**ATTAQUE SUR RSA**

**Catalogue**

1. **Introduction de RSA**
2. **Nombre d'attaques arithmétiques**

* **Factorisation violente**

1. **Factoriser n directement**
2. **Méthode de Fermat**
3. **Pollard p-1**

* **Attaques à chiffres choisis**
* **Attaques de Wiener**
* **Attaque par le module commun**
* **Attaque de coppersmith**
* **Attaque de Hastad**

**4.Attaque de chronométrage(attaque de réseau)**

**5.Une attaque sur protocole de crypto avant la signature**

**(6.améliorer)**

**Introduction de RSA**

1 . Choisir p,q deux grands nombres premiers aléatoires.

2.Poser n=pq

3.Calculer =(p-1)(q-1)

4.Choisir e(Z/Z)

5.Calculer d=mod

ALGO DE RSA

Clé public n :produit des deux nombres premier pq(p,q sont confidentiel)

e : e est premier avec (p-1)(q-1)

clé privé d :mod(p-1)(q-1)

chiffré c=mod n

déchiffré m=mod n

**Nombre d’attaques arithmétiques**

* **Factorisation violente**

*1. Factoriser n directement*

Si n n'est un nombre très grand, on peut factoriser n pour obtenir p et q, et après avec p,q, on peut calculer le clé privée d pour déchiffré.(Effectué par le code 1)

*2.Méthode de Fermat*

(le code 2)

*3.pollard p-1*

(le code 3)

* **Attaques à chiffres choisis**

RSA est faible dans l'attaque à chiffres choisis .L'attaquant déguise le chiffre intercepté en un nouveau message chiffré et il sera signé par la clé privée.

Eva(attaquant)peut voir les clés publiques et intercepte une partie de chiffre

Clé priveé:d

Clé public:n=pq,et e=(p-1)(q-1)

**Bob**

**Alice**

**m**

**c**

**m**

*Transmission entre Alice et Bob*

1.Déguiser un nouveau message

Pour obtenir m, Eva choisis un nombre aléatoire r et r<n. Elle calcule

*x=mod n*

2.Elle encapsule le message déguisé dans y.

*y=xc mod n*

3.on fait t=mod n

Par algo de RSA ,si x=mod n ,donc r=mod n.Eva envoyai y=xc mod n à Ailce, car Ailce vu jamais y,elle fait un signature de y, et obtenir

*u=mod n.*

Maintenat,Eva calcule

*tu mod n=mod n=mod n*

*=mod n=m*

Après ça,Eva obtient le message clair m.

(on va essayer cette attaque par les codes 4 .)

* **Attaque par le module commun**

Pour communiquer dans un groupe de personnes,on pourrait envisager l'utilisation d'un module RSA n commun avec des paires de clé distinctes(,).Si on utilise(n,)et(n,)pour chiffre le message m, et puis on obtient ,.

Car ,,n sont clé public,donc maintenant on a ,,,n. On fait , sont premiers entre eux, pgcd(,)=1.

Car le théorème de Bézout,+=1,donc （\*）modn=((\*()modn

=()modn

=modn

Maintenant, avec l'attaque du module commun, on peut obtenir le message m.

(Le code 5)

* **Faible exposant privé**

On sait que la sécurité de l'algorithme RSA repose sur la difficulté de factoriser de grands entiers. Selon RSA, e(Z/Z)，si on choisit e mauvais, il rendra cet algorithme de chiffrement non sécurisé.

Comme l'attaque de Wiener,si d est trop petit (d<),l'attaque Wiener peut casser l'algorithme de chiffrement RSA.

**(Démonstration :pourquoi d<?)**

Tout d'abord, on doit introduire' la fraction continue' .

Une fraction continue est une expression de la forme

+

Pour tout entier, on peut le décomposer en fractions continues，par exemple,(72,28)

=2+=2+=……=2+

Quand on décompose une fraction en fraction continue, en fait, on utilise l'algorithme d'Euclide constamment. Par conséquent, on arrive à une conclusion :il existe toujours un nombre fini de fraction continue pour tous les nombres rationnels. Pour la division d'algorithme d'Euclide de deux nombres, on obtenira le pgcd de deux nombres.

Après l'introduction de fraction continue, on retourne l'algo RSA. N=pq et =(p-1)(q-1)=pq-(p+q)+1=N-(p+q)+1,p et q sont grands nombres premiers,pq est plus grand que (p+q),donc on peut considérer N.On sait que d=mod ,et puis on a une égalité :ed=1mod,c'est-à-dire :ed-1=k.On divise par d des deux côtés de l'équation，et obtiens une autre l'équation comme suivant :

-=

Car N,on peut l'ecrire aussi :

-=

Évidement,d\*est très grand, donc est beaucoup moins petit.C'est à dire que est juste un peu plus grand que .

Pour e et N on déjà connu,avec on décompose par fraction continue, l'un d'eux sera égal .(on doit faire un test pour chaque fraction de ,tester si pq égal n)