

Cryptosystème RSA



Rivest

Shamir

Adleman

Primalité

Définition

Un nombre p est premier si ses seuls diviseurs positifs sont p et 1.

Liste : 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, ...

Primalité

Définition

Un nombre p est premier si ses seuls diviseurs positifs sont p et 1.

Liste : 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, ...

Propriétés

- Entre n et $2n$, il y a toujours un nombre premier.
- Un nombre pair est toujours la somme de 2 premiers.
- Un nombre impair (>5) est la somme de 3 premiers.

Théorème d'Euclide

Il existe une infinité de nombres premiers.

Décomposition en facteurs premiers

Théorème fondamental de l'arithmétique

Tout entier n s'écrit de façon unique comme produit de puissances de nombres premiers :

$$n = \prod_{i=1}^k p_i^{\alpha_i}$$

PGCD

Si $a = \prod_i p_i^{\alpha_i}$ et $b = \prod_i p_i^{\beta_i}$, alors :

$$\text{pgcd}(a, b) = \prod_i p_i^{\min(\alpha_i, \beta_i)}$$

Distribution des nombres premiers



Question

Il existe une infinité de nombres premiers.
(Euclide)

Comment sont-ils répartis ? ? ?

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Fonction d'Euler

Définition

$\varphi(n)$ est le nombre d'entiers de $[1, n]$ qui sont premiers avec n .

Fonction d'Euler

Définition

$\varphi(n)$ est le nombre d'entiers de $[1, n]$ qui sont premiers avec n .

Propriétés

si p est premier et q premier :

- $\varphi(p) = p - 1$
- $\varphi(p^e) = p^{e-1}(p - 1) = p^e - p^{e-1}$
- $\varphi(pq) = \varphi(p)\varphi(q)$ si $\text{pgcd}(p, q) = 1$

Fonction d'Euler

Calcul de $\varphi(n)$

Formule générale pour $n = \prod_i^k p_i^{\alpha_i}$:

$$\varphi(n) = \prod_{i=1}^k (p_i^{\alpha_i} - p_i^{\alpha_i-1}) = \prod_{i=1}^k p_i^{\alpha_i-1} (p_i - 1)$$

n	$\varphi(n)$
1	1
2	1
3	2
4	2
5	4
6	2
7	6

Théorème des restes chinois

Problème

Pour p et q premiers et a et b entiers on cherche x tel que :

$$x = a \mod p \quad \text{et} \quad x = b \mod q$$

Théorème des restes chinois

Problème

Pour p et q premiers et a et b entiers on cherche x tel que :

$$x = a \mod p \quad \text{et} \quad x = b \mod q$$

Théorème CRT (Chinese Remainder Theorem)

La solution x est unique modulo pq et se calcule par l'algorithme de Gauss :

$$x = aq(q^{-1} \mod p) + bp(p^{-1} \mod q) \mod pq$$

Resoudre

$$x = 9 \mod 17 \quad \text{et} \quad x = 3 \mod 5$$

Fonctions à sens unique

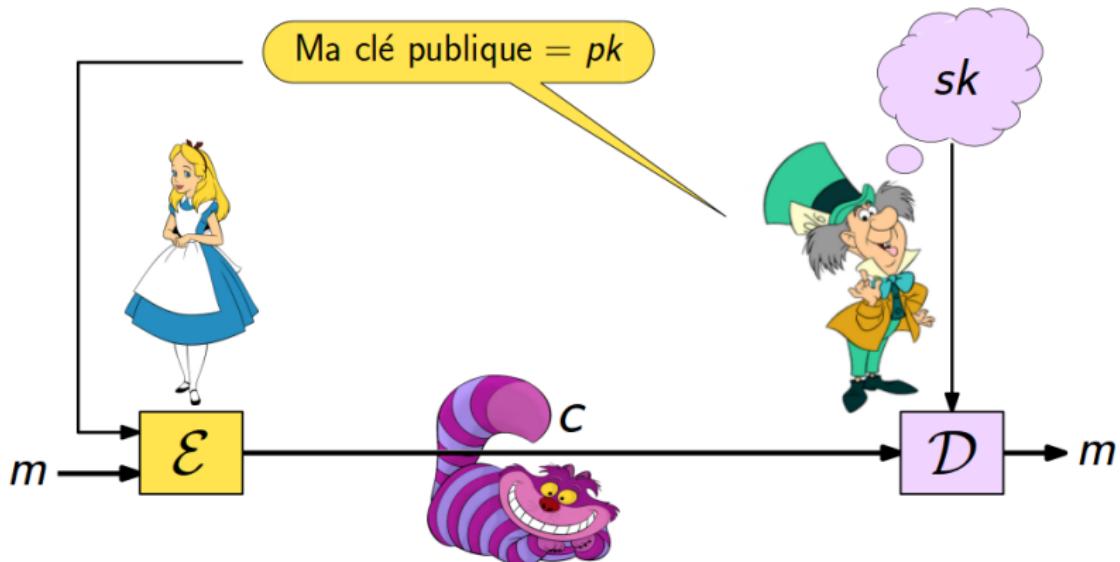
multiplication \leftrightarrow factorisation

$(p, q) \rightarrow p \cdot q$ facile $\leftrightarrow n = p \cdot q \rightarrow (p, q)$ difficile

Meilleur algorithme connu (crible algébrique) :

$$\mathcal{O}\left(e^{1.92(\ln n)^{1/3}(\ln \ln n)^{2/3}}\right)$$

Chiffrement à clé publique



Chiffrement à clé publique

Protocole

- **Algorithme de génération des clés** $\mathcal{KG}(\ell) = (\text{pk}, \text{sk})$
à partir d'un paramètre de sécurité, il produit une paire de clés
- **Algorithme de chiffrement** $\mathcal{E}(\text{pk}, m) = c$
produit le chiffré d'un message m , par la clé publique
- **Algorithme de déchiffrement** $\mathcal{D}(\text{sk}, c) = m$
utilise la clé secrète/privée sk pour retrouver m à partir de c

Protocole RSA

RSA - Génération des clés

$$\mathcal{KG}(\ell) = (\text{pk}, \text{sk})$$

- Soit $n = p \cdot q$ (p et q premiers)
- $\varphi(n) = (p - 1)(q - 1)$
- Soit e un entier premier avec $\varphi(n)$
- Soit d un entier qui satisfait $d \cdot e = 1 \pmod{\varphi(n)}$

Protocole RSA

RSA - Génération des clés

$$\mathcal{KG}(\ell) = (\text{pk}, \text{sk})$$

- Soit $n = p \cdot q$ (p et q premiers)
- $\varphi(n) = (p - 1)(q - 1)$
- Soit e un entier premier avec $\varphi(n)$
- Soit d un entier qui satisfait $d \cdot e = 1 \pmod{\varphi(n)}$

clé publique

- $n = pq$: module public
- e : exposant public

clé secrète

- $d = e^{-1} \pmod{\varphi(n)}$
- les premiers p et q

RSA - Exemple simplifié

Deux petits premiers : $p = 5$ et $q = 7$

RSA - Exemple simplifié

Deux petits premiers : $p = 5$ et $q = 7$

- $n = 5 \cdot 7 = 35$, $\varphi(n) = (5 - 1) \cdot (7 - 1) = 24$
- e et d : $ed = 1 \pmod{24}$
 - $ed = 1$: Non, trop petit
 - $ed = 25$: Ok, mais $e = d = 5$ et alors clé privée = clé publique
 - $ed = 49$: Pareil, $e = d$
 - $ed = 73$: 73 est premier, raté
 - $ed = 97$: 97 est premier, raté
 - $ed = 121$: 11 au carré, encore raté
 - $ed = 165$: $165 = 5 * 33$, et 5 est premier : Ok
- Clé publique = (n, 5) • Clé privée = (33, p, q).

RSA-Chiffrement-Dechiffrement

Configuration

- ➊ On choisit deux entiers premiers assez grands **p** et **q**, calculer $n = pq$ et $\varphi(n) = (p - 1)(q - 1)$
- ➋ choisir **e** (clé de cryptage) tel que $\text{pgcd}(e, \varphi(n)) = 1$
- ➌ calculer **d** (clé de déchiffrement) tel que $e.d \equiv 1 \pmod{\varphi(n)}$
- ➍ rendre **n** et **e** publique, et garde **d,p,q** secrets

Chiffrement -Dechifrement

- ➊ récupérer **n** et **e** de destinataire
- ➋ chiffre un message **m** en calculant $c \equiv m^e \pmod{n}$
- ➌ à la reception on déchiffre en calculant $m \equiv c^d \pmod{n}$

RSA-Chiffrement-Dechiffrement

ALICE

$p = 3$ et $q = 7$

$n = p \times q = 21$

$f = (p-1)(q-1) = 2 \times 6 = 12$

e premier avec f donc $e = 5$

Je calcule d , inverse de e mod f

$5d = 1 \text{ mod } 12$

$5 \times 5 = 1 \text{ mod } 12$

$d = 5$

Public(e, n)

Privé(p, q, d, f)

etape 1

Je calcule z

$z = y^d \text{ mod } n$

$z = 11^5 \text{ mod } 21$

$z = 44 \text{ mod } 21$

$z = 2 \text{ mod } 21$

$z = x \text{ mod } n$

$z = 2 \text{ mod } 21$

Public(e, n)

etape 2

BOB

envoyé $x = 2$

Codage du message

$y = x^e \text{ mod } n$

$y = 2^5 \text{ mod } 21$

$y = 32 \text{ mod } 21$

$y = 11$

etape 3

Conseils d'utilisation du RSA



RSA - Précautions

Il y a de nombreuses manières de **mal utiliser** RSA et d'ouvrir des failles de sécurité !

- Ne jamais utiliser de valeur n trop petite
- Ne jamais utiliser d'exposant e trop petit
- N'utiliser que des clés fortes
($p - 1$ et $q - 1$ ont un grand facteur premier)
- Ne pas chiffrer de blocs trop courts
- Ne pas utiliser de n communs à plusieurs clés

Attaques RSA



RSA - Attaques mathématiques

- 💣 factoriser $n = pq$ et par conséquent trouver $\varphi(n)$ et puis d
- 💣 déterminer $\varphi(n)$ directement et trouver d
- 💣 trouver d directement (si petit)
- 💣 attaques "broadcast"
- 💣 attaques sur modulo n commun
- 💣