

Ronald Rivest, Adi Shamir et Leonard Adleman



Fig.: Ronald Rivest, Adi Shamir et Leonard Adleman, dans *A Method for Obtaining Digital Signatures and Public-key Cryptosystems* ont eu l'idée d'utiliser les anneaux $\mathbb{Z}/n\mathbb{Z}$ et le petit théorème de Fermat pour obtenir des fonctions trappes, ou fonctions à sens unique à brèche secrète.

R.S.A.

Alice veut envoyer M à Bob.

- ▶ M un entier représentant un message.
- ▶ Bob choisit p et q deux nombres premiers et on note n leur produit.
- ▶ Bob choisit e un entier premier avec $p - 1$ et $q - 1$.
- ▶ On a $\varphi(n) = (p - 1)(q - 1)$ donc e est premier avec $\varphi(n)$ et on obtient (via Bézout) qu'il est inversible modulo $\varphi(n)$, i.e. il existe un entier d tel que $ed \equiv 1 \pmod{\varphi(n)}$.
- ▶ Le message chiffré sera alors représenté par :

$$C = M^e \pmod{n}$$

- ▶ Pour déchiffrer C , on calcule d l'inverse de $e \pmod{\varphi(n)}$, ensuite on calcule $C^d \pmod{n}$.

R.S.A.

- ▶ On a alors,

$$C^d \pmod{n} \equiv (M^e)^d \pmod{n} \equiv M^{ed} \pmod{n}$$

- ▶ Comme $ed \equiv 1 \pmod{\varphi(n)}$ par définition de modulo, on a

$$ed = 1 + k\varphi(n), \text{ avec } k \in \mathbb{N}.$$

- ▶ D'où,

$$M^{ed} \pmod{n} \equiv M \cdot M^{k\varphi(n)} \pmod{n} \equiv M \cdot (M^{\varphi(n)})^k \pmod{n}$$

- ▶ Or si x est premier avec n ; on a $x^{\varphi(n)} \equiv 1 \pmod{n}$, d'après le théorème d'Euler.
- ▶ Donc finalement, si le message M est premier avec n :

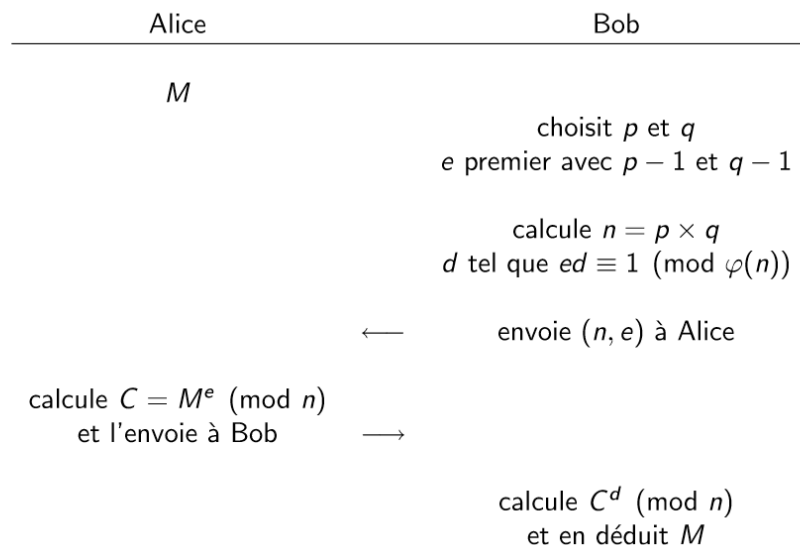
$$C^d \equiv M \pmod{n}.$$

R.S.A.

- ▶ Le cas où le message M n'est pas premier avec n est un peu plus compliqué mais le résultat reste le même :

$$C^d \equiv M \pmod{n}.$$

- ▶ (n, e) est appelé clef publique
- ▶ (n, d) est appelé clef privée.
- ▶ pour chiffrer, il suffit de connaître e et n .
- ▶ pour déchiffrer, il faut d et n , autrement dit connaître la décomposition de n en facteurs premiers.



Le cryptosystème RSA : Exemple

Prenons $p = 47$ et $q = 59$.

- ▶ On calcule $n = p.q = 47.59 = 2773$
- ▶ On choisit e , premier par rapport à $\phi(n)$. Ex : $e = 17$.
- ▶ On calcule alors, par l'algorithme d'Euclide étendu¹, d tel que $d.e = 1 \mod (p-1)(q-1)$, soit $d = 157$.

Clef publique : $(e, n) = (17, 2773)$

Clef privé : $d = 157$.

- ▶ Chiffrement du message $M = 01000010 = 66$:

$$C = M^e \mod n = 66^{17} \mod 2773 = 872$$

- ▶ Déchiffrement de C :

$$C^d \mod n = 872^{157} \mod 2773 = 66$$