

Intervention de Mme Rossi

Chiffrement RSA

✦ Référence historique :

Le chiffrement RSA a été décrit en 1977 par Ronald Rivest, Adi Shamir et Leonard Adleman. C'est un algorithme de cryptographie asymétrique.

I Chiffrement

Bob souhaite envoyer un message secret à Alice.

Alice crée sa clé publique en choisissant deux nombres premiers p et q . Elle appelle n leur produit, donc $n = p \times q$.

Alice choisit un nombre e qui n'a pas de diviseur commun avec le produit $(p - 1) \times (q - 1) = \varphi$. La clé publique d'Alice est donc le couple $(n ; e)$. Alice n'a plus qu'à laisser en libre accès.

👁 Exemple :

✧ Choisissons $p = 3$ et $q = 11$, donc $n = \dots\dots\dots$, $\varphi = \dots\dots\dots$ et choisissons $e = \dots\dots\dots$

00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

👤 Méthode :

Pour chiffrer un message :

- remplacer chaque lettre par le nombre correspondant ;
- élever le nombre à la puissance e (ici $e = \dots\dots\dots$) ;
- calculer le reste de la division euclidienne par n (ici $n = \dots\dots\dots$).

Lettre	M	A	T	H	S
Nombre					
Résultat de la puissance					
Reste					

Donc « MATHS » devient $c = \dots\dots\dots$

II Déchiffrement

Pour déchiffrer le message Alice possède une clé qu'elle seule connaît d . La clé secrète d est l'inverse de e modulo φ ($(E): d \times e - \varphi \times k = 1$).

Ici on connaît $e = \dots\dots\dots$ et $\varphi = \dots\dots\dots$ Prenons $d = \dots\dots\dots$ et $k = \dots\dots\dots$

Vérifions l'égalité (E) , $\dots\dots\dots \times \dots\dots\dots - \dots\dots\dots \times \dots\dots\dots = \dots\dots\dots$

Méthode :

Pour déchiffrer un message :

- élever le nombre à la puissance d (ici $d = \dots\dots\dots$);
- calculer le reste de la division euclidienne par n (ici $n = \dots\dots\dots$);
- le reste trouvé correspond à une lettre.

Nombre	01	29	00	21	05
Résultat de la puissance					
Reste					
Lettre					

III Conclusion

Pour « attaquer », c'est à dire déchiffrer en connaissant seulement n et e , il faudrait connaître la valeur de d . La seule manière connue de retrouver d est de décomposer n en produit de facteurs premiers.

La sécurité du chiffrement RSA réside donc dans la complexité à écrire en produit de facteurs premiers le nombre n .

Exemples :

ζ $55 = \dots\dots\dots \times \dots\dots\dots$; $391 = \dots\dots\dots \times \dots\dots\dots$; $3763 = \dots\dots\dots \times \dots\dots\dots$

En réalité les nombres ont dans les 300 chiffres, c'est donc très difficile de les factoriser, même pour un très bon ordinateur aujourd'hui.

Voici un exemple avec 113 chiffres :

$n = 93\ 106\ 888\ 845\ 493\ 018\ 793\ 075\ 612\ 605\ 237\ 434\ 172\ 899\ 346\ 251\ 026\ 077\ 768\ 956\ 358\ 420\ 215\ 936\ 469\ 010\ 538\ 484\ 475\ 601\ 243\ 033\ 175\ 190\ 837\ 780\ 374\ 243$.

Ici $p = 752\ 364\ 524\ 132\ 679\ 877\ 650\ 987\ 654\ 678\ 546\ 534\ 322\ 145\ 658\ 675\ 654\ 435\ 731$ et
 $q = 123\ 752\ 364\ 524\ 132\ 679\ 877\ 650\ 987\ 654\ 623\ 423\ 421\ 343\ 152\ 267\ 887\ 965\ 553$.