n = p * q, avec p et q premiers

e premier avec Φ(n) = (p - 1) * (q - 1)

d : e * d $\equiv$ 1 (mod Φ(n))

Alice et Bob, clé publique : n, e, secrète : d

Signature de M, m = H(M)

c = m^d (mod n)

à Bob, M, c

Bob:

1. Recalcule m = H(M)
2. c^e = m (mod n)

p et q grands : environ $2^{500}2^{3000}$

p - q : grand.

p - 1: grand facteur premier : r

r - 1: grand facteur premier

q - 1: grand facteur premier

Difficultés du RSA

1. Maurice connait n et e. => factoriser n = pq
2. Maurice : n, e, c => c = m^d, retrouver d ??, problème du logarithme discret
3. Extraire une racine e-iéme

Situation à éviter

- Connaissance de n et Φ(n). La connaissance de n et Φ(n) permet de retrouver p et q

? n = p * q, Φ(n) = (p - 1) * (q - 1) = pq - p - q + 1 = n - p - q + 1

pq = n, p+q = n + 1 - Φ(n)

La connaissance de n, e et d permet de retrouver p et q.

n = p * q

ed = kΦ(n) + 1

(ed - 1) = kΦ(n)

Φ(n) = (ed - 1) / k

Tests de primalité

Un nombre au hasard : n, est-il premier ?

Tester:

1. Essayer les facteurs $\leq \sqrt{n}$

Test de Fermat

n fixé (en entrée), on prend a 1. si a^{n-1} !$\equiv$ 1 (mod n), alors n non premier 3. Si a^{n-1} $\equiv$ 1 (mod n), a un témoin de Fermat pour n

Test de Miller Rabin

n, n -1 = 2^s * d

a : donné

On va tester a^d; a^{2d}; a^{4d}; $\ldots$; $a^{2^s d}$

Si $\exists$ a, a^d $\equiv$ 1 (mod n) et ($\forall$r $\leq$ s) $a^{2^r d}$ $\equiv$ -1 (mod n)

n composé, sinon a témoin de Miller Rabin

Pour n composé, (3/4) * n des a permet de rejeter n

Exemple

p = 1039, pas de diviseur $\leq$ 32, p premier

Z/pZ,+,* un corps

u^{-1} $\equiv$ 2 (mod 1039)

2u $\equiv$ 1 (mod 1039)

2u = 1039k + 1

$2u - 1039k = 1$

Théorème Bézout:

Algorithe Euclide Etendu

$k = 1$ (solution évidente)

$2u = 1040$, $u = 520$