NOMBRES PREMIERS
et
CRYPTOGRAPHIE

Jean Cailliez

HISTORIQUE

- **Code de César** : permutation et substitution
  (code monoalphabétique)
- **Analyse des fréquences d'apparition** (Al-Kindi 9ème siècle)

- **Code de Vigenère** (code polyalphabétique 16ème siècle)

  exemple simplifié

  alphabet ordinaire : abcdefghijklmnopqrstuvwxyz

  alphabet chiffré 1 : fghijklmnopqrstuvwxyzabcde

  alphabet chiffré 2 : jklmnopqrstuvwxyzabcdefghi

  codage en fonction du rang d'apparition du caractère

  Code déchiffré par Babbage en 1854

ERE INDUSTRIELLE

Machines à crypter électro-mécaniques

Enigma

Sherbius 1923 : machine munie de rotors utilisée à des fins commerciales

rachetée par l'armée allemande en 1928 en y apportant des améliorations

passage de 3 rotors actifs à 5 rotors au cours de la 2de guerre mondiale

carnet de codes associé (indiquant la position initiale des rotors et modifiée chaque jour)

le principe consistant à changer de substitution à chaque frappe d'un caractère

ERE MODERNE

- **Système DES** (Data Encryption Standart)

- **Diffie et Hellman** 1975

  cryptage asymétrique

  échange de clés

- **Système RSA** 1978

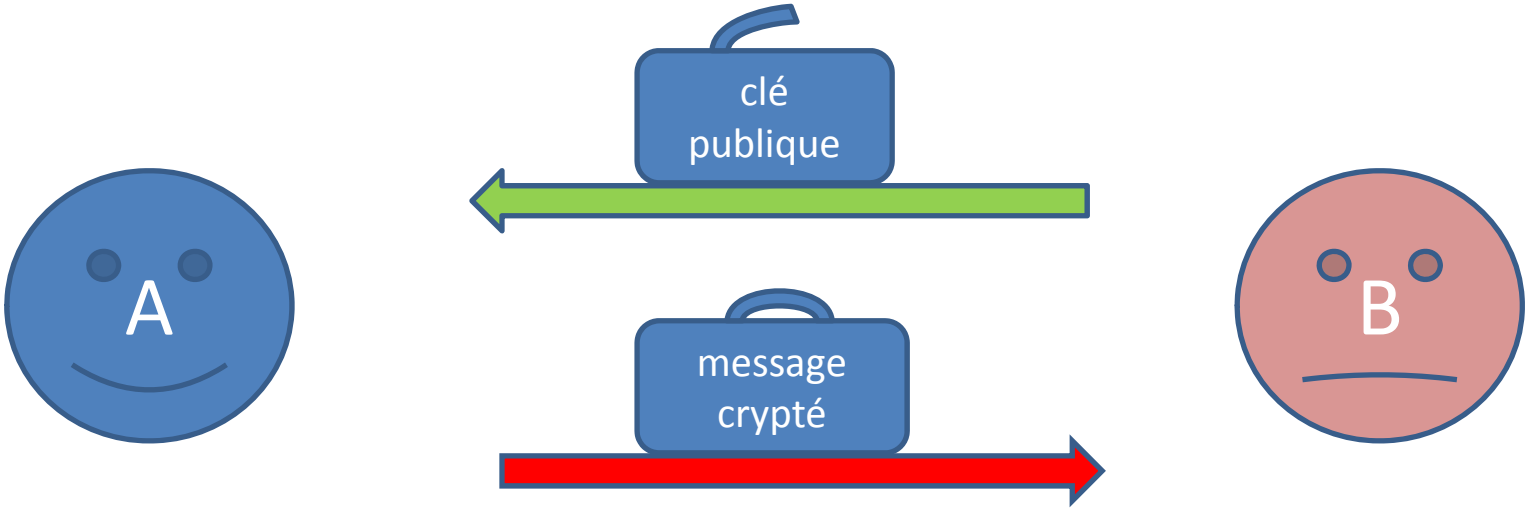
  cryptage asymétrique

  système à 2 clés : publique et privée

- **Cryptage par courbe elliptique** 1980 : Koblitz, Lenstra

Cryptage asymétrique

A veut envoyer à B un message confidentiel



B décrypte avec sa clé privée

Interprétation mathématique

Clé publique **f** (éventuellement indexée)

Clé privée **g** : application réciproque de **f**

Cryptage asymétrique :

Si M est le message :

$\mathbf{f}_B$: **B** ⟹ **A**

$\mathbf{f}_B$ (M) : **A** ⟹ **B**

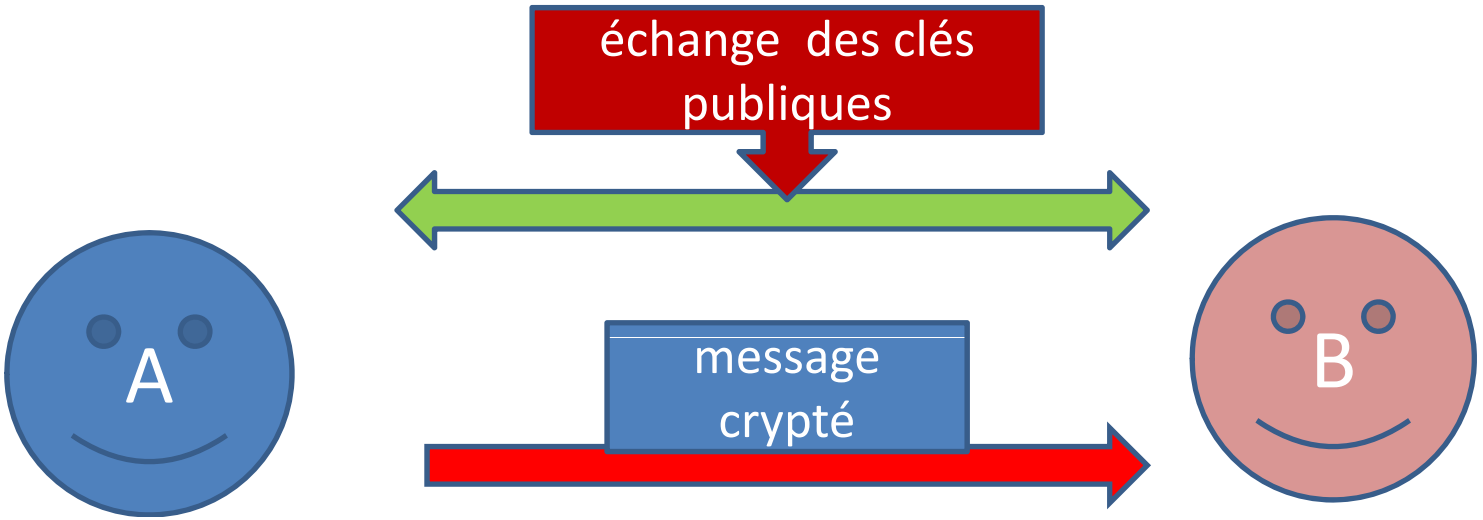
B décrypte en formant $\mathbf{g}_B$ ($\mathbf{f}_B$ (M))=M

Cryptage avec authentification :

M'=$\mathbf{g}_A$ ($\mathbf{f}_B$ (M)) : **A** ⟹ **B**

B décrypte en formant : $\mathbf{g}_B$ ($\mathbf{f}_A$ (M'))=M

Cryptage asymétrique
(avec authentification)



NOMBRES PREMIERS

$\mathbf{N}$ = {0,1,2,3,….}

$\mathbf{Z}$ = {… -3,-2,-1,0,1,2,…}

$\mathbf{P}$ = {2,3,5,7,11,13,17,…,$2^{43112609}$ -1,…}

Nombres de Mersenne : $\mathbf{M_n = 2^n - 1}$

Nombres de Fermat : $\mathbf{F_k = 2^{f(k)} + 1}$ avec $\mathbf{f(k)=2^k}$

THEOREME FONDAMENTAL DE L'ARITHMETIQUE

Tout entier se décompose de façon unique (à l'ordre près des facteurs) en un produit de nombres premiers

Arithmétique dans $\mathbb{Z}$

Arithmétique modulaire

Soit n dans $\mathbf{N}$, n ≥ 2, on dira que $a \equiv b \pmod{n}$ si n divise a-b

$$\mathbf{Z_n} = \{0,1,2,\ldots,n-1\}$$

Théorème : si p est premier alors $\mathbf{Z_p}$ est un **corps**

a et b sont **premiers entre eux** si PGCD (a,b) = 1

Indicatrice d'Euler : $\varphi(n)=Card\{1\leq k\leq n\}$, $PGCD(k,n)=1\}$

Si p est premier $\varphi(p)=p-1$

Si n=pq, p et q premiers distincts, $\varphi(n)=(p-1)(q-1)$

Théorème d'Euler : soit $n \geq 2$, PGCD(a,n)=1 alors

$$a^{\phi(n)} \equiv 1 \pmod{n}$$

<u>variante</u> : si n=pq avec p et q premiers distincts et k entier :

$$a^{1+k\phi(n)} \equiv a \pmod{n}$$

cette variante est à la base du système RSA

Système RSA
(Rivest, Shamir, Adleman)

1- M : A $\longrightarrow$ B	M := x+y=9
2- choix par B de p et q premiers	p=7 q=13
n=pq $\phi(n)$=n'=(p-1)(q-1)	n=91 n'=72
PGCD(e,n')=1 ed ≡ 1 (mod n')	e=5 d=29
(n,e) : B $\longrightarrow$ A	(91,5)
3- **(n,e) clé publique de B**	
(n,d) clé privée de B	
4- M' codage (ASCII) de M	M' = 120043121061057
5- écriture de M' en base n	02 29 35 62 61 01 65 12
soit m<n	m=12
6- **cryptage** : $m^e \equiv m' \pmod n$	$12^5 \equiv 38 \pmod{91}$
7- m' : A $\longrightarrow$ B	
8- **décryptage** : $m'^d \equiv m \pmod n$	$38^{29} \equiv 12 \pmod{91}$

Implémentation et sécurité

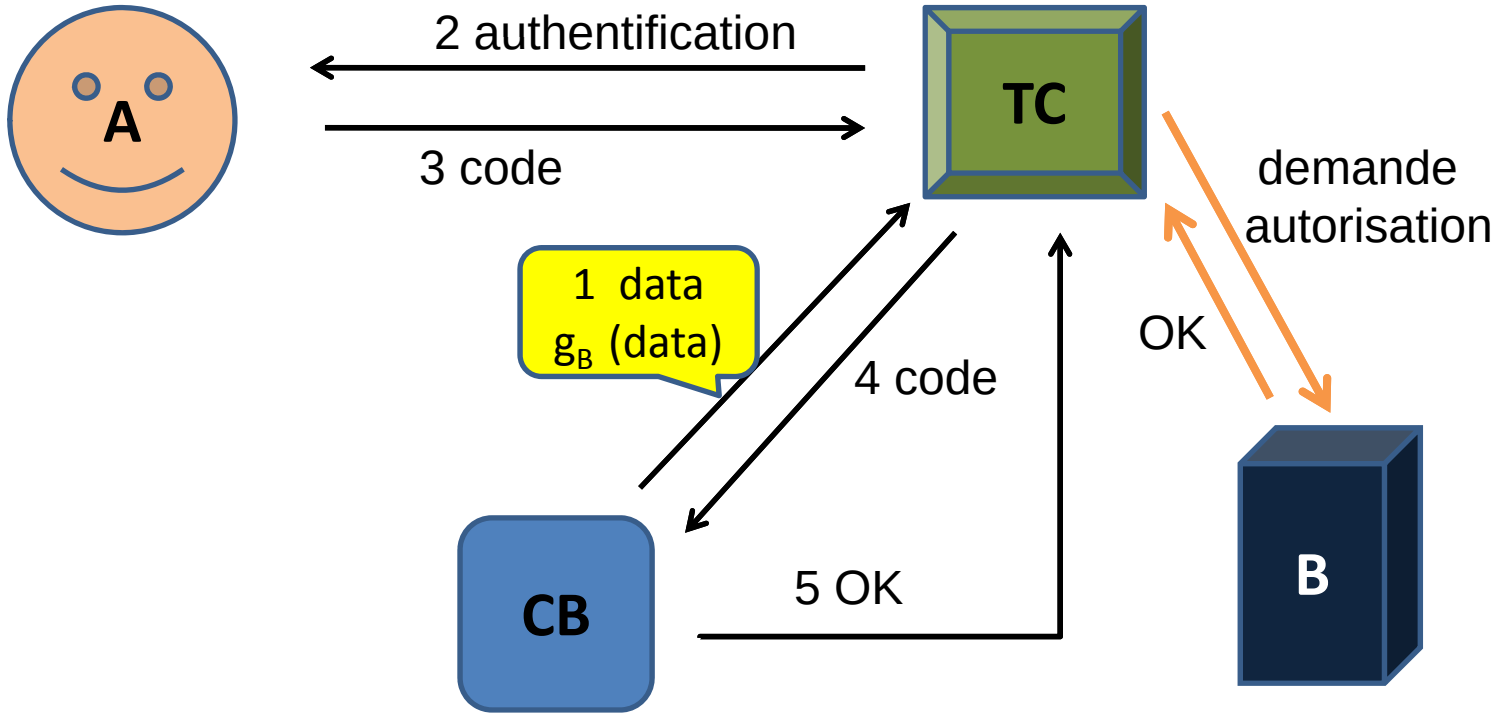
- choix de n : 1024 bits minimum (n est un nombre de plus de 300 chiffres en base décimale)

  à l'avenir 2048 bits sont fortement conseillés
- les nombres premiers p et q supérieurs à 150 chiffres
- difficulté de factoriser les grands nombres
- protocole SSL (Secure Socket Layer)
- protection des cartes bancaires

paiement par carte bancaire

(f_B ,g_B) clés publique et privée de la banque **B**

TC : terminal du commerçant



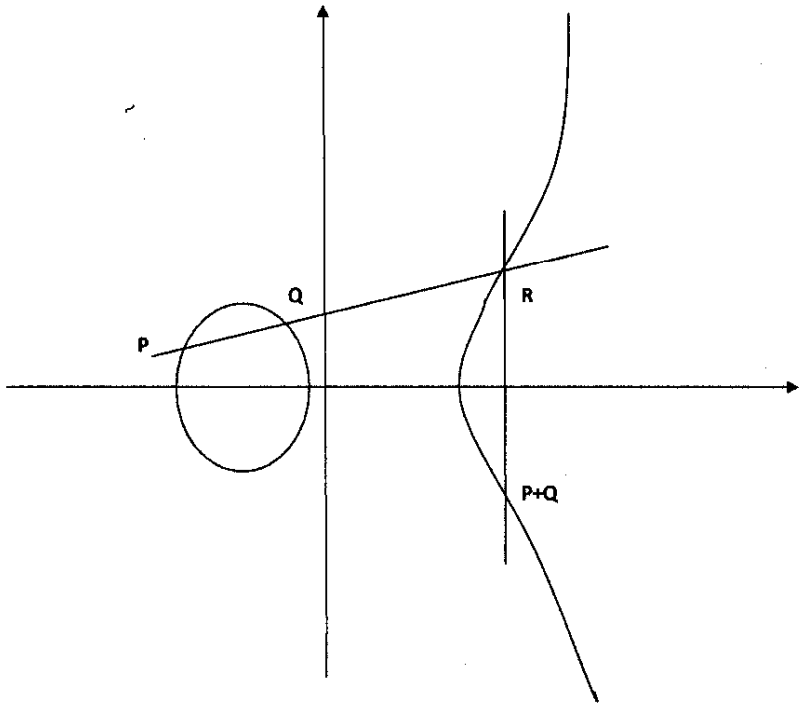
Cryptage par courbe elliptique

$E(a,b) : y^2 = x^3 + ax + b$

a et b paramètres réels $(4a^3 + 27\,b^2 \neq 0)$

addition des points sur E(a,b)

structure de **groupe commutatif**



Si $(P+Q)(x,y) = P(x_1,y_1) + Q(x_2,y_2)$, pour $x_1 \neq x_2$

$$z = (y_2 - y_1)/(x_2 - x_1)$$

$$x = z^2 - (x_1 + x_2)$$

$$y = z(x_1 - x) - y_1$$

$$-P(x,y) = P(x,-y)$$

(formule similaire dans le cas $x_1 = x_2$)

Pour k entier soit $P_k = kP$

E(a,b,p) : courbe définie sur $\mathbf{Z_p}$ (p premier)

Transfert d'un alphabet en une suite de points sur E(a,b,p)

Transmission de message
(avec clé publique)

1- E(a,b,p) et P (point de base) choisis par **A** et **B**

le message M est une suite de points sur E(a,b,p)

2- **B** choisit k entier (secret) et forme $P_k = kP$

(P,P_k) **clé publique**

(P,k) **clé privée**

3- P_k : **B** ⟶ **A**

4- **cryptage** : si S est un point de E(a,b,p)

A choisit h entier et envoie à **B** le couple (P_h , $S+hP_k$)

5- **décryptage** : **B** forme kP_h puis $S+hP_k–kP_h = S$

nécessité de connaitre k pour décrypter

Logarithme discret

Calculer k dans une relation de la forme

Q = kP

où P et Q sont deux points de la courbe

la difficulté de déterminer k assure la fiabilité de la méthode

NOMBRES PREMIERS

et

CRYPTOGRAPHIE