Le RSA


Math sans jeans ?
NON
Le RSA devoilé
Mise a nue dimanche matin par
les eleves du lycée Camille Sée

Introduction

Principe du codage dit « symétrique »

Ici la méthode de codage est secrète et permet aussi bien de coder que de décoder.

Introduction

Ex:

ceci n’est pas un message code

dfdj o’ftu qbt nfttbhf dpef

Introduction

Avantage :

- Très rapide

Inconvénient :

- « Facilement » cassable
- Méthode doit être tenue secrète

Introduction

Comment résoudre se problème ?

Introduction

Système de codage dit « asymétrique »

- Méthode connue

- Il existe 2 clefs 1 publique et 1 secrète

Introduction

Ex :

Codage

Message A 

Message B

Introduction

- Décodage

Message A

Message B

Introduction

R.S.A.

Ravest Shamir Adleman

Créé en 1978

Plan

- Partie théorique
- Le RSA simple
- Une complexification

Théorie

Nous allons ici vous expliquer un certain nombre de théorèmes d’arithmétique qui sont nécessaires a la compréhension du R.S.A.

Théorie

- Congruences

$$a \equiv b \ [n]$$

a-b divisible par n

Théorie

- Indicatrice d'Euler

Si on prend p premier:

$$\varphi(p) = p-1$$

On généralise pour p et q premiers entre eux

$$\varphi(pq) = (p-1)(q-1)$$

Théorie

- Petit théorème de Fermat

Si p est un nombre premier

Si a est un entier naturel non divisible par p

Alors $a^{p-1} \equiv 1 [p]$

Théorie

- 1er théorème du RSA

p et q nombres 1ers avec $n=p*q$

e entier tel que:

$2 < e < (p-1)(q-1) - 1$

e 1er avec $(p-1)(q-1)$

Alors $ed \equiv 1 \; [(p-1)(q-1)]$

Théorie

- 2nd théorème du RSA

Si $b \equiv a^d$ [pq] alors $a \equiv b^e$ [pq]

Plan

- Partie théorique
- Le RSA simple
- Une complexification

Le RSA simple

- Clef publique et clef privée
  - Clef publique

    On prend le produit de 2 nombre premiers

    n=pq

    Et ton choisit un autre nombre premier d

    → Clef publique (n,d)
  - Clef privée

    On cherche ici d tel que ed ≡ 1 [φ(pq)]

    → Clef privée (n,e)

Le RSA simple

- Exemple de génération d'1 « trousseau » de clefs

  Clef publique

  p=19 et q=23 donc n=437

  On prend d=317

  Clef privée

  On trouve ici e=5

Le RSA simple

- Le chiffrement des lettres

A	B	…	Z	« »	?
1	2	…	26	27	28

Le RSA simple

Voyons maintenant la pratique du chiffrage de notre message

« ceci n est pas un message code »

3 5 3 9 27 14 27 5 19 20 27 16 119 27 21 14 27 13 5 19 19 1 7 5 27 3 15 4 5

Le RSA simple

Passons maintenant a l ’aspect purement codage de notre programme

En théorie

On prend le reste de la division euclidienne de a^{317} par 437

Le RSA simple

Mais c'est sans compter sur les limitations machines

Utilisation des propriétés des congruences

Calcul du reste r1 de a^100

Calcul du reste r2 de b^3

Calcul du reste r3 de a^17

Calcul du reste b de r1*r3

Le RSA simple

Avant

« ceci n est pas un message code »

Apres

409 310 409 347 335 412 335 310 171 419 335 123 1 171 335 224 412 335 325 310 171 171 1 429 310 335 409 60 358 310

Le RSA simple

Décodage

Même principe mais en sens inverse :

- Décryptage avec la seconde clef
- Déchiffrement

Le RSA simple

Avant

« ceci n est pas un message code »

Apres

409 310 409 347 335 412 335 310 171 419 335 123 1 171 335 224 412 335 325 310 171 171 1 429 310 335 409 60 358 310

Le RSA trop simple ???

Existence de répétition !!!

Cassage simple grâce a la fréquence d'apparition des caractères

Plan

- Partie théorique
- Le RSA simple
- Une complexification

Une complexification

Nous avons étudie une méthode permettant de rendre plus sur le codage RSA : les changements bases.

Une complexification

Qu’est ce qu’une base?

La base est le nombre par lequel on doit multiplier une unité pour passer d’un ordre au suivant.

Une complexification

Ex: la base 10

5649 peut aussi s'écrire

10^n	…	10^5	10^4	10^3	10^2	10^1	10^0
				5	6	4	9

$5*10^3+6*10^2+4*10^1+9*10^0 = 5649$

Une complexification

Nous allons maintenant changer la base notre code.

Une fois le message chiffre il existe toujours une correspondance. D’où l’intérêt de changer cette base(29) en une autre (ici 437).

Une complexification

Pour passer d'une base a une autre, on passe par la base 10

Ex:

Chiffrage du message « allo » : (1,12,12,15)

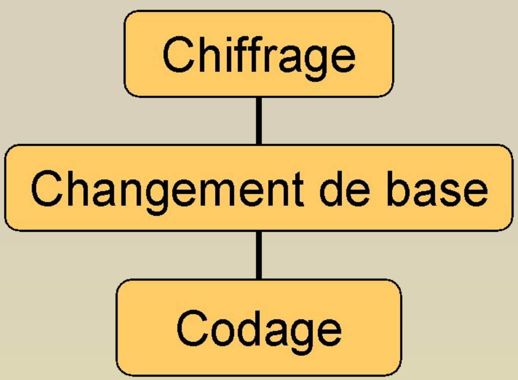
Ce qui s'écrit en base 10 : $1*29^3+12*29^2+12*29^1+20*29^0 = 34844$

Soit en base 437: (437,321)

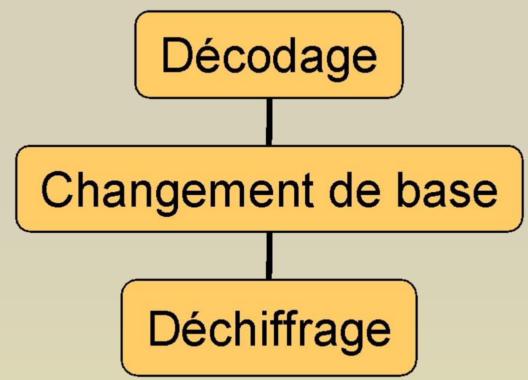
car 79*437+321=34844

Une complexification

On incorpore cette opération dans notre algorithme



Encodage



Décodage

Conclusion


INTERNATIONAL BANK
Corporate Card
VISA
4000 0012 3456
VISA CORPORATE
A CARDHOLDER

Conclusion

Ce systeme de codage n’est pas le plus sur ni le plus rapide mais il est, de loin, le plus utilise en ce moment.

Conclusion

Merci de votre attention