

RSA

Rivest / Shamir / Adleman (1977)

1. Chiffrement RSA : E et D
2. Validité de RSA
 1. $E(D(x)) = D(E(x)) = x$
 2. E est facile à calculer
 3. E est difficile à inverser sans connaître D
3. Signature RSA
 1. Directe
 2. Avec résumé du message

Chiffrement RSA

Alice

Veut envoyer M secret à Bob

Eve

Bob

1/ Construction clefs Bob

- p, q premiers grands
- $n = p \times q$
- $\varphi(n) = (p-1)(q-1)$
- e petit, premier avec $\varphi(n)$
- $d = e^{-1} \pmod{\varphi(n)}$

• Clé privée: (d, n)

• Clé publique: (e, n)

• $\forall x \in \{0, \dots, n-1\}$:

$D^{Bob}(x) = x^d \pmod{n}$

$E^{Bob}(x) = x^e \pmod{n}$

$E^{Bob}(x)$

Chiffrement RSA

Alice

Veut envoyer M secret à Bob

2. $M = M_1 M_2 \dots M_m$ tel que $M_i \in \{0, \dots, n-1\}$ ($\log_2 n$ bits)

3. Calcule $S_i = E^{Bob}(M_i)$

4. Envoie $S_1 \dots S_i \dots S_m$

Eve

Bob

1/ Construction clefs Bob

- $\forall x \in \{0, \dots, n-1\}$:
- privé: $D^{Bob}(x) = x^d \pmod{n}$
- public: $E^{Bob}(x) = x^e \pmod{n}$

5. Calcule $M_i = D^{Bob}(S_i)$

$M = M_1 M_2 \dots M_m$

$E^{Bob}(x)$

Validité de RSA

- D^{Bob} est la réciproque de E^{Bob} :
 - $\forall x \in \{0, \dots, n-1\}$: $D^{Bob}(E^{Bob}(x)) = E^{Bob}(D^{Bob}(x)) = x$
- E^{Bob} est une fonction à sens unique *chausse-trappe*:
 - $E^{Bob}(x)$ est peu coûteuse à calculer
 - $D^{Bob}(x)$ est peu coûteuse à calculer
 - Calculer d à partir de (n et e) est calculatoirement aussi difficile que factoriser n
- Générer une clef RSA [(n,d), (n,e)] est peu coûteux

Applications

Chiffrement à clef publique / RSA

- Authentification
- Signature

Signature RSA

Alice

Reçoit un message M signé par Bob et vérifie l'authenticité de la signature

3. Reçoit M, S

4. Calcule: $T = E(S)$

5. Vérifie la signature de Bob en testant $T = M$?

Eve

Bob

- veut envoyer M signé à Alice

1. Calcule $S = D^{Bob}(M)$
2. Envoie (M, S) à Alice

$E^{Bob}(x)$

Signature RSA du résumé

Alice

Reçoit un message M signé par Bob et vérifie l'authenticité de la signature

3. Reçoit M, S

4. Calcule: $T = E(S)$

5. Vérifie la signature de Bob: $T = h(M)$?

Eve

Bob

veut envoyer M signé à Alice ne signe que le résumé $h(M)$ où h est une fonction à sens unique. Ex: $h = \text{SHA1, MD5, ...}$

1. Calcule $S = D^{Bob}(h(M))$
2. Envoie (M, S) à Alice

$E^{Bob}(x)$