Cryptographie : Comment l'arithmétique est devenue science appliquée

6 juin 2019

"Personne n'a encore découvert d'applications militaires à la théorie des nombres ou à la théorie de la relativité, et il est vraisemblable que personne n'en découvrira dans le futur."

G. H. Hardy *The Mathematician's Apology (1940)*

Vocabulaire

- Chiffrer ou crypter : transformer un message pour le rendre incompréhensible aux destinataires non autorisés.
- Déchiffrer ou décrypter : retrouver le message clair, à l'aide du « mode d'emploi » (c'est la tâche du destinataire régulier) ou sans disposer du « mode d'emploi » (c'est le travail de l'espion).
- Les cryptographes conçoivent les systèmes de cryptage.
- Les cryptanalystes sont les spécialistes du décryptage sans mode d'emploi (« attaque »).

L'histoire de la cryptographie est celle de la lutte opposant cryptographes et cryptanalystes, qui sont souvent les mêmes personnes.

Il y a un peu plus de 2000 ans : le Chiffre de César

César choisit une lettre pour clé. Par exemple la lettre C

Le cryptage est le décalage qui envoie A sur C :

```
ABCDEFGHIJKLMNOPQRSTUVWXYZ
CDEFGHIJKLMNOPQRSTUVWXYZAB
```

Cryptage d'un message

```
DEMAIN MATIN A LYON
FGOCKP OCVKP C NAQP
```

Décryptage du Chiffre de César

- Décryptage : Le destinataire effectue le décalage inverse de celui utilisé pour chiffrer.
- L'attaque est un jeu d'enfant car l'ensemble des clés est très petit. On essaie successivement les 26 clés possibles.

Décryptons `FGOCKP` :

- Clef A : `FGOCKP` $\rightarrow$ `FGOCKP`
- Clef B : `FGOCKP` $\rightarrow$ `EFNBJO`
- Clef C : `FGOCKP` $\rightarrow$ `DEMAIN`

Un peu d'arithmétique : César et l'addition modulo 26

Numérotons les lettres de 0 à 25.

A	B	C	D	E	F	G	...	U	V	W	X	Y	Z
0	1	2	3	4	5	6	...	20	21	22	23	24	25

Le Chiffre de César agit sur les numéros :

0	1	2	3	4	5	6	...	20	21	22	23	24	25
2	3	4	5	6	7	8	...	22	23	24	25	0	1

Le numéro du cryptage de X s'obtient en ajoutant $C = 2$ au numéro de X, et, si le résultat est ≥ 26, en soustrayant 26.

Cette opération s'appelle l'addition modulo 26.

Décryptage du Chiffre de César et addition des lettres

Décryptage : on décrypte en soustrayant la clé, c'est à dire en ajoutant l'opposé de la clé.

$\mathtt{Y} + \mathtt{C} = 24 + 2 = 26 = 0 = \mathtt{A}$, donc l'opposé de $\mathtt{C}$ est $\mathtt{Y}$.

Cryptage et décryptage

$$\begin{array}{rr} & \mathtt{DEMAIN\ A\ LYON} \\ + & \mathtt{CCCCCC\ C\ CCCC} \\ \hline = & \mathtt{FGOCKP\ C\ NAQP} \end{array} \qquad \begin{array}{rr} & \mathtt{FGOCKP\ C\ NAQP} \\ + & \mathtt{YYYYYY\ Y\ YYYY} \\ \hline = & \mathtt{DEMAIN\ A\ LYON} \end{array}$$

Cryptage par substitution alphabétique

La clé secrète est une permutation σ des 26 lettres de l'alphabet.

$$\sigma = \begin{pmatrix} \texttt{A B C D E F G H I J K L M N O P Q R S T U V W X Y Z} \\ \texttt{G Y D E A F B O Z P V X H I U R W N L S C T M K Q J} \end{pmatrix}$$

Cryptage : on applique la substitution σ à chacune des lettres.

$$\texttt{DEMAIN A LYON} \longrightarrow \texttt{EAHGZI G XQUI}$$

Décryptage : on remplace σ par la permutation inverse.

$$\sigma^{-1} = \begin{pmatrix} \texttt{A B C D E F G H I J K L M N O P Q R S T U V W X Y Z} \\ \texttt{E G U C D F V M N Z X S W R H J Y P T V C K Q L B I} \end{pmatrix}$$

Attaque du cryptage par substitution

Un première idée : on essaie toutes les clés ?

Nombre de clés :

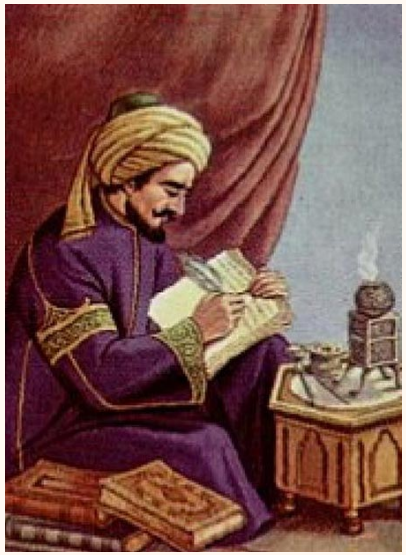
$$\begin{aligned} 26! &= 1 \times 2 \times 3 \times \cdots \times 26 \\ &= 403\,291\,461\,126\,605\,635\,584\,000\,000 \end{aligned}$$

C'est-à-dire environ 130 000 siècles en testant 1000 milliards de clés par seconde...

Mais il est assez facile de décrypter en analysant les fréquences d'occurrences des caractères.

Une attaque redoutable : l'analyse des fréquences

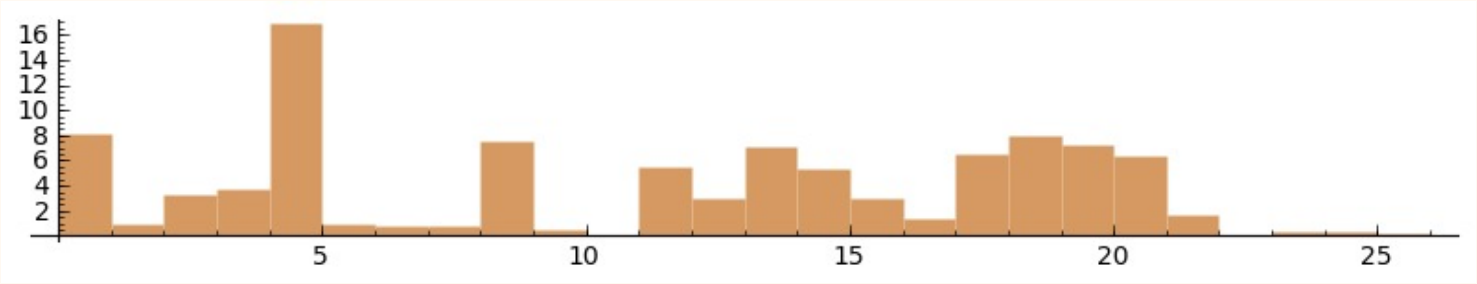
Al-Kindi (801-873)



Première page du manuscrit de Al-Kindi sur le déchiffrement des messages cryptographiques par analyse des fréquences.

Fréquences d'occurrence des lettres en français

Fréquences d'apparition des lettres en français



Le A, le pic du E, le I et les bosses LMNOP et RSTUV.

Informations additionnelles :

- bigrammes les plus fréquents : ES, DE, LE
- Lettres doublées les plus fréquentes : EE, SS, LL
- ...

Décryptage d'un cryptage par substitution

Message à décrypter.

```
CEGCL AM NMGAL LJC ZWIWJLL LH CYEWJ RMYCWLJ ZEHC
GHL LJC UMQWCLL RMY ALJ QLANLJ A MGCYL RMY ALJ
MVGWCMWHJ AM CYEWJWLPL RMY SLGF VGW ZMHJ ALGY AMHNGL
JL HEPPLHC SLACLJ LC ZMHJ AM HECYL NMGAEWJ
```

On attaque en considérant les fréquences d'apparition des lettres.

E	A	S	I	N	T	R	L
17,3%	8,4%	8,1%	7,4%	7,1%	7,0%	6,6%	6,0%

L	M	C	J	A	W	H	G
27	16	15	15	12	11	10	10

Décryptage d'un cryptage par substitution

Message à décrypter.

CEGCL AM NMGAL LJC ZWIWJLL LH CYEWJ RMYCWLJ ZEHC
GHL LJC UMQWCLL RMY ALJ QLANLJ A MGCYL RMY ALJ
MVGWCMWHJ AM CYEWJWLPL RMY SLGF VGW ZMHJ ALGY AMHNGL
JL HEPPLHC SLACLJ LC ZMHJ AM HECYL NMGAEWJ

Décryptage avec (L, M) $\rightarrow$ (E, A)

CEGCE AA NAGAE EJC ZWIWJEE EH CYEWJ RAYCWEJ ZEHC
GHE EJC UAQWCEE AY AEJ QEANEJ A AGCYE RAY AEJ
AVGWCAWHJ AA CYEWJWEPE RAY SEGF VGW ZAHJ AEGY AAHNGE
JE HEPPEHC SEACEJ EC ZAHJ AA HECYE NAGAEWJ

Décryptage d'un cryptage par substitution

Décryptage avec (L, M) $\rightarrow$ (E, A)

CEGCE AA NAGAE EJC ZWIWJEE EH CYEWJ RAYCWEJ ZEHC
GHE EJC UAQWCEE AY AEJ QEANEJ A AGCYE RAY AEJ
AVGWCAWHJ AA CYEWJWEPE RAY SEGF VGW ZAHJ AEGY AAHNGE
JE HEPPEHC SEACEJ EC ZAHJ AA HECYE NAGAEWJ

On essaye de deviner des lettres...

CEGCE AA NAGAE EJC ZWIWJEE EH CYEWJ RAYCWEJ ZEHC
GHE EJC UAQWCEE RAY AEJ QEANEJ A AGCYE RAY AEJ
AVGWCAWHJ AA CYEWJWEPE RAY SEGF VGW ZAHJ AEGY AAHNGE
JE HEPPEHC SEACEJ EC ZAHJ AA HECYE NAGAEWJ

Décryptage d'un cryptage par substitution

Décryptage avec (L, M, A) $\rightarrow$ (E, A, L)

CEGCE LA NAGLE EJC ZWIWJEE EH CYEWJ RAYCWEJ ZEHC
GHE EJC UAQWCEE RAY LEJ QELNEJ L AGCYE RAY LEJ
AVGWCAWHJ LA CYEWJWEPE RAY SEGF VGW ZAHJ LEGY LAHNGE
JE HEPPEHC SELCEJ EC ZAHJ LA HECYE NAGLEWJ

Décryptage avec (L, M, A, J) $\rightarrow$ (E, A, L, S)

CEGCE LA NAGLE ESC ZWIWSEE EH CYEWS RAYCWES ZEHC
GHE ESC UAQWCEE RAY LES QELNES L AGCYE RAY LES
AVGWCAWHS LA CYEWSWEPE RAY SEGF VGW ZAHS LEGY LAHNGE
SE HEPPEHC SELCES EC ZAHS LA HECYE NAGLEWS

...

Chiffre de Vigenère : cryptage

Vigenère (diplomate français) : Traité des chiffres (1586).

Clé secrète : un mot. (Exemple : la clé HUGO.)

Cryptage : on ajoute les lettres du message avec les lettres de la clé répétée.

Cryptage d'un message :

	AU CLAIR DE LA LUNE MON AMI PIERROT
+	HU GOHUG OH UG OHUG OHU GOH UGOHUGO
=	HO IZHCX RL FG ZBHK AVH GAP JOSYLUH

Chiffre de Vigenère : décryptage

Décryptage : on ajoute l'opposée de la clé.

L'opposé de HUGO est TGUM

	HUGO		7	20	6	14
+	TGUM		19	6	20	12
=	AAAA		0	0	0	0

Décryptage d'un message :

	HO IZHCX RL FG ZBHK AVH GAP JOSYLUH
+	TG UMTGU MT GU MTGU MTG UMT GUMTGUM
=	AU CLAIR DE LA LUNE MON AMI PIERROT

Chiffre de Vigenère : les attaques

- Le chiffre de Vigenère a été considéré comme incassable pendant près de 300 ans.
- Vers 1850, C. Babbage et F. Kasiski ont cassé ce chiffre.

Chiffre de Vigenère : attaque pour longueur de clé connue

Considérons le message suivant crypté avec une clé inconnue de longueur 4.

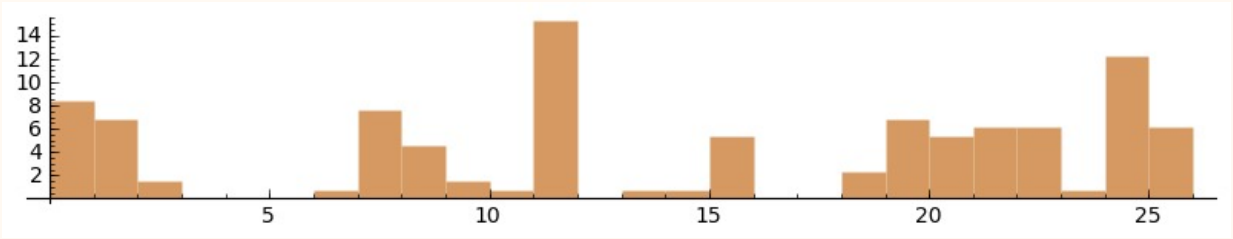
TUOHYYICYVKOBMAFBHGFILKDLLIVLNKBHCZSUMUBIYIIUZXC
TUMSTUOHYYXSUUXRWUXZVXKIYURZLWNSSOOHPHZOWYADYYYQ
LFGBNUMSOYHCUDUIYGUBZCKIYXAQVLHSHOWILPUIZYZSZDUZ
PKASCIAGTYYSTVRSGVKOBMGBZGKBACXGPPUHYYXOTUMSZYXO
WJUFAYGJVNXSWFAAHAKJVOYSAYYZLJNSUCDRLMNCAYYRLWKG
IIOGHWKGTIZGSYICYVKOBHKGLMKBAJGGKYPCPYKHWIAFTITH
YYXGHVKZSYBCPROZVOBFLOTZHLMSIYIZHCYGLNUAIYXGHJXC
PYRSYYTOYXYSUMGWZCZSAXOHTITPVHSCUMOSBLGDWLKBLTWI
LNUIAZROANKIYPOHHODRLJKBZXKQLFAWXOOZLWUIAYISANKZ
LWUBCUAHICKBBHLFVGGULMGBZXUIAYRSJIXPLUAVVHZSBRKH
JITTBMPIYUSOPMABWYAHHLJEBITBLFEDYYTRYUOHWFAG

Chiffre de Vigenère : attaque pour longueur de clé connue

Message extrait (de 4 en 4 partant du rang 0) :

TYYBBILLHUIUTTYUWVYLSPWYLNOUYZYVHLZZPCTTGBZAPYTZ
WAVWHVALULALIHTSYBLAKPWTYHSPVLHIHLIHPYYUZATVUBWL
LAAYHLZLXLAALCIBVLZAJLVBJBYPWHBLYYW

Ce message est obtenu en ajoutant à chaque lettre du message clair la même lettre de la clé. C'est donc un Chiffre de César



Histogramme des fréquences du message extrait

La première lettre de la clé est $11 - 4 = 7 =$ H.

Chiffre de Vigenère : attaque dans le cas général

- Si on connait la longueur de la clé, l'analyse des fréquences permet de décrypter le message crypté.

- Le décryptage du Chiffre de Vigenère se fait en essayant une longueur de clé de 2, 3, 4,... jusqu'à obtenir le texte clair.

Derniers cryptages par substitution

- La machine électromécanique Enigma (Arthur Scherbius, 1918) utilisée par l'armée allemande à partir de 1926. Cryptage par un renforcement du Chiffre de Vigenère.
- Premières attaques réussies par le polonais M. Rejewsky (années 1930). Peu avant l'invasion de la Pologne, Rejewsky communique ses informations aux français et britanniques.
- Pendant la 2^{e} guerre mondiale, le gouvernement britannique établit à Bletchley Park une importante équipe ($\approx 7\,000$ personnes) réunissant des mathématiciens, des logiciens, des linguistes, des cruciverbistes sous la direction de A. Turing.
- A l'aide de gros calculateurs électromécaniques, puis électroniques, cette équipe parvient à casser le code Enigma et ses perfectionnements.

Un exemplaire de la machine Enigma

Conclusion sur les cryptages alphabétiques

Désavantage principal. Petite taille des alphabets utilisés (quelques dizaines de lettres).

Attaques par l'étude des fréquences d'occurrences et leurs variations permettent d'identifier de courts extraits du message clair.

La cryptographie moderne

- Principe de Kerckhoff : publicité des algorithmes
- Fin des petits alphabets : cryptage par blocs
- Cryptographie à clé publique

Principe de Kerckhoff

Auguste Kerckhoff (professeur à l'Ecole des Hautes Etudes Commerciales) dans le Journal Des Sciences Militaires (1883) :

> *. . . si l'Administration veut mettre à profit tous les services que peut rendre un système de correspondance cryptographique bien combiné, elle doit absolument renoncer aux méthodes secrètes, et établir en principe qu'elle n'acceptera qu'un procédé qui puisse être enseigné au grand jour dans nos écoles militaires, que nos élèves seront libres de communiquer à qui leur plaira . . .*

Le principe de Kerckhoff : pourquoi ?

- On ne peut jamais garantir qu'un secret sera préservé.
- Les algorithmes de cryptage et de décryptages sont publics mais les protagonistes partagent une clé secrète.
- Il est plus facile de changer de clé que d'algorithme de cryptage.
- La publicité de l'algorithme est le meilleur moyen de s'assurer de sa robustesse.

Cryptage par blocs

- En cryptographie moderne, on commence par regrouper les caractères du message à crypter en blocs d'une taille fixe.
- On remplace ainsi l'alphabet des caractères par l'alphabet des blocs (en général binaires).
- Le nombre de lettres de l'alphabet est tout petit, mais le nombre de blocs d'une taille donnée est grand. Pour une taille de bloc de 64 bits, le nombre de blocs différents est

$$2^{64} = 18\,446\,744\,073\,709\,551\,616.$$

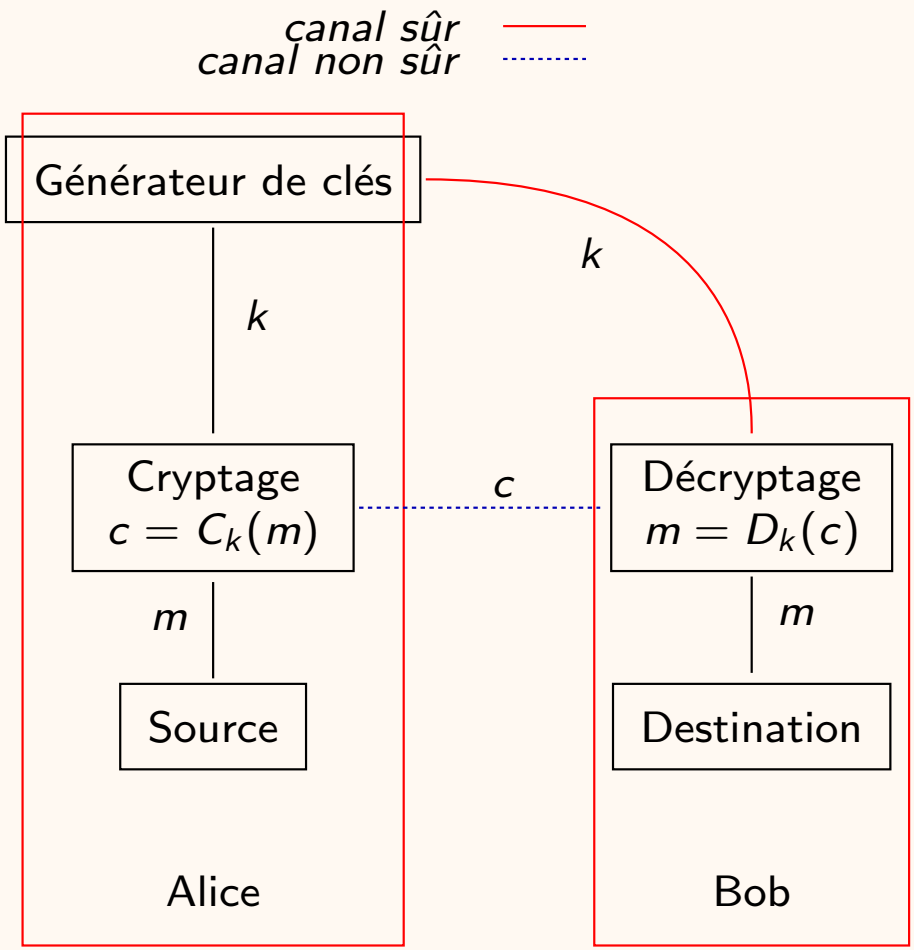
(Environ 3 000 000 "Library of Congress" [200 millions de livres])

- L'analyse des fréquence devient impossible.

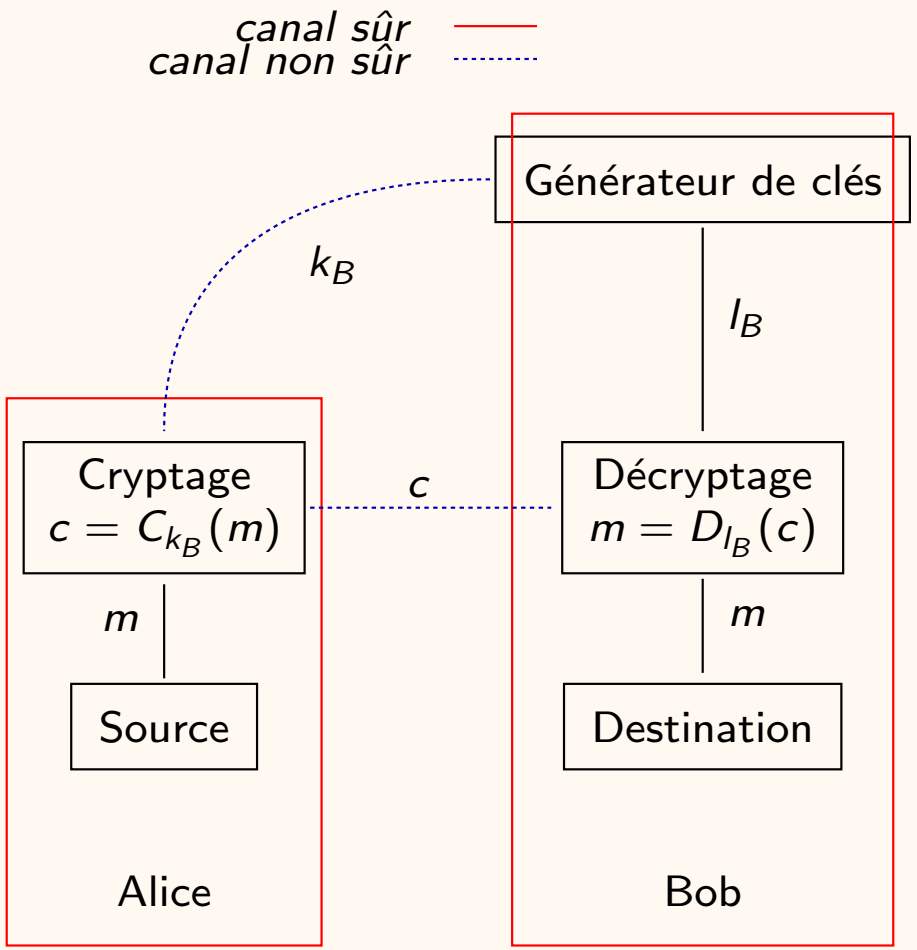
Cryptographie à clé publique (Diffie 1975)

- La sécurité du cryptage ne repose plus sur le partage d'une clé secrète.
- Le protocole contient deux clés : une clé publique pour crypter le message et une clé secrète pour décrypter le message.
- Il ne propose pas cependant de protocole effectif...

Protocoles à clé secréte et à clé publique



Protocole à clé secrète



Protocole à clé publique

Protocoles symétriques modernes : D. E. S et A. E. S

1976 : création du protocole à clé secrète D. E. S (Data Encryption Standard) suite à un appel d'offre du National Bureau of Standards en 1973. C'est le protocole dominant des années 1980-2000.

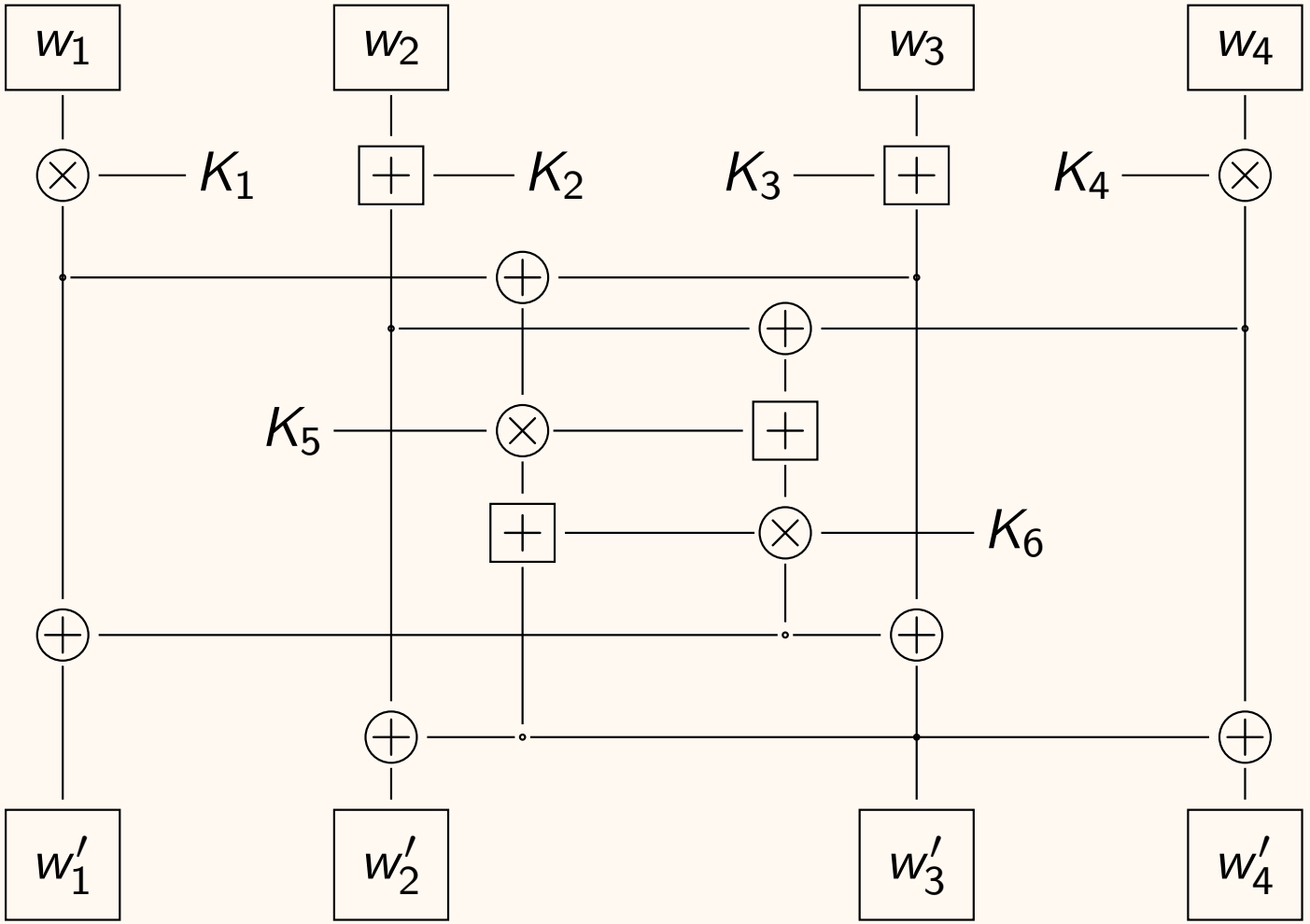
- Clefs de 56 bits. Cryptage par blocs de 64 bits.

Aujourd'hui, une attaque casse un message chiffré par D. E. S. en quelques heures.

1997 : Nouvel appel d'offre avec adoption en 2001 de A. E. S (Advanced Encryption Standard).

- Clé de 128, 192 ou 256 bits.
- Cryptage par blocs de 128 bits.
- Rapide $\approx$ 100 Mo par seconde.

Diagramme de base pour I.D.E.A. (une ronde)



Le tournant des années 1975-1980

Au début des années 1970.

- Cryptages rapides et sûrs avec D. E. S et variations.
- A condition de partager une clé avec chaque correspondant.
- Avec des d'échanges de plus en plus nombreux et de plus en plus lointains.
- Le problème du partage des clés devient inextricable.

Diffie et Hellmann apportent deux solutions à ce problème.

- Le protocole de Diffie–Hellman : Il est possible d'échanger un clé secrète au moyen d'une conversation que tout le monde peut entendre.
- La cryptographie asymétrique ou cryptographie à clé publique.

Un peu de math... L'anneau $\mathbb{Z}/m\mathbb{Z}$

- Réduire un nombre modulo m c'est le remplacer par le reste de sa division euclidienne par m (toujours entre 0 et $m-1$).
- Effectuer une addition ou une multiplication modulo m de x par y, c'est additionner ou multiplier x et y, puis réduire le résultat modulo m.
- Pour $m > 1$ un entier, $\mathbb{Z}/m\mathbb{Z}$ est l'ensemble des entiers réduits modulo m, muni de l'addition et de la multiplication modulo m (c'est un anneau).

Par exemple, $\mathbb{Z}/10\mathbb{Z}$ est l'ensemble $\{0,1,2,3,4,5,6,7,8,9\}$ et

$5+7 \equiv 2, \quad 3-7 \equiv 6, \quad 3 \cdot 2 \equiv 6, \quad 3 \cdot 9 \equiv 7, \quad 6 \cdot 5 \equiv 0.$

$(\mathbb{Z}/m\mathbb{Z})^*$ et $(\mathbb{Z}/p\mathbb{Z})^*$

Le sous-ensemble des entiers inversibles modulo m est défini par

$$(\mathbb{Z}/m\mathbb{Z})^* = \{0 \leq x \leq m-1 : \mathrm{PGCD}(x, m) = 1\}$$

est un groupe multiplicatif, c'est-à-dire :

Pour tout $x \in (\mathbb{Z}/m\mathbb{Z})^*$, il existe $y \in (\mathbb{Z}/m\mathbb{Z})^*$ tel que $xy \equiv 1$.

Exemple : $(\mathbb{Z}/10\mathbb{Z})^* = \{1, 3, 7, 9\}$ et $3 \cdot 7 \equiv 1$.

Pour $x \in (\mathbb{Z}/m\mathbb{Z})^*$, on pose

$$\langle x \rangle = \{x^0 = 1, x^1 = x, x^2, x^3, \cdots\} \subset (\mathbb{Z}/m\mathbb{Z})^*.$$

Exemple : $x = 5$ dans $(\mathbb{Z}/7\mathbb{Z})^* = \{1, 2, 3, 4, 5, 6\}$

$$\langle 5 \rangle = \{1,\ 5,\ 4,\ 6,\ 2,\ 3\}$$

Théorème : Soit p un nombre premier. Il existe $g \in (\mathbb{Z}/p\mathbb{Z})^*$ tel que $\langle g \rangle = (\mathbb{Z}/p\mathbb{Z})^*$. (C'est un groupe cyclique de générateur g).

Le protocole de Diffie-Hellman ou comment échanger une clé

- Alice : Choix de p (premier) et g générateur de $(\mathbb{Z}/p\mathbb{Z})^*$

  $p = 30\,967\,624\,360\,979\,079\,013 \quad g = 11\,595\,598\,273\,653\,509\,247.$

  - Choix de a (secret) et calcul de $A = g^a \mod p$

    $A = 23\,606\,831\,717\,615\,331\,161.$

  - Envoi sur canal publique de p, g et A à Bob.

- Bob : Choix de b (secret) et envoie sur canal publique à Alice de

  $B = g^b \mod p \equiv 14\,308\,194\,949\,994\,250\,745.$

- Alice calcule B^a et Bob calcule A^b. C'est le secret commun car

  $A^b = (g^a)^b = g^{ab} = (g^b)^a = B^a$

Le protocole de Diffie-Hellman d'échanger de clé

Que peut faire l'attaquant Eve ?

- Elle connait $A = g^a$, $B = g^b$, p et g.
- Elle ne connait pas a, b, ni ab. Comment trouver g^{ab} ?
- Il faut pouvoir résoudre le problème suivant :

  Etant donnés A, p et g. Trouver $a \in \{0, \ldots, p-1\}$ tel que

  $$g^a \mod p = A.$$

- C'est le problème du logarithme discret.

Problème du logarithme discret

Soit G un groupe fini cyclique d'ordre n de générateur g. Donc

$$G = \{g^0, g^1, g^2, \ldots, g^{n-1}\}.$$

Soit $x \in G$. Trouver $a \in \{0, \ldots, n-1\}$ tel que $x = g^a$.

Méthode directe. On calcule $g^0, g^1, g^2, \ldots$ jusqu'à obtenir $g^a = x$. coût $\approx n$ opérations dans G.

Méthodes génériques. Pour un groupe G de type *boîte noire*, il faut $\approx \sqrt{\ell}$ opérations dans G avec ℓ le plus grand nombre premier divisant n par la méthode Baby Step - Giant Step.

Pour $G = (\mathbb{Z}/p\mathbb{Z})^*$. On sait faire beaucoup mieux avec les méthodes d'indice.

Remarque. Si $g, x \in \mathbb{R}^+$ alors $a := \log(x)/\log(g)$.

Problème du logarithme discret : Baby step - Giant Step

Soit G un groupe fini cyclique d'ordre n engendré par g. Soit $x \in G$. Trouver $a \in \{0, \ldots, n-1\}$ tel que $x = g^a$.

Méthode. On pose $m = \lceil \sqrt{n} \rceil$. On calcule et on stocke

$$(j, g^j) \quad \text{pour} \quad j = 0, 1, \ldots, m-1.$$

Pour $k = 0, 1, \ldots,$ on teste si $xg^{-km} = g^j$ avec $j \in \{0, \ldots, m-1\}$. Si oui, on renvoie $km + j$.

Preuve. Par division euclidienne $a = km + j$ avec $0 \leq j < m$ et $k < m$ par choix de m.

Rapport $n \leftrightarrow \sqrt{n}$. 1h $\leftrightarrow$ 1mn, 1 mois $\leftrightarrow$ 27mn, 1 an $\leftrightarrow$ 1h35...

Protocole RSA (Rivest, Shamir, Adleman 1977)

- Clé secrète : p et q deux grands nombres premiers
- Clé publique : $N = pq$ et un exposant e (en général 3 ou $2^{16} + 1 = 65\,537$).
- Message : entier $x \in (\mathbb{Z}/N\mathbb{Z})^*$.
- Le cryptage est l'application $x \mapsto x^e$
- Le décryptage est l'application $y \mapsto y^d$ avec $ed = 1 \pmod{(p-1)(q-1)}$.

Preuve. On a

$$(\mathbb{Z}/N\mathbb{Z})^* \simeq (\mathbb{Z}/p\mathbb{Z})^* \times (\mathbb{Z}/q\mathbb{Z})^*$$

donc c'est un groupe d'ordre $(p-1)(q-1)$ et $x^{(p-1)(q-1)} = 1$.

Calculer d est facile si on peut retrouver p et q à partir de N.
Pour casser RSA, il faut résoudre le problème de la factorisation.

Factorisation : la méthode ρ de Pollard

Paradoxe des anniversaires.

Question. Combien faut-il de personnes pour en avoir (au moins) deux avec le même anniversaire ? et avec une probabilité $> 1/2$?

Formalisation. $E := \{e_1, \ldots, e_n\}$. Eléments $x_1, \ldots, x_k$ dans E au hasard *avec répétition possible*.
Probabilité p_k qu'il existe $i \neq j$ tels que $x_i = x_j$?

Pobabilité que tous les x_i soient distincts :

$$\frac{n(n-1)\cdots(n-(k-1))}{n^k} = \prod_{i=1}^{k-1}\left(1-\frac{i}{n}\right) \approx \exp\left(\frac{-k(k-1)}{2n}\right)$$

Théorème. Si $k \geq 1, 2\sqrt{n}$, alors $p_k > 1/2$.

Réponse. pour $n = 365$, on trouve $\lceil 1, 2\sqrt{n} \rceil = 23$.

Factorisation : la méthode ρ de Pollard

But. Factoriser $N = pq$.

Idée. $x_1, \ldots, x_k$ nombres au hasard entre 0 et $N-1$. Pour $k \approx \sqrt{p}$, avec probabilité $> 1/2$, il existe $i \neq j$ tels que $x_i \equiv x_j \pmod{p}$ et donc

$$\mathrm{PGCD}(x_i - x_j, N) > 1.$$

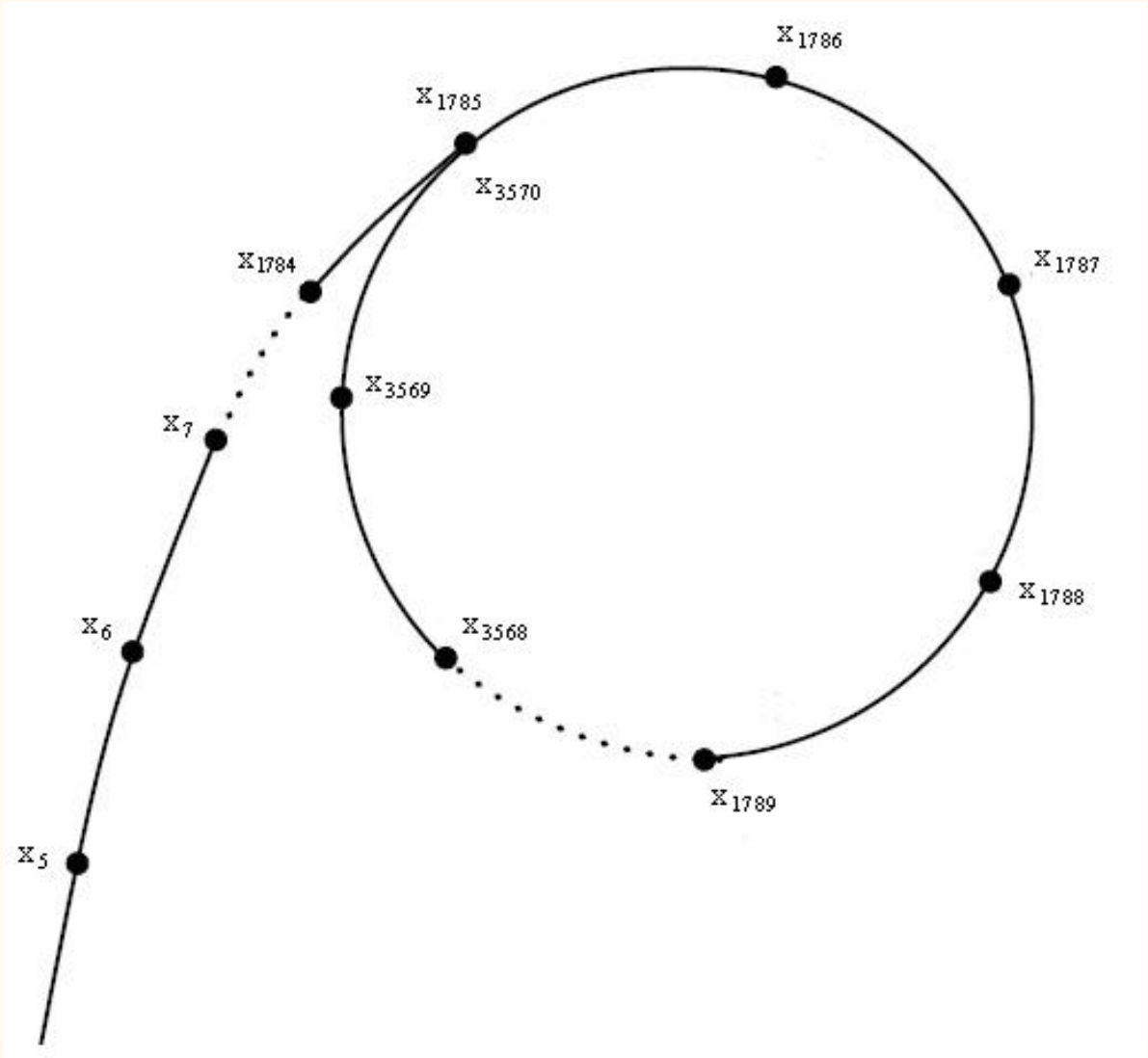
Problème. il faut stocker toutes les valeurs et tester toutes les paires !

Solution. On utilise la suite $x_1 = \lceil \sqrt{N} \rceil$ et $x_i = x_{i-1}^2 + c \mod N$. La suite $(x_i)_{i \geq 0}$ (presque une suite aléatoire pour $c \neq 0, -2$) et est ultimement périodique modulo p.

Théorème. Si (x_n) est un suite ultimement périodique, il existe $m \geq 1$ tel que $x_m = x_{2m}$.

Estimation du coût. $\approx \sqrt{p} \approx N^{1/4}$ opérations.

Factorisation : la méthode ρ de Pollard



Factorisation : la méthode ρ de Pollard

Exemple. Factoriser $N = 127\,199$.

m	x_m	x_{2m}	PGCD	m	x_m	x_{2m}	PGCD
1	357	251	1	11	125075	105564	1
2	251	7210	1	12	59412	28503	1
3	63002	97662	1	13	13495	103617	1
4	7210	114009	1	14	93257	97895	1
5	86909	54078	1	15	18022	99548	1
6	97662	59412	1	16	53438	42431	1
7	103628	93257	1	17	2295	44053	1
8	114009	53438	1	18	51867	115435	1
9	95068	51867	1	19	54039	28231	1
10	54078	106079	1	20	106079	123495	311

D'où la factorisation $N = 311 \cdot 409$

Conclusion générale

- On ne peut pas préjuger de l'applicabilité de la recherche fondamentale.
- L'arithmétique a beaucoup apporté à la cryptographie.
- Inversement, les problèmes posés par la cryptographie, on revivifié des domaines mathématiques déjà anciens, comme la factorisation des entiers, en y apportant de nouveaux points de vue et de nouvelles questions.

Bibliographie

- Histoire des codes secrets. Simon Singh J. C. Lattès (1999)
  Traduction par Catherine Coqueret de The Code Book.

- Histoire des codes secrets. LGF Livre de Poche (2001)