

# The Traveling Logician

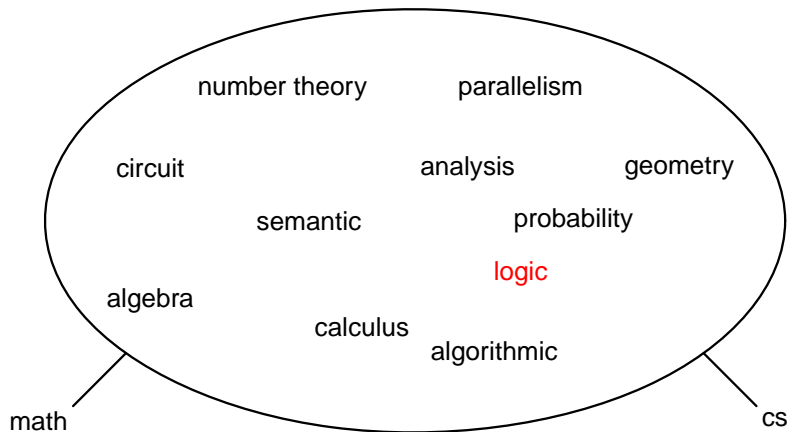
Serge Vaudenay



ÉCOLE POLYTECHNIQUE  
FÉDÉRALE DE LAUSANNE

<http://lasecwww.epfl.ch/>

# Mathematics and Computer Science at ENS in 1989

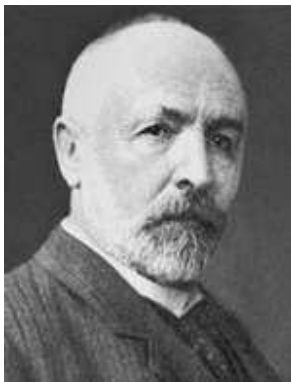




- 1 Travel #1: the Logic Homeland
- 2 Travel #2: the Information Theory Island
- 3 Travel #3: the Crypto Land
- 4 Travel #4: a New Math Continent
- 5 Travel #5: the Complexity World

# Some Negative Results

Georg Cantor 1891

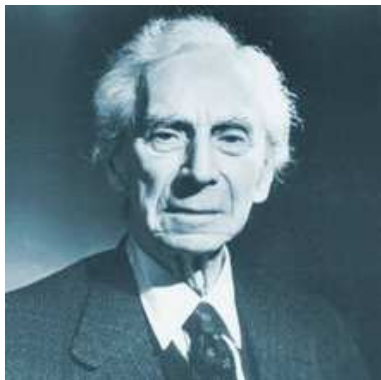


- sets have more subsets than elements
- even though  $\mathbf{N}$  is unbounded,  $\mathbf{R}$  is larger

infinity is unbounded!

# Some Negative Results

Bertrand Russell 1901



- there is no set of all sets

nothing is big enough for all sets!

# Some Negative Results

Kurt Gödel 1931



- there are statements on numbers which cannot be proven

arithmetic problem-solvers are bound to fail!

# Some Negative Results

Alan Turing 1936



- there is no algorithm capable of saying whether a program eventually halts when executed or not

there is no guaranty that a running computer may halt!

# Solvability of Diophantine Equations

Yuri Matiyasevich 1970



- a r.e. set  $\mathcal{S}$  is Diophantine: there exists a Diophantine equation  $f(n, x_1, \dots, x_k) = 0$  and a function  $n$  such that

$$s \in \mathcal{S} \iff \exists x_1, \dots, x_k \in \mathbf{N} \quad f(n(s), x_1, \dots, x_k) = 0$$

the proof of that is constructive

## Yet Another Negative Result

- the set of provable statements in a recursively presented theory is recursively enumerable
- consequence: we can exhibit a Diophantine equation  $f(n, x_1, \dots, x_k) = 0$  such that for some  $n$  values

$$\forall x_1, \dots, x_k \in \mathbf{N} \quad f(n, x_1, \dots, x_k) \neq 0$$

is not provable in any recursive extension of Peano arithmetics (even though  $f(n, x_1, \dots, x_k) = 0$  has no solution)

# Quantifier Elimination

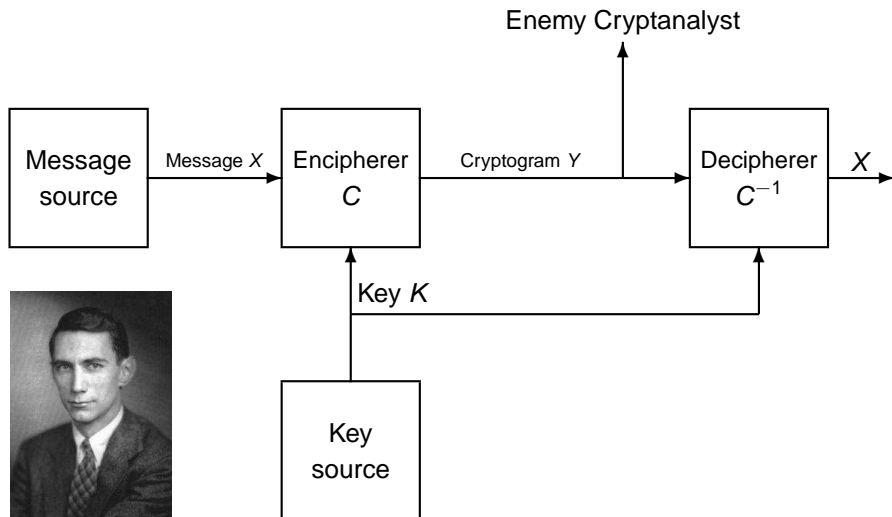
- for some theories, for any formula we can find an equivalent formula without quantifiers
- this is the case of the theory of algebraically closed fields!
- consequence: any closed formula with terms of polynomial form over  $\mathbf{C}$  can be decided

# So What?

- there must be something wrong with the theory of arithmetics
- but arithmetics is *real*, not a theory
- let's get out of here and move to information theory

# The Shannon Model for Encryption

Claude Shannon 1949



# Cipher

## Definition

A cipher is defined by

- a distribution for the plaintext  $X$
- an independent distribution for the key  $K$
- an algorithm mapping a plaintext  $x$  and a key  $k$  to a ciphertext  $\text{Enc}_k(x)$
- an algorithm mapping a ciphertext  $y$  and a key  $k$  to a plaintext  $\text{Dec}_k(y)$

and is such that

$$\Pr[\text{Dec}_K(\text{Enc}_K(X)) = X] = 1$$

we set  $Y = \text{Enc}_K(X)$

# Perfect Secrecy

## Definition

A cipher  $(X, K, \text{Enc}, \text{Dec})$  provides perfect secrecy if  $X$  and  $Y = \text{Enc}_K(X)$  have independent probability distributions:

$$\forall A, B \text{ mesurable} \quad \Pr[X \in A, Y \in B] = \Pr[X \in A] \Pr[Y \in B]$$

## Example: Vernam Cipher over a Finite Domain

- $\mathcal{X}$ : a finite set given a group structure
- $K$  uniformly distributed in  $\mathcal{X}$
- $\text{Enc}_k(x) = x + k$
- $\text{Dec}_k(y) = y - k$

for any random variable  $X$  with value in  $\mathcal{X}$  which is independent from  $K$ : for any  $x, y \in \mathcal{X}$

$$\begin{aligned}\Pr[X = x, Y = y] &= \Pr[X = x, x + K = y] \\ &= \Pr[X = x] \Pr[K = -x + y] \\ &= \frac{1}{\#\mathcal{X}} \Pr[X = x]\end{aligned}$$

so we deduce (by summing over all  $x$ s) that  $Y$  is uniformly distributed and independent from  $X$

## Example: Vernam Cipher over a Continuous Domain

- $\mathcal{X} = [0, 1]$  with addition modulo 1
- $K$  uniformly distributed in  $\mathcal{X}$
- $\text{Enc}_k(x) = x + k \bmod 1$
- $\text{Dec}_k(y) = y - k \bmod 1$

for any random variable  $X$  with value in  $\mathcal{X}$  which is independent from  $K$ : for any  $x, y \in \mathcal{X}$ ,  $\Pr[X \leq x, Y \leq y]$  equals

$$\Pr \left[ X \leq x, \left\{ \begin{array}{ll} K \in [-X \bmod 1, y + (-X \bmod 1)] & \text{if } y + (-X \bmod 1) \leq 1 \\ K \notin [y - 1 + (-X \bmod 1), -X \bmod 1] & \text{if } y + (-X \bmod 1) > 1 \end{array} \right\} \right]$$

thus  $\Pr[X \leq x, Y \leq y] = y \Pr[X \leq x]$ . Therefore

$$\forall x \in \mathbf{R} \quad \forall y \in \mathbf{R} \quad \Pr[X \leq x, Y \leq y] = \Pr[X \leq x] \Pr[Y \leq y]$$

so we have perfect secrecy

# Perfect Secrecy over $\aleph_0$ is Impossible

## Theorem

*If a cipher  $(X, K, \text{Enc}, \text{Dec})$  provides perfect secrecy and  $\mathcal{X} = \text{Supp}(X)$  is enumerable, then  $\mathcal{X}$  must be finite.*

**Proof:** Take  $x_1 \in \mathcal{X}$  and  $k \in \text{Supp}(K)$  arbitrary.

Let  $y = \text{Enc}_k(x_1)$  so  $\Pr[Y = y | X = x_1] \neq 0$ .

We have

$$\forall x_0 \in \mathcal{X} \quad \Pr[\text{Enc}_K(x_0) = y] = \Pr[Y = y | X = x_0] = \Pr[Y = y | X = x_1]$$

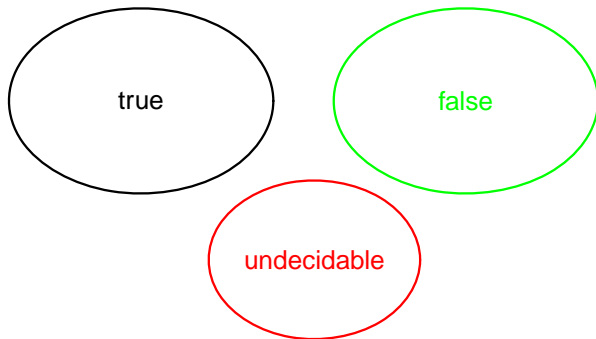
so  $\Pr[\text{Dec}_K(y) = x_0] \geq \Pr[\text{Enc}_K(x_0) = y] = \Pr[Y = y | X = x_1]$ .

Summing over all  $x_0 \in \mathcal{X}$  we get  $1 \geq \Pr[Y = y | X = x_1] \times \#\mathcal{X}$  so  $\mathcal{X}$  must be finite. □

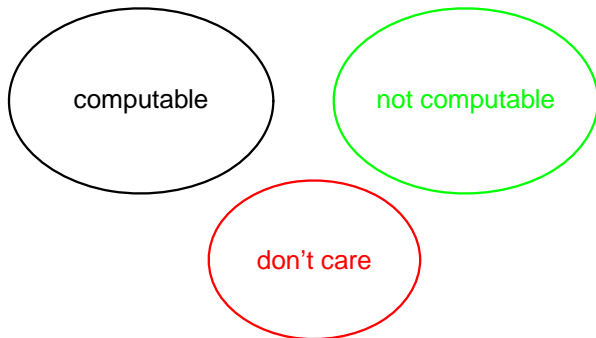
# So What?

- still something wrong with our discrete computational model
- no hope for perfect security
- business as usual

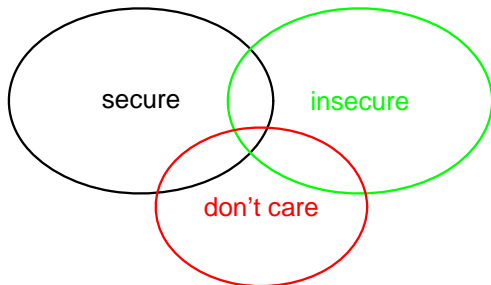
# The Logic World



# The Computer Science World



# The Crypto World



# A Fuzzy World

- what is secure in a theoretical model may be insecure in practice  
e.g. random oracle-based security
- what is secure in practice may be insecure in theory  
e.g. collision-resistant hash function
- what is secure at time  $t$  may be insecure at time  $t + 1$   
e.g. any crypto standard in the real world
- what is mathematically wrong may be cryptographically correct

# Cryptopunk



# Cryptanalysis

cryptanalysis = proving or breaking a scheme

## proving

- must describe the setup model
- must describe the adversary objectives
- must describe the adversary capabilities
- must state the hypotheses
- rigorous proof required (formal)

## breaking

- must describe the setup model
- must describe the adversary objectives
- must describe the adversary capabilities
- must assess the complexity
- **any dirty proof allowed** (experimental)

# Twisting Galois

Coppersmith-Stern-Vaudenay 1993

- Shamir's signature scheme based on birational permutation
- let  $N = p \times q$  be the product of two primes (secret key)
- consider the field  $\mathbf{K} = \mathbf{Z}/N\mathbf{Z}$
- construct a polynomial  $P(x)$  whose roots depend on the secret
- consider the field extension  $\mathbf{K}[x]/(P(x))$
- express the symmetries in the roots
- sign a message in this extension
- the result ends up in  $\mathbf{K}$  and is a valid signature

quiz:

Q: what is a prime number?

A: n ahzore sbe juvpu jr xabj ab cebcre snpgbe

▶ ROT13



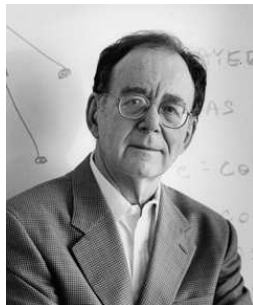
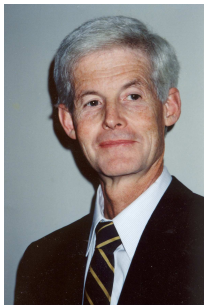
# What is a Proof?

Shafi Goldwasser, Silvio Micali, Charles Rackoff 1985

- for logicians: a sequence of statements following inference rules
  - for a photographer: a trial print
  - for a publisher: an impression made to check for errors
  - for a judge: a factual evidence that helps to establish the truth
  - for computer scientists: a program (Curry-Howard)
- the act of validating, finding, or testing the truth
- for cryptographers: an interactive protocol between P and V
    - PSPACE=IP (Adi Shamir 1992)
    - zero-knowledge
    - access control
    - identification
    - digital signature

# What is a Computability?

Stephen Cook 1971, Richard Karp 1972



“something computable in polynomial time by a Turing machine”

Example: the traveling logician problem

**Instance** several conferences scheduled in different places

**Problem** can we show up to all by traveling less than  $B$  miles?

# The Hitchhiker's Guide to Cryptography

