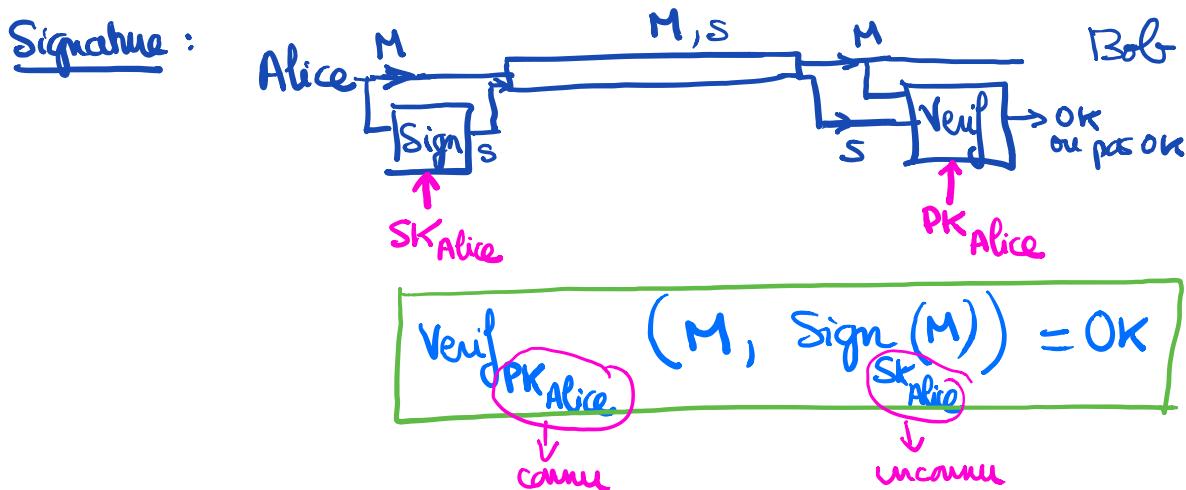
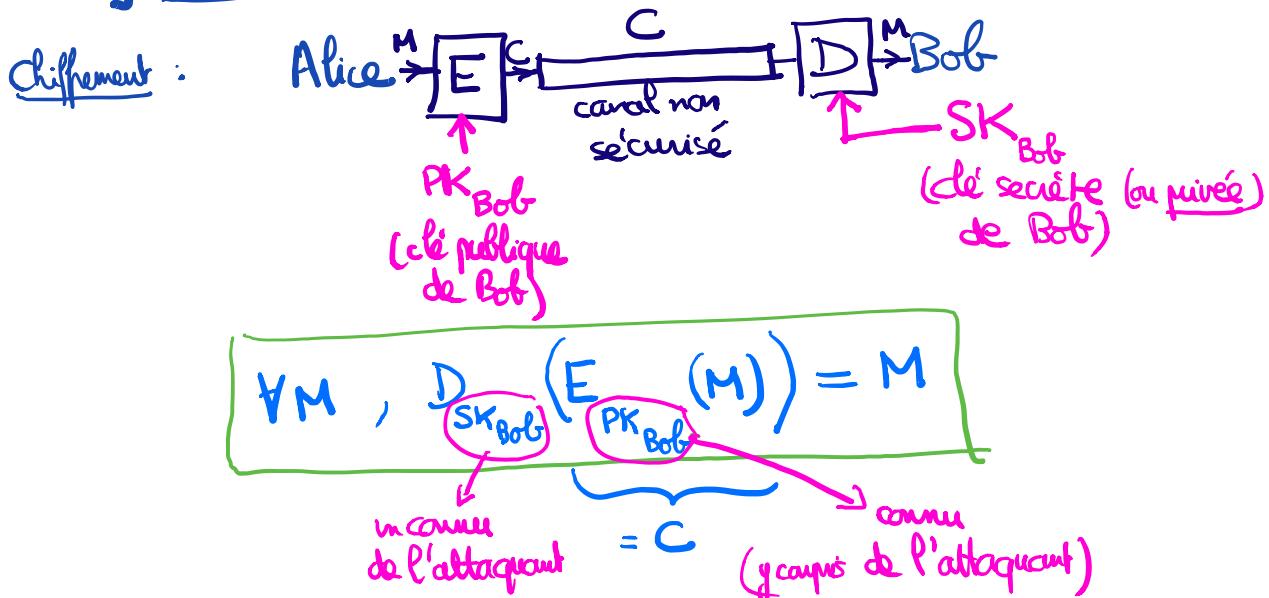


ch 4: L'algorithme RSA

I] Contexte asymétrique



of W. Diffie, M. Hellman: New Directions in Cryptography (1976)

1977: résolution par Merkle ("puzzles de Merkle")

1977: R. Rivest, A. Shamir, L. Adleman ont proposé l'algorithme RSA

II] Description de l'algorithme RSA

① Clés

SK Clé secrète : comporte deux nombres premiers p et q

PK Clé publique : $n = p \times q$

relation explicite entre PK et SK

Question : Etant donné n , peut-on retrouver p et q ?

$$\text{ex: } n=15 \rightarrow \{p, q\} = \{3, 5\}$$

$$n=91 \rightarrow \{p, q\} = \{7, 13\}$$

\Rightarrow Pb de la factorisation : existe-t-il un algorithme efficace pour trouver p et q à partir de n ($= p \times q$)?

- Idée "naïve" : essayer de diviser n par tous les entiers successifs (de 2 à $n-1$) \rightarrow complexité $O(n)$
 - il suffit de prendre $n \geq 2^{80}$ pour avoir une sécurité en 2^{80}
- Idée supplémentaire : il suffit d'essayer les diviseurs jusqu'à \sqrt{n} (de 2 à \sqrt{n})

En effet si $n = p \times q$ avec $p < q$,

$$\text{alors } p^2 < p \times q = n \Rightarrow p < \sqrt{n}$$

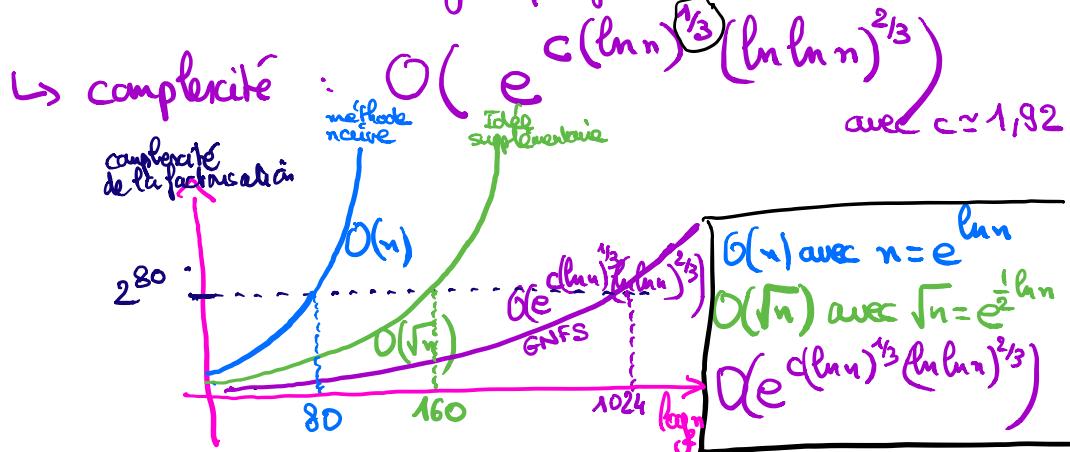
\Rightarrow complexité $O(\sqrt{n})$

↳ il suffit de prendre $n \geq 2^{160}$ (\Leftrightarrow n fait au moins 160 bits)

pour avoir une sécurité en 2^{80}

- Meilleur algorithme connu pour factoriser :

GNFS (General Number Field Sieve) (1990)
(Crible algébrique général)



② Fonction RSA

$$f: \begin{cases} \mathbb{Z}/n\mathbb{Z} & \longrightarrow \mathbb{Z}/n\mathbb{Z} \\ x & \longmapsto x^e \text{ mod } n \end{cases}$$

Exemple : $e=3$, $f(x) = x^3 \text{ mod } n$

Théorème : Soient p, q deux entiers premiers, $p \neq q$

Soit $n = p \times q$

Soit e un entier tel que $\text{pgcd}(\overbrace{e}^{\text{impair}}, \overbrace{p-1}^{\text{pair}}) = 1$
et $\text{pgcd}(\overbrace{e}^{\text{impair}}, \overbrace{q-1}^{\text{pair}}) = 1$

Alors $f: \begin{cases} \mathbb{Z}/n\mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z} \\ x \mapsto x^e \text{ mod } n \end{cases}$

est une bijection

De plus la bijection réciproque est donnée par

$$f^{-1} : \begin{cases} \mathbb{Z}/n\mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z} \\ y \longmapsto y^d \bmod n \end{cases}$$

où d est l'inverse de e modulo $\underbrace{(p-1)(q-1)}_{\text{noté } \varphi(n)}$

[indicatrice d'Euler de n]

Remarque: $\text{pgcd}(e, \underbrace{(p-1)(q-1)}_{=\varphi(n)}) = 1$

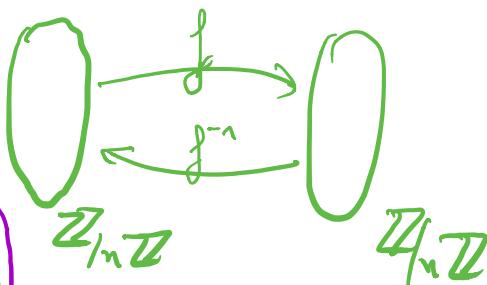
donc e possède bien un inverse modulo $\varphi(n)$
(on utilise le th. de Bezout)

Démonstration du théorème:

Il suffit de démontrer que

$$\boxed{\forall x \in \mathbb{Z}/n\mathbb{Z}, \quad (x^e)^d = x \bmod n}$$

$$f^{-1}(f(x)) = x$$



Montrons tout d'abord que $(x^e)^d = x \bmod p$

d est l'inverse de e mod $\varphi(n)$

$$\Leftrightarrow e \times d = 1 \bmod \varphi(n)$$

$$\Leftrightarrow \exists \lambda \in \mathbb{Z} / e \times d = 1 + \lambda \varphi(n)$$

$$\text{Donc } (x^e)^d = x^{ed} = x^{1 + \lambda \varphi(n)} = x \times (x^{\varphi(n)})^\lambda$$

$$\Rightarrow (x^e)^d = x \times (x^{p-1})^{\lambda(q-1)}$$

On sait que, si $x \neq 0 \pmod{p}$,

$$x^{p-1} = 1 \pmod{p}$$

petit théorème de Fermat

Dès lors si $x \neq 0 \pmod{p}$, $(x^e)^d = x \times (x^{p-1})^{d(p-1)} = x \pmod{p}$

$$\Rightarrow (x^e)^d = x \times 1 = x \pmod{p}$$

et donc, dans tous les cas : $(x^e)^d = x \pmod{p}$

(si $x = 0 \pmod{p}$, c'est vrai aussi, car $0=0$)

De même, $(x^e)^d = x \pmod{q}$

On a $\begin{cases} (x^e)^d = x \pmod{p} \Leftrightarrow [(x^e)^d - x] \text{ divisible par } p \\ (x^e)^d = x \pmod{q} \Leftrightarrow [(x^e)^d - x] \text{ divisible par } q \end{cases}$

$\Rightarrow (x^e)^d - x$ divisible par $p \times q = n$

$$\Rightarrow (x^e)^d = x \pmod{n}$$

Remarque : Une preuve du petit théorème de Fermat

Th : $\begin{cases} p \text{ premier} \\ \text{Si } x \neq 0 \pmod{p}, \text{ alors } x^{p-1} = 1 \pmod{p} \end{cases}$

Preuve : Considérons la fonction $g : \mathbb{Z}/p\mathbb{Z} \rightarrow \mathbb{Z}/p\mathbb{Z}$

$$\begin{cases} u \mapsto x \cdot u \pmod{p} \end{cases}$$

Montrons que g est une bijection

Il suffit de montrer que g est injective

Supposons que $g(u) = g(u')$, montrons qu'alors $u = u'$

$$g(u) = g(u') \Leftrightarrow [x \cdot u = x \cdot u' \text{ mod } p]$$

$$\text{Or } x \neq 0 \text{ mod } p \Rightarrow \text{pgcd}(x, p) = 1$$

car p ne divise pas x

$$\xrightarrow{\text{Th. Bézout}} \exists \alpha, \beta \in \mathbb{Z} \text{ tels que } \underline{\alpha x + \beta p = 1}$$

$\Rightarrow \alpha$ est l'inverse de x mod p

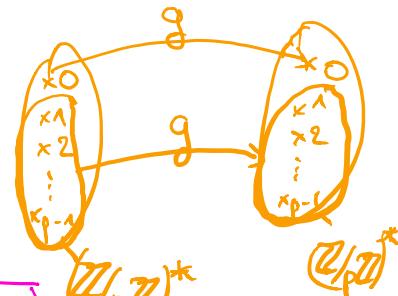
$$(\alpha \cdot x = 1 \text{ mod } p)$$

$$\alpha \cdot (x \cdot u) = \alpha \cdot (x \cdot u') \text{ mod } p$$

$$(\underbrace{\alpha \cdot x}_{=1 \text{ mod } p}) \cdot u = (\underbrace{\alpha \cdot x}_{=1 \text{ mod } p}) \cdot u' \text{ mod } p$$

$$\Rightarrow u = u' \text{ mod } p$$

$\Rightarrow g$ est une bijection de $(\mathbb{Z}/p\mathbb{Z})^*$ sur $(\mathbb{Z}/p\mathbb{Z})^*$



Donc

$$1 \times 2 \times 3 \times \dots \times (p-1) = g(1) \times g(2) \times \dots \times g(p-1)$$

produit de tous les éléments de $(\mathbb{Z}/p\mathbb{Z})^*$

$$1 \times 2 \times \dots \times (p-1) = (x \cdot 1) \times (x \cdot 2) \times \dots \times (x \cdot (p-1)) \text{ mod } p$$

$$\cancel{1 \times 2 \times \dots \times (p-1)} = x^{p-1} \times \cancel{(1 \times 2 \times 3 \times \dots \times (p-1))} \text{ mod } p$$

$$\text{pgcd}(2, p) = 1 \text{ (car } p \text{ est premier)}$$

$$\xrightarrow{\text{Th. Bézout}} \exists \alpha_2, \beta_2 / \alpha_2 \times 2 + \beta_2 \times p = 1$$

inverse de 2 mod p

De même $\text{pgcd}(3, p) = 1$, donc 3 a un inverse mod p

$\text{pgcd}(p-1, p) = 1$, donc $(p-1)$ a un inverse mod p

On obtient donc $x^{p-1} \equiv 1 \pmod{p}$

③ Sécurité de RSA

"En gros", pour chiffrer un message M, écrit sous la forme d'un entier $x \in \mathbb{Z}/n\mathbb{Z}$

on calculera $y = f(x) = \underline{\underline{x^e \bmod n}}$
le message chiffré

Scénario 1 : L'attaquant cherche à retrouver la clé secrète

$$\begin{cases} \text{PK} = (n, e) \\ \text{SK} = (p, q, d) \end{cases} \quad (d = e^{-1} \bmod \frac{\varphi(n)}{(p-1)(q-1)})$$

L'attaquant doit être capable de factoriser n

↳ meilleure méthode connue : GNFS

complexité: $O(e^{C(\ln n)^{1/3}(\ln \ln n)^{2/3}})$

qui sera $\geq 2^{80}$ si n fait au moins 1024 bits

Scénario 2 : L'attaquant veut simplement déchiffrer un ou plusieurs messages

c'est à dire : à partir de y , trouver x tel que $x^e \equiv y \pmod{n}$

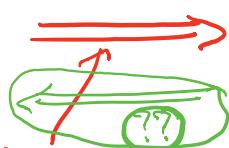
("inverser la fonction f ")

Pb du calcul de racine e -ième modulo n

Etant donné $y \in \mathbb{Z}/n\mathbb{Z}$ et e premier avec $p-1$ & $q-1$
peut on trouver $x \in \mathbb{Z}/n\mathbb{Z}$ tel que $\boxed{x^e = y \text{ mod } n}$

x
inconnue

Savoir trouver
la factorisation



Savoir trouver
des racines e -ième mod n

il suffit de
retrouver $d = e^{-1} \text{ mod } (p-1)(q-1)$