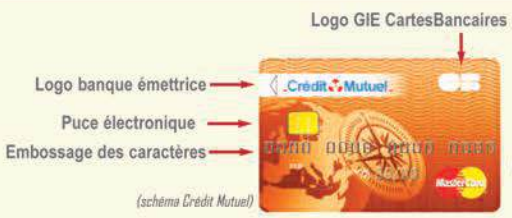

A. Shamir


C. Bennett


G. Brassard

Cryptographie et codages

La carte bancaire



1967 - Le système de paiement par carte est introduit en France avec la Carte Bleue.
1971- Apparition de la piste magnétique et possibilité de retrait dans des distributeurs automatiques de billets (DAB).
1992 - Sécurité renforcée par l'adoption de la puce électronique. La fraude est divisée par trois.
2000 - Adoption du cryptogramme visuel pour sécuriser les achats en ligne.

3 façons, selon les pays, d'utiliser la carte, de la moins sécurisée à la plus sécurisée.

Embossage : Les caractères en relief forment des bosses permettant des copies carbonne à l'aide d'une machine familièrement appelée *fer à repasser.*

Lecture de la piste magnétique : l'utilisation la plus répandue au monde.

Lecture de la puce électronique : l'utilisation la plus répandue en France, donnant un maximum de sécurité.

Puce, vous avez dit puce ?

La puce est née en 1974 de l'idée géniale de l'inventeur français Roland Moreno qui déposa plusieurs brevets relatifs à certains dispositifs contrôlant l'accés à l'information portée par les cartes.
La puce est en fait un tout petit ordinateur nanti d'un microprocesseur et d'une mémoire persistante pouvant enregistrer plusieurs fichiers. Elle permet de lire ou recevoir des données, de les mettre en mémoire. Elle comporte aussi divers dispositifs de calculs destinés entre autres à la cryptographie DES (*Data Enscription Standard*), AES *(Advanced Encryption Standard)*, RSA, ... La France joue un rôle précurseur sur tout ce qui touche les puces et leurs applications.

Mathématiques de transmission

Les mathématiques interviennent dans la sécurité des transactions à trois niveaux :

Vérification de l'authenticité de la carte bancaire par signature RSA

Identification du porteur par son code Pin *(Personal Identification Number)*

Demande d'accord auprès du centre de paiement par authentification DES *(Data Encryption Standard)*

(schéma GIE CB)

Le code DES

Le *Data Encryption Standard* (DES) est né en mars 1978. Les messages sont des suites de bits (de 0 et de 1) tronçonnées en mots de 64 bits. Le DES opère sur un mot M ; il en fait d'abord une permutation initiale pour obtenir M_0 puis scinde M_0 en deux parties, une gauche G_0 et une droite D_0 ; il calcule M_1 en deux parties G_1(G_1=D_0) et D_1 (D_1= G_0 + f(D_0,K_0), K_0 étant une partie de la clé utilisée) puis DES réitère 16 fois cette opération ….Dès la fin des années 1990, DES n'était plus considéré comme un algorithme assez sûr. Pour pallier à ses faiblesses, on a mis en place un système de chiffrement qui enchaîne trois applications successives du système DES (le triple DES) sur le même bloc de données de 64 bits avec 2 ou 3 clés différentes.

10

Panneau 10
Cartes bancaires

La carte bleue dans tous ses états

Documentation : Groupement d'Intérêt Economique-Carte Bancaire

Trois types de fraudes

La fraude aux cartes de paiement peut se définir comme l'utilisation d'une carte par une personne qui n'en est pas le titulaire légitime. Trois cas de figure se présentent :

- L'utilisation par un tiers d'une carte perdue ou volée ;
- La contrefaçon d'une carte ;
- L'utilisation des identifiants de la carte (numéro, date d'expiration…) par une autre personne que le titulaire et que celui-ci est toujours en possession de sa carte. Ce type de fraude concerne la vente à distance.

Les cas de contrefaçon concernent la piste magnétique de la carte. En effet, la reproduction de la piste peut permettre une utilisation frauduleuse dans les pays où la technologie de la carte à puce n'est pas utilisée. La copie de la piste magnétique - soit par une personne malveillante, soit grâce à un dispositif placé sur le terminal de paiement ou sur le DAB - est connue sous le nom de "skimming".

Lutter contre la fraude

Pour lutter efficacement contre la fraude, il est nécessaire de bénéficier d'un maximum d'informations et d'être réactif.

Détecter et caractériser les fraudes

Le système CB dispose d'une base de données alimentées en permanence : le Système d'Information Cartes Bancaires (SICB). Cet outil est essentiel pour caractériser le plus finement possible les fraudes constatées (mode opératoire, lieu, etc.). Il permet également de détecter très rapidement des opérations potentiellement suspectes, par exemple des retraits inhabituels dans un pays étranger où le niveau de sécurité des opérations par carte est plus faible qu'en France.

Collaborer avec les forces de l'ordre et la justice

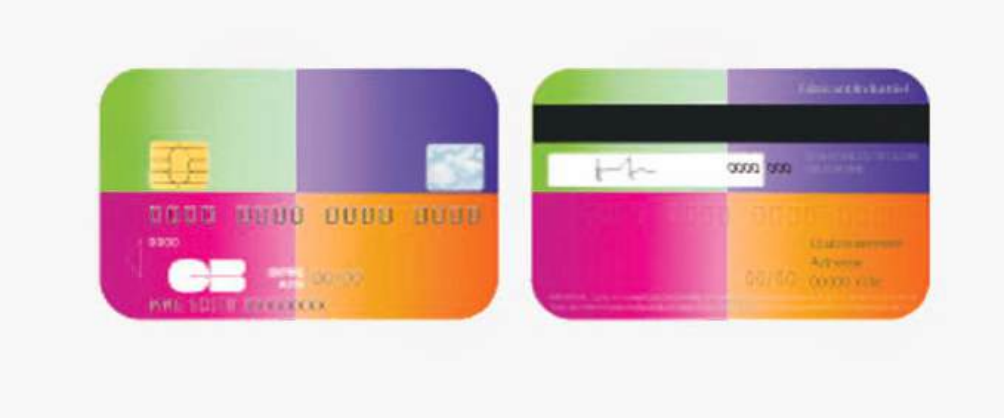
CB ne peut lutter seul contre les fraudes. Il collabore en premier lieu avec ses membres, à qui il signale toutes les suspicions de fraudes, afin qu'ils puissent prévenir les porteurs concernés. La lutte contre la fraude est un processus communautaire où chaque banque

prend la décision finale. Au sein de CB, une équipe dédiée coopère avec la justice, ainsi qu'avec les forces de police et de gendarmerie :

- L'Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication (OCLCTIC) http://www.interieur.gouv.fr/sectio...,
- Les brigades spécialisées de la Préfecture de Police de Paris, notamment la Brigade des fraudes aux moyens de paiement (BFMP) http://www.prefecturedepolice.inter...
- L'Institut de recherche criminelle de la gendarmerie nationale (IRCGN). http://www.gendarmerie.interieur.go...

Sécuriser les cartes

Le cœur de la sécurité des Cartes Bancaires CB est la puce. C'est une sorte de coffre-fort, hautement sécurisé grâce à la cryptographie. Ce "coffre" contient des données dont le niveau de protection doit être maximum. En particulier : des clés cryptographiques spécifiques à chaque carte, le code secret, qui forme un couple unique avec le numéro de la carte, et le compteur d'essais, qui permet de bloquer la carte au bout de trois codes erronés.



Les caractéristiques techniques de la puce sont en constante évolution. Sous l'égide de CB, les fabricants de composants électroniques destinés aux cartes CB doivent ainsi obligatoirement soumettre leurs produits à des tests de sécurité "à l'état de l'art" dans des laboratoires indépendants agréés par L'Agence Nationale de Sécurité des Systèmes d'Information (ANSSI).

S'agissant d'une industrie en évolution permanente, la puce de votre prochaine carte sera ainsi encore plus sécurisée que celle qui équipe votre carte actuelle.

Un des éléments de sécurisation des transactions à distance est constitué par trois chiffres inscrits au dos de la carte, dans le panneau de signature. Associés aux autres caractéristiques de la carte (numéro, date de fin de validité) ils forment une combinaison spécifique à chaque carte.

L'ensemble de ces éléments constituent les données de personnalisation des cartes, calculées par les outils cryptographiques de chaque banque émettrice ; ils sont ensuite transmis à des ateliers de personnalisation des cartes agréés par CB et régulièrement audités. Ces ateliers possèdent un niveau de protection, tant sur le plan physique que logique, équivalent notamment à ceux qui fabriquent les billets pour la Banque de France.

La cryptographie est une discipline dont l'objectif est ici d'assurer l'authentification de la carte, de contribuer à la confidentialité du dialogue entre celle-ci et le terminal de paiement ou le DAB, et de fournir une "signature" de la transaction par la puce. Elle utilise pour cela des algorithmes de chiffrement et des clés secrètes dont la configuration évolue en permanence pour être les meilleures possibles.

Pour un degré de sécurité encore plus élevé, la cryptographie mise en œuvre dans le système CB est basée sur la technique "DDA", ou *Dynamic Data Authentication*. Elle consiste à intégrer dans les échanges puce-terminal des éléments variables spécifiques à chaque transaction ainsi identifiée comme unique, afin que cet identifiant ne puisse être copié ou rejoué.

Sécuriser les terminaux et les automates

Les automates et terminaux de paiement répondent à des exigences de **standardisation** et de sécurité principalement élaborés au niveau international par le **PCI-SSC** pour les terminaux *(Payment Card Industry - Security Standards Council)*.

Cet organisme met à jour et diffuse ses spécifications selon un cycle de 3 ans, au terme duquel une nouvelle version s'impose aux industriels qui souhaitent obtenir la certification "PCI" pour leurs nouveaux modèles de terminaux.

A partir des exigences initiales sur la sécurité des données couvertes par **PCI-DSS**, PCI-SSC a défini en particulier deux référentiels très importants, l'un pour les applications de paiement **PA-DSS**, l'autre pour le terminal et la protection du code secret **PCI- PTS** *(Pin Transaction Security).*

En Europe, CB participe activement au groupe de travail **EAST** *(European ATM Security Team)* qui se concentre sur les attaques spécifiques aux DAB.

Protections physiques et logiques

Chaque type de terminal ou d'automate, possède ses propres référentiels de sécurité. Les protections sont d'abord physiques, avec des dispositifs destinés à rendre extrêmement difficile la copie de la piste magnétique (standards **AFAS** *Anti Fishing-Anti Skimming CB*) notamment sur les DAB ou les automates de paiement, ou encore la frappe du code secret (protection visuelle du clavier par un "bouclier" de confidentialité).
Elles sont également logiques, en conformité avec le référentiel **PCI- PTS** et avec des exigences fortes de chiffrement protégeant le code secret, lors de sa frappe au clavier et tout au long du dialogue entre la carte et le terminal.

Enfin, les transactions sur les DAB, les automates de paiement et tout particulièrement les DAC (Distributeurs Automatiques de Carburant) font l'objet d'une demande d'autorisation systématique.

Sécuriser les données

Tous les acteurs responsables de la sécurité travaillent ensemble à protéger les données sensibles des cartes de paiement.
Sur les systèmes d'information de certains commerçants, des sites de e-commerçants ou des plates-formes de paiement par carte insuffisamment sécurisés, les données sensibles

des cartes CB peuvent parfois être la cible de compromissions et peuvent être ensuite utilisées frauduleusement pour réaliser des paiements en vente à distance, des paiements de proximité et des retraits principalement à l'étranger sur des systèmes de paiements peu sécurisés.

Il est donc fondamental que, quelle que soit la taille des acteurs concernés (banques, commerçants, prestataires), des investissements adaptés soient consentis dans la sécurisation des données sensibles des transactions par carte. Assurer la confidentialité de ces informations, c'est garantir aux titulaires de cartes CB une protection contre les risques de fraude mais aussi contre les possibles atteintes à la vie privée.Tout savoir sur ces normes de sécurité.

C'est pourquoi la communauté bancaire et CB partagent les objectifs du référentiel PCI-DSS, lui-même décliné à partir des standards ISO de sécurité des systèmes d'information, et visant un haut niveau de protection des données sensibles des cartes. La communauté considère que les objectifs de sécurité définis par le référentiel PCI-DSS correspondent à l'état de l'art de ce que recommandent aujourd'hui les experts pour sécuriser les bases de données, les échanges d'informations, ou pour protéger les contrôles d'accès.

Depuis plusieurs années, tous les acteurs concernés ont lancé des programmes de sécurisation de ces données sensibles ; à ce jour, de nombreux commerçants et prestataires de service ont déjà terminé ou sont sur le point de finaliser leur mise en conformité **PCI-DSS.**

Sécuriser les achats en ligne

Des sécurités supplémentaires pour les achats en ligne : 3D Secure

Dans une transaction en commerce électronique, le client doit fournir au minimum le N° de sa carte CB, la date de validité de celle-ci ainsi que les 3 chiffres figurant au verso de la carte.

Un niveau de sécurité supplémentaire a été introduit pour les transactions en ligne avec "3D Secure" : il s'agit d'un ensemble de procédures permettant d'authentifier le titulaire de la carte qui effectue l'ordre de paiement.

Des procédures d'authentification spécifiques sont mises en place dans trois domaines (3-D) : relation entre la banque et son client titulaire de carte, relation entre la banque et son client e-commerçant, relation entre la banque du client et celle du e-commerçant.

Concrètement, cela se traduit pour le porteur qui effectue un achat chez un e-commerce "3D-S" par des procédures qui peuvent varier d'une banque à l'autre :

Code non-rejouable envoyé par SMS au numéro de portable donné à votre banque ;

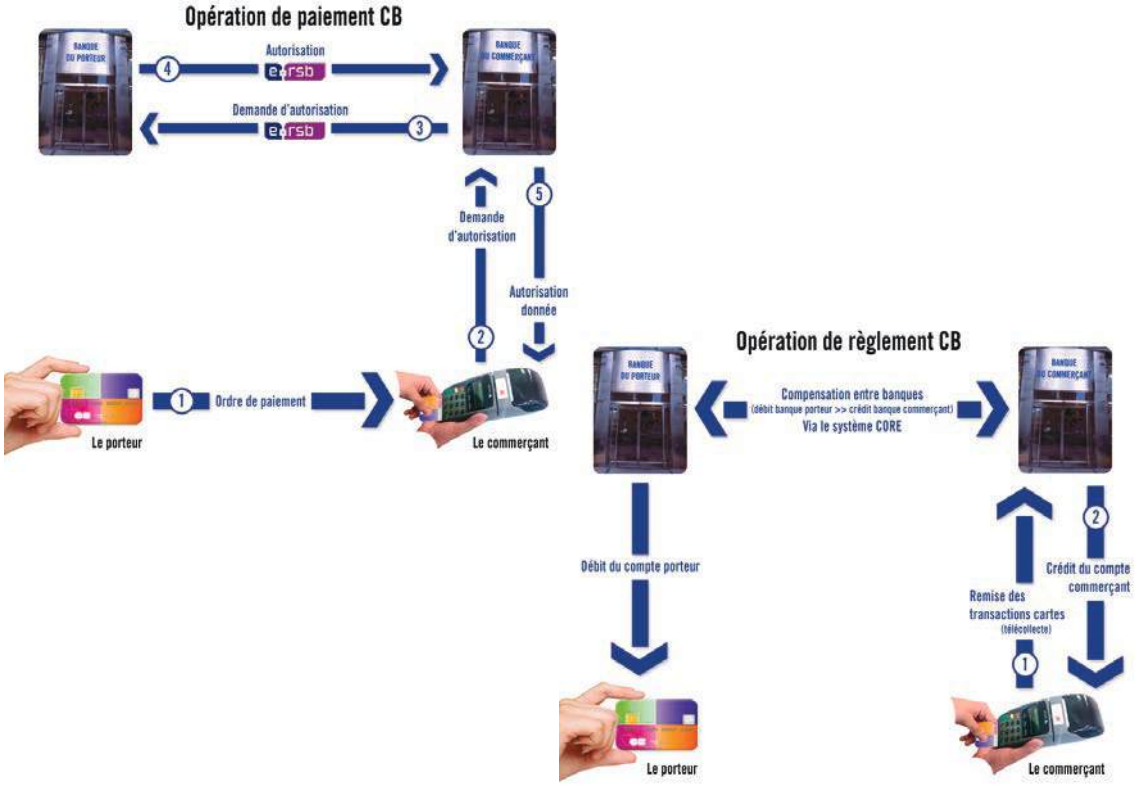
	A	B	C	D	E
1	30	3 255	15	259	695
2	476	000	788	523	56
3	5 699	8 577	852	258	777
4	898	333	52	6 834	9 999
5	698	333	564	22	46
6	789	21	693	5 444	666

Procédure de type "bataille navale" (à partir d'une grille fournie par votre banque, vous saisissez le code situé dans la case indiquée en cours de transaction) ;

Lecteur portable de carte à puce qui calcule un cryptogramme spécifique à la transaction ;

"Token" (ou jeton en français),
écran dédié aux calculs d'une valeur ;

Demande de saisie d'une donnée choisie par le titulaire de la carte.



Bien acheter en ligne

Pour bien acheter en ligne il faut, en plus des règles de prudence générales :

- Ne pas stocker son numéro de carte bancaire dans son ordinateur ni envoyer ses informations confidentielles dans un simple mail ;
- Vérifier la sécurisation du site avec le cadenas apparaissant en bas de l'écran, le https qui précède l'adresse Internet du site dans le navigateur, et le routage vers le site de la banque lors du paiement ;
- Etre vigilant sur les tentatives "pirate" de "Phishing" par mail à l'orthographe parfois approximative vous demandant de fournir des données sensibles (voir image ci-contre).
- Contacter le commerçant si nécessaire ou en cas de doute ;
- Vérifier attentivement ses relevés bancaires afin de signaler toute anomalie à sa banque ;
- Bien choisir son commerçant en s'assurant de ses coordonnées (adresse, numéro de téléphone, contact avec le service client) et en lisant les conditions générales de vente.

MAIL DE "PHISHING"

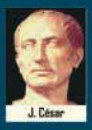
Quelques règles de prudence

La sécurisation de la carte bancaire CB n'empêche pas de suivre quelques règles de bon sens pour l'utiliser en toute sécurité :

- N'écrire nulle part son code confidentiel, ni le communiquer à un tiers quel qu'il soit ;
- Toujours composer le code confidentiel à l'abri des regards indiscrets, par exemple en protégeant le clavier de son autre main ;
- Ne pas composer 3 fois son code personnel erroné, lors d'un retrait ou d'un paiement ;
- Ne pas se laisser distraire par un tiers lors d'un retrait ;
- Conserver sa carte en lieu sûr et ne la confier à personne ;
- Conserver ses tickets (y compris électroniques) et vérifier régulièrement ses relevés bancaires ;
- Signaler immédiatement toute anomalie sur son relevé bancaire à la banque ;
- Ne jamais perdre de vue sa carte pendant le paiement chez un commerçant ;
- Mettre immédiatement la carte en opposition si elle est conservée par un distributeur, perdue ou volée ;
- Garder en lieu sûr le numéro de la carte et sa date d'expiration pour pouvoir la mettre en opposition plus rapidement.

Dates marquantes de la Carte Bleue : http://www.cartes-bancaires.com/spip.php?rubrique32

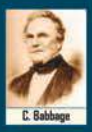
Quelques chiffres


J. César


Al-Kindi


B. de Vigenère


L. Euler


C. Babbage


A. Turing


C.E. Shannon


R. Rivest


L. Adleman


A. Shamir


C. Bennett


G. Brassard

Cryptographie et codages

Les technologies sans contact

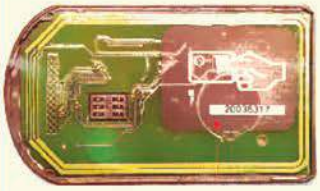
Le passe Navigo

Le développement de la billettique Navigo s'appuie sur trois grands principes, utilisant différentes normes :

- Un protocole de communication radio sans contact. Ce protocole permet de faire communiquer les passes Navigo avec les terminaux sans avoir besoin d'alimenter la carte en énergie et de manière rapide (moins de 250 ms).
- Une structure de données unique dans le passe sur la base d'une norme internationale (EN 1545)
- Une gestion de la sécurité qui s'appuie sur la technologie Calypso largement utilisée en France et dans le monde.

Navigo en quelques chiffres

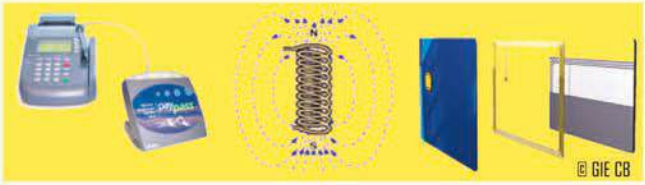
Distance de transmission : 5 à 10 cm ajustable ; possibilité de lecture à distance (1 m).
Vitesse de transmission : 106 000 bits par seconde.
Durée de la transaction : moins de 150 millisecondes.
Sécurité : codage sur 12 clés de 64 bits pour les différentes applications avec algorithme DES.
Lancé en 2001 par la RATP, le système Navigo compte plus de 7 000 000 d'abonnés en 2012.
Plus de 30 000 000 d'utilisateurs de passes dans le monde basés sur le protocole Calypso.



Le boîtier renferme la puce qui stocke les informations et l'antenne enroulée dans l'épaisseur du plastique qui permet d'alimenter en énergie le microprocesseur.

Si on ajoute un écran au boîtier, il devient interactif et des informations peuvent être échangées : crédit de son porte-monnaie électronique, nature de ses abonnements, appels d'urgence, ...

Le passeport électronique / La carte bleue sans contact



La technologie NFC (Near Field Communication, communication par champ proche) permet de faire des paiements par carte sans contact ou par mobile NFC. La carte sans contact, alimentée par induction via son antenne, dispose de moins d'énergie qu'une carte classique pour ses calculs.

Il est possible de diviser par 4 le temps de calcul RSA en utilisant le Théorème des Restes Chinois, qui dit qu'il est équivalent de calculer modulo $n = pq$ ou en parallèle modulo p et modulo q.

Un entier x dans $[0, n\text{-}1]$ est alors représenté par un couple $(x_p, x_q) = (x \bmod p, x \bmod q)$.

Le calcul $y = x^d \bmod n$ se fait en calculant le couple correspondant $(y_p\ , y_q)$ puis en recomposant $y = (y_p\ , y_q)$.

Cette technique impose de prendre des précautions pour éviter toute erreur (involontaire ou provoquée) survenant pendant le calcul de y_p.

Les puces des cartes CB ou du passeport électronique doivent obtenir un certificat de l'État attestant qu'elles résistent à ce type d'erreur (entre autres) avant de pouvoir être distribuées aux porteurs.

Panneau 11

Les technologies sans contact

Ce panneau présente une des applications nouvelles de la carte à puce et a été réalisé grâce aux documents fournis par la RATP et le Groupement Carte Bleue.

À la fin des années 80, le service Télématique de la RATP a étudié des solutions de remplacement aux péages magnétiques installés dans les années 70. À cette époque, deux techniques nouvelles venaient d'apparaître: la carte à puce et les systèmes de lecture sans contact : 1 'innovation a été de marier ces deux techniques. Puis, dès 1992, il est apparu évident que ce nouveau produit pouvait offrir bien d'autres services qu' un « sésame» pour les transports, et la RATP s'est orientée vers la réalisation d'un véritable passe urbain :
Les voyageurs ont expérimenté le passe sans contact dès 1997 dans quelques 44 stations de métro, les gares de RER et deux lignes de bus. Plébiscité par les
usagers, il va se généraliser auprès de tous les voyageurs à partir de 2003 : c'est la carte NAVIGO.
Les services du porte-monnaie électronique seront proposés ultérieurement dans la carte MODEUS.

La standardisation du passe sans contact :
Les opérateurs de 4 villes européennes (Venise, Constance, Lisbonne et Paris) ont développé et expérimenté différentes fonctionnalités du passe sans contact au sein des projets ICARE (télébillettique transport, 1996-1997) et CALYPSO (complément porte-monnaie électronique et services, 1998-1999).

Plus de 160 villes, collectivités et fédérations de transporteurs européens se sont regroupés au sein d'une association, CLUB (*Contact Less technology Users Board)*, afin de promouvoir des échanges et une standardisation du produit. Le passe sans contact est conforme à 1' ensemble des normes européennes existantes.

Il faut aussi bien sûr citer MONEO, porte-monnaie électronique, qui a fait son apparition en France.

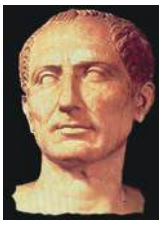
Quelques grands noms liés à l'histoire de la Cryptographie

Eratosthène

Bibliothécaire d'Alexandrie, géographe, astronome, historien, enfin mathématicien, Eratosthène est né vers -276 av J.C. et mort vers en -196 av J.C. Son exploit le plus retentissant est sans doute, d'avoir estimé la circonférence de la Terre par des calculs d'angle. Eratosthène trouve 39 375 km contre 40 075 aujourd'hui.

Jules César

César est né à Rome le 12 ou le 13 juillet 100 av. J.-C. et mort le 15 mars 44 av. J.-C. (aux Ides de Mars). Son destin exceptionnel marque le monde romain et l'histoire universelle : ambitieux et brillant, il s'appuye sur le courant réformateur et démagogue pour son ascension politique ; stratège et tacticien habile, il repousse les frontières romaines jusqu'au Rhin et l'Océan Atlantique en conquérant la Gaule, puis utilise ses légions pour s'emparer du pouvoir. Il se fait nommer dictateur à vie, et est assassiné peu après par une conspiration de sénateurs.



Al Kindi

Abû Youssouf Ya'qûb Ibn Ishâq Al-Kindi (800-873) est né à Kûfah, aujourd'hui en Irak. Surnommé le « philosophe des Arabes », il a rédigé plus de 200 ouvrages sur les sujets les plus divers : astronomie, optique, chimie, médecine, musique … Il est l'un des tout premiers traducteurs des œuvres grecques en arabe.

Blaise de Vigenère

Né le 5 avril 1523 à Saint-Pourçain-sur-Sioule et mort le 19 février 1596 à Paris, est un diplomate, cryptographe, alchimiste et astrologue français. Il a laissé son nom au chiffrement de Vigenère dont la paternité revient à Giovan Battista Bellaso, mais qui lui a été faussement attribué au XIX^{e} siècle.

Pierre de Fermat:

Né en 1601 à Beaumont de Lomagne, Fermat poursuit ses études à Toulouse pour les langues puis à Bordeaux pour les mathématiques.

Une carrière de magistrat l'attend. A 30 ans, il est conseiller au parlement de Toulouse. C'est dans cette ville qu'il se marie et a cinq enfants. De son vivant, célèbre sans éclat, il laisse peu d'œuvres éditées (la plupart resteront manuscrites), et une abondante correspondance. Ses travaux en théorie des nombres ont peu de retentissement jusqu'à ce qu'ils soient redécouverts par Euler.

Léonhard Euler

Né en 1707 à Bâle, il est le fils d'un pasteur féru de sciences qui lui apprend les mathématiques, mais il est destiné aux études théologiques.
À l'Université de Bâle, il suit les cours de Bernoulli et devient docteur en philosophie. À partir de 1726, Euler enseigne la physique, puis les mathématiques à 1' Académie des sciences de Saint-Pétersbourg. En 1741, il rejoint Berlin pour cinq ans, mais un conflit avec le roi de Prusse le pousse à revenir à Saint-Pétersbourg. Peu après, il devient aveugle. Il continue cependant à écrire et à enseigner jusqu'à sa mort en 1783.

Samuel Finly Breeze Morse

Peintre américain, il est le développeur d'un télégraphe électrique et de l'alphabet qui portent son nom. Il est né le 27 avril 1791 à Charlestown, Massachusetts, et mort le 2 avril 1872 à New York.

Charles Babbage

Mathématicien, inventeur, visionnaire britannique du XIXe siècle, il est l'un des principaux précurseurs de l'informatique. Vers la fin de sa vie, il dit qu'il accepterait une mort immédiate à condition de pouvoir passer trois jours, cinq cents ans plus tard, avec un guide scientifique qui lui expliquerait toutes les inventions faites depuis sa mort.

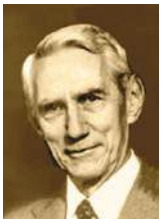
Il est le premier à énoncer le principe d'un ordinateur. C'est en 1834, pendant le développement d'une machine à calculer destinée au calcul et à l'impression de tables mathématiques (machine à différences) qu'il a l'idée d'y incorporer des cartes du métier Jacquard, dont la lecture séquentielle donne des instructions et des données à sa machine, et donc imagine l'ancêtre mécanique des ordinateurs d'aujourd'hui. Il ne finira jamais sa machine analytique, mais il passe le reste de sa vie à la concevoir dans les moindres détails et à en construire un prototype. Un de ses fils construira l'unité centrale (le moulin) et l'imprimante en 1888 et fera une démonstration réussie de calcul de table à l'Académie Royale d'astronomie en 1908.

Alan Turing

Né en 1912, très tôt, ses enseignants reconnaissent son génie précoce pour les sciences et son affinité pour les chiffres et les énigmes. Il est le père des ordinateurs modernes, au moins pour leur partie théorique. Sa machine de Turing, est le premier calculateur universel programmable. Mais un suicide prématuré en 1964, l'a plongé injustement pourquelques années dans l'anonymat de l'histoire

Claude Elwood Shannon

Né le 30 avril 1916 à Petoskey, Michigan et décédé le 24 février 2001 à Medford, Massachusetts, Shannon est un ingénieur électricien et mathématicien américain.



Il est l'un des pères, si ce n'est le père fondateur, de la théorie de l'information. Claude Shannon est connu non seulement pour ses travaux dans les télécommunications, mais aussi pour l'étendue et l'originalité de ses hobbies, comme la jonglerie, la pratique du monocycle et l'invention de machines farfelues : une souris mécanique sachant trouver son chemin dans un labyrinthe, un robot jongleur, un joueur d'échecs, etc

Claude Chappe

Claude Chappe est né le 25 décembre 1763 à Brûlon (Sarthe) en France et il est mort le 23 janvier 1805 à Paris, inhumé au cimetière du Père-Lachaise. Il est l' inventeur du premier télégraphe au monde permettant la communication par sémaphore. Il est le premier entrepreneur des télécommunications dans l'histoire de l'humanité.

Les Pères du RSA : Rivest, Shamir et Adleman

En 1977, Rivest, Shamir et Adleman décrivent le premier algorithme de chiffrement à clé publique, nommé RSA selon leurs initiales. Ils reçoivent en 2002 pour cette découverte le prix Turing de l'Association for Computing Machinery.

Léonard Max Adleman est en Californie, le 31 décembre 1945, il grandit à San Francisco et étudie l'université de Berkeley. Chercheur en informatique théorique et professeur en informatique et en biologie moléculaire à l'Université de la Californie du Sud il est co-inventeur du cryptosystème RSA (Rivest, Shamir, Adleman) en 1977, Adleman a également travaillé dans la bio-informatique.

Ronald Linn Rivest, né en 1947 à New York, est un cryptologue américain d'origine canadienne-française. Diplômé de l'université Yale en 1969 et docteur de Stanford en 1974, il rejoint les laboratoires du MIT où il fonde un groupe travaillant sur la sécurité de l'information et la cryptographie. Il y met au point les algorithmes à clé secrète.

Adi Shamir, né à Tel Aviv en 1952, est un cryptologue, professeur au département de mathématiques appliquées de l'Institut Weizmann depuis 1984, où il occupe la chaire Borman de science informatique. Adi Shamir est l'une des figures emblématiques de la cryptographie et de la cryptanalyse à travers le monde. Il a introduit et mis en œuvre la notion de partage du secret qui s'est révélée être une idée fondamentale, utilisée non seulement dans la pratique, mais également dans des centaines de travaux théoriques.

Les pères de la cryptographie quantique : Bennett et Brassard

Charles Henry Bennett, né en 1943, est un physicien et cryptologue américain qui travaille dans les laboratoires de recherche d'IBM Research. Les travaux récents de Bennett chez IBM ont consisté en un réexamen des bases physiques de l'information et l'application de la physique quantique aux problèmes des flux d'informations. Ses travaux ont joué un rôle majeur dans le développement d'une interconnexion entre la physique et l'information. Il a également travaillé sur un projet de cryptographie quantique à l'Université de Montréal avec Gilles Brassard.

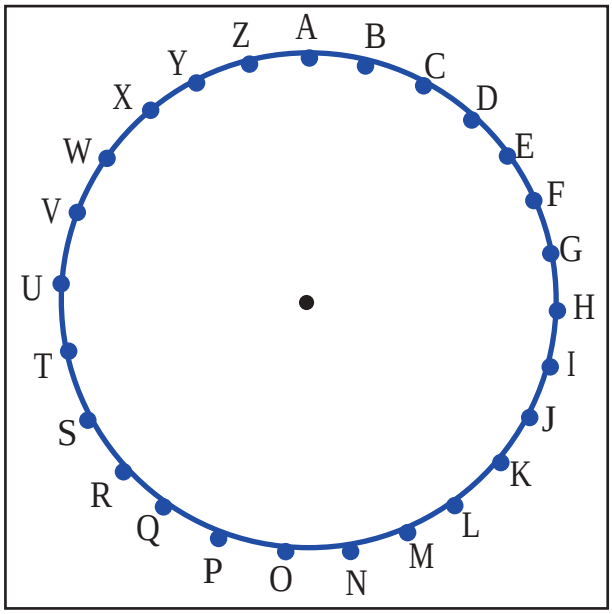
Gilles Brassard né en 1955 à Montréal est un cryptologue canadien. Dès son plus jeune âge, il est passionné par les mathématiques, passion qu'il a reçue de son grand frère, Robert Brassard, qui prenait plaisir à lui enseigner des concepts avancés de mathématiques.

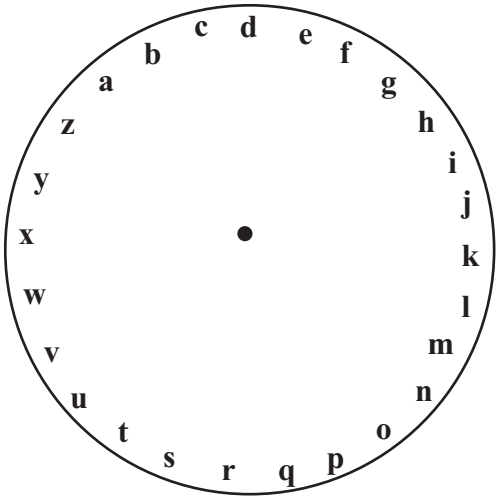
En 1984, avec Charles H. Bennett, Brassard invente le protocole BB84, un protocole de cryptographie quantique. Plus tard, il a davantage contribué au sujet en y incluant le protocole de correction d'erreurs par cascade, ce qui détecte et corrige efficacement le bruit causé par un observateur externe d'un signal cryptographique quantique. En 1993, avec d'autres chercheurs, il jette les bases de la téléportation quantique et parvient à téléporter des photons sur une courte distance. Le journal scientifique *Science* considérait alors qu'il s'agissait d'une des plus importantes découvertes de l'année.

Des jeux autour de la cryptographie pour devenir un briseur de codes

(solutions page 49)

Activité 1 : Avec l'Alphabet de Jules César





Découpez le petit disque mobile et fixez-le sur le grand disque du carré.

La manipulation proposée : décrypter les noms écrits ci-dessous pour retrouver le nom de grands arithméticiens.

GWENKFG	CHNOGZMSD	PISRLEVH IYPIV
LEANNA ZA BANIWP	HUDWRVIOEQH	ZJYGQC NYQAYJ
YLBPCU UGJCQ	KGVOJI	VRSKLH JHUPDLQ
BQFBKKB YBWLRQ	HTKGFTKEJ ICWUU	QZLZMTIZM

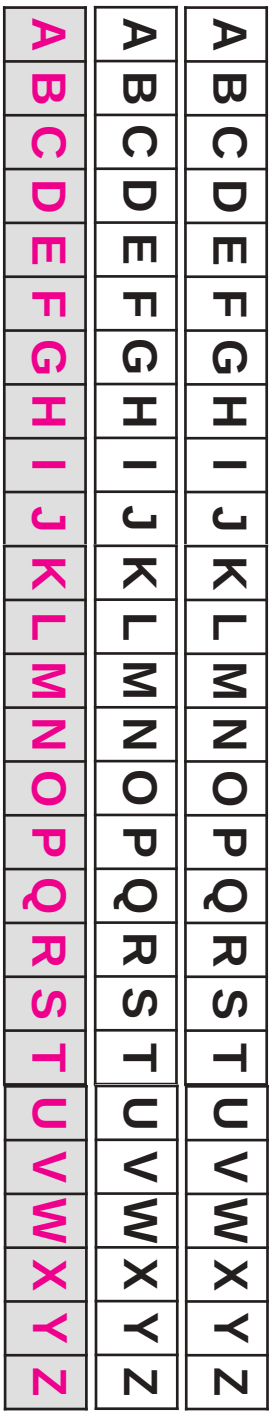
on pourra en profiter pour faire un peu d'histoire des nombres.

La manipulation proposée ci-dessus peut-être l'occasion de faire une introduction, pour tous, à la trigonométrie et pour les bons élèves, au raisonnement sur les congruences. Comment ?

Si on définit le disque fixe pour le «clair» et le disque mobile pour le « cryptogramme » tourner de + 2 (+ 2 compté dans le sens trigonométrique) revient à remplacer le A par C, le B par D, etc ...on peut que constater que tourner de +2 ou de -50 revient au même, en effet (+2)_-(-50) est un multiple de 26, ce que l'on écrit +2= -50 (mod 26) et qui ce lit +2 est congru à -50 modulo 26.
On peut bien sûr- multiplier les exemples : + 3 et 29 ; +5 et -47 ...
- faire trouver des exemples ...
- se demander ce qui se passe si on intervertit le rôle des deux disques ?

Activité 2 : Avec la réglette de Saint Cyr (voir modèle à droite)

Elle est composée de deux réglettes : l'une fixe (en gris) portant l'alphabet, l'autre (en deux morceaux blancs à accoler) mobile par rapport à la fixe portant au moins deux fois l'alphabet à la suite…Elle peut-être utilisée pour chiffrer ou déchiffrer selon l'alphabet de César.



Activité 3 : Avec le chiffre de Vigenère

Pour transformer le message, RENDEZ VOUS VENDREDI SOIR, (ou celui que vous voulez) avec pour clé le mot AMIE (ou tout autre mot) utilisez le carré de Vigenère ci-dessous.

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

Activité 4 : Construction du crible d'Eratosthène des entiers jusqu'à 100

~~1~~	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Sur une table portant les nombres de 2 à 100, on place quatre feuillets transparents

- en soulevant les quatre premiers feuillets transparents, on a donc tous les nombres entiers de 2 à 100 ;

-en abattant le premier feuillet, on raye les multiples de 2 sauf 2 ;

- en abattant le deuxième feuillet, on raye les multiples de 3 sauf 3 ;

- en abattant le troisième feuillet, on raye les multiples de 5 sauf 5 ;

-en abattant le quatrième feuillet, on raye les multiples de 7 sauf 7 .

Les nombres restants (non rayés) sont les nombres premiers inférieurs à 100.

On peut poser de nombreuses questions autour de cette construction :
Comment construire les nombres premiers de 2 à 1000 ? (On rayerait jusqu'aux multiples de 31)

Activité 5 : Comment transmettre en secret sans donner la clé ?

Les facteurs indélicats

Dans ce pays , les facteurs sont indélicats : ils ne résistent pas à la tentation de voler le contenu d'un paquet mal fermé. Ce pays est donc imaginaire ! Par contre, si le paquet est cadenassé, ils n'y toucheront pas. Dans ce pays les habitants ne possèdent que des cadenas à clé, chaque cadenas ayant son unique clé….
Comment Anatole peut-il faire parvenir, en toute sécurité, à Belle, le beau bijou qu'il lui destine ?

Activité 6 : Etes-vous perspicace ?

Six cartes numérotées 3, 4, 5, 6, 7 et 8 sont disposées ainsi

3	4	5
6	7	8

En ne déplaçant que deux cartes pouvez vous faire en sorte que la somme des trois nombres sur la première rangée soit égale à la somme des trois nombres sur la deuxième rangée ?

Activité 7 : Un peu de logique avec des codes postaux français

Sur le courrier que vous recevez par la poste, vous avez peut être remarqué une série de bâtonnets inscrits en bas à droite des enveloppes.

Il s'agit en fait d'un codage du code postal utilisé pour le tri automatique du courrier par lecture optique.

Le tableau ci-dessous vous montre cinq exemples de code postal avec leur codage en bâtonnets (pour simplifier la lecture nous avons remplacé les blancs par des points et espacés les nombres).

Examinez-les attentivement afin de retrouver le code postal représenté dans la dernière ligne …

Code postal	Codage en bâtonnets et points pour les blancs
5 1 1 0 0	..IIII ..IIII .I.III .I.III I.I.II
5 2 1 3 0	..IIII .III.I .I.III .II.II I.I.II
0 8 4 0 0	..IIII ..IIII I..III II.I.I ..IIII
7 5 0 0 6	I.II.I ..IIII ..IIII I.I.II II..II
1 3 0 0 7	II..II ..IIII ..IIII .III.I .I.III
? ?	..IIII .I.III .III.I I..III III..I

Activité 8 : l'alphabet codé

a	π
b	◀
c	Δ
d	¤
e	◊
f	•
g	@
h	#
i	Ω
j	±
k	∫
l	®
m	∞

n	&
o	♀
p	/
q	♠
r	÷
s	☼
t	»
u	×
v	«
w	♂
x	□
y	)(
z	¡

Quelle est cette évidence ?

♀& π ∞π÷Δ#◊
☼×÷ ®π ®×&◊

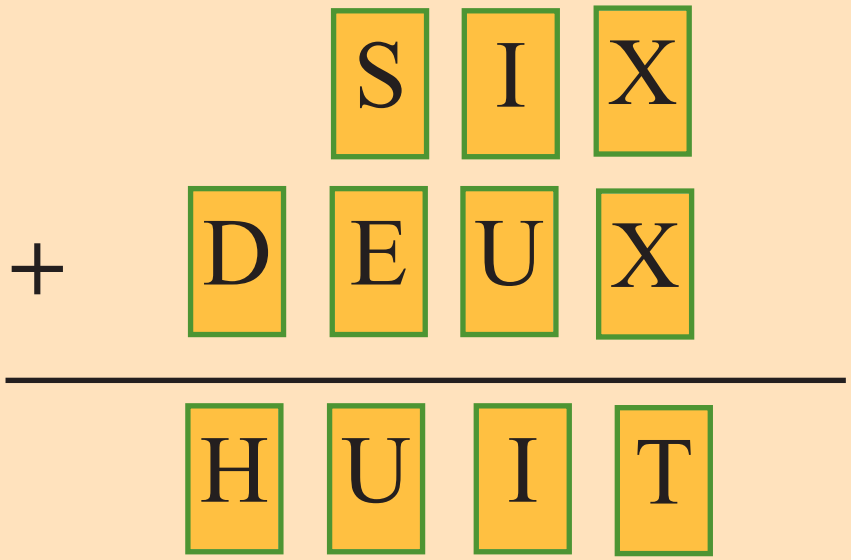
Qui est l'auteur de ce début de citation ?

Ω® & ◊□Ω☼»◊ ♠×◊ ¤◊×□ Δ#♀☼◊☼
Ω&•Ω&Ω◊☼ ® ×&Ω«◊÷☼ ◊» ®π
◀◊»Ω☼◊ #×∞πΩ&◊

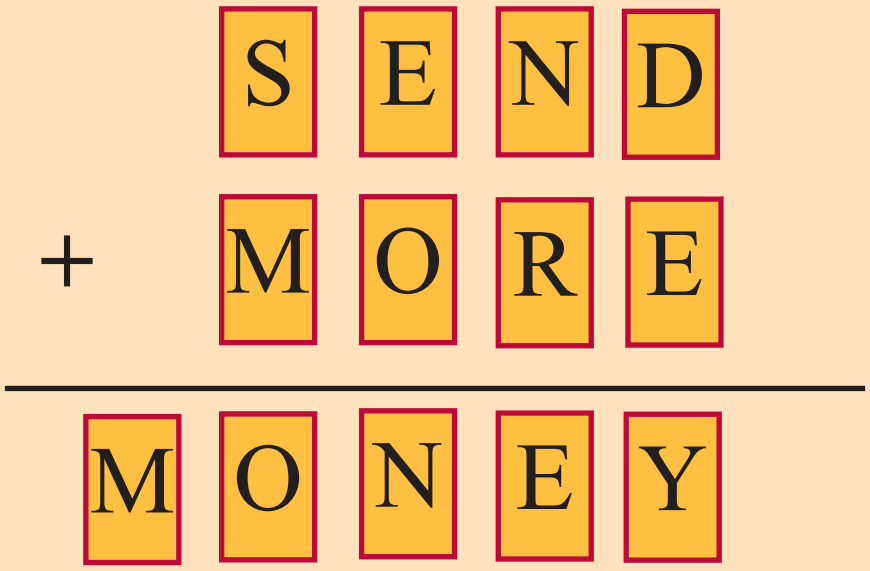
Activité 9 : Réflexion et cryptogrammes

Un cryptogramme est une opération codée dans laquelle chaque lettre correspond à un chiffre et un seul.

Cryptogramme 1
Quel est le plus grand résultat possible de cette addition ?



Cryptogramme 2
Un cryptogramme célèbre que Henry Dudeney envoya à son éditeur

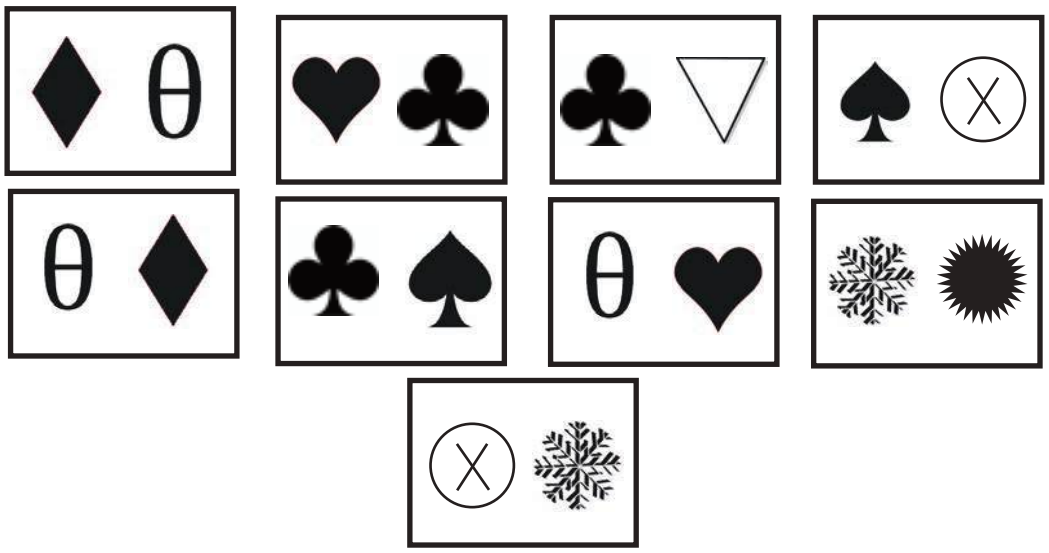


Activité 10 : symboles et codages

Codages

Un symbole remplace un chiffre. Mettre en correspondance les cartes avec les nombres proposés.

19		74	
28		76	
37		91	
45		93	
52			



Corrections des manipulations

Activité 1 : Avec l'Alphabet de Jules César

Les noms des arithméticiens à découvrir :
-Euclide (vers 323-283 av. J.C) : on a tourné de +2. (GWENKFG)
-Diophante (IVe siècle) : on a tourné de-l. (CHNOGZMSD)
- Léonhard Euler (1707 -1783): on a tourné de +4. (PISRLEVH IYPIV)
-Pierre de Fermat (1601- 1665): on a tourné de -4 (LEANNA ZA BANIWP)
- Eratosthène (vers 275- 195 av. J.C) : on a tourné de+ 3. (HUDWRVIOEQH)
-Blaise Pascal (1623- 1662) : on a tourné de -2.(ZJYGQC NYQAYJ)
- Andrew Wiles (1953) : on a tourné de -2 (YLBPCU UGJCQ)
-Platon (427- 347): on a tourné de - 5 (KGVOJI)
-Sophie Germain (1776-1831): on a tourné de +3 (VRSKLH JHUPDLQ)
-Etienne Bézout (1730-1783): on a tourné de - 3 (BQFBKKB YBWLRQ)
-Friedrich Gauss (1777-1855): on a tourné de +2 (HTKGFTKEJ ICWUU)
-Ramanujan (1887-1920): on a tourné de -1 (QZLZMTIZM)

Activité 3 : Le chiffre de Vigenère

Rendez-vous vendredi soir avec la clé AMIE
RQVHEL DSUE DINPZIDU ASID

Activité 4 : Crible d'Eratosthène

~~1~~	~~2~~	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	~~49~~	~~50~~
~~51~~	~~52~~	53	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	59	~~60~~
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	67	~~68~~	~~69~~	~~70~~
71	~~72~~	73	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	79	~~80~~
~~81~~	~~82~~	~~83~~	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	~~89~~	~~90~~
~~91~~	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	97	~~98~~	~~99~~	~~100~~

Activité 5 : Comment transmettre en secret sans donner la clé ?

- A envoie à B un paquet qu'il a fermé avec un cadenas X.
- B recevant le paquet avec le cadenas X, ne l'ouvre pas, y ajoute le cadenas Y et envoie le tout à A.
- A reçoit le paquet avec les cadenas X et Y, il enlève le cadenas X (le sien, il sait faire) et renvoie à B le paquet avec le cadenas Y, celui de B, qu'elle saura ouvrir !!

Moralité : Espérons qu'en ce pays les frais postaux ne sont pas très élevés On ne doit pas payer bien cher des postiers aussi peu fiables …

Activité 6 :

Il faut intervertir le 3 et le 6 et … retournez le 6 pour en faire un 9 !

Activité 7 : Un peu de logique avec des codes postaux français

? ? : ..IIII .I.III .III.I I..III III..I
= 01 349

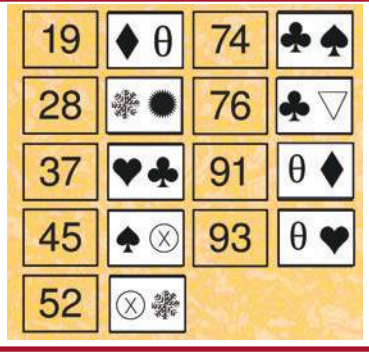
Activité 8 : l'alphabet codé

Une évidence : on a marché sur la lune
Citation : Einstein : il n'existe que deux choses infinies, l'univers et la bêtise humaine,...

Activité 9 : Réflexion et cryptogrammes

794 + 1304 = 2098
et
9567 + 1085 = 10 652

Activité 10 : symboles et codages



La Cryptographie et l'histoire

L'art du secret Pour la Science juillet-octobre 2002.

La guerre des codes secrets de David Kahn Inter-Éditions.

Histoire des codes secrets de Simon Singh publié en livre de poche se lit comme un polar.

La France gagne la guerre des codes secrets, 1914-1918 de Sophie de Lastours publié chez *Tallandier* apporte des éclairages passionnants sur 1'histoire de la cryptographie et plus particulièrement son rôle pendant la guerre de 14-18.

Cryptographie et Codes secrets Bibliothèque Tangente HS n° 26

La guerre des codes secrets d' Hervé Lehning publié chez *Ixelles éditions*

La Cryptographie et la littérature

Au 19ème siècle, la fascination grandissante exercée par les techniques de la cryptographie amène codes et chiffres à figurer en bonne place dans la littérature

Voyage au centre de la terre de Jules Verne
Dans ce roman le déchiffrement d'un parchemin couvert de caractères runiques constitue le premier pas de ce voyage épique. Les caractères proviennent d'un chiffre de substitution qui engendre un texte en latin qui ne prend son sens que lorsqu'on inverse les lettres

Le Scarabée d'or d'Edgar Poe
Publiée en 1843, cette nouvelle de pure fiction même si elle a à voir avec une histoire réellement arrivée met en scène un système de chiffrement pour retrouver le trésor du capitaine Kidd. Les cryptographes professionnels s'accordent à la considérer comme le meilleur texte de littérature romanesque sur le sujet.

La Cryptographie pour les plus jeunes

Le monde des codes secrets publié dans la collection «Aux couleurs du monde» chez *Circonflexe* peut être lu par les enfants dès l'âge de huit ans.

Des jeux autour de la Cryptographie

« pour devenir un briseur de codes »

À la manière des Spartiates une occasion de proposer une petite manipulation :
Trouver des bambous et ou des bâtons de différents diamètres.

Sur l'un des bambous, on enroule un ruban, écrit un message, puis on déroule le ruban ...

**Nous remercions particulièrement
ceux qui nous ont aidés dans l'élaboration et la diffusion
de l'exposition «Cryptographie et Codages» :**
L'Université de Limoges,
le Groupement Carte Bleu,
l'Agence Nationale de la Sécurité des Systèmes d'Information,
Le Crédit Mutuel Enseignant