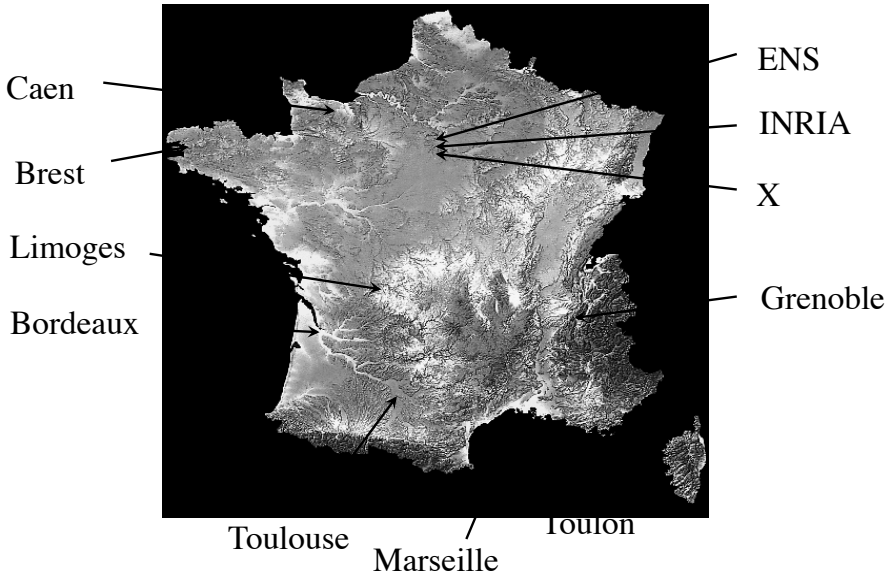
mise à jour: 2016

Une introduction élémentaire à la Cryptographie

Michel Waldschmidt
Université P. et M. Curie - Paris VI

http://www.math.jussieu.fr/~miw/



Théorie des Nombres et Cryptographie en France

École Polytechnique
INRIA Rocquencourt
École Normale Supérieure
Université de Bordeaux
ENST Télécom Bretagne
Université de Caen + France Télécom R&D
Université de Grenoble
Université de Limoges
Université de Marseille
Université de Toulon
Université de Toulouse

http://www.math.jussieu.fr/~miw/

http://www.lix.polytechnique.fr/

École Polytechnique

Laboratoire d'Informatique LIX

http://www.lix.polytechnique.fr/english/us-presentation.pdf

http://www-rocq.inria.fr/codes/

Institut National de Recherche en Informatique et en Automatique

INRIA - Projet CODES

Codes and Cryptography

- People of CODES
- Our Research topics
- Publications
- Activity report (in French)
- Conferences on coding and cryptography
- How to contact us
- Introduction to cryptography (in French)
- Watermarking for Intellectual Property Right Protection (in French)
- Algebraic curves and Cryptography (action de recherche "COURBES") (in French)
- Links on coding and cryptography
- Other links
- How to cook a tiramisu

WCC 2007 (International Workshop on Coding and Cryptography)(Rocquencourt, France)

SASC 2006 - Stream Ciphers Revisited (ECRYPT Workshop), Leuven, Belgium, February 2-3, 2006.

http://www.di.ens.fr/CryptoRecherche.html

École Normale Supérieure

École Normale Supérieure
Département d'Informatique

Main

Accueil
Mot du directeur

Recherche
Équipes
Membres
Séminaires
Annuaire

Enseignement
Diplôme de l'ENS – spécialité informatique
MPRI

Research in the Crypto Team

Our research deals mainly with cryptology and extends to all related domains.

- **Activity reports.** If you want a precise description of our activity, you may read the activity reports (in french) for the years 1994–1997, 1998–2001 or 2001–2004.
- **Software developpement.**
  - ZEN: a new C toolbox for computations in finite extensions of finite integer rings.
  - DFC: our submission for the AES standard.
  - CS-cipher: developped with CS Group and now used by Trustycom. The 56-bits context was winned by distributed.net.
- **International collaborations.**
  - NESSIE
  - STORK
  - ECRYPT

http://www.math.u-bordeaux1.fr/maths/

Institut de Mathématiques de Bordeaux

UNIVERSITÉ BORDEAUX 1 Sciences Technologies
UNIVERSITÉ BORDEAUX 2 Victor Segalen

Théorie des nombres et Algorithmique Arithmétique

IMB > Equipes > A2X > Thématiques > Codes et Réseaux

Le thème principal de nos recherches est l'étude des réseaux

Les maxima de la constante d'Hermite, qui mesure la densité de sphères, associé à un réseau, s'étudient grâce à la théori


Georgy Voronoï
[http://www-groups.dcs.st-and.ac.uk/%7Ehistory/Mathemati

Réseaux et combinatoire

http://departements.enst-bretagne.fr/sc/recherche/turbo/

École Nationale Supérieure des Télécommunications de Bretagne

Turbocodes

École Nationale Supérieure des Télécommunications de Bretagne

département d'enseignement et recherche
Signal et Communications

Université de Caen Basse-Normandie

Cryptologie à Caen

Laboratoire de Mathématiques Nicolas Oresme
CNRS UMR 6139

http://www.math.unicaen.fr/lmno/

GREYC Groupe de Recherche en Informatique, Image, Automatique et Instrumentation de Caen

Bienvenue sur le site du laboratoire GREYC

http://www.grey.unicaen.fr/

France Télécom R&D Caen

GRENOBLE I UNIVERSITE JOSEPH FOURIER SCIENCES. TECHNOLOGIE. MEDECINE

http://www-fourier.ujf-grenoble.fr/

Cryptologie à Grenoble

INPGrenoble

- ACI (Action concertée incitative)
- CNRS (Centre National de la Recherche Scientifique)
- Ministère délégué à l'Enseignement Supérieur et à la Recherche
- ANR (Agence Nationale pour la Recherche)

CNRS CENTRE NATIONAL DE LA RECHERCHE SCIENTIFIQUE

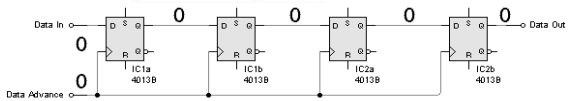
ANR

Xlim institut de recherche

LIMOGES

UNIVERSITE DE LIMOGES

Accès authentifiés

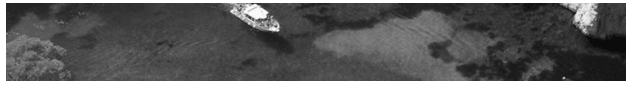


http://www.xlim.fr/

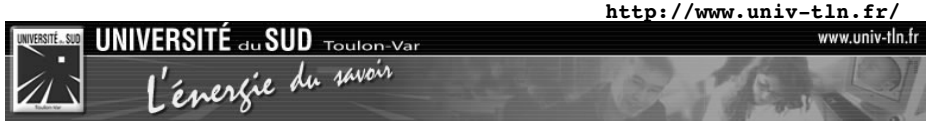
Marseille: Institut de Mathématiques de Luminy

Institut de Mathématiques de Luminy

Arithmetic and Information Theory
Algebraic geometry over finite fields



http://www.univ-tln.fr/



Université du Sud Toulon-Var

Groupe de Recherche en Informatique & Mathématiques

Yacc is "Another" Conference on Cryptography

http://www.ias.ac.in/resonance/

A sketch of Modern Cryptology

by *Palash Sarkar*

Resonance journal of science education

Volume 5 Number 9 (september 2000), p. 22-40

Université de Toulouse

LAAS Laboratory for Analysis and Architecture of Systems

http://www.laas.fr/laas/

IRIT: Institut de Recherche en Informatique de Toulouse

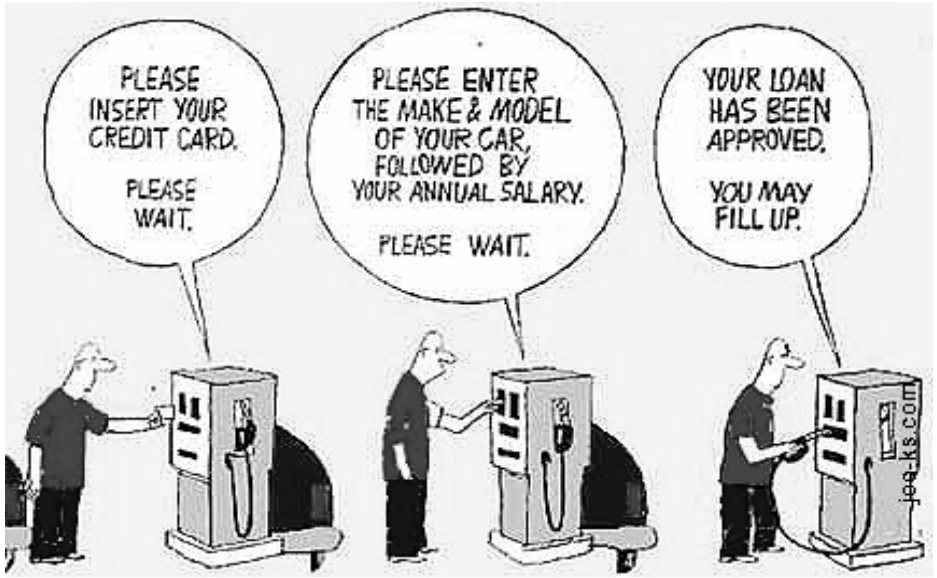
LILAC: Logic, Interaction, Language, and Computation

http://www.irit.fr/

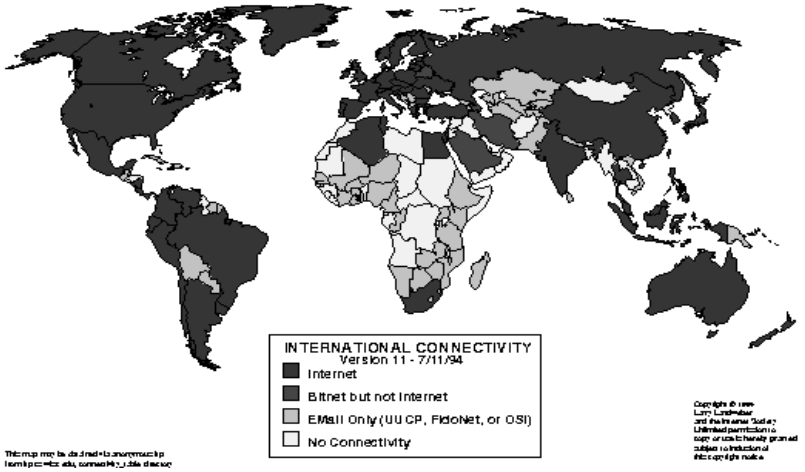
IMT: Institut de Mathématiques de Toulouse

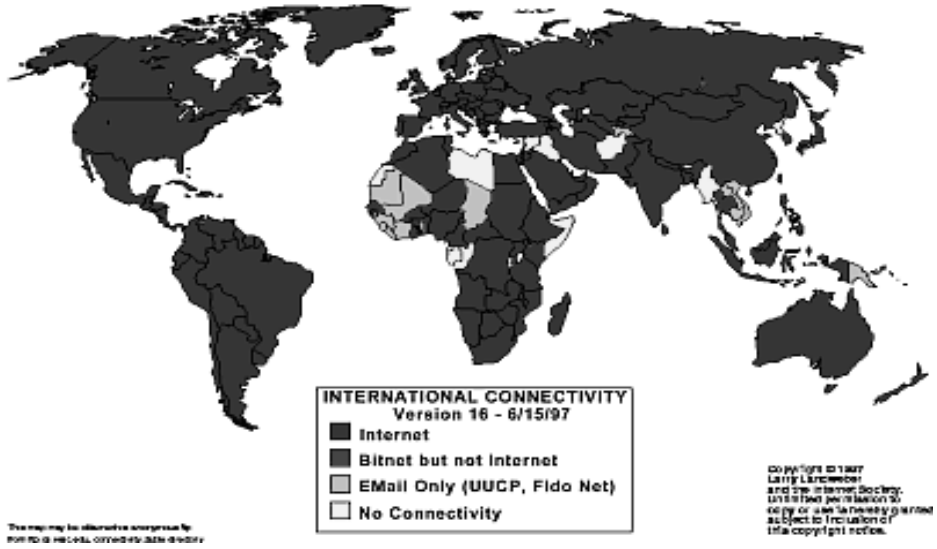
http://www.univ-tlse2.fr/grimm/algo

Crypter pour la sécurité



Larry Landweber's International Connectivity maps **1994**



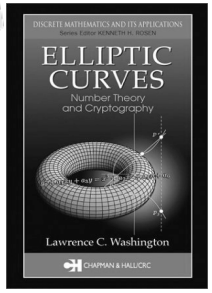


Larry Landweber's International Connectivity maps 1997

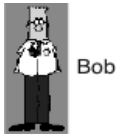
Sécurité des communications: téléphones, télécommunications, télévision cryptée,…

Mathématiques en cryptographie

- Algèbre
- Arithmétique, théorie des nombres
- Géométrie
- Topologie, tresses
- Probabilités



Échange de valises



- Alice a une valise, un cadenas et une clé; elle veut envoyer la valise à Bob sans que Charlie ne puisse savoir ce qu'il y a dedans.

- Bob possède aussi un cadenas et une clé, mais qui ne sont pas compatibles avec ceux d'Alice.

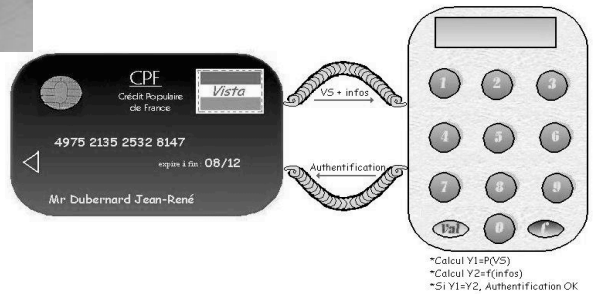
Le protocole

- Alice ferme la valise avec son cadenas et sa clé et l'envoie à Bob.
- Bob y met son propre cadenas et renvoie à Alice la valise avec les deux cadenas.
- Alice enlève son cadenas grâce à sa clé et renvoie la valise à Bob.
- Finalement Bob peut ouvrir la valise grâce à sa clé.

- *But: en donner une traduction mathématique*.

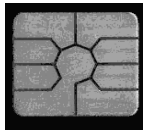
Cartes à puce

ATM: Automated Teller Machine



La carte à puce a été inventée par deux ingénieurs français, Roland Moreno (1974) et Michel Ugon (1977)

- La sécurité des cartes à puces fait intervenir trois processus différents; le code PIN, le protocole RSA et le code DES.



http://www.cartes-bancaires.com

La carte à puce.

- Les messages que vous envoyez ou que vous recevez ne doivent pas révéler votre code secret.
- Tout le monde (y compris la banque) ayant accès aux messages échangés peut vérifier que vous connaissez ce code secret, mais cela ne leur permet pas de le connaître.

- *La banque vous envoit un message aléatoire.*
- *Votre réponse dépend de ce message et de votre code secret.*

Code secret d'une carte bancaire

- Vous devez vous identifier auprès de la banque. Vous avez deux clés: une publique que tout le monde connaît, une secrète (le code PIN) que personne d'autre que vous ne connaît.

Cryptographie: aperçu historique

Transpositions alphabétiques et substitutions

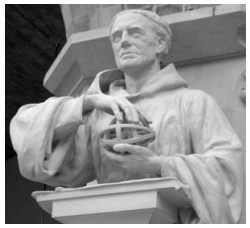
- Jules César: remplacer une lettre par une autre dans le même ordre (décalage)

- Exemple: (décaler de 3) remplacer
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
par
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

- *Exemple:*
CRYPTOGRAPHIE devient FUBSWRJUDSKLH
- *Exemples plus sophistiqués:* prendre une permutation quelconque (ne respectant pas forcément l'ordre).

• 800-873, Abu Youssouf Ya qub Ishaq **Al Kindi**

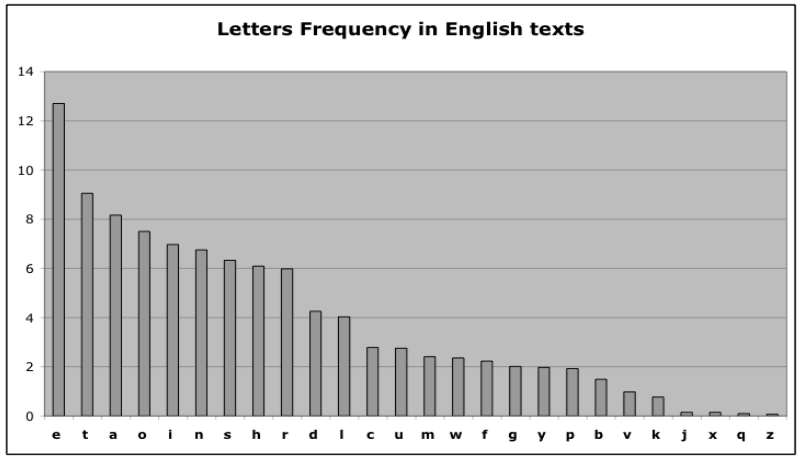
Manuscrit sur le décryptage des messages.
Vérification de l' authenticité des textes sacrés de l'Islam.

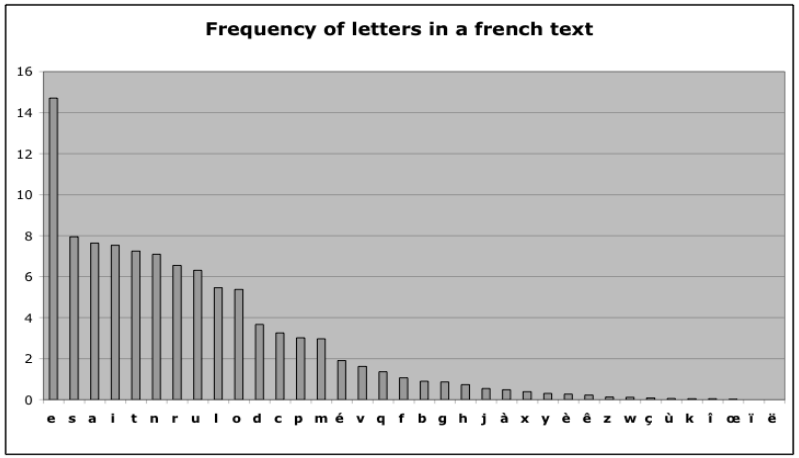


• XIIIè siècle, Roger Bacon: sept méthodes pour chiffrer des messages.

•1586, Blaise de Vigenère
(clé: «table of Vigenère»)
Cryptographe, alchimiste, écrivain, diplomate

• 1850, Charles Babbage (fréquence lettres)
Machine de Babbage (ancêtre de l'ordinateur)
Ada, comtesse de Lovelace: premier programme





Alphabet International de Morse

Samuel Morse,
1791-1872

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

Déchiffrage des hiéroglyphes

- Jean-François Champollion (1790-1832)

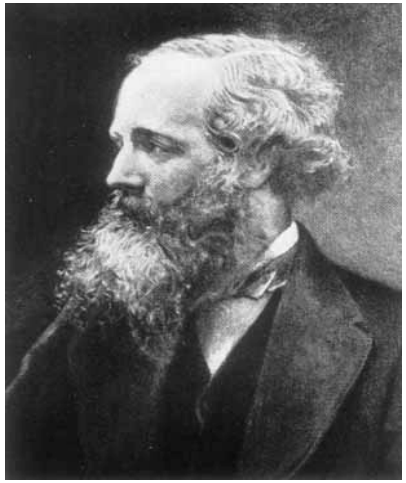
- Pierre de Rosette (1799)

Transmission des données

- ***Pigeons voyageurs : première croisade – Siège de Tyr, Sultan de Damas***
- ***Guerre franco-allemande de 1870, siège de Paris***
- ***Centres militaires pour l'étude des pigeons voyageurs : Coëtquidan et Montoire.***

Transmission des données

- ***James C. Maxwell*** *(1831-1879)*
- ***Électromagnétisme Herz, Bose: radio***



Auguste Kerckhoffs

«La cryptographie militaire»,
Journal des sciences militaires, vol. IX,
pp. 5–38, Janvier 1883,
pp. 161–191, Février 1883 .

Toute méthode de chiffrement doit être supposée connue par l'ennemi: la sécurité du système doit dépendre uniquement du choix de clés, qui doivent être changées régulièrement.

1917, Gilbert Vernam (**masque jetable)**
Exemple: le téléphone rouge entre le Kremlin et la Maison Blanche

Message Original:	0 1 1 0 0 0 1 0 1 …
Clé	0 0 1 1 0 1 0 0 1…
Message envoyé	0 1 0 1 0 1 1 0 0…

1950, *Claude Shannon* pour garantir la sécurité, il faut une clé secrète au moins aussi longue que le message à envoyer.

Alan Turing

Déchiffre les messages de la machine *Enigma*

Début de l'informatique

Colossus

Max Newman,
premier ordinateur électronique programmable
(Bletchley Park, avant1945)

Théorie de l'information

Claude Shannon

A mathematical theory of communication

Bell System Technical Journal, 1948.

Sécurité

Sécurité inconditionnelle: le message codé ne révèle aucune information sur le message source, la seule méthode est d'essayer toutes les clés possibles.

En pratique, aucun système utilisé dans la réalité ne satisfait cette condition.

Sécurité pratique: le message codé ne donne aucune information sur le message source **en un temps raisonnable.**

Claude E. Shannon

" Communication Theory of Secrecy Systems ",

Bell System Technical Journal ,

28-4 (1949), 656 - 715.

DES:
Data Encryption Standard

En 1970, le NBS (*National Board of Standards*) lance un appel d'offre au *Federal Register* pour définir un algorithme de cryptage

- ayant un niveau de sécurité élevé qui ne dépend pas de la confidentialité de l'algorithme mais seulement des clés secrètes,
- qui fait intervenir des clés secrètes pas trop grandes,
- rapide, robuste, bon marché,
- facile à implémenter.

Le DES a été approuvé en 1978 par le NBS

L'algorithme DES:

combinaisons, substitutions et permutations entre le texte et la clé

- Le texte est découpé en blocs de *64* bits
- Les blocs sont permutés
- Ils sont coupés en deux: droite et gauche
- On effectue *16* fois un cycle de permutations et de substitutions faisant intervenir la clé secrète
- On regroupe les parties gauche et droite puis on effectue les permutations inverses.

Diffie-Hellman:

Cryptographie à clé publique

- Whit Diffie and Martin E. Hellman, New directions in cryptography, *IEEE Transactions on Information Theory,* **22** (1976), 644-654

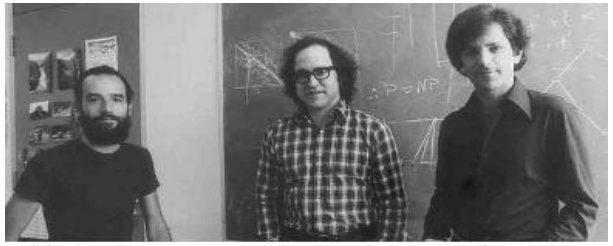
Cryptographie
Symétrique versus **Asymétrique**

- **Symétrique** (clé secrète):
- Alice et Bob ont chacun une clé de la boîte aux lettres. Alice utilise sa clé pour déposer sa lettre dans la boîte. Bob utilise sa clé pour récupérer la lettre.
- Alice et Bob sont les seuls à pouvoir ouvrir la boîte aux lettres.

- **Asymétrique** (clé publique)
- Alice trouve l'adresse de Bob dans un annuaire public, elle envoie sa lettre à Bob, qui utilise sa clé secrète pour la lire.
- Tout le monde peut envoyer un message à Bob, lui seul peut les lire.

RSA

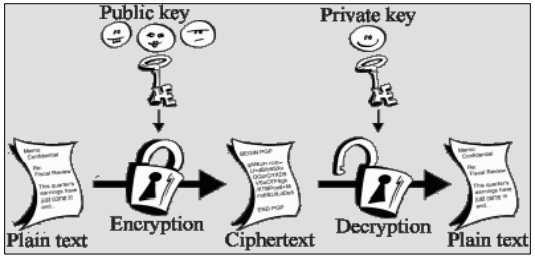
*(**R**ivest, **S**hamir, **A**dleman - 1978)*



Adi Shamir Ron Rivest Len Adleman

R.L. **R**ivest, A. **S**hamir,
et L.M. **A**dleman

A method for obtaining digital signatures and public-key cryptosystems,
Communications of the ACM
(2) **21** (1978), 120-126.



Exemple d'une fonction trappe: le logarithme discret
(version simplifiée)

On part d'un nombre à trois chiffres x.
On calcule le cube de x, à savoir : $x \times x \times x = x^3$.
On ne conserve que les trois derniers chiffres = reste de la division par 1000: c'est y.

- Partant de ***x,*** trouver ***y*** est facile.
- Connaissant ***y,*** retrouver ***x*** est difficile.

Fonction trappe

$x \rightarrow y$

est une fonction *trappe – à sens unique* si

- Étant donné x, il est facile de calculer y
- Étant donné y , il est difficile de trouver x, sauf si on connaît une clé.

Les exemples font intervenir des problèmes mathématiques connus pour être difficiles.

Le logarithme discret modulo 1000

- Exemple: sachant que les trois derniers chiffres de x^3 sont *631*, ce que l'on écrit $x^3 \equiv 631$ modulo *1000*, ***trouver*** x.
- Solution brutale: essayer toutes les valeurs de *x=001, 002, …*

  on trouve ainsi *x=111* – c'est la seule solution.
- *Vérification: $111 \times 111 = 12\,321$*
- On ne garde que les trois derniers chiffres:

  $111^2 \equiv 321$ modulo *1000*
- Puis $111 \times 321 = 35\,\mathbf{631}$

Racine cubique modulo 1000

Résoudre $x^3 \equiv 631$ modulo *1000*.

- **Autre méthode:** *utiliser une clé secrète*.
  La clé publique est *3*, car on calcule x^3.
  Une clé secrète est *67*.
- *Cela signifie que si on calcule la puissance 67 de 631, on trouve x*:

  $631^{67} \equiv x$ modulo *1000*.
- $(x^3)^{67} \equiv x$ modulo *1000*

Racine 7ème modulo 1000

- Pour une clé publique *3*, une clé secrète est *67*.
- Autre exemple: clé publique *7*, clé secrète *43*.
- Sachant $x^7 \equiv 871$ modulo *1000*
- on calcule $871^{43} \equiv 111$ modulo *1000*
- donc $x = 111$.

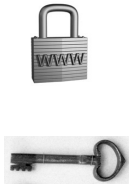


Protocole de l'échange de valises


- Alice a une valise, un cadenas et une clé; elle veut envoyer la valise à Bob sans que Charlie ne puisse savoir ce qu'il y a dedans.

- Bob possède aussi un cadenas et une clé, mais qui ne sont pas compatibles avec ceux d'Alice.

Échange de valises











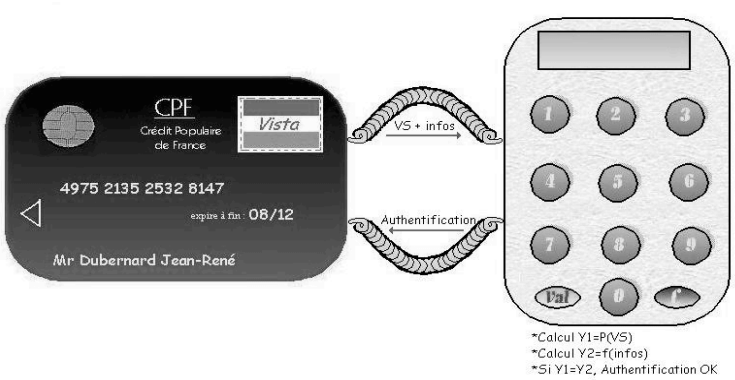


111 *7* *3* *43* *67* *111*

$111^7 \equiv 871$ $311^{43} \equiv 631$

$871^3 \equiv 311$ $631^{67} \equiv 111$

Cartes à puce



Message modulo n

- On choisit un entier *n (à la place of 1000)*: c'est la taille des messages qui seront échangés.
- Tous les calculs seront faits modulo *n* : on remplace chaque entier par le reste de sa division par *n*.
- *n* sera un entier avec environ *300* chiffres.

ATM

message aléatoire	Code Pin	Clé Publique
631	*67*	*3*
	$631^{67} \equiv 111$	$111^{3} \equiv 631$

Connaissant la clé publique *3* et le message *631* envoyé par la banque, on vérifie que la réponse *111* est correcte, mais cela ne permet pas de deviner le code secret *67*.

Il est plus facile de vérifier une démonstration que de la trouver

Multiplier deux nombres, même un peu grands, est facile.

Si on sait qu'un nombre donné est le produit de deux nombres, trouver les facteurs peut être difficile.

2047 est-il le produit de deux nombres plus petits?

Réponse: oui $2047=23\times89$

Exemple

p=11139543251488279879254901754770248440709228448 43

q=19174817025245044393757862682308621806969341892 93

pq=21359870359209100823950227049996287970510953418264174064425241650085839577464450884050094308659 99

Tests de primalité et algorithmes de factorisation

- Étant donné un entier, déterminer s'il est premier ou non **(test de primalité).**
- Étant donné un nombre composé, trouver sa décomposition en facteurs premiers **(algorithme de factorisation).**

Choix de n

On prend pour n le produit de deux nombres premiers de *150* chiffres chacun

Le produit a environ *300* chiffres: les ordinateurs ne peuvent pas actuellement trouver les facteurs.

Tests de primalité

- Étant donné un entier, déterminer s'il est premier ou non

  Limite actuelle: environ 1000 chiffres

Algorithmes de factorisation

- Étant donné un nombre composé, trouver sa décomposition en facteurs premiers

  Limite actuelle: environ 150 chiffres

Agrawal-Kayal-Saxena

- Manindra Agrawal, Neeraj Kayal and Nitin Saxena, ***PRIMES is in P***

  (July 2002)

http://www.cse.iitk.ac.in/news/primality.html

Les quatre plus grands nombres premiers explicites

7 janvier 2016 — $2^{74\,207\,281} - 1$

22 338 618 chiffres décimaux

8 février 2013 — $2^{57885161} - 1$

17 425 170 chiffres

23 août 2008 — $2^{43\,112\,609} - 1$

12 978 189 chiffres

12 avril 2009 — $2^{42\,643\,801} - 1$

12 837 064 chiffres

http://primes.utm.edu/largest.html

Nombres premiers industriels

- **« Tests » probabilistes:** ne garantissent pas qu'un nombre est premier: un faible taux d'erreur est toléré.

Electronic Frontier Foundation
Defending Freedom in the Digital World

Cooperative Computing Awards
» Rules » Frequently Asked Questions » Status » Resources

Through the EFF Cooperative Computing Awards,
EFF will confer prizes of:

* $50 000 to the first individual or group who discovers a prime number with at least 1 000 000 decimal digits (6 avril 2000)
* $100 000 to the first individual or group who discovers a prime number with at least 10 000 000 decimal digits (6 septembre 2008)
* $150 000 to the first individual or group who discovers a prime number with at least 100 000 000 decimal digits.
* $250 000 to the first individual or group who discovers a prime number with at least 1 000 000 000 decimal digits.

http://www.eff.org/awards/coop.php

Grands nombres premiers

- Les *11* plus grands nombres premiers connus sont de la forme $2^p - 1$ (on en connaît *49*)
- On connaît

  170 nombres premiers ayant plus de *1 000 000* chiffres

  1498 nombres premiers ayant plus de *500 000* chiffres.
- Liste des *5 000* plus grands nombres premiers connus :

  `http://primes.utm.edu/primes/`

Mise à jour: 9 mai 2016

GIMPS

The Great Internet Mersenne Prime Search

Finding 10 World Record Primes!

2^P-1 MAY BE PRIME!

Marin Mersenne (1588-1648), préface de *Cogitata Physica-Mathematica* (1644): *les nombres* $2^n - 1$ *sont premiers pour*

$n = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127$ *et* 257

et ils sont composés pour toutes les autres valeurs de $n < 257$.

Liste corrigée:

2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107 et *127*.

`http://www.mersenne.org/`

Nombres de Mersenne (1588-1648)

- Nombres de la forme $M_p = 2^p - 1$ avec p premier.
- On en connaît seulement *49* , les plus petits sont *3, 7, 31, 127*
- $3 = M_2 = 2^2 - 1$, $7 = M_3 = 2^3 - 1$, $31 = M_5 = 2^5 - 1$, $127 = M_7 = 2^7 - 1$

- 1536, Hudalricus Regius: $M_{11} = 2^{11} - 1$ n'est pas premier: $2047 = 23 \times 89$.

Nombres parfaits

- Un entier n est *parfait* s'il est égal à la somme de ses diviseurs en omettant n.
- Les diviseurs de *6* sont *1, 2, 3* et $6 = 1 + 2 + 3$.
- *Remarque:* $6 = 2 \times 3$ *et* $3 = M_2 = 2^2 - 1$.
- *6* est un nombre parfait.

Nombres parfaits

- Les diviseurs de *28* sont *1, 2, 4, 7, 14* et *28=1+2+4+7+14*.
- *Remarque: 28=4 × 7 et 7=M_3=2^3-1*.
- Autres nombres parfaits:

  496=16 × 31=2^4M_5 et M_5=2^5-1,

  8128=64 × 127=2^6M_7 et M_7=2^7-1,…

Nombres parfaits pairs (Euclide)

- Les nombres parfaits pairs sont les nombres de la forme $2^{p-1} \times M_p$ avec $M_p = 2^p - 1$ nombre premier de Mersenne (donc *p* est premier).
- Y a-t-il une infinité de nombres parfaits?
- Existe-t-il des nombres parfaits impairs?

Nombres de Fermat (1601-1665)

- Un nombre de *Fermat* est un nombre de la forme $F_n=2^{2^n}+1$.
- Construction à la règle et au compas de polygones réguliers.
- $F_1=5$, $F_2=17$, $F_3=257$, $F_4=65537$ sont des nombres premiers
- Fermat a suggéré en1650 que tous les F_n seraient premiers.

Euler (1707-1783)

- $F_5 = 2^{32}+1$ est divisible par *641*

4 294 967 297= 641 × 6 700 417

$F_5=2^{32}+1$ est divisible par 641

- $641 = 625 + 16 = 5^4 + 2^4$
- $641 = 5 \times 128 + 1 = 5 \times 2^7 + 1$
- 641 divise $x = 2^{28} \times (5^4 + 2^4) = 5^4 \times 2^{28} + 2^{32}$
- $t^4 - 1 = (t+1)(t-1)(t^2+1)$ $\quad t = 5 \times 2^7 = 640$
  641 divise $y = (5 \times 2^7)^4 - 1 = 5^4 \times 2^{28} - 1$
- Donc 641 divise $x - y = 2^{32} + 1$

Nombres premiers de Fermat

- Y a-t-il une infinité de nombres premiers de Fermat?
- On en connaît seulement cinq
  $F_0=3, F_1=5, F_2=17, F_3=257, F_4=65537.$

- *The On-Line Encyclopedia of Integer Sequences*
  http://oeis.org/A000215

Nombres premiers de Fermat

- Factorisés: $F_5, F_6, F_7, F_8, F_9, F_{10}, F_{11}$
- $F_{11} = 319489 \cdot 974849 \cdot 167988556341760475137 \cdot 3560841906445833920513 \cdot P564$

http://www.prothsearch.net/fermat.html

Algorithmes de factorisation

- Décomposer un entier en facteurs premiers
- Limite actuelle: environ *150* chiffres décimaux pour un entier au hasard
- Algorithme le plus efficace pour les grands nombres: ***number field sieve*** (crible de théorie des nombres)

http://www.crypto-world.com/FactorWorld.html

RSA Laboratories

RSA The Security Division of EMC

Challenge Number Prize $US

- RSA-576 $10,000 Factorisé en Décembre *2003*
- RSA-640 $20,000 Factorisé en Novembre *2005*
- RSA-704 $30,000 Non Factorisé
- RSA-768 $50,000 Factorisé en Novembre *2009*
- RSA-896 $75,000 Non Factorisé
- RSA-1024 $100,000 Non Factorisé
- RSA-1536 $150,000 Non Factorisé
- RSA-2048 $200,000 Non Factorisé

`http://www.rsasecurity.com/rsalabs/`

Fermé en 2007

RSA Laboratories

RSA The Security Division of EMC

RSA-768

Status: Factored December 12, *2009*

Decimal Digits: *232* Digit sum *1018*

123018668453011775513049495838496272077285356959533479219732245215172640050726365751874520219978646938995647494277406384592519255732630345373154826850791702612214291346167042921431160222124047927473779408066535141959745985690214341 3

=

33478071698956898786044169848212690817704794983713768568912431388982883793878002287614711652531743087737814467999489

*

367460436667995904282446337996279526322791581643430876426760322838157396665112792333734171433968102700927987363089 17

http://www.crypto-world.com/announcements/rsa768.txt

RSA Laboratories

RSA The Security Division of EMC

RSA-704 Prize: $*30,000*

Status: Not Factored

Decimal Digits: *212*

- *74037563479561712828046796097429573142593188889231289084936232638972765034028266276891996419625117843995894330502127585370118968098286733173273108930900552505116877063299072396380786710086096962537934650563796359*

- Digit Sum: *1009*

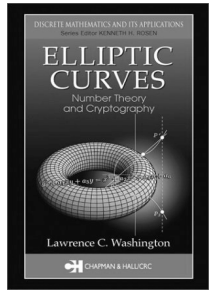
Autres problèmes de sécurité dans le monde industriel moderne

- Signatures digitales
- Identification
- Partage de secrets
- *Zero knowledge proofs*

Tendances actuelles en cryptographie

- Calculer modulo *n* signifie travailler dans le groupe multiplicatif des entiers modulo *n*
- Des groupes de *grande* taille sont nécessaires.
- On peut remplacer ce groupe par un autre dans lequel on calcule facilement, et dans lequel le logarithme discret est un problème difficile.
- Pour les cartes à puce, les téléphones portables … il faut un objet mathématique *petit*.
- Les courbes elliptiques sur les corps finis sont de bons candidats.

Directions de recherche



Calculer efficacement le groupe des points d'une courbe elliptique rationnels sur un corps fini

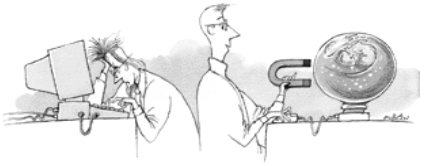
Vérifier la vulnérabilité aux attaques connues

Trouver de nouveaux invariants pour développer de nouvelles attaques

Genre supérieur: logarithme discret sur la jacobienne de courbes algébriques

Cryptographie quantique

- Peter Shor – résonnance magnétique nucléaire



Quizz: How to become a hacker?

Answer: Learn mathematics !

- **http://www.catb.org/~esr/faqs/hacker-howto.html**

27 juin 2013

Université de Pau et des Pays de l'Adour
Laboratoire de Mathématiques et de leurs applications
Colloquium de mathématiques

Introduction à la Cryptographie

Michel Waldschmidt
Université P. et M. Curie - Paris VI

http://www.math.jussieu.fr/~miw/