Cryptographie : Comment l'arithmétique est devenue science appliquée

Marc Deléglise

Université Ouverte Lyon 1
Des mathématiques tout autour de nous

18 octobre 2012
Bibliothèque Marie Curie, INSA de Lyon

Les vraies mathématiques n'ont aucun effet sur la guerre. Personne n'a encore trouvé un objectif militaire qui serait dépendant de la théorie des nombres

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

Vocabulaire

- Chiffrer un message c'est le rendre incompréhensible au non destinataire. Un cryptogramme est un message chiffré.
- Déchiffrer le cryptogramme c'est retrouver le message clair, à l'aide du « mode d'emploi ». C'est la tâche du destinataire régulier.
- Décrypter le cryptogramme c'est retrouver le message clair sans disposer du « mode d'emploi ». C'est le travail de l'espion.
- Les cryptographes conçoivent les systèmes de chiffrement.
- Les cryptanalystes sont les spécialistes du décryptement.

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 chiffrement de César

Soit l'alphabet ABCDEFGHIJKLMNOPQRSTUVWXYZ.

César choisit une clef par exemple la clef C

Le chiffrement est le décalage qui envoie A sur C, le décalage de 2.

DEMAIN MATIN A LYON
FGOCKP OCVKP C NAQP

Déchiffrement et décryptage du Chiffre de César

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

Décryptons `C FHOCKP` :

- Clef A : `C FHOCKP` $\rightarrow$ `C FHOCKP`
- Clef B : `C FHOCKP` $\rightarrow$ `B EGNBJO`
- Clef C : `C FHOCKP` $\rightarrow$ `A 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 chiffrement 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 rang du chiffrement de X s'obtient en ajoutant 2 au rang de X, et, si le résultat est ≥ 26 on en retranche 26.

Cette opération s'appelle l'addition modulo 26.

Déchiffrement du Chiffre de César et addition des lettres

On chiffre en ajoutant la clef, on déchiffre en soustrayant la clef, c'est à dire en ajoutant l'opposé de la clef.

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

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

Chiffrement par substitution alphabétique

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

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

Pour chiffrer un message on applique la substitution σ à chacune des lettres de ce message.

$$\mathtt{DEMAIN\ A\ LYON} \quad \longrightarrow \quad \mathtt{EAHGZI\ G\ XQUI}$$

On déchiffre en remplaçant σ par la permutation inverse.

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

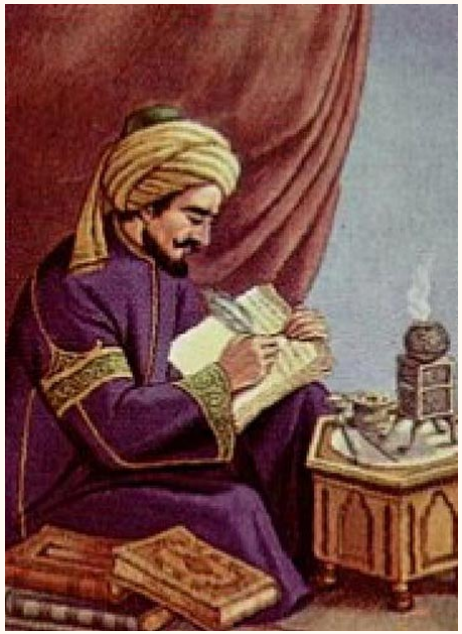
Décryptage du chiffrement par substitution

On essaie toutes les clefs ?

- Nombre de clefs $= 26\,! = 1\ x\ 2\ x\ 3\ x\ \cdots\ x\ 26 =$ 403291461126605635584000000
- Mais il est assez facile de décrypter en analysant les fréquences d'occurences des caractères.

Une attaque redoutable : l'analyse des fréquences

Al-Kindi (801-873)

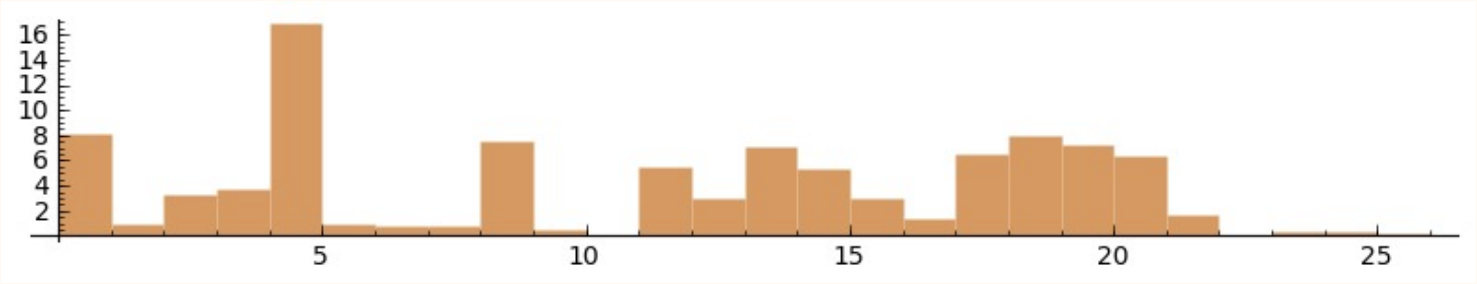


The first page of al-Kindi's manuscript *On Deciphering Cryptographic Messages*, containing the oldest known description of cryptanalysis by frequency analysis.

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

Fréquences d'occurence 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.

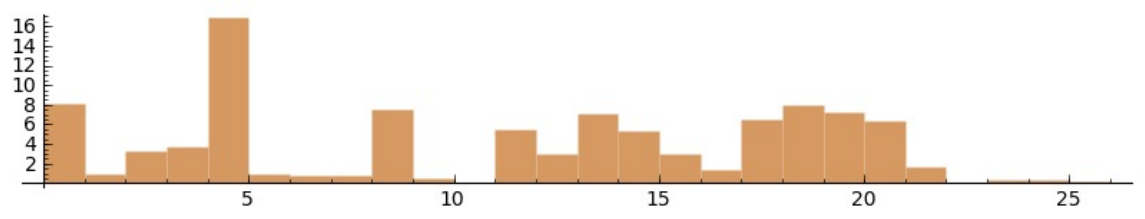
Décryptage d'un chiffrement par substitution

On utilise les informations statistiques sur les occurences de certains assemblages de lettres :

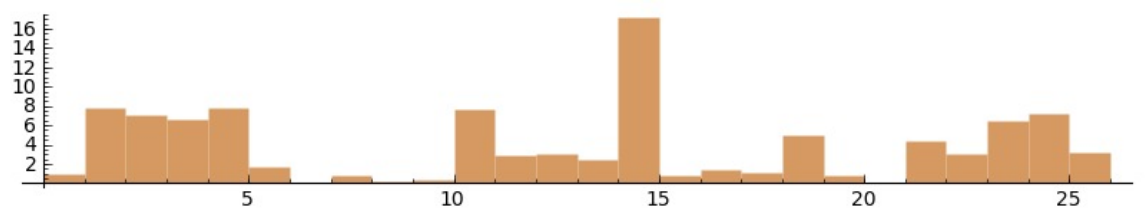
- Le `E` l'emporte de loin.
- Les lettres les plus fréquentes sont ensuite `O, A, I`.
- bigrammes les plus fréquents : `ES, DE, LE`
- Lettres doublées les plus fréquentes : `EE, SS, LL`
- ...

La connaissance de ces informations, l'habileté et l'intuition faisaient la qualité du cryptanalyste dans les siècles passés. Jusqu'à la deuxième guerre mondiale les bureaux du chiffre employaient des linguistes, des érudits, ou même des cruciverbistes ...

Décryptage graphique d'un chiffre de César



Histogramme français moyen



Histogramme d'un message chiffré par César

La clef est 14 - 4 = 10 = K.

Chiffrement de Vigenère

- Au XV^{e} siècle les chiffrements utilisés reposaient essentiellement sur la substitution.
- Malgré quelques perfectionnements les cryptanalystes les brisaient de plus en plus facilement. L'avantage était du côté des cryptanalystes.
- Reprenant des idées de Leon Battista Alberti (≈ 1467), puis de Giovan Battista Bellaso (≈ 1550), le diplomate français Vigenère publie son Traité des chiffres en 1586.

Chiffrement de Vigenère : le chiffrement

- La clef secrète est un mot. Choisissons la clef HUGO
- Les lettres successives du message sont chiffrées par la méthode de César avec les clefs successives HUGOHUGOH...

Alice chiffre en effectuant, lettre par lettre, les additions

$$\begin{array}{rl} & \texttt{AUCLAIRDELALUNEMONAMIPIERROT} \\ + & \texttt{HUGOHUGOHUGOHUGOHUGOHUGOHUGO} \\ \hline = & \texttt{HOIZHCXRLFGZBHKAVHGAPJOSYLUH} \end{array}$$

Chiffrement de Vigenère : Déchiffrement

Comme le chiffrement en remplaçant la clef par son opposée

L'opposé de HUGO est TGUM

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

Bernard déchiffre le message reçu d'Alice en effectuant les additions

	HOIZHCXRLFGZBHKAVHGAPJOSYLUH
+	TGUMTGUMTGUMTGUMTGUMTGUMTGUM
=	AUCLAIRDELALUNEMONAMIPIERROT

Chiffrement de Vigenère : Décryptage

- Le chiffrement de Vigenère a été considéré comme indécryptable pendant près de 300 ans.
- C. Babbage et F. Kasiski on cassé ce chiffrement (≈ 1850).

Décryptage de Vigenère à longueur de clef connue

Si la longueur de la clef est connue, le décryptage est très simple. Décryptons le cryptogrammme suivant, chiffré avec une clef inconnue, mais de longueur connue 4.

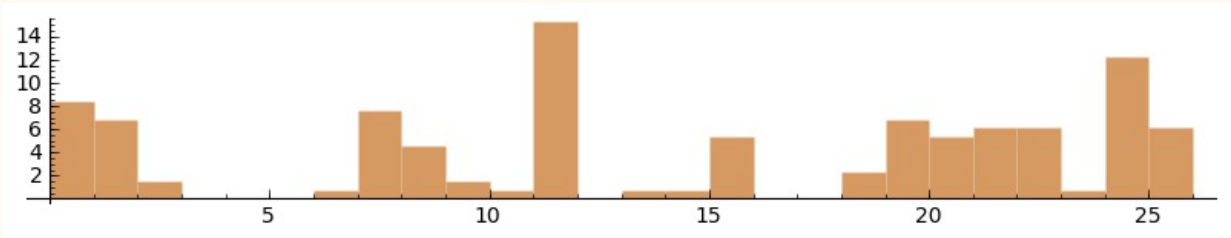
```
TUOHYYICYVKOBMAFBHGFILKDLLIVLNKBHCZSUMUBIYIIUZXC
TUMSTUOHYYXSUUXRWUXZVXKIYURZLWNSSOOHPHZOWYADYYYQ
LFGBNUMSOYHCUDUIYGUBZCKIYXAQVLHSHOWILPUIZYZSZDUZ
PKASCIAGTYYSTVRSGVKOBMGBZGKBACXGPPUHYYXOTUMSZYXO
WJUFAYGJVNXSWFAAHAKJVOYSAYYZLJNSUCDRLMNCAYYRLWKG
IIOGHWKGTIZGSYICYVKOBHKGLMKBAJGGKYPCPYKHWIAFTITH
YYXGHVKZSYBCPROZVOBFLOTZHLMSIYIZHCYGLNUAIYXGHJXC
PYRSYYTOYXYSUMGWZCZSAXOHTITPVHSCUMOSBLGDWLKBLTWI
LNUIAZROANKIYPOHHODRLJKBZXKQLFAWXOOZLWUIAYISANKZ
LWUBCUAHICKBBHLFVGGULMGBZXUIAYRSJIXPLUAVVHZSBRKH
JITTBMPIYUSOPMABWYAHHLJEBITBLFEDYYTRYUOHWFAG
```

Décryptage de Vigenère avec clef de longueur 4

Cryptogramme-4-0 (de 4 en 4 partant du rang 0) :

TYYBBILLHUIUTTYUWVYLSPWYLNOUYZYVHLZZPCTTGBZAPYTZ
WAVWHVALULALIHTSYBLAKPWTYHSPVLHIHLIHPYYUZATVUBWL
LAAYHLZLXLAALCIBVLZAJLVBJBYPWHBLYYW

Puisque la longueur de clef est 4, ce cryptogramme s'obtient en ajoutant à chaque lettre du message clair la première lettre de la clef. C'est donc un chiffrement de César



Histogramme des fréquences du Cryptograme-4-0

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

Calcul de la longueur de la clef d'un chiffre de Vigenère

- Nous venons de voir que si l'on connait la longueur de la clef, l'analyse des fréquences permet de décrypter facilement un cryptogramme.
- Le décryptage du chiffrement de Vigenère se réduit donc à la détermination de la longueur de la clef. Il suffit de recommencer ce que l'on vient de faire en essayant les longueurs de clef 2, 3, 4,... jusqu'à obtenir le texte clair.

Les derniers chiffrements par substitution

- La machine éléctromécanique Enigma, conçue en 1918 par Arthur Scherbius sera utilisée par l'armée allemande à partir de 1926. Son chiffrement était un renforcement du chiffre de Vigenère.
- Les cryptanalystes eurent le plus grand mal à décrypter ses messages. Les premiers succès sont dûs au polonais M. Rejewsky dans les années 1930. Peu avant l'invasion de la Pologne, Rejewsky transmet 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 comme A. Turing, des linguistes, et même des cruciverbistes.
- Sous la direction d'A. Turing, et à l'aide de gros calculateurs électromécaniques, puis électroniques, ils vinrent à bout des chiffrements produits par Enigma et ses perfectionnements.

Un exemplaire de la machine Enigma

Machine Colossus, à Bletchey-Park ($\approx$ 1944)

Première machine éléctronique, et non plus électromécanique

Conclusion sur les chiffrements alphabétiques

Le talon d'Achille commun à tous les procédés de chiffrement alphabétique est la petite taille des alphabets utilisés. L'alphabet source et l'alphabet de chiffrement sont constitués d'au plus quelques dizaines de caractères.

Ceci permet au cryptanalyste d'analyser les fréquences d'occurences de certains caractères, ou petits groupes de caractères, et d'identier de courts extraits du message clair.

Une exception : le chiffrement de G. Vernam (1917)

G. Vernam, ingénieur à l'A.T.T [1] a proposé en 1917 de chiffrer un message par la méthode de Vigenère avec une clef aléatoire de même longueur que le message

	DEMAINNEUFHEURESALYON
+	HUDECJHEIONLACDEPKGSQ
=	KYPEKWUICTUPUTHWPVEGD

	DEMAINDIXHEURESAPARIS
+	HUDECJRAFMQVDPPWAVNYL
=	KYPEKWUICTUPUTHWPVEGD

1. American Telegraph & Telephon

Le chiffre de Vernam est parfait mais difficilement utilisable

- Ceci montre qu'un même texte chiffré peut être le chiffrement de n'importe quel message clair, en choisissant convenablement la clef.
- Ce procédé de chiffrement est donc parfait.
- A condition de ne pas réutiliser la clef.
- Et d'utiliser une clef aléatoire.

Pourquoi l'histoire de la cryptographie ne s'est elle pas achevée en 1917 ?

- Il est difficile d'échanger une clef avec un correspondant éloigné.
- Surtout si l'on doit recommencer l'échange à chaque envoi.
- Le chiffre de Vernam a peu été employé.
- Américains et russes l'auraient utilisé sur la ligne rouge après la crise de Cuba (1962).

Les premiers chiffrements modernes

- Principe de Kerckhoff : publicité des algorithmes
- Fin des petits alphabets : chiffrement par blocs

Principe de Kerckhoff

Auguste Kerckhoff, professeur à l'Ecole des Hautes Etudes Commerciales, écrivait en 1883 dans le Journal Des Sciences Militaires :

> *. . . 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 chiffrement et de déchiffrement sont publics mais Alice et Bernard partagent une clef secrète.
- Il est plus facile de changer de clef que d'algorithme de chiffrement.
- La publicité de l'algorithme est le meilleur moyen de s'assurer de sa robustesse.

Le chiffrement par blocs

- Les pages précédentes ont mis en évidence les dangers des substitutions alphabétiques sur de petits alphabets.
- Elles ouvrent une brèche au cryptanalyste : l'analyses des fréquences d'occurences des caractères.
- En cryptographie moderne l'unité de chiffrement n'est pas la lettre. On commence par regrouper les caractères du message à chiffrer en blocs d'une taille fixe.
- On remplace ainsi l'alphabet des caractères par l'alphabet des blocs.
- Le nombre de lettre de l'alphabet est tout petit, mais le nombre de blocs d'une taille donnée est grand. Pour une taille de bloc de 16 octets, soit 128 bits le nombre de blocs différents est
$$2^{128} \approx 3.4 \times 10^{38}.$$
- L'analyse des fréquence devient considérablement plus difficile.

Transformer un message en une suite de blocs

Découpons le message `MAITRE CORBEAU SUR UN ARBRE.` en blocs de 4 charactères,

MAIT RE C ORBE AU S UR U N AR BRE.

Les codes ASCII[2] des charactères de MAIT sont 77, 65, 73, 84, ou, en base 2, 01001101, 01000001, 01001001, 01010100.

En juxtaposant ces 4 nombres, on obtient l'écriture binaire d'un entier 01001101010000010100100101010100 dont l'écriture décimale est 1296124244.

Le message est de cette façon transformé en une suite d'entiers. L'algorithme de chiffrement va transformer chacun des ces entiers en un autre entier.

2. American Standard Code for Information Interchange

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

En 1973 le N. B. S.[3] lance un appel d'offres pour un chiffrement public a clef secrète qui donne naissance en 1976 au protocole dominant des années 1980-2000, le protocole D. E. S

- Clefs de 56 bits. Chiffrement par blocs de 8 charactères (64 bits)

Aujourd'hui, avec de puissants moyens de calcul, on peut décrypter un message chiffré à l'aide de D. E. S. en quelques jours.

1997 : Un nouvel appel d'offres du N. I. S. T[4] conduit à l'adoption en 2001 de A. E. S

- Robuste et implémentable sur toutes sortes de machines.
- Assez rapide, il chiffre couramment 10 Mo par seconde.

3. National Bureau of Standards
4. National Institute of Standards and Technology

La situation de la décénnie 1970-1980

- On ne chiffre plus lettre par lettre, mais par bloc de quelques dizaines ou centaines de bits.
- Les algorithmes sont publics.

- Chiffrements rapides et surs.
- A condition de partager une clef avec chaque correspondant.
- De plus en plus d'echanges, de plus en plus lointains.
- L'échange de clefs devient un problème sérieux.

Construire des cadenas arithmétiques

La multiplication modulaire

- Réduire un nombre modulo m c'est le remplacer par le reste de sa division par m.
- Effectuer la multiplication modulo m de x par y, c'est multiplier x par y, puis réduire le résultat modulo m.
- Si m est un entier > 1 on note $\mathbb{Z}_m$ l'ensemble des entiers réduits modulo m, muni de la multiplication modulo m.

Par exemple, $\mathbb{Z}_{10}$ est l'ensemble $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$, muni de la multiplication modulo 10.

Voici quelques multiplications dans $\mathbb{Z}_{10}$

$$3 \cdot 2 = 6, \qquad 3 \cdot 9 = 7, \qquad 6 \cdot 5 = 0.$$

L'exponentiation modulaire

L'opération arithmétique la plus utilisée en cryptographie moderne est l'exponentiation modulaire : m, u et b sont trois entiers. Il s'agit de calculer $u^b \mod m$ c'est à dire le résultat de la multiplication modulo m de u par lui même, répétée b fois.

Si $m = 10$, $u = 7$ et $b = 3$. Modulo 10 on obtient successivement :

$$u \times u = 7 \times 7 = 49 = 9, \quad (u \times u) \times u = 9 \times 7 = 63 = 3.$$

Pour de grandes valeurs de u, b, m, quelques centaines de chiffres décimaux, il est absolument exclu d'effectuer b multiplications. Comment faire ?

Multiplication du pauvre

Pour multiplier 19 par 37

19	37
9	74
4	148
2	296
1	592

$$19 \times 37 = 37 + 74 + 592 = 703$$

Ecriture décimale de 2357

Comment obtenir les chiffres de l'écriture en base 10 de 2357 ?

2357	7
235	5
23	3
2	2

- A droite, le reste de la division par la base 10
- Au dessous, le quotient de la division par 10

Ecriture binaire de 19

Comment obtenir les chiffres de l'écriture en base 2 de 19 ?

Au lieu de diviser par 10 on divise par 2.

19	1
9	1
4	0
2	0
1	1

$$19 = 1 \times 16 + 0 \times 8 + 0 \times 4 + 1 \times 2 + 1$$

Explication : écriture binaire de 19

Revenons à la multiplication du pauvre, en ajoutant deux colonnes

19	1	1	37
9	1	2	74
4	0	4	148
2	0	8	296
1	1	16	592

Voila l'explication : $19 = 1 + 2 + 16$

L'algorithme d'exponentiation modulaire

Pour calculer $37^{19} \pmod{100}$, dans la dernière colonne on remplace $t \mapsto 2t$ par $t \mapsto t^2$ modulo 100.

19	$37 \bmod 100$	$= 37$
9	$37^2 \bmod 100$	$= 69$
4	$69^2 \bmod 100$	$= 61$
2	$61^2 \bmod 100$	$= 21$
1	$21^2 \bmod 100$	$= 41$

En multipliant les éléments non rayés de la dernière colonne on obtient, modulo 100,

$$37^{19} = 37 \times 37^2 \times 37^{16} = 37 \times 69 \times 41 = 73.$$

Coût de l'exponentiation modulaire

- Pour calculer $u^{1\,000\,000\,000\,000} \pmod{m}$ il suffit d'environ 70 multiplications.
- En réalité il faut tenir compte du fait que le coût d'une multiplication d'entiers de même taille est proportionnel au carré de leur taille.
- Si on remplace m par un entier 10 fois plus long, le temps de calcul est multiplié par $10 \times 10 \times 10 = 1000$.

$\mathbb{Z}_p$ possède un *générateur* lorsque p est premier

Considérons l'élément $g = 5$ de $\mathbb{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\}$. Partons de 1, et multiplions par g, en n'oubliant pas de réduire le résultat modulo 7 à chaque fois,

$$1,\ 5,\ 4,\ 6,\ 2,\ 3,\ 1\ \ldots$$

On obtient tous les éléments non nuls de $\mathbb{Z}_7$. On dit encore que 5 est un générateur multiplicatif de $\mathbb{Z}_7$.

On démontre que chaque fois que p est un nombre premier $\mathbb{Z}_p$ possède au moins un générateur multiplicatif.

L'exponentiation modulaire est un cadenas

$p = 486727636231140268491894 1$ est un nombre premier et 2 un générateur multiplicatif de $\mathbb{Z}_p$.

Comment calculer x tel que, modulo p, on ait $2^x = 10$.

Réponse : On ne sait pas si p a plus de 200 chiffres décimaux[5].

- À partir de x on calcule facilement $u = 2^x \pmod{p}$
- Impossible de revenir en arrière i.e. retrouver x à partir de u.
- L'exponentiation modulaire $x \mapsto g^x$ est un cadenas. Calculer x à partir de g^x est le problème du logarithme discret.

5. Ici p n'est pas très grand et $x = 344802304910661024310497 9$

Un autre cadenas

- Soit p et q deux nombres premiers de 150 chiffres. Il est facile de calculer
$$N = p \times q$$
- Mais à partir de la seule donnée de N, aujourd'hui, personne n'est capable de retrouver p et q.
- La fonction $(p, q) \mapsto pq$ est le cadenas qui est à la base du système R.S.A.

Le tournant des années 1975-1980

Au début des années 1970

- Chiffrements rapides et surs avec D. E. S puis A. E. S.
- A condition de partager une clef avec chaque correspondant.
- De plus en plus d'echanges, de plus en plus lointains.
- Le problème du partage de clef devient inextricable.

Diffie et Hellmann apportent deux solutions à ce problème.

- Le protocole de Diffie–Hellman : Il est possible d'échanger un clef secrète au moyen d'une conversation que tout le monde peut entendre.

- La cryptographie asymétrique, clef de chiffrement publique, clef de déchiffrement secrète.

Medaillés Kobayashi de l'I.E.E.E[6] , 1999-2000

R. Rivest, L. Adleman, A. Shamir (2000) W. Diffie, M. Hellmann, R. Merkle (1999)

Shamir, Rivest, Adleman, Merkle, Hellman, Diffie

6. Institute of Electrical and Electronics Engineers

Le protocole de Diffie-Hellman, ou comment échanger un secret sur une place publique

- Alice et Bernard désirent partager une clef secrète. Eve intercepte toutes leurs conversations.
- Le problème semble insoluble.
- W. Diffie et M. Hellman proposent en 1976 une solution simple.

Voici le dialogue d'Alice et Bernard :

- Alice :
  $p = 30967624360979079013 \quad g = 11595598273653509247$,
  - J'ai choisi secrètement a et calculé $A = g^a \mod p$

    $$A = g^a = 23606831717615331161.$$
  - Peux tu choisir en secret b et me donner la valeur de $B = g^b$?
- Bernard : Voici ma réponse : $B = 14308194949994250745$.

- Alice : Calcule A^b, pendant que, de mon côté, je calcule B^a.
  C'est le secret que nous partageons, car, modulo p,

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

Que peut faire Eve ?

- Elle connait A, B, p et g.
- Elle ne connait pas ab. Comment trouver g^{ab} ?
- On ne voit pas. A moins de savoir calculer les logarithmes en base g.
- Car, dans ce cas, à partir de $A = g^a$, on calcule a, puis, de même, b à partir de $B = g^b$.

Ce protocole permet-il de communiquer ?

- Remarquons que ni Alice, ni Bernard, ne connait a priori le secret partagé.
- Le protocole de Diffie-Hellman, à lui tout seul, ne permet pas d'échanger des informations.
- Il permet d'obtenir une clef secrète, puis de l'utiliser pour chiffrer des messages à l'aide, par exemple de A. E. S.

Les chiffrements à clef publique

Diffie publie en 1975 un article dans lequel il propose le développement de nouveaux systèmes de chiffrement.

- Pourquoi la sécurité du chiffrement devrait-elle nécessairement reposer sur la partage par Alice et Bernard d'une clef secrète ?
- Il semblait que personne n'avait encore imaginé qu'on puisse s'écarter de ce schéma. [7]

7. Selon le gouvernement anglais, la cryptographie publique a été inventée par James Ellis au début des années 1970. Mais son travail était alors couvert par le secret.

Cryptographie à deux clefs

Voici la proposition de Diffie :

- Chaque individu dispose d'une clef publique c et d'une clef privée k.
- Deux algorithmes publics Chiffre et Dechiffre

$$\text{Chiffre}\ (c, x) \mapsto y \quad \text{et} \quad \text{Dechiffre}\ (k, y) \mapsto x$$

- Les clefs publiques c sont disponibles sur un annuaire.
- Si c_a est la clef publique d'Alice, pour lui adresser le message x on lui envoie le cryptogramme $y = \text{Chiffre}(c_a, x)$
- Avec sa clef secrète k_a, Alice obtient $x = \text{Dechiffre}(k_a, y)$.

Chiffrement de Rivest, Shamir et Adleman (1977)

C'est le premier système de chiffrement à deux clefs qui se soit imposé. Il est le plus utilisé aujourd'hui.

- Les clefs publique et privée d'Alice sont

$$c_a = (N, e) \quad \text{et} \quad k_a = (N, d).$$

$N = pq$ est le produit de deux grands nombres premiers p et q.

$ed - 1$ est un multiple de $(p-1)(q-1)$.

- Le chiffrement est l'application $x \mapsto x^e \mod N$
- Le déchiffrement est l'application $y \mapsto y^d \mod N$

Signature : Qui m'envoie ce message ?

Bernard, banquier d'Alice, reçoit ce message :

> *Veuillez prélever* 10 000 € *sur mon compte et expédier cette somme à mon adresse.* *Alice 18 rue des Tilleuils.*

L'expéditeur est il Alice ou Eve ? Il faut un procédé permettant de garantir que l'expéditeur est bien Alice. C'est ce qu'on appelle un algorithme de signaure.

Tout système de chiffrement à deux clefs fournit, en prime, un algorithme de signature.

La situation aujourd'hui.

- Il n'y a plus de problème d'échange de clef.
- Le problème de signature a une solution simple.
- Les chiffrements à clef publique sont lents, environ 1000 fois plus lents que A. E. S
- Ce n'est pas gênant, car, pour envoyer un message :
  1. On partage une clef symétrique c, par un procédé lent, RSA ou Diffie-Hellman.
  2. Le message proprement dit, qui peut être long, est crypté avec un chiffrement symétrique rapide commes A. E. S en utilisant la clef secrète partagée c.

Le futur

- Remplacement des ensembles $\mathbb{Z}_m$ par des courbes elliptiques
- La cryptographie quantique

$\mathbb{Z}_p$ est–il indispensable ?

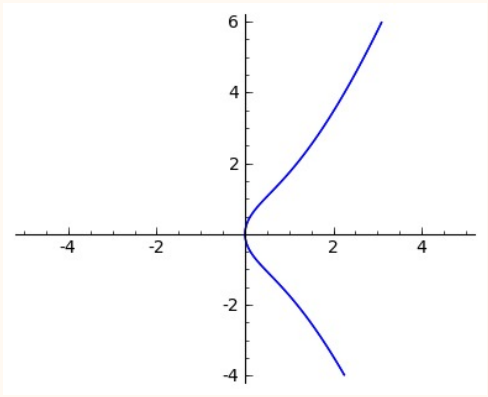
- Si G est un groupe dont un élément g est fixé. Le problème du logarithme discret en base g est :

  Soit $u = g^x$. Calculer x en ne connaissant que g et u.

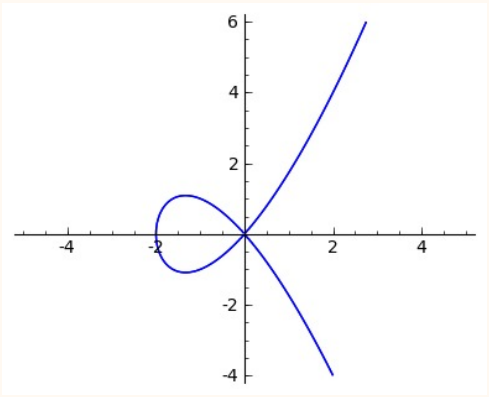
- Les protocoles actuels utilisant le problème du logarithme discret modulo p, peuvent être remplacés par des protocoles basés sur les logarithmes discrets sur le groupe constitué des points d'une courbe elliptique.

Les courbes elliptiques

- Une courbe elliptique est une courbe sans points singuliers définie par une équation $P(x, y) = 0$ où P est un polynôme de degré 3. La courbe de droite a un point singulier.



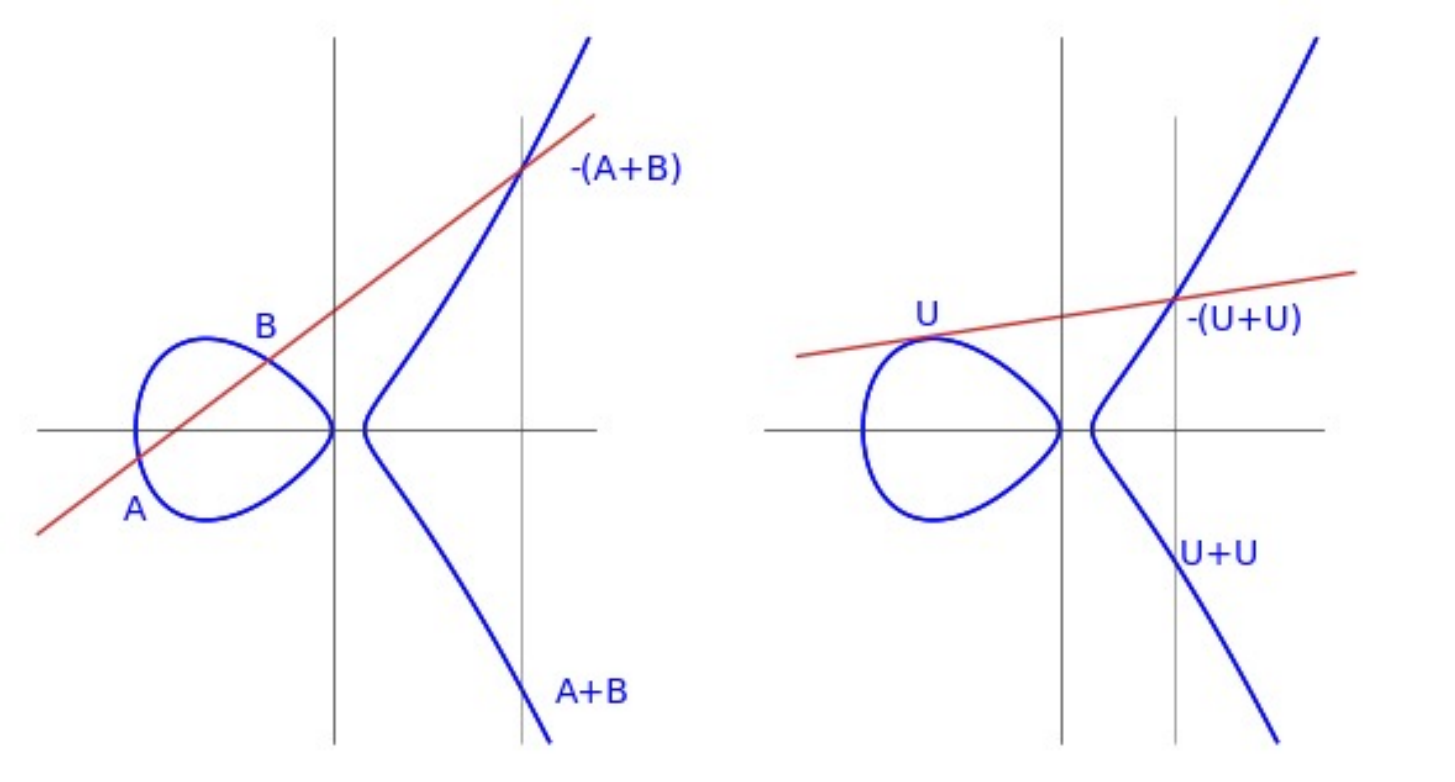
$y^2 = x^3 + 2x$



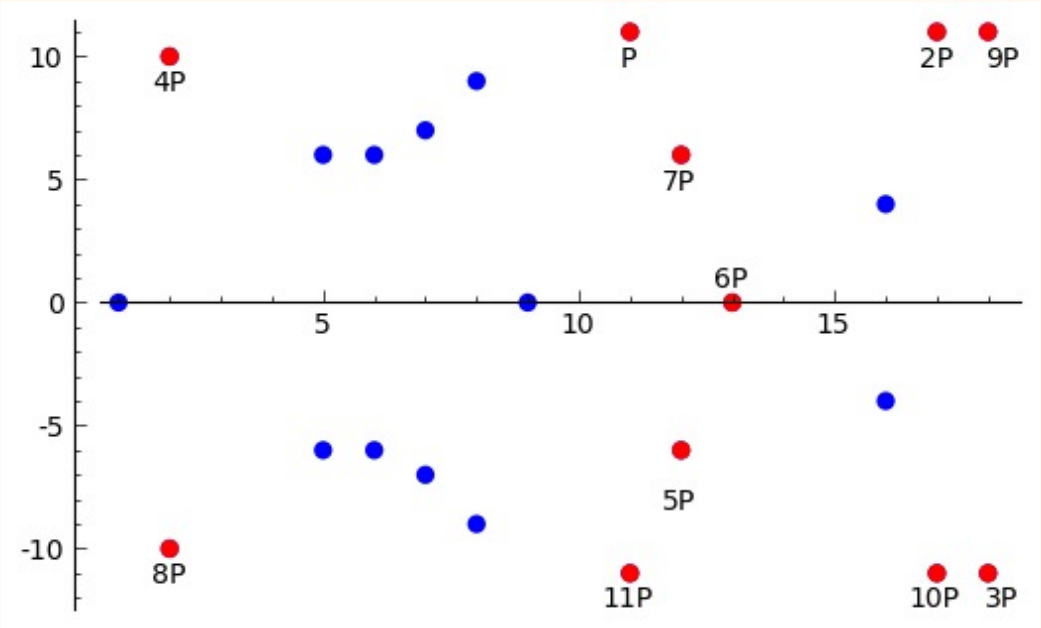
$y^2 = x^3 + 2x^2$.

- Théorème : on peut munir chaque courbe elliptique d'une addition des points qui fait de cette courbe un groupe commutatif.

Additions sur la courbe réelle $y^2 = (x-1)x(x+6)$



Courbe $y^2 = (x-1)(x^2+x+2)$ sur $\mathbb{Z}_{23}$



Les coordonnées des points sont des éléments de $\mathbb{Z}_{23}$ au lieu d'être des réels. Il n'y a plus d'interprétation géométrique de l'addition. On calcule la somme de deux points avec les mêmes formules que dans le cas réel.

Les courbes elliptiques sonts plus économiques

- Le calcul d'un logarithme discret dans $\mathbb{Z}_p$ est difficile, mais il existe des algorithmes de calcul du logarithme discret fonctionnant pour les valeurs de p modérément grandes. C'est pourquoi les protocoles cryptographiques basés sur le problème du logarithme discret dans $\mathbb{Z}_p$ nécessitent de grandes valeurs de p pour se protéger des attaques (environs 200 chiffres décimaux).

- Pour le calcul du logarithme discret sur une courbe elliptique on ne connait pas d'algorithme efficace même pour des valeurs de p moyennement grandes. Pour le même niveau de sécurité, il suffit donc d'utiliser des nombres plus petits, ce qui permet des calculs plus rapides.

- Les algorithmes utilisant les courbes elliptique ne sont pas encore utilisés, mais remplaceront les algorithmes actuels dans un futur proche.

Physique quantique

Les grandeurs de la physique classique, la position d'un objet, sa vitesse . . . ont à tout instant une valeur déterminée, susceptible d'être mesurée avec une précision arbitraire, sans que cette mesure n'affecte sensiblement l'état de l'objet.

À l'échelle microscopique, les objets satisfont les lois de la physique quantique, qui sont contraires à notre intuition

La superposition quantique : Tant que l'on ne cherche pas à mesurer une grandeur cette grandeur n'a, en général, pas de valeur déterminée. Comme si l'objet flottait entre différents états. On dit que l'objet est dans un état de superposition.

À chaque mesure est associé un ensemble d'états, et la mesure force l'objet considéré à choisir, de manière aléatoire, l'un de ces états. En particulier, immédiatement après une mesure, l'objet n'est plus dans un état de superposition.

L'ordinateur quantique : mythe ou réalité ?

On peut envisager la construction de circuits logiques quantiques, semblables aux circuits logiques à la base des ordinateurs classiques.

Mais grâce au phénomène de superposition, ces circuits seraient susceptibles d'effectuer en parallèle, tous les calculs qu'un circuit classique ne pourrait effectuer que les uns après les autres.

L'ordinateur quantique rendrait caducs tous les protocoles actuels, basés sur la difficulté de la factorisation des entiers où du calcul d'un logarithme discret.

Mais la superposition quantique est très fragile. L'ordinateur quantique n'est peut être qu'un rêve.

Cryptographie quantique

- Si l'ordinateur quantique est encore lointain, la cryptographie quantique est déja presque réalité.
- Alice et Bernard utilisent le protocole de Vernam.

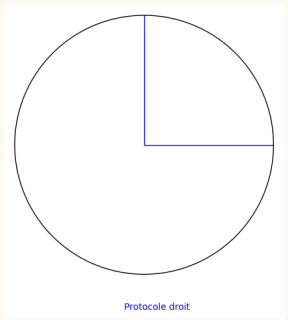
La polarisation d'un photon et sa mesure

- Un photon se propageant dans la direction de l'axe Oz peut être polarisé selon un axe quelconque du plan $x0y$. Les lois de la physique quantique ont des repercussions drastiques sur la mesure de la polarisation.

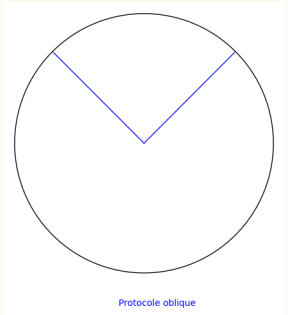
- Pour mesurer la polarisation d'un photon on est obligé de choisir a priori deux directions perpendiculaires. Après la mesure le photon sera polarisé dans l'une ou l'autre de ces 2 directions.

- Le seul cas où la mesure n'affecte pas la polarisation du photon est le cas où celui-ci était déja polarisé selon l'une des deux directions de l'appareil de mesure.

Transmettre un quBit. Les protocoles $\mathcal{A}$ et $\mathcal{B}$



Protocole $\mathcal{A}$ Alice emet un photon polarisé verticalement ou horizontalement. Pour coder le 1 Alice envoie un photon polarisé verticalement. Pour coder le 0 elle envoie un photon polarisé horizontalement. Bernard utilise un polariseur d'axes vertical et horizontal.



Protocole $\mathcal{B}$ Alice emet un photon polarisé obliquement. Pour coder le 1 Alice envoie un photon polarisé vers la gauche. Pour coder le 0 elle envoie un photon polarisé vers la droite. Bernard utilise un polariseur d'axes obliques.

Alice et Bernard partagent un mot sur l'alphabet $\{0, 1\}$

- Alice choisit $(x_1, x_2, \ldots, x_{2000})$ éléments de $\{0, 1\}$.
- Pour chaque $i \in \{1, \ldots, 2000\}$ elle choisit, au hasard l'un des 2 protocoles $\mathcal{A}$ ou $\mathcal{B}$ et transmet x_i en utilisant ce protocole.
- Bernard ne connait pas les choix d'Alice. Il est réduit, pour chaque i, à choisir au hasard $\mathcal{A}$ ou $\mathcal{B}$. Il reçoit ainsi y_i qui est égal à x_i si Bernard a fait le bon choix. Sinon c'est, avec équiprobabilté, x_i ou $1 - x_i$.
- Quand la transmission des 2000 quBits est terminée, sur une ligne téléphonique ordinaire, Alice envoie à Bernard la liste des protocoles utilisés. Bernard lui répond en donnant les valeurs de i pour lesquelles il a fait le bon choix.
- La clef partagée par Alice et Bernard est la suite des x_i $(= y_i)$ restreinte à ces valeurs de i (de longueur environ 1000).

Que se passe-t'il si Eve espionne la transmission ?

- Si Eve interpose un polariseur sur le trajet du photon, une fois sur deux elle choisit la mauvaise orientation, ce qui, une fois sur deux modifie la polarisation du photon.
- Il ne lui est donc pas possible de réémettre à Bernard un photon identique à l'original. Un fois sur deux elle fera suivre à Bernard un signal opposé à celui qu'elle a reçu.
- Au cours de leur conversation téléphonique, Alice et Bernard, après avoir échangé la liste des numéros des bons choix de Bernard, s'assurent sur un échantillon de valeurs de i pour lesquelles Bernard a fait le bon choix, qu'on a bien $x_i = y_i$. Si ce n'est pas le cas, c'est que Eve a brouillé la communication.

Réalisabilité de la cryptographie quantique

Un photon est un objet très fragile, et, pour le moment on ne peut pas transporter un photon sur plus de quelques dizaines de kilomètres. Mais des chercheurs travaillent à la réalisation de répéteurs quantiques qui rendraient viable la cryptographie quantique à grande distance. [8]
La situation n'est pas encore figée, un article récent [9] présente une attaque contre ce procédé de chiffrement.

8. Un répéteur quantique n'est en theorie pas plus complexe qu'un ordinateur quantique a 2 quBits.

9. Hacking commercial quantum cryptography systems by tailored bright illumination Nature Photonics 4, 686–689 (2010)

Conclusion générale

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

Complément : Chiffrement asymétrique et signature

Alice sépare le corps du texte x, et sa signature s,

$$x = \textit{Veuillez prélever...} \qquad s = \textit{Alice 18 rue des Tilleuils}$$

1. Elle commence par déchiffrer s et obtient $s_1 = \text{Dechiffre}(k_a, s)$.
2. Elle chiffre normalement x et s_1 envoie à Bernard les cryptogrammes $y = \text{Chiffre}(c_b, x)$ et $t_1 = \text{Chiffre}(c_b, s_1)$.
3. Bernard les déchiffre et retrouve $x = \text{Dechiffre}(k_b, y)$ et $s_1 = \text{Dechiffre}(k_b, t_1)$
4. Enfin il chiffre s_1 avec la clef publique d'Alice et obtient

$$\text{Chiffre}(c_a, s_1) = \text{Chiffre}(c_a, \text{Dechiffre}(k_a, s)) = s$$

Alice est bien l'expéditeur car pour construire s_1 il faut utilser k_a, que seule Alice connait.