Updated: 2016

An elementary introduction to Cryptography

Michel Waldschmidt

Emeritus Professor

Université P. et M. Curie - Paris VI

Centre International de Mathématiques

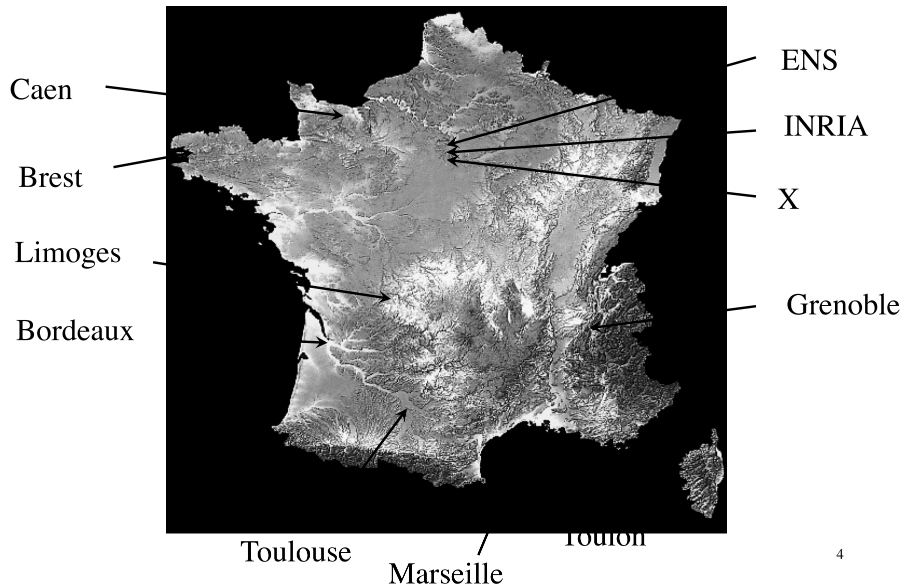
Pures et Appliquées - CIMPA

Data transmission, Cryptography and Arithmetic

Among the unexpected features of recent developments in technology are the connections between classical arithmetic on the one hand, and new methods for reaching a better security of data transmission on the other. We will illustrate this aspect of the subject by showing how modern cryptography is related to our knowledge of some properties of natural numbers. As an example, we explain how prime numbers play a key role in the process which enables you to withdraw safely your money from your bank account using your PIN (Personal Identification Number) secret code.

Number Theory and Cryptography in 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.lix.polytechnique.fr/

ÉCOLE POLYTECHNIQUE

École Polytechnique

Laboratoire d'Informatique LIX
Computer Science Laboratory at X

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

ÉCOLE POLYTECHNIQUE

LIX

- Fundamental problems targetting real applications whose solution requires scientific breakthroughs
- Algorithms, networks, formal methods
- Applicative areas : algorithms&engineering for telecommunications, design and validation of complex systems, security
- 90 people, about half phds, 10 groups including 6 INRIA and 1 CEA projects
- Industrial collaborations: Alcatel, Axalto, CRIL, EADS, Ergelis, Eurocontrol, France-Telecom, GEMPLUS, Hitachi, ILOG, Philip Moris, Thalès, Trusted Logics.

ÉCOLE POLYTECHNIQUE

Research teams

- Algebraic Models and Computer Algebra: Marc Giusti, Michel Fliess (Alien)
- Combinatorial Models: Gilles Schaeffer
- Bioinformatics: Jean-Marc Steyaert
- Algorithms for optimisation: Philippe Baptiste
- Hipercom: Philippe Jacquet
- Tanc: François Morain
- Parsifal: Dale Miller
- LogiCal: Gilles Dowek
- Comète: Catuscia Palamidessi
- Complex Systems: Éric Goubault, Daniel Krob

ÉCOLE POLYTECHNIQUE

Scientific success stories

- Hipercom: Optimal Link State Routing protocol (IETF)
- LogiCal: Complete formal proof of the 4 colors theorem using Coq (with Microsoft)
- Tanc: The biggest proven ordinary prime

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

Institut **N**ational de **R**echerche en **I**nformatique et en **A**utomatique

National Research Institute in Computer Science and Automatic

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

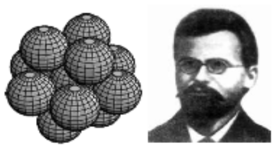
UNIVERSITÉ BORDEAUX 1 Sciences Technologies
UNIVERSITÉ BORDEAUX 2 Victor Segalen

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

Lattices and combinatorics

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

École Nationale Supérieure des Télécommunications de Bretagne

Turbocodes

École Nationale Supérieure des Télécommunications de Bretagne

Université de Caen Basse-Normandie

Cryptology in 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

Research group in computer science, image, automatic and instrumentation

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

France Télécom R&D Caen

CAEN

***C**ryptologie et **A**lgorithmique **E**n **N**ormandie*

- Electronic money, RFID labels (**R**adio **F**requency **ID**entification)
- Braid theory (*knot theory, topology*) for cypher

Number Theory:

- Diophantine equations.
- LLL algorithms, Euclidean algorithm analysis, lattices.
- Continued fraction expansion and factorization using elliptic curves for analysis of RSA crypto systems.
- Discrete logarithm, authentification with low cost.

GRENOBLE I UNIVERSITE JOSEPH FOURIER SCIENCES. TECHNOLOGIE. MEDECINE

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

Cryptologie in Grenoble

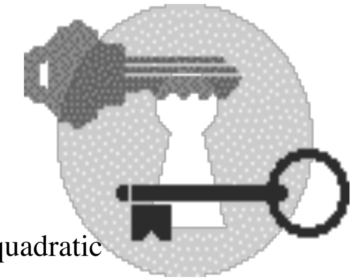
INP Grenoble

- 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 — ministère délégué à l'enseignement supérieur et à la recherche — ANR

Xlim institut de recherche

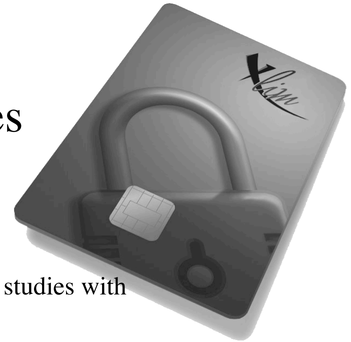
Research Laboratory of LIMOGES



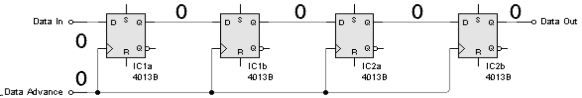
- Many applications of number theory to cryptography
  - Public Key Cryptography: Design of new protocols (probabilistic public-key encryption using quadratic fields or elliptic curves)
  - Symetric Key Cryptography: Design of new fast pseudorandom generators using division of *2*-adic integers (participation to the Ecrypt Stream Cipher Project)

`http://www.xlim.fr/`

Research Axes



- With following industrial applications
  - Smart Card: Statistical Attacks,
    Fault analysis on AES
  - Shift Registers: practical realisations of theoric studies with price constraints



  - Erro
  - Security in adhoc network, using certificateless public key cryptography

Teams / Members

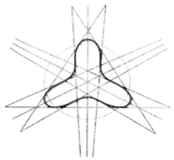
- 2 teams of XLIM deal with Cryptography:
  - PIC2: T. BERGER
  - SeFSI: JP. BOREL
- 15 researchers
- Industrial collaborations with France Télécom, EADS, GemAlto and local companies.

UNIVERSITE DE LIMOGES

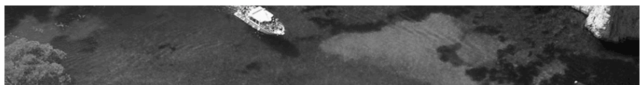
Accès authentifiés

Marseille: Institut de Mathématiques de Luminy

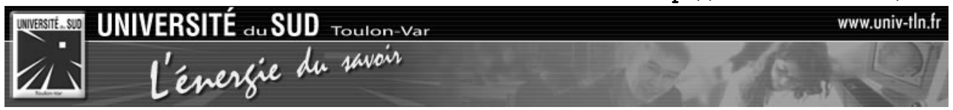
Institut de Mathématiques de Luminy



Arithmetic and Information Theory
Algebraic geometry over finite fields



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



Université du Sud Toulon-Var

GRIM

Groupe de Recherche en Informatique & Mathématiques

Yacc is "Another" Conference on Cryptography

Université de Toulouse

LAAS Laboratory for Analysis and Architecture of Systems

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

IRIT: Institut de Recherche en Informatique de Toulouse
(Computer Science Research Institute)

LILAC: Logic, Interaction, Language, and Computation

http://www.irit.fr/

IMT: Institut de Mathématiques de Toulouse
(Toulouse Mathematical Institute)

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

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

A sketch of Modern Cryptology
by *Palash Sarkar*

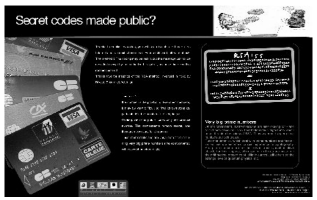
Resonance journal of science education

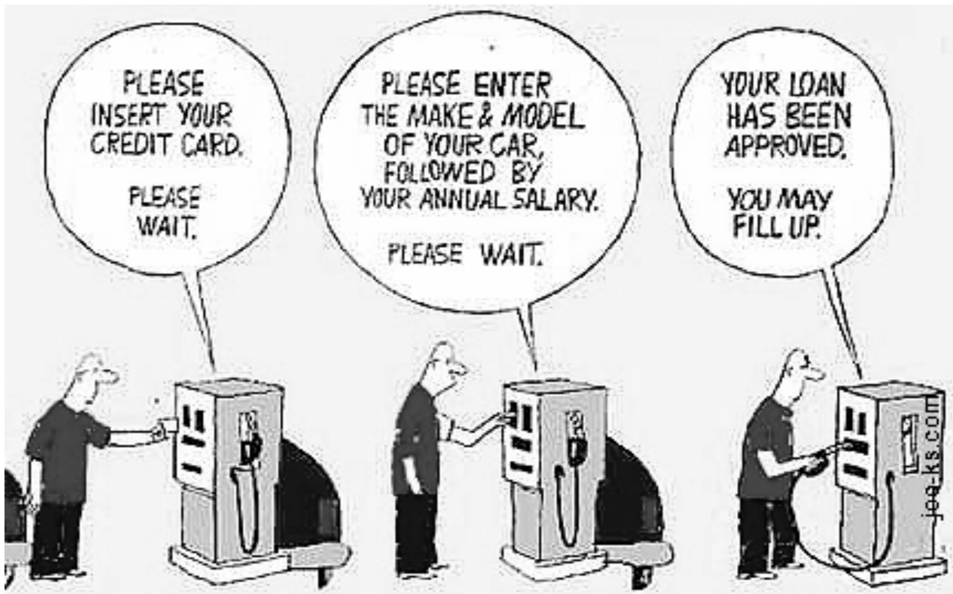
Volume 5 Number 9 (september 2000), p. 22-40

RSA SECURITY™

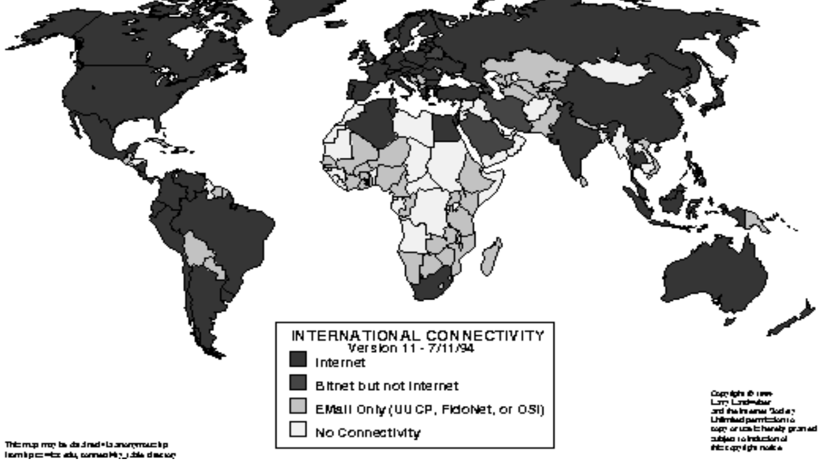
Encryption for security

PGP

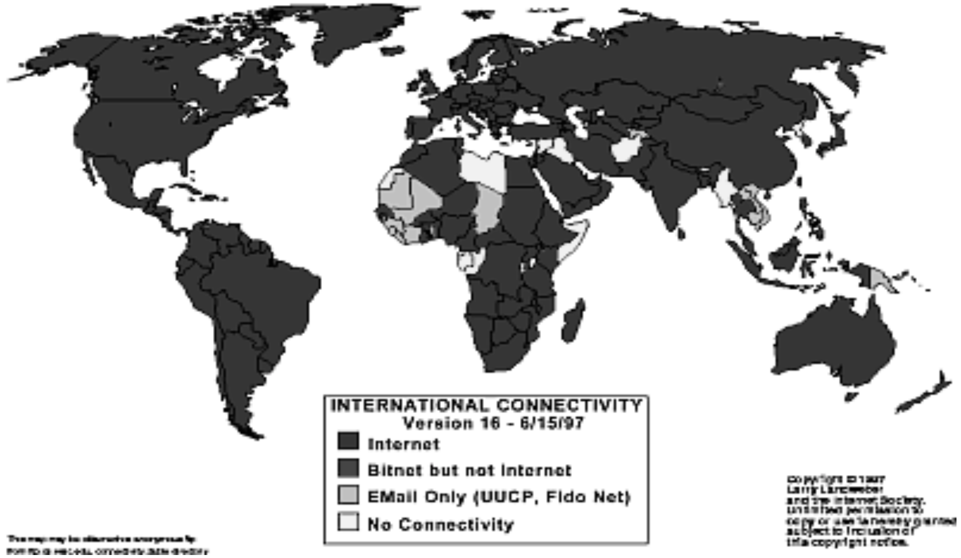




1994



Cryptology and the Internet: security norms, e-mail, web communication (SSL: Secure Socket Layer), IP protocol (IPSec), e-commerce…



Larry Landweber's International Connectivity maps 1997

Security of communication by cell phone, Telecommunication, Pay TV, Encrypted television,…

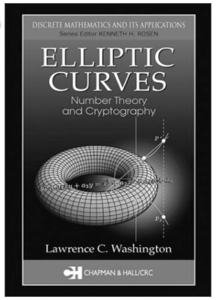
Activities to be implemented digitally and securely.

- Protect information — Code book, lock and key
- Identification — Driver's license, Social Security number, password, bioinformatics,
- Contract — Handwritten signature, notary
- Money transfer — Coin, bill, check, credit card
- Public auction — Sealed envelope
- Public election — Anonymous ballot
- Poker — Cards with concealed backs
- Public lottery — Dice, coins, rock-paper-scissors
- Anonymous communication — Pseudonym, ransom note

http://www.cs.princeton.edu/introcs/79crypto/

Mathematics in cryptography

- Algebra
- Arithmetic, number theory
- Geometry
- Topology
- Probability





Sending a suitcase

Alice  Charlie   Bob


- Assume Alice has a suitcase and a lock with the key; she wants to send the suitcase to Bob in a secure way so that nobody can see the content of the suitcase.

- Bob also has a lock and the corresponding key, but they are not compatible with Alice’s ones.

The protocol of the suitcases

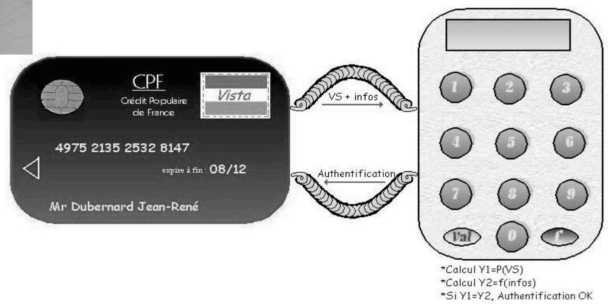


- Alice closes the suitcase with her lock and sends it to Bob.
- Bob puts his own lock and sends back to Alice the suitcase with two locks.
- Alice removes her lock and sends back the suitcase to Bob.
- Finally Bob is able to open the suitcase.

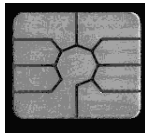
- *Later: a mathematical translation.*

Secret code of a bank card

ATM: Automated Teller Machine



The memory electronic card (chip or smart card) was invented in the 70's by two french engineers, Roland Moreno and Michel Ugon.

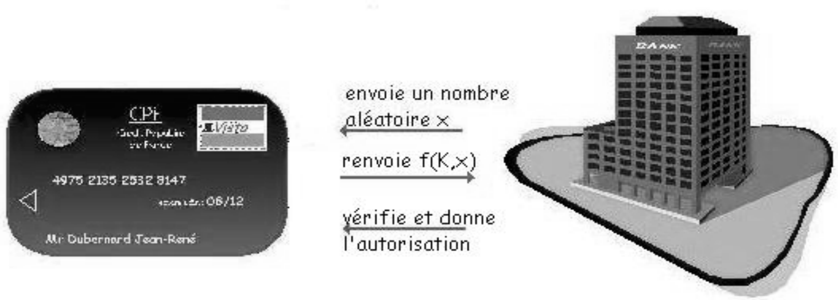


- France adopted the card with a microprocessor as early as 1992.
- In 2005, more than 15 000 000 bank cards were smart cards in France.
- In European Union, more than 1/3 of all bank cards are smart cards.

http://www.cartes-bancaires.com

Secret code of a bank card

- You need to identify yourself to the bank. You know your secret code, but for security reason you are not going to send it to the bank. Everybody (including the bank) knows the public key. Only **you** know the secret key.



The memory electronic card (chip card) .

- The messages you send or receive should not reveal your secret key.
- Everybody (including the bank), who can read the messages back and forth, is able to check that the answer is correct, but is unable to deduce your secret code.

- *The bank sends you a random message.*
- *Using your secret code (also called secret key or password) you send an answer.*

Cryptography: a short history

Encryption using alphabetical transpositions and substitutions

- Julius Caesar: replaces each letter by another one in the same order (shift)

- For instance, (shift by 3) replace

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
by
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

- *Example:*

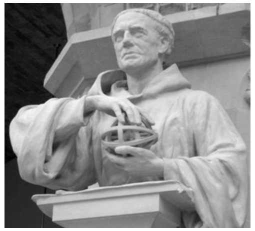
CRYPTOGRAPHY becomes FUBSWRJUDSKB

- *More sophisticated examples:* use any permutation (does not preserve the order).

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

Manuscript on deciphering cryptographic messages.

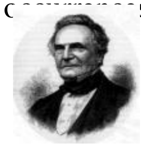
Check the authenticity of sacred texts from Islam.

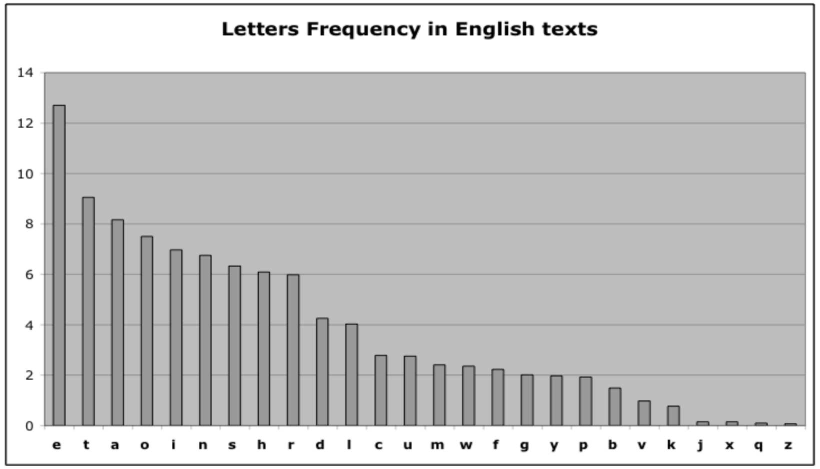


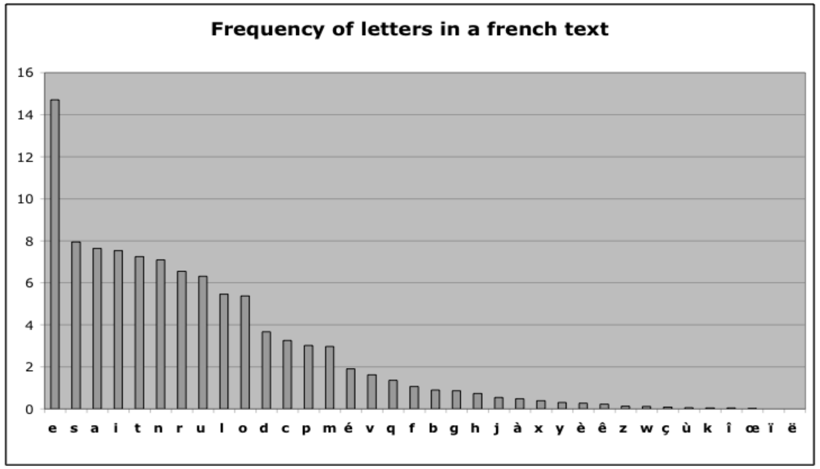
• XIIIth century, Roger Bacon: seven methods for encryption of messages.

•1586, Blaise de Vigenère
(key: «table of Vigenère») 
Cryptograph, alchimist, writer, diplomat

• 1850, Charles Babbage (frequency of c…s of letters)
Babbage machine (ancestor of computer)
Ada, countess of Lovelace: first programmer







International Morse code alphabet

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	..--..

Interpretation of hieroglyphs

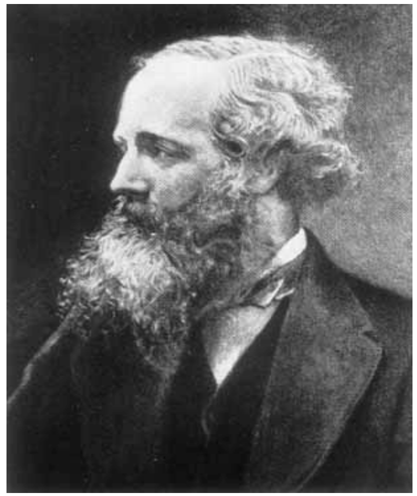
- Jean-François Champollion (1790-1832)
- Rosette stone (1799)

Data transmission

- ***Carrier-pigeons : first crusade - siege of Tyr, Sultan of Damascus***
- ***French-German war of 1870, siege of Paris***
- ***Military centers for study of carrier-pigeons created in Coëtquidan and Montoire.***

Data transmission

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



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

Any secure encyphering method is supposed to be known by the enemy
The security of the system depends onl he choice of keys.

1917, Gilbert Vernam (**disposable mask)**
Example: the red phone Kremlin/White House
One time pad

Original message:	0 1 1 0 0 0 1 0 1 …
Key	0 0 1 1 0 1 0 0 1…
Message sent	0 1 0 1 0 1 1 0 0…

1950, *Claude Shannon* proves that the only secure secret key systems are those with a key at least as long as the message to be sent.

Alan Turing

Deciphering coded messages
(*Enigma)*

Computer science

Colossus

Max Newman,
the first programmable electronic computer (Bletchley Park before 1945)

Information theory

Claude Shannon

A mathematical theory of communication

Bell System Technical Journal, 1948.

Claude E. Shannon

" Communication Theory of Secrecy Systems ",

Bell System Technical Journal ,

28-4 (1949), 656 - 715.

Secure systems

Unconditional security: knowing the coded message does not yield any information on the source message: the only way is to try all possible secret keys.

In practice, all used systems do not satisfy this requirement.

Practical security: knowing the coded message does not suffice to recover the key nor the source message **within a reasonable time.**

DES: Data Encryption Standard

In 1970, the NBS (*National Board of Standards*) put out a call in the *Federal Register* for an encryption algorithm

- with a high level of security which does not depend on the confidentiality of the algorithm but only on secret keys
- using secret keys which are not too large
- fast, strong, cheap
- easy to implement

DES was approved in 1978 by NBS

Algorithm DES:
combinations, substitutions and permutations between the text and the key

- The text is split in blocks of *64* bits
- The blocks are permuted
- They are cut in two parts, right and left
- Repetition *16* times of permutations and substitutions involving the secret key
- One joins the left and right parts and performs the inverse permutations.

Diffie-Hellman:
Cryptography with public key

- Whit Diffie and Martin E. Hellman,

  New directions in cryptography,

  IEEE Transactions on Information Theory,

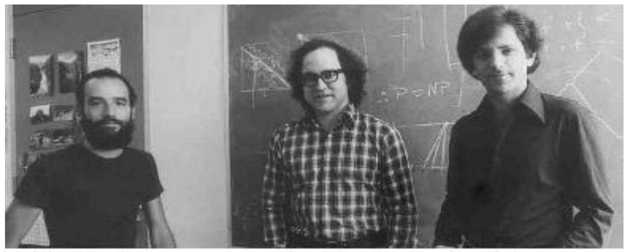
  22 (1976), 644-654

Symmetric versus **Assymmetric** cryptography

- **Symmetric** (secret key):
- Alice and Bob both have the key of the mailbox. Alice uses the key to put her letter in the mailbox. Bob uses his key to take this letter and read it.
- Only Alice and Bob can put letters in the mailbox and read the letters in it.

- **Assymmetric** (Public key):
- Alice finds Bob's address in a public list, and sends her letter in Bob's mailbox. Bob uses his secret key to read the letter.
- Anybody can send a message to Bob, only ***he*** can read it

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



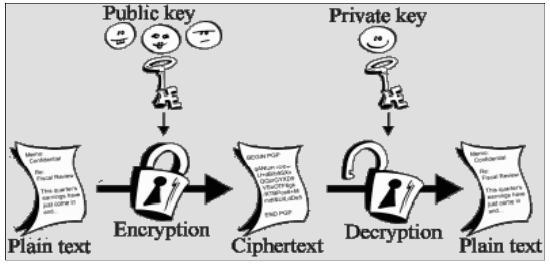
Adi Shamir Ron Rivest Len Adleman

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

A method for obtaining digital signatures and public-key cryptosystems,

Communications of the ACM

(2) **21** (1978), 120-126.



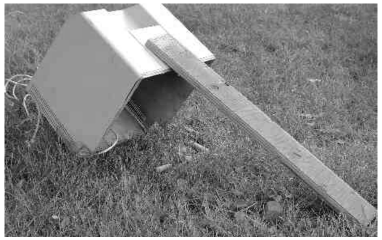
Trap functions

$x \to y$

is a *trap-door one-way function* if

- given x, it is easy to compute y
- given y , it is very difficult to find x, unless one knows a key.

Examples involve mathematical problems known to be difficult.



Example of a trapdoor one-way function: The discrete logarithm

(Simplified version)

Select a three digits number x.

Compute the cube: $x \times x \times x = x^3$.

Keep only the last three digits = remainder of the division by 1000: this is y.

- Starting from ***x,*** it is easy to find ***y.***
- If you know ***y,*** it is not easy to recover ***x.***

The discrete logarithm modulo 1000

- Example: assume the last three digits of x^3 are *631*: we write $x^3 \equiv 631$ modulo *1000*. ***Goal****: to find x.*
- Brute force: try all values of *x=001, 002, …*
  you will find that *x=111* is solution.
- *Check: 111 × 111 = 12 321*
- Keep only the last three digits:

  $111^2 \equiv 321$ modulo 1000
- Next *111 × 321 = 35 631*
- Hence $111^3 \equiv 631$ modulo *1000*.

Cube root modulo 1000

Solving $x^3 \equiv 631$ modulo 1000.

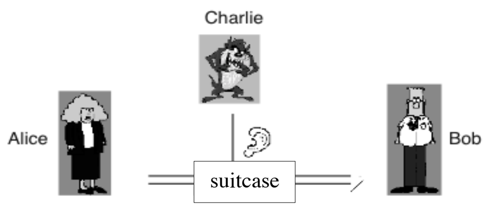
- **Other method:** *use a secret key*.
  The public key here is 3, since we compute x^3.
  A secret key is *67*.
- *This means that if you raise 631 to the power 67, you will find x*:

$$631^{67} \equiv x \text{ modulo } 1000.$$

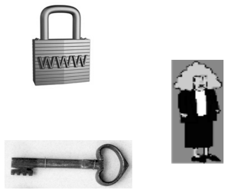
Retreive x from x ^{7} modulo 1000

- With public key 3, a secret key is 67.
- Another example: public key 7, secret key is 43.
- If you know $x^7 \equiv 871$ modulo 1000
- Check $871^{43} \equiv 111$ modulo 1000
- Therefore $x = 111$.

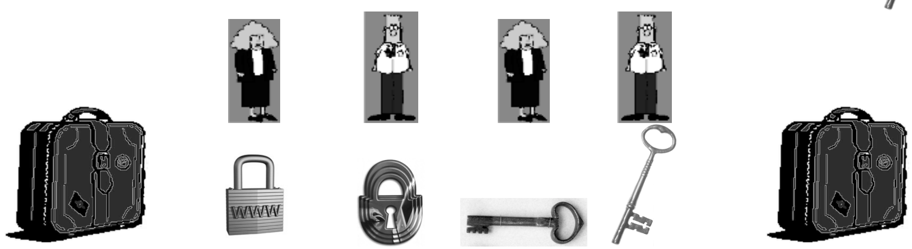
Sending a suitcase



- Assume Alice has a suitcase and a lock; she wants to send the suitcase to Bob in a secure way so that nobody can see the content of the suitcase.
- Bob also has a lock and the corresponding key, but they are not compatible with Alice's ones.



Sending a suitcase

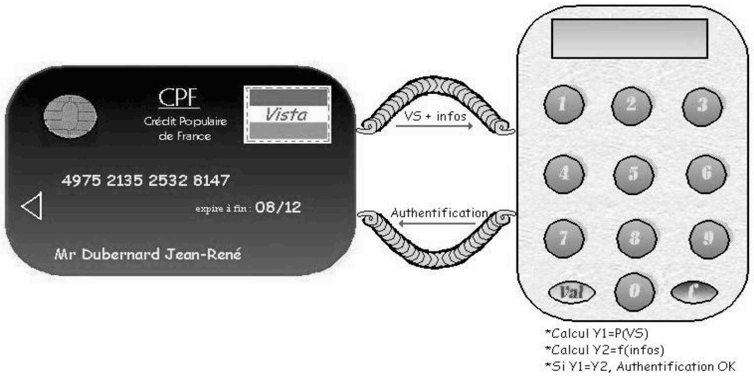


111 *7* *3* *43* *67* *111*

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

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

Security of bank cards



ATM

Random message	Pin Code	Public key
631	*67*	*3*
	$631^{67} \equiv 111$	$111^3 \equiv 631$

Everybody who knows your public key *3* and the message *631* of the bank, can check that your answer *111* is correct, but cannot find the result without knowing the pin code *67* (unless he uses the brute force method).

Message modulo n

- Fix a positive integer n *(in place of 1000)*: this is the size of the messages which are going to be sent.
- All computation will be done modulo n : we replace each integer by the remainder in its division by n.
- n will be a integer with some *300* digits.

It is easier to check a proof than to find it

Easy to multiply two numbers, even if they are large.

If you know only the product, it is difficult to find the two numbers.

Is *2047* the product of two smaller numbers?

Answer: yes $2047=23\times89$

Example

p=11139543251488279879254901754770248440709
22844843

q=19174817025245044393757862682308621806969
34189293

pq=21359870359209100823950227049996287970510
9534182641740644252416500858395774644508
8405009430865999

Size of n

We take for n the product of two prime numbers with some *150* digits each.

The product has some *300* digits: computers cannot find the two prime numbers.

Prime numbers, primality tests and factorization algorithms

- The numbers $2, 3, 5, 7, 11, 13, 17, 19, \ldots$ are prime.
- The numbers $4=2\times2$, $6=2\times3$, $8=2\times2\times2$, $9=3\times3$, $10=2\times5$, $2047=23\times89$ … are composite.
- Any integer ≥ 2 is either a prime or a product of primes. For instance $12=2\times2\times3$.
- Given an integer, decide whether it is prime or not **(primality test).**
- Given a composite integer, give its decomposition into a product of prime numbers **(factorization algorithm).**

Primality tests

- Given an integer, decide whether it is the product of two smaller numbers or not.

Today's limit : more than 1000 digits

Factorization algorithms

- Given a composite integer, decompose it into a product of prime numbers

Today's limit : around 150 digits

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

Industrial primes

- **Probabilistic Tests** are not genuine primality tests: they do not garantee that the given number is prime. But they are useful whenever a small rate or error is allowed. They produce the **industrial primes.**

The four largest known primes:

January 7, 2016	$2^{74\,207\,281} - 1$
	22 338 618 decimal digits
February 8, 2013	$2^{57\,885\,161} - 1$
	17 425 170 digits
August 23, 2008	$2^{43\,112\,609} - 1$
	12 978 189 digits
April 12, 2009	$2^{42\,643\,801} - 1$
	12 837 064 digits

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

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:

* $100 000 (1 lakh) to the first individual or group who discovers a prime number with at least 10 000 000 decimal digits.

* $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

Large primes

- The *11* largest known primes can be written as $2^p -1$ (and we know *49* such primes)
- We know

  170 primes with more than *1 000 000* digits (*11* in *2007*),

  1498 primes with more than *500 000* digits (*55* in *2007*).
- The list of *5 000* largest known primes is available at

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

Update: May 9, 2016

Mersenne numbers (1588-1648)

- *Mersenne* numbers are numbers of the form $M_p=2^p -1$ with p prime.

- There are only 49 known Mersenne primes, the first ones are *3, 7, 31, 127* with $3= M_2= 2^2 -1$, $7= M_3= 2^3 -1$, $31= M_5= 2^5 -1$, $127= M_7= 2^7 -1$.

- 1536, Hudalricus Regius: $M_{11}= 2^{11} -1$ is not prime: $2047= 23\times 89$.

Marin Mersenne (1588-1648), preface to *Cogitata Physica-Mathematica* (1644): *the numbers* $2^n -1$ *are prime for*

n = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127 and 257

and composite for all other positive integers n < 257.

The correct list is:

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

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

A large composite Mersenne number

- $2^{2\,944\,999} -1$ is composite: divisible by *314584703073057080643101377*

Perfect numbers

- An integer n is called *perfect* if n is the sum of the divisors of n distinct from n.
- The divisors of 6 distinct from 6 are $1, 2, 3$ and $6=1+2+3$.
- The divisors of 28 distinct from 28 are $1, 2, 4, 7, 14$ and $28=1+2+4+7+14$.
- *Notice that* $6=2\times 3$ *and* $28=4\times 7$
  while $3=M_2$ *and* $7=M_3$.
- Other perfect numbers are $496=16\times 31$, $8128=64\times 127,\ldots$

Even perfect numbers (Euclid)

- Even perfect numbers are numbers which can be written $2^{p-1}\times M_p$ with $M_p = 2^p - 1$ a Mersenne prime (hence p is prime).
- Are there infinitely many perfect numbers?
- Nobody knows whether there exists any odd perfect number.

Fermat numbers (1601-1665)

- A *Fermat* number is a number which can be written $F_n=2^{2^n}+1$.
- Construction with rule and compass of regular polygons.
- $F_0=3, F_1=5, F_2=17, F_3=257, F_4=65537$ are prime numbers.
- Fermat suggested in 1650 that all F_n are prime numbers.

Euler (1707-1783)

- $F_5 = 2^{32}+1$ is divisible by 641

$$4\,294\,967\,297 = 641\times 6\,700\,417$$

$$641 = 5^4 + 2^4 = 5\times 2^7 + 1$$

- Are there infinitely many Fermat primes?
- Only 5 Fermat primes F_n are known:
  $F_0=3, F_1=5, F_2=17, F_3=257, F_4=65537$.

Factorization algorithms

- Given a composite integer, decompose it into a product of prime numbers
- Today's limit : around *150* decimal digits for a random number
- Most efficient algorithm: ***number field sieve*** Factorization of RSA-155 (*155* decimal digits) in *1999*
- Factorization of a divisor of $2^{953}+1$ with *158* decimal digits in *2002*.
- ***A number with 313 digits on May 21, 2007.***

http://www.loria.fr/~zimmerma/records/factor.html

RSA Laboratories

Challenge Number Prize $US

- RSA-576 $10,000 Factored December *2003*
- RSA-640 $20,000 Factored November *2005*
- RSA-704 $30,000 Not Factored
- RSA-768 $50,000 Factored December *2009*
- RSA-896 $75,000 Not Factored
- RSA-1024 $100,000 Not Factored
- RSA-1536 $150,000 Not Factored
- RSA-2048 $200,000 Not Factored

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

Closed in 2007

RSA Laboratories

RSA-768

Status: Factored December 12, *2009*

Decimal Digits: *232* Digit sum *1018*

1230186684530117755130494958384962720772853569595334792197322452151726400507263657 518745202199786469389956474942774063845925192557326303453731548268507917026122 1 429134616704292143116022212404792747377940806653514195974598569021434 13

=

3347807169895689878604416984821269081770479498371376856891243138898288379387800228 761471165253174308773781446799948 9

*

3674604366679959042824463379962795263227915816434308764267603228381573966651127923 337341714339681027009279873630891 7

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

RSA Laboratories

RSA-704 Prize: $*30,000*

Status: Not Factored

Decimal Digits: *212*

- *74037563479561712828046796097429573142593188889231 28908493623263897276503402826627689199641962511784 39958943305021275853701189680982867331732731089309 00552505116877063299072396380786710086096962537934 650563796359*

- Digit Sum: *1009*

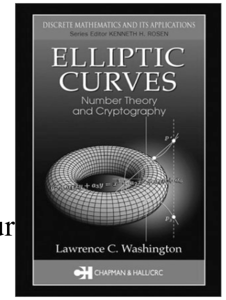
Other security problems of the modern business world

- Digital signatures
- Identification schemes
- Secret sharing schemes
- Zero knowledge proofs

Current trends in cryptography

- Computing modulo n means working in the multiplicative group of integers modulo n
- Specific attacks have been developed, hence a group of *large* size is required.
- We wish to replace this group by another one in which it is easy to compute, where the discrete logarithm is hard to solve.
- For smart cards, cell phones, … a *small* mathematical object is needed.
- A candidate is an elliptic curve over a finite field.

Research directions



To count efficiently the number of points on an elliptic cur over a finite field

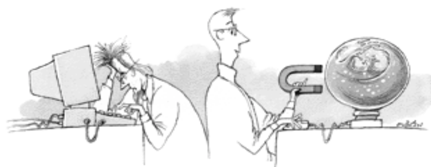
To check the vulnerability to known attacks

To find new invariants in order to develop new attacks.

Discrete logarithm on the Jacobian of algebraic curves

Modern cryptography

- Quantum cryptography (Peter Shor) - magnetic nuclear resonance



Quizz: How to become a hacker?

Answer: Learn mathematics !

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

$F_5 = 2^{32} + 1$ is divisible by 641

- $641 = 625 + 16 = 5^4 + 2^4$
- $641 = 5 \times 128 + 1 = 5 \times 2^7 + 1$
- 641 divides $2^{28} \times (5^4 + 2^4) = 5^4 \times 2^{28} + 2^{32}$
- $x^4 - 1 = (x+1)(x-1)(x^2+1)$

  641 divides $(5 \times 2^7)^4 - 1 = 5^4 \times 2^{28} - 1$
- Hence 641 divides $2^{32} + 1$