La cryptologie: des messages secrets aux transactions sécurisées

40ème anniversaire du LAAS
Toulouse, 20 juin 2008

Jacques Stern

professeur à l'Ecole normale supérieure

président de l'ANR

président d'INGENICO

Résumé

- Bref aperçu historique
- Qu’est-ce que la cryptologie?
- Quatre questions
- Un exemple d’application

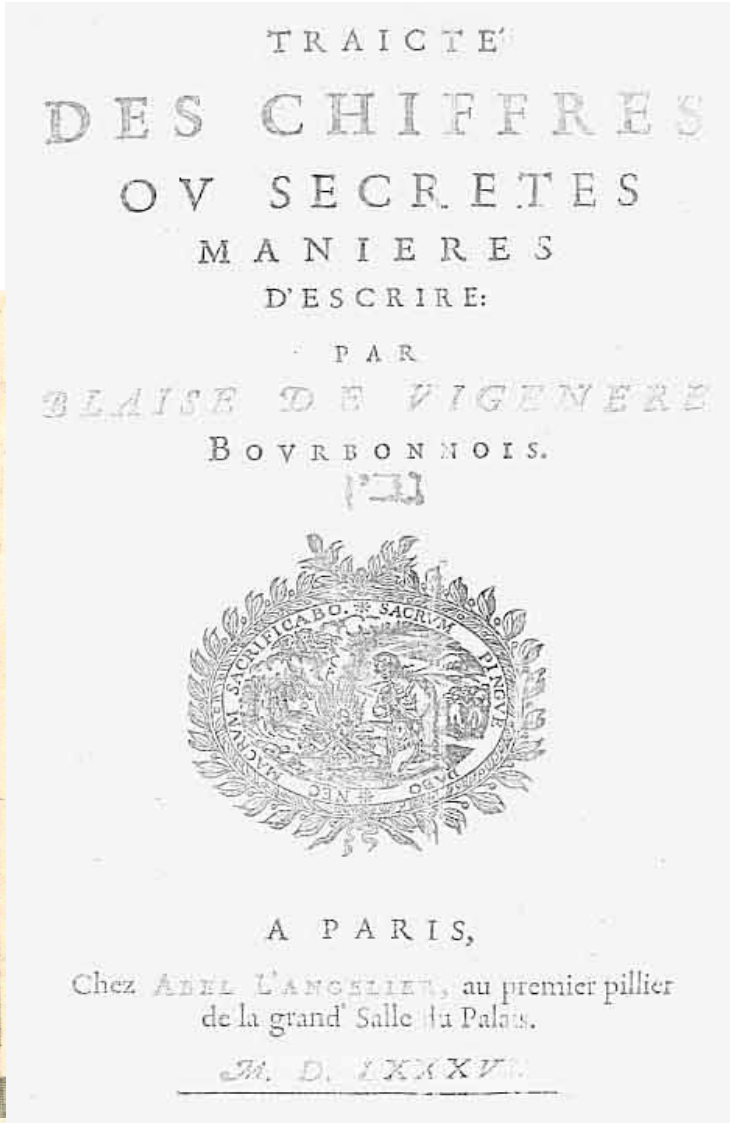
Un art ancien

- papier
- cadrans et cylindres
- machines chiffrantes

Avertissement : Les illustrations de cette planche (et de plusieurs autres planches) étant non libres de droits, elles ont été supprimées pour permettre une large diffusion de ce document.

Une science ancienne

- al-Kindi (850)
- Vigenere (1585)
- Schott (1665)


TRAICTE'
DES CHIFFRES
OV SECRETES
MANIERES
D'ESCRIRE:
PAR
BLAISE DE VIGENERE
BOVRBONNOIS.

A PARIS,
Chez ABEL L'ANGELIER, au premier pillier
de la grand' Salle du Palais.
M. D. LXXXV.

Une science longtemps duale : la guerre des codes

- Contre l'ENIGMA
- Gagnée par Alan Turing et les Britanniques

Une science intimement liée à l'informatique

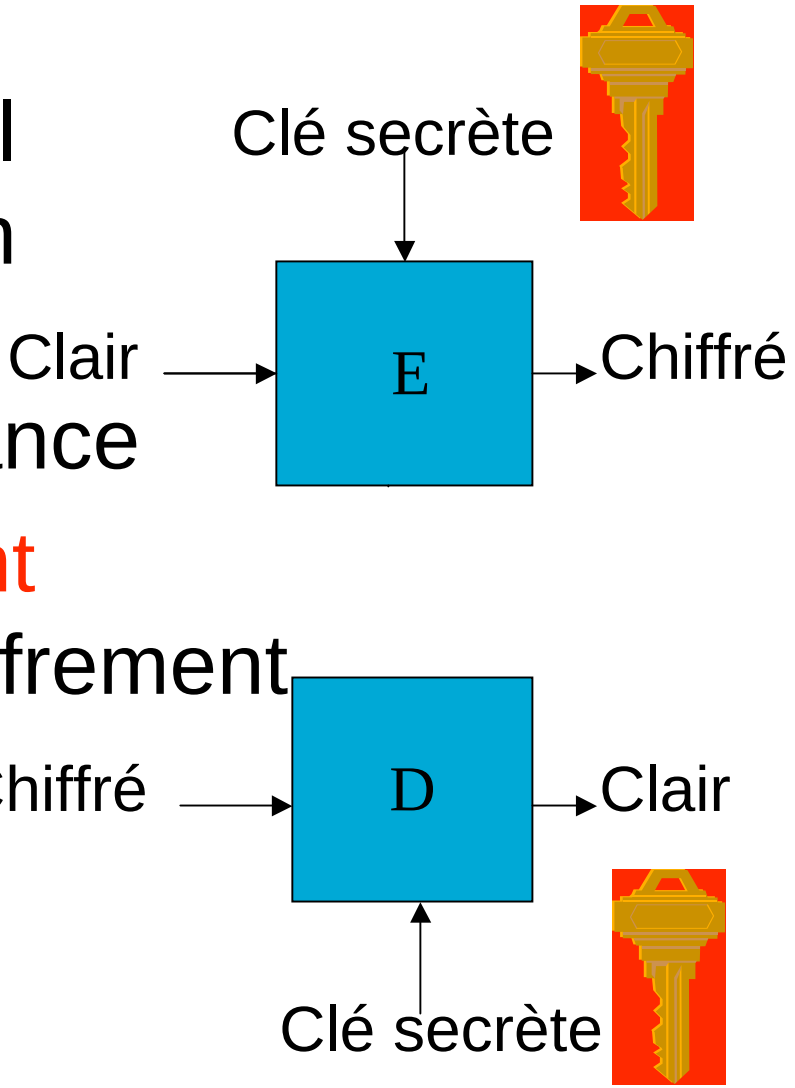
- 1944 : Colossus, machine informatique suggérée par Turing
- 1976 : Invention de la cryptologie à clé publique pour une communication sûre entre machines ; anticipation d'Internet

Qu’est ce que la cryptologie

- La science des messages secrets
- La trilogie fondamentale :
  - Intégrité
  - Authenticité
  - Confidentialité

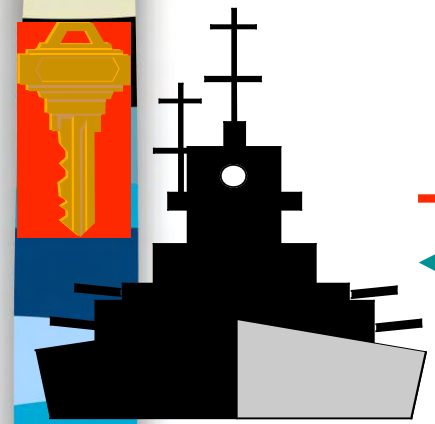
Confidentialité: le chiffrement

- Transmettre un message sur un canal non sécurisé de façon qu'un tiers ne puisse en prendre connaissance
- Une clé préalablement échangée sert au chiffrement et au déchiffrement
- Exemples DES, 3-DES, RC4, AES



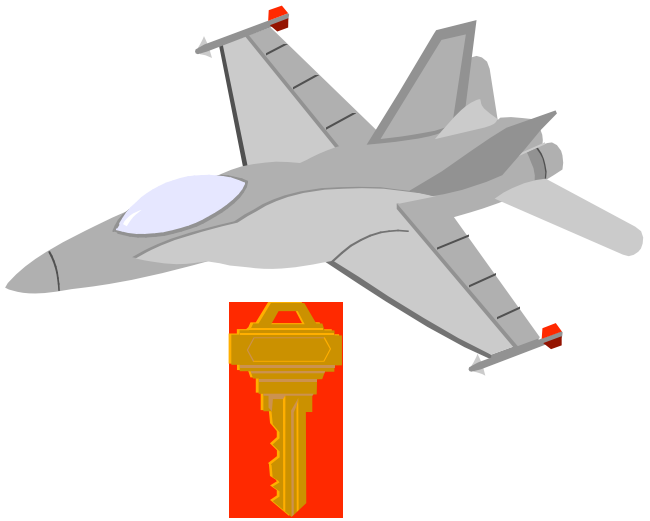
Authenticité

- La capacité de chiffrer et déchiffrer garantit l'authenticité
- Cette authenticité n'est pas opposable aux tiers



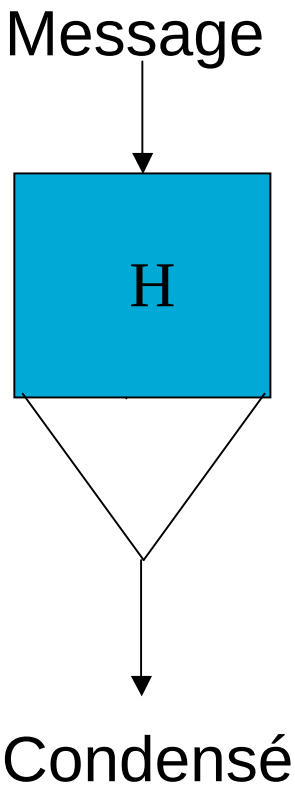
Message chiffré aléatoire

Message



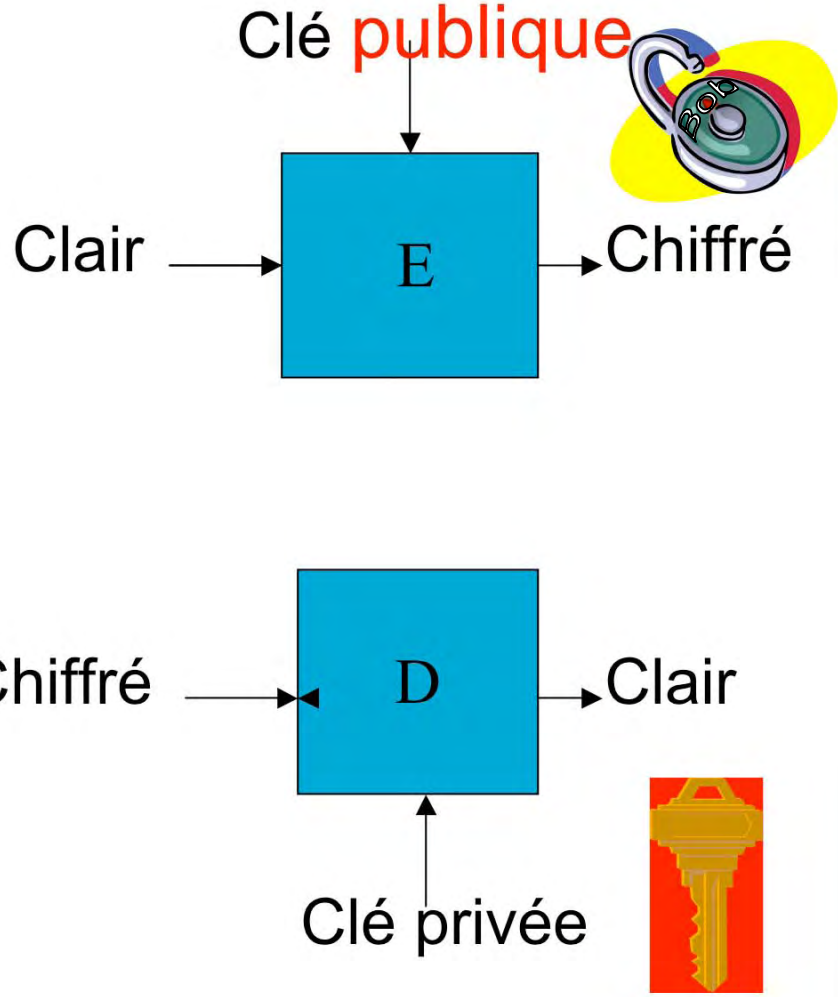
Intégrité: fonctions de hachage

- L'intégrité peut être garantie sans clé.
- Une valeur calculée par une *fonction de hachage* H est transmise par un canal sûr (ou authentifiée).
- Propriété paradoxale:H doit résister aux collisions: $x \neq y$ $H(x) = H(y)$



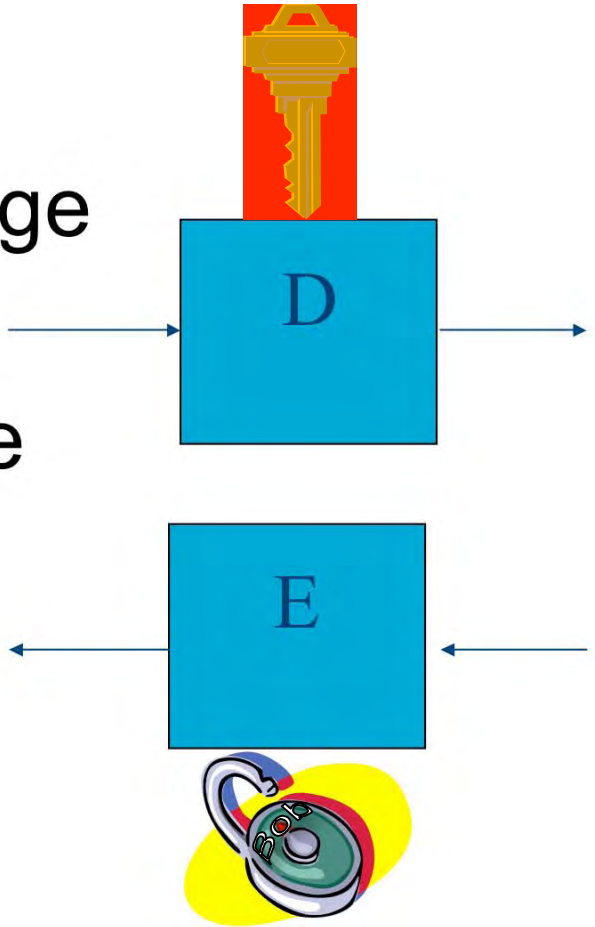
1976-78: la cryptologie asymétrique

- Inventée par Whitfield Diffie et Martin Hellman
- Elimine tout échange préalable
- Réalisée par Ron Rivest, Adi Shamir et Len Adleman



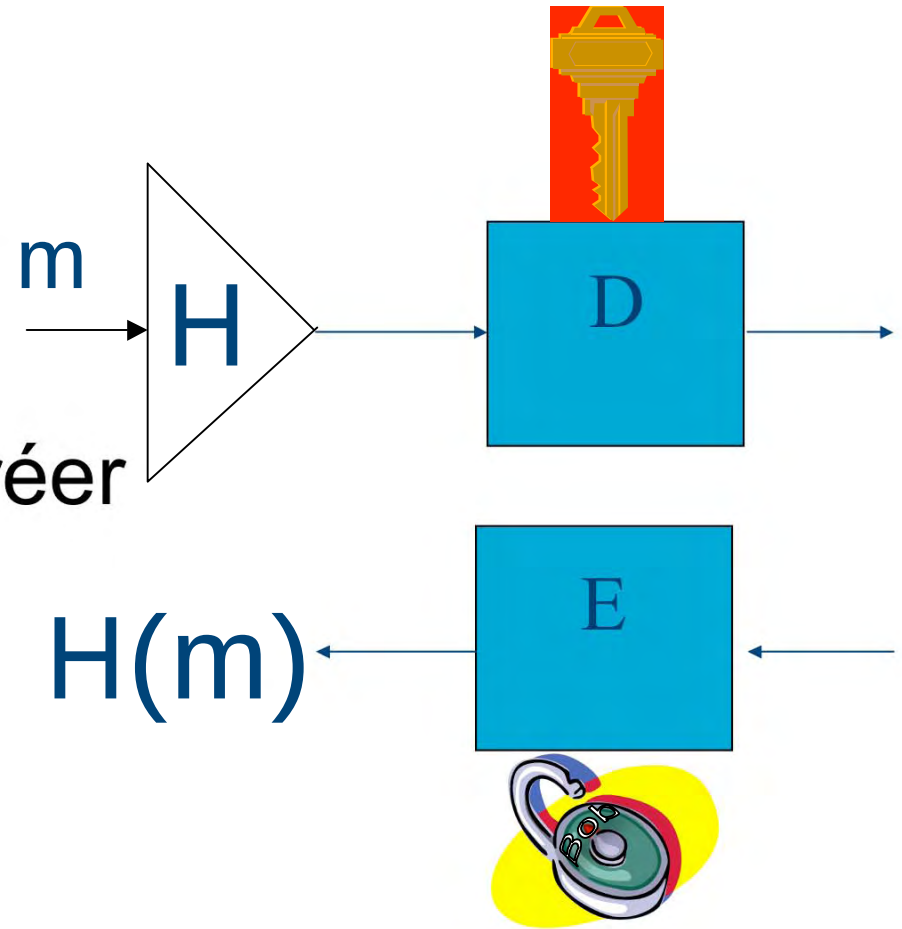
La cryptographie à clef publique mène aux signatures

- En appliquant D au message m pour créer la signature
- La vérification ne nécessite que la clef publique
- Rend opposable aux tiers l'authentification



Plus précisément:

- On applique D au condensé H(m) du message m pour créer la signature
- La vérification met en jeu H(m)



Le cryptosystème RSA

- 1978: Rivest, Shamir Adleman
- module n et exposant petit e
- n produit de p q premiers
- Le chiffrement de x est

$$y = x^e \bmod n$$

- Le déchiffrement de y est

$$x = y^d \bmod n$$

- d calculé à partir de p,q (secrets)

$$e.d = 1 \bmod \phi(n)$$

Euler
1707-1783

Sécurité algorithmique

- Fondée sur la difficulté de trouver deux nombres premiers p and q à partir de leur produit n
- Le record ⟶
- Précédent 173: 12/03; recommandé1024 bits (328) ou 2048

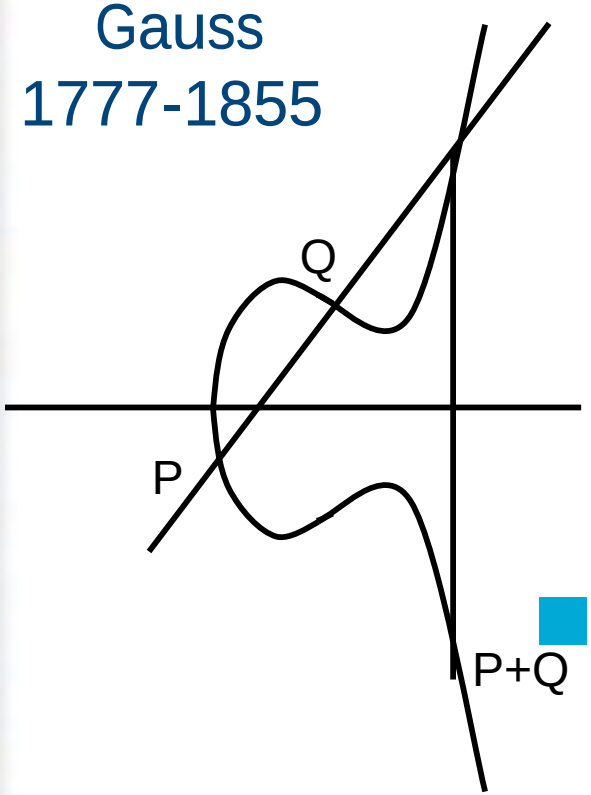
Date: Mon, 9 May 2005 18:05:10 +0200 (CEST)
From: "Thorsten Kleinjung"
Subject: rsa200
We have factored RSA200 by GNFS. The factors are
3532461934402770121272604978198464368671197400197625023649303468776121253679423200058547956528088349
and
7925869954478333033347085841480059687737975857364219960734330341455767872818152135381409304740185467
More details will be given later.
F. Bahr, M. Boehm, J. Franke, T. Kleinjung

Quatre questions après RSA?

- Peut-on faire plus court?
  [taille des clés]
- Peut-on faire plus rapide?
  [complexité des calculs]
- Peut-on prouver la sécurité?
  [sous certaines hypothèses]
- Peut-on choisir la clé publique?
  [son adresse mail?]

Plus court

Gauss
1777-1855



- Cryptographie fondée sur les fonctions/courbes « elliptiques ». Idée: remplacer le groupe multiplicatif des entiers non nuls mod n
- 1985 : Koblitz et Miller independamment

Abel 1802-1829

Pourquoi?

- Parce qu'il n'y a pas d'algorithme « sous-exponentiel » connu pour la résolution de l'équation

$$x.G = P$$

sur une courbe *(log discret)*

- Record : courbes de 109 bits (2002/2005)

Comment?

- Un point G, un point P
- valeur x telle que

$$x\,G = P$$

- Pour chiffrer créer une clé éphémère $k = H(r\,P)$ à partir d'un aléa r . Emetttre le chiffré c et le point $Q = r\,G$
- Déchiffrer avec $k = H(x\,Q)$

Plus rapide: défense et attaque

- 1997 : cryptanalyse d'un algorithme de chiffrement « rapide » proposé par Ajtai et Dwork (IBM)
- 2007: cryptanalyse de l'algorithme de signature « rapide » SFLASH en voie d'adoption comme norme

L'attaque de AD

- Un hyperplan caché de l'espace R^n $(xa)=b$
- Des points proches des hyperplans // $(xa)=b\mathbf{Z}$

Minkovski
1864-1909

- Chiffrer un bit 0/1 par un point proche/loin
- Déchifer avec l' équation cachée
- Cryptanalyse fondée sur la géométrie des nombres (JS, P. Nguyen)

L'attaque de SFLASH

- Un polynôme quadratique dans un corps fini binaire $F(2^n)$:

  $Y=X^{\theta}$ AVEC $\theta = 2^i + 2^j$

- Des changements de variables affines
- → $k<n$ équations quadratiques liant $x=(x_1, \ldots, x_n)$ et $y=(y_1, \ldots, y_k)$
- Signer en résolvant pour H(m)= y
- Cryptanalyse fondée sur la recherche de matrices « antisymétriques » (JS + Shamir + P.A. Fouque + V. Dubois)

Sylvester
1814-1897

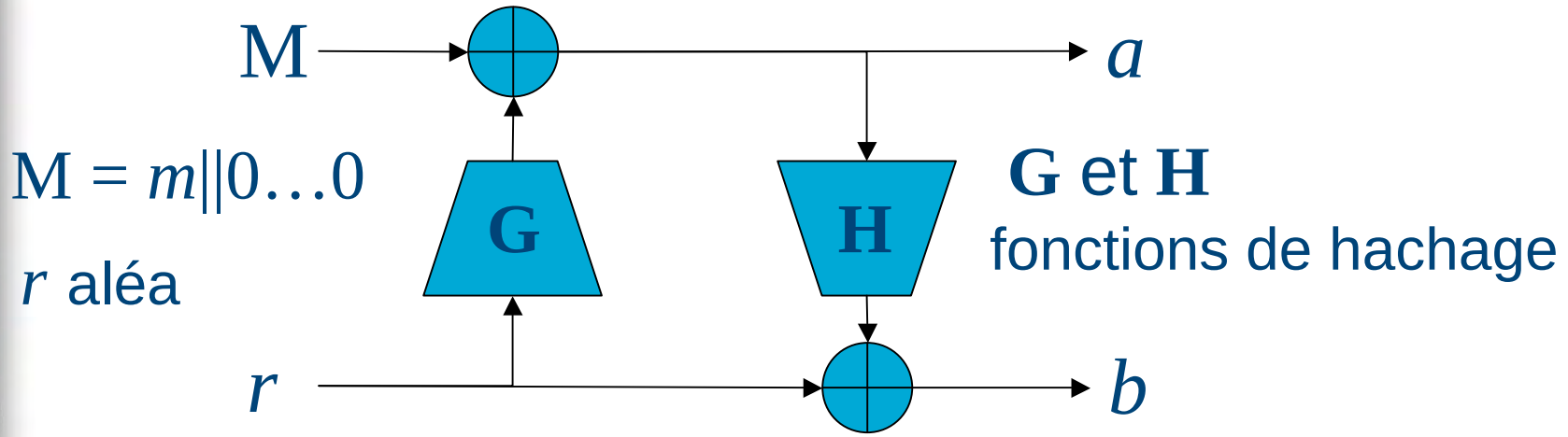
Prouvable?

- 1990-2000 : Méthode de « sécurité prouvée »: Version du 1er principe de Kerchkoffs (1883), « *Le système doit être matériellement sinon mathématiquement indéchiffrable* », utilisant la théorie de la complexité algorithmique

Kerckhoffs
1835-1903

- Ne peut « prouver » RSA mais permet de résister à des attaques variées (ex. CCA), sous l'hypothèse qu'on ne peut inverser RSA.

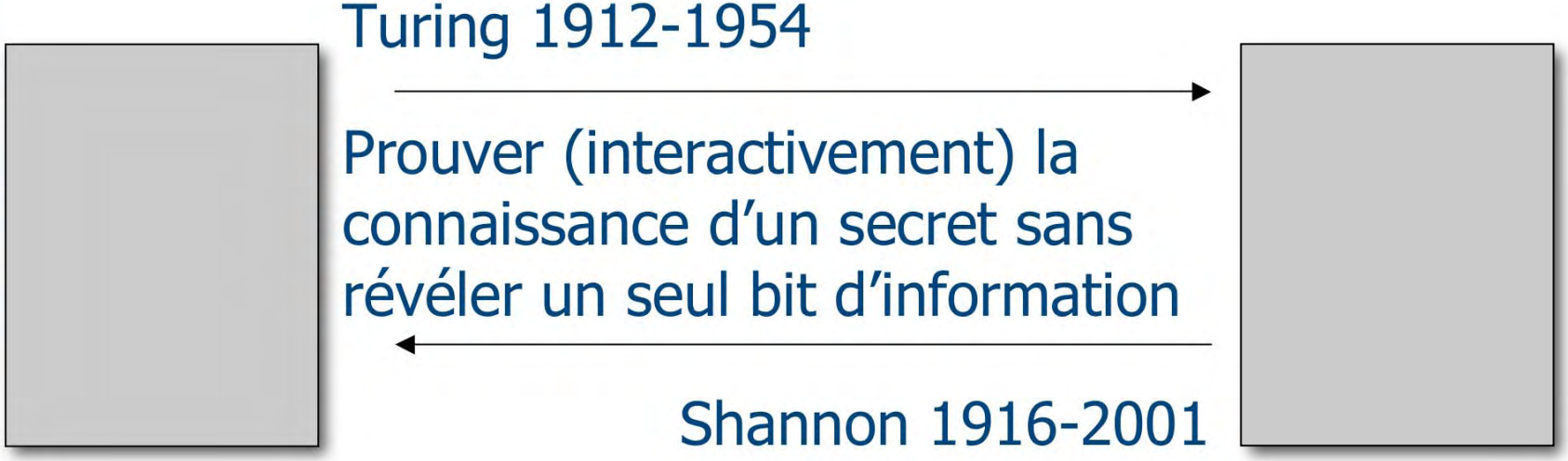
OAEP Bellare-Rogaway 1994



- méthode de sécurité prouvée appliquée à OAEP (format RSA normalisé)
- 2000 : la preuve est reconnue fausse!
- 2001: preuve correcte (JS + D. Pointcheval + T. Okamoto + E. Fujisaki)

Choisir sa clé publique

- Problème posé par Shamir en 1984
- Résolu en 1986 par Fiat et Shamir dans le cas des signatures
- S'appuie sur la théorie du "zero-knowledge"



Cryptographie fondée sur l'identité

- Problème résolu pour le chiffrement en 2001par Boneh et Franklin

Weil 1906-1998

- Utilise le "couplage" de Weil, opération math.

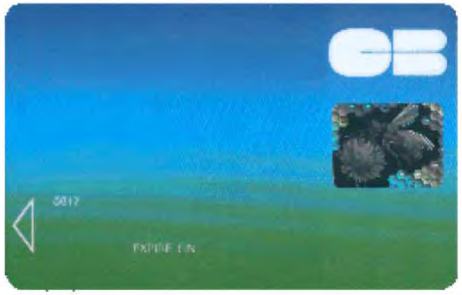
$$G \times G \rightarrow G_1$$

G groupe des points de q-torsion d'une courbe elliptique, G_1 groupe des racines q-ièmes de l'unité

Les applications :

- Nous portons sur nous deux processeurs cryptographiques
- et utilisons des connexions sécurisées

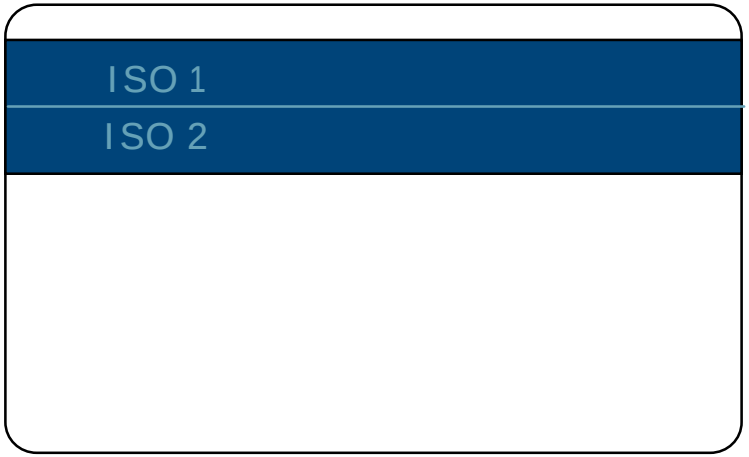
Etude de cas: Les cartes bancaires



- 1967: cartes
- 1971: cartes à piste magnétique
- 1990-1992: vers la puce
- 2004- : vers EMV et le DDA

Premier niveau de sécurité: piste

- Données (en clair)
  - PAN(numéro)
  - date d'expiration
  - données de service
- Données chiffrées : PIN CODE chiffré



Menaces

- La piste est copiable
- Le CODE PIN visible

Second niveau de sécurité: puce

- Authentification hors ligne
- CODE PIN
- Authentification des transactions par cryptogramme

CODE PIN

PIN CODE

OUI/NON

Continuer

FAIL

SDA: Static Data Authentication

Emetteur

RSA sign de PAN+data

signature RSA

RSA sign OK

Continuer

FAIL

Vérification en ligne du cryptogramme

Emetteur

Cryptogramme

Clé secrète « Triple DES »

Cryptogramme OK

Transaction

Cryptogramme 3-DES

Continuer

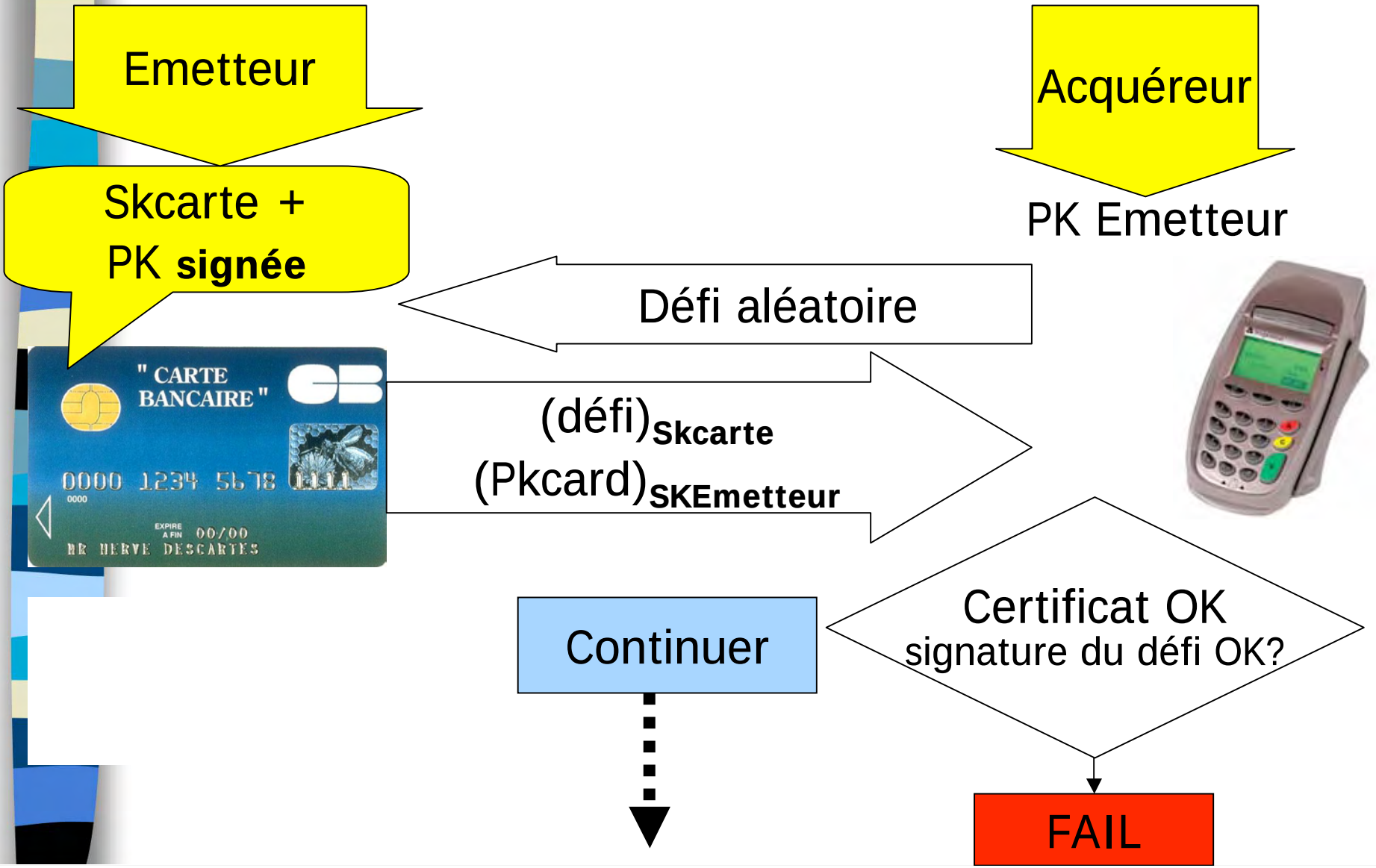
Cryptogramme OK

FAIL

Menaces: « Yes cards »

- La signature statique RSA est copiable
- Et des « clones » peuvent ainsi être utilisés et sont connus sous le nom de « yes-cards »

Troisième niveau de sécurité: DDA



Conclusion : l'ubiquité de la cryptologie au XXIème siècle fondée sur des maths du XVIIIème/XIXème siècle