Introduction à RSA

Description des variables pour l'utilisation de l'encryption
e : Première partie de la clef publique
d : Première partie de la clef privée
n : Deuxième partie des clefs privées et publiques
m : Message à envoyer
c : Message encrypté en utilisant la clef publique

Description des variables nécessaires à la création des clefs

p, q : Grand entier premier
$\Phi(n)$: Totient, $\Phi(n) = (p-1) * (q-1)$
n : Base du modulo, $p * q = n$

Génération des clefs

1. Choisir deux grands nombre premiers p et q
2. Calculer $n = p * q$
3. $\Phi(n) = (p-1) * (q-1)$
4. Choisir e tel que $pgcd(e, \Phi(n)) \equiv 1$ et $1 < e < \Phi(n)$
5. Calcuer d tel que $e * d \equiv 1 \pmod{\Phi(n)} \Rightarrow (e * d) \bmod phi(n) = 1$

Clef privée : (d, n)
Clef publique : (e, n)

Utilisation

Encryption d'un message m :
$c = m^{e_b} \bmod n_b$

Décryption d'un message c :
$m = c^{d_b} \bmod n_b$

Signature du message m :
$sig = m^{d_a} \bmod n_a$

Vérification de la signature du message m :
$estValide = (m == sig^{e_a} \bmod n_a)$