L'ATTAQUES DE RSA

Jiayan Jiang et Mebrek khadidja

4 juin 2022

Projet encadré par Mme.Herblot

Résumé

Dans cette article ,on va présenter l'algo de chiffrement RSA et ses attaques comme des factorisation violente,module commun,aveuglant,attaque de wiener,attaque de coppersmith,attaque de hasard.....

Tous les codes dans cette mémoire peuvent être trouvé sur le lien https://github.com/jiangjiayan/memoire/tree/main/Downloads/memoire

1 Introduction de RSA

Le chiffrement RSA est un algorithme de cryptographie asymétrique, le plus utilisé actuellement ,L'algorithme RSA est théoriquement solide, avec une bonne sécurité, et peut être utilisé pour le chiffré des données, les signatures numériques et l'authentification d'identité, répondant ainsi aux différents besoins de sécurité des réseaux.

1.1 ALGO DE RSA

1.Choisir p,q deux grands nombres premiers aléatoires
2.Poser n=pq
3.Calculer$\phi(n) = (p-1)(q-1)$
4.$Choisire \in (Z/\phi(n)z)*$
5.$Calculerd = e^{-1} \pmod{\phi(n)}$

Clé plublic	n (n=pq),e :e est premier avec $\phi(n)$
Clé privé	$d = e^{-1} \pmod{\phi(n)}$
Chiffré	$c = m^e \pmod{n}$
Dechiffré	$m = c^d \pmod{n}$

2 Nombre d'attaques arithmétiques

2.1 Factorisation violente

2.1.1 Factorisation n directement

Si n n'est pas très grand ,on peut factoriser n directement pour obtenir p et q .Et après avec p et q c'est facile de calculer la clé privée d pour déchiffrer l'algo rsa. Comment factoriser n ? On présente deux exemples "méthode Fermat" et "pollard p-1"

2.1.2 Méthode Fermat

En arithmétique modulaire, la méthode de factorisation de Fermat est un algorithme de décomposition en produit de facteurs premiers d'un entier naturel.

Tous les entiers naturels impairs N peuvent être considérés comme la différence de deux nombres carrés : N=a^2-b^2. Algébriquement, N peut aussi se factorise en (a + b)(a – b) et, si ni a + b ni a – b n'est égal à 1, alors ce sont des facteurs non triviaux de N.

Il existe une telle représentation pour tout nombre impair composé. Si N = cd est une factorisation de N, alors

$$\mathrm{N} = \left(\tfrac{c+d}{2}\right)^2 - \left(\tfrac{c-d}{2}\right)^2$$

Puisque N est entier impair,donc $\left(\tfrac{c+d}{2}\right)^2$ et $\left(\tfrac{c-d}{2}\right)^2$ sont des nombres entiers.

C'est-à-dire qu'après ces étapes, il est inévitable que le produit des deux facteurs apparaisse sous la forme (a+b)(a-b). Par conséquent, le nombre d'origine peut être écrit comme les deux variances des deux nombres : a^2 - b^2.Par conséquent, nous devons pouvoir trouver a et b par la méthode de Fermat. En d'autres termes, s'il n'est pas trouvé, cela signifie que le nombre d'origine doit être un nombre premier.

Mais cette méthode a des limites, elle est très efficace lorsque les deux facteurs sont relativement proches

2.1.3 Pollard p-1

Soit n un entier divisible par un nombre premier p, avec n p. D'après le petit théorème de Fermat, on a

$$a^{p-1} = 1 \pmod{P}$$

cela implique que pour tout muliple M de p-1,on a

$$a^{M} = 1 \pmod{P}$$

car $a^{k(p-1)} = (a^{p-1})^k = 1^k = 1 \pmod{P}$

Si p – 1 est B-superlisse pour un certain seuil B, alors p – 1 divise le plus petit commun multiple des entiers de 1 à B. Donc, si l'on pose M = ppcm(1, . . . , B), on a

$$a^{M} = 1 \pmod{P} \text{ pour tout a premier avec p.}$$

Autrement dit, p divise a^M-1 et donc le pgcd de n et a^M-1 est supérieur ou égal à p. En revanche, il est possible que ce pgcd soit égal à n lui-même auquel cas, on n'obtient pas de facteur non trivial.

Mais comme l'image suivant ,il est facile de factoriser les nombre petit ,pour les nombres grands il va prendre beaucoup de temps ,jusqu'à j'ai terminé cette mémoire ,le deuxième exemple n'est pas factorisé.[1]

2.2 Aveuglant

2.2.1 Introduction

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.

2.2.2 L'attaque aveuglante

1.Déguiser une nouveau message
Pour obtenir m,Eva choisis un nombre aléatoire r,r<n.Elle calcule

$$x = r^e \pmod{n}$$

2.Elle mets le message déguisé dans y.

$$y = xc \pmod{n}$$

3.On fait t=$r^{-1} \pmod{n}$
Par algo RSA,si x=$r^e \pmod{n}$, donc r=$x^d \pmod{n}$. Eva envoyai $y = xc \pmod{n}$ à Alice,car Alice vu jamais y,elle fait un signature de y et obtenir

$$u = y^d \pmod{n}$$

Maintenant Eva calcule

$$tu \pmod{n} = r^{-1}y^d \pmod{n}$$

$$=r^{-1}x^dc^d \pmod{n}$$

$$c^d \pmod{n} = m$$

Après ça ,Eva obtient le message clair m

2.3 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(d_i,e_i).Si on utilise(n,e_1)et(n,e_2)pour chiffre le message m, et puis on obtientc_1,c_2.
Car e_1,$e_2$sont clé public,donc maintenant on a c_1,c_2,e_1,e_2,n.e_1,$e_2$sont premières entre eux,donc pgcd(e_1,e_2)=1
Avec la théorème de bézout,e_1s_1+e_2s_2=1,donc

$$(c_1^{s_1} * c_2^{s_2}) \pmod{n}$$

$$= ((m^{e_1} \pmod{n})^{s_1}) * ((m^{e_2} \pmod{n})^{s_2}) \pmod{n}$$

$$=m^{e_1s_1+e_2s_2} \pmod{n}$$

$$=m_1 \pmod{n}=\text{m}$$

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

2.4 Faible exposant privée (Attaque de wiener)

2.4.1 Introduction de fraction continue

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

Comme l'attaque de Wiener,si d est trop petit comme d$<\frac{1}{3}N^{\frac{1}{4}}$. l'attaque Wiener peut casser l'algorithme de chiffrement RSA.

(On va expliquer pourquoi d$<\frac{1}{3}N^{\frac{1}{4}}$ plus tard)

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

Théorème :Tout nombre réel positif x a une écriture unique comme fraction continue suivant :

$$\text{x}=a_0+\cfrac{1}{a_1+\cfrac{1}{a_2\cfrac{1}{a_3+\cfrac{1}{a_4+.....}}}} = [a_1\ ,\ a_2\ ,\ a_3\ .....]$$

Ici on définit : soit $[a_1\ ,\ a_2\ ,\ a_3\ .....]$ une fraction continue d'un nombre x. Ou les a_i sont des entier positifs. De plus,la fraction continue est fini,si et seulement si le nombre x est relationnel .

Démonstration : Soit x un nombre réel positif,on pose x = x_0 **On considère la partie entier** a_0 **=**$[x_0]$**.**

Si x_0 est un entier,$a_0 = x_0$ et la fraction continue de x est x=$[a_0]$

Si x n'est pas un entier,on définit

$$x_1 = \frac{1}{x_0-a_0}>1$$

dans ce cas ,on a 0$<x_0$ -x_1 $<$1 et 1 x_0 - a_0 $>$1

Puisque $x_0 = a_0+(x_0-a_0)$,on définit x_1 par Ce qui donne

$$\text{x} = a_0 + \frac{1}{x_1}$$

x = $[a_0,a_1,q_2,.....]$:

$$a_0=[\text{x}]$$

$$x_1 = \frac{1}{x-a_0}$$

$$a_1 = [x_1]$$

$$x_2 = \frac{1}{x_1-a_1}$$

$$a_2 = [x_2]$$

$$x_3 = \frac{1}{x_2 - a_2}$$

Si on connaît a_m,x_m,**si** $x_n \in N, ([\mathbf{a}_n = x_n]$**,on s'arrête .Sinon :)**

$$x_{n+1} = \frac{1}{x_n - a_n}$$

$$a_{n+1} = [x_{n+1}]$$

On recommence le processus pour x_1,on a a_n=$[x_n]$,avec a_n >1 et dans ce cas,la fraction continue de x est

$$\text{x}=a_0+\cfrac{1}{a_1+\cfrac{1}{a_2\cfrac{1}{a_3+\cfrac{1}{a_4+.....}}}} = [a_1\ ,\ a_2\ ,\ a_3\ .....]$$

Si x est nombre irrationnel le processus continue indéfinitivement et on obtient pour x une fraction continue infinie : [a_1,a_2,a_3.....]

Les nombre rationnels $[a_1, a_2, a_3...a_k]$s'appelle les réduits de x. **Pour un nombre x donc la fraction continue est** $[a_1, a_2, a_3$**...**$a_k]$,on peut facilement calculer les premières convergences

$$[a_0] = a_0 = p_0\ \text{q}_0$$

$$[a_0, a_1] = a_0 + \frac{1}{a_1} = \frac{a_0 a_1 + 1}{a_1} = \frac{p_1}{q_1}$$

$$[a_0, a_1, a_2] = a_0 + \frac{1}{a_1 + \frac{1}{a_2}} = \frac{a_0 a_1 a_2 + a_0 + a_2}{a_1 a2 + 1} = \frac{p_2}{q_2}$$

On observe facilement que

$$p_2 = (a_2(a_0 a_1 + 1) + a_0 = a_2 p_1 + p_0$$

Théorème : Soit [a_1,a_2,a_3.....] la fraction continue de x.Pour tout n¿0. On definit les nombres p_n et q_n par

$$p_n = a_n p_{n-1} + p_{n-2}$$

$$q_n = a_n qn - 1 + q_{n-2}$$

Avec tout n>0,on a $\frac{p_n}{q-n}$ =[a_1,a_2,a_3.....a_n] .

Démonstration : La preuve se fait par récurrence sur n.On a déjà vu que $[a_0] = \frac{p_0}{q_0}$.

Supposons que

$$p_n = a_n p_{n-1} + p_{n-2}$$

$$q_n = a_n q_{n-1} + q_{n-2}$$

Et $[a_1,a_2,a_3.....a_n] = \frac{p_n}{q-n}$.Alors on a aussi en utilisent la récurrence.

$$[a_1,a_2,a_3.....a_n,a_{n+1}] = a_1,a_2,a_3.....a_n + \frac{1}{a_{n+1}}$$

$$= \frac{(a_n+\frac{1}{a_{n+1}})p_{n-1}+pn-2}{(a_n+\frac{1}{a_{n+1}})q_{n-1}+qn-2}$$

$$= \frac{(a_n an+1+1)p_{n-1}+a_{n+1}p_{n-2}}{(a_n an+1+1)q_{n-1}+a_{n+1}q_{n-2}}$$

$$= \frac{a_{n+1}(a_n p_{n-1}+p_{n-2})+p_{n-1}}{a_{n+1}(a_n q_{n-1}+p_{n-2})+q_{n-1}}$$

$$= \frac{a_{n+1}p_n+pn-1}{a_{n+1}q_n+qn-1}$$

$$= \frac{p_{n+1}}{q_{n+1}}$$

2.4.2 Fraction continue applique à attaque de wiener

Après l'introduction de fraction continue, on retourne l'algo RSA. N=pq et$\phi(n)$=(p-1)*(q-1)

$$\phi(n)\text{=(p-1)*(q-1)}$$

$$\text{=pq-(p+q)+1}$$

$$\text{=N-(p+q)+1}$$

p et q sont grands nombres premiers,pq est plus grand que (p+q),donc on peut considérer

$$\phi(n) \approx N$$

On sait que d=$e-1 \pmod n$,et puis on a une égalité :

$$\text{ed=1 } (\text{mod } n)$$

c'est à dire :

$$\text{ed-1=k*}\phi(n)$$

On divise par d des deux côtés de l'équationet obtiens une autre l'équation comme suivant

$$\frac{e}{\phi(n)} - \frac{k}{d} = \frac{1}{d*\phi(n)}$$

Avec $\phi(n) \approx N$,Car (n)N,on peut l'écrire aussi

$$\frac{e}{N} - \frac{k}{d} = \frac{1}{d*\phi(n)}$$

Évidemment ,d*$\phi(n)$est grand ,donc $\frac{1}{d*\phi(n)}$ est trop petit .C'est à dire que $\frac{e}{N}$ est juste un peu plus grand que $\frac{k}{d}$.Car e et N on déjà connu,avec décomposer $\frac{e}{N}$par fraction continue ,l'un d'eux sera égal $\frac{k}{d}$.[**?**]

2.4.3 Pourquoi $\frac{k}{d}$est l'un d'étendue de fraction continue $\frac{e}{N}$?

Il y a une théorème important de fraction continue :
The important result is that if p et q are two integers with

$$\left|\alpha - \frac{p}{q}\right| \leq \frac{1}{2q^2}$$

then $\frac{p}{q}$is a convergent in the continued fraction expansion of α
Démonstration :
Soit $\frac{p_n}{q_n}$ est un nombre rationnel .Puisque la suit des démonstrations (q_n) des convergentes $\frac{p_n}{q_n}$ de x est strictement croissantes,alors $q_n \leq q$<q_{n+1}
Preuve :Dans $p_n = a_n p_{n-1} + p_{n-2}$ et $q_n = a_n q_{n-1} + q_{n-2}$,$p_{n-2}$et q_{n-2} sont tous positifs .a_n est supérieur que 1.Donc les convergentes $fracp_n q_n$est strictement croissantes.
pour un entier n >,on a une hypothèse $\left|x - \frac{p}{q}\right| < \frac{1}{2q^2}$

$$\left|\frac{p}{q} - \frac{p_n}{q_n}\right| \leq \left|\frac{p}{q} - x\right| + \left|x - \frac{p_n}{q_n}\right| \leq 2\left|x - \frac{p}{q}\right| < \frac{1}{q^2}$$

Il en resulte que $|pq_n - p_n q| < \frac{q_n}{q} \leq 1$
Ansi $pq_n - p_n q = 0$ et donc $\frac{p}{q} = \frac{p_n}{q_n}$
Ceci termine la preuve .
Maintenant on utilise cette théorème à l'algo de RSA. Supposons que q < p < 2q. Puisque N=pq > q^2 ,alors q < $\sqrt{N}$ D'autre part, on a
Si e est une clé publique et d la clé privée ,alors on a

$$\phi(N)\text{=(p-1)(q-1)=N-p+q)+1.}$$

donc

$$\text{ed=1+k(n-(p+q)+1)}$$

ce qui donne en divisant par dN les relations successives suivantes :

$$\frac{e}{N} = \frac{k}{d} + \frac{1+k-k(p+q)}{dN}$$

$$\left|\frac{e}{N}-\frac{k}{d}\right|=\frac{k(p+q)-k-1}{dn}$$

$$\left|\frac{e}{N}-\frac{k}{d}\right|<\frac{k(p+q)}{dN}$$

$$\left|\frac{e}{N}-\frac{k}{d}\right|<\frac{kq(\frac{p}{q}+1)}{dN}$$

$$\left|\frac{e}{N}-\frac{k}{d}\right|<\frac{3kq}{dN}$$

$$\left|\frac{e}{N}-\frac{k}{d}\right|<\frac{3k}{\sqrt{N}d}$$

De plus, k=$\frac{ed-1}{\phi n}<\frac{ed}{\phi n}$<d<$\frac{1}{3}N^{\frac{1}{4}}$
donc si :

$$\mathrm{d}\leq\frac{n^{0.625}}{\sqrt{6}}$$

Donc 3d <$N^{\frac{1}{4}}$

$$\left|\frac{e}{N}-\frac{k}{d}\right|<\frac{3*\frac{1}{3}N^{\frac{1}{4}}}{dN^{\frac{1}{2}}}$$

$$<\frac{1}{dN^{\frac{1}{4}}}$$

$$<\frac{1}{3d^2}$$

Et en conséquence : $\left|\frac{e}{N}-\frac{k}{d}\right|<\frac{1}{2d^2}$
Comme on connaît e et N,L'attaque peut développer e et N en fraction continue .Avec une réduit $\frac{e}{N}$
D'autres part on peut calculer $\phi(N)$ par relation(factorisation de N),

$$\phi(N)=\frac{ed-1}{k}$$

$\phi(N)$=(p-1)(q-1)=pq-p-q+1=N-p-q+1
En multipliant par p ou q ,on trouve p*$\phi(N)$ =Np- p^2 -pq+p
Donc p*$\phi(N)$ -Np+ p^2 +pq -p =0
Donc p^2 -(N-$\phi(N)$ +1)*p+N=0 p et q sont solutions de l'équation x^2 -(N- $\phi(N)$ +1)*x+N=0
$\delta=(N-\phi+1)^2$ -4N,q= $\frac{N-\phi(N)+1-\sqrt{\delta}}{2}$,p=$\frac{N-\phi(N)+1+\sqrt{\delta}}{2}$ [2]

2.4.4 Comment éviter l'attaque de wiener

La méthode la plus facile est :on doit assurer la clé "d" assez grand. Par example,soit n est 1024 bits,d doit être supérieur à 256 bits .

Mais la plupart des appareils électroniques dans nos vie n'ont pas la capacité de calculer des nombres aussi grandes.Pour cela, Wiener donne également plusieurs autres moyens de se défendre contre cette attaque.

1.Il faut un grand "e" :

Avec un grand e,e $\pmod{\phi n}$ est grand aussi.Donc ici on choisi "e'"remplacer "e", e' = e+t*ϕn.On chiffres les messages avec e',quand une large valeur est utilisé,le ke de la preuve ce dessus n'est plus petit.Un simple calcule montre que si e'>$N^{1.5}$,alors ,n'importe la taille de d,l'attque ce dessus ne peut pas être montée. Malheureusement ,des grands valeurs de e entraînant une augmentation du temps de chiffrement.

2.Avec lemme chinoise

Supposons que d soit choisi de manière à ce que $d_p = d \pmod{p-1}$ et $d_q = d \pmod{q-1}$ soient tous petits.Par exemple, les deux sont de 128 bits. Ensuite, le décryptage rapide suivant du chiffré C peut être déchiffré : Tout d'abord,calculer la somme $M_p = C^{d_p} \pmod{p}$ et $M_q = C^{d_q} \pmod{q}$.Et puis on utilise la théorème chinoise de calculer la valeur M.

$$\text{M}= M_p \pmod{p}$$

$$\text{M}= M_q \pmod{q}$$

la résulta M satisfaite M=$c^d \pmod{N}$.Bien que d_p et d_q soient petits,la valeur de $d \pmod{\phi N}$ peut aussi grande.Cette attaque n'est plus efficace.[3]

2.5 Hastad Attaque

Hastad Attaque également s'appelle attaque de diffusion.Si on chiffre le même message avec le même exposant de chiffrement **e** à plus de **e** personnes différentes, RSA peut faire l'objet d'une attaque de diffusion

Par exemple :Alice envoie le même message crypté RSA m à trois destinataires, en utilisant des modules différents n_1,n_2,n_3,ils sont premiers . Mais ils utilisent le même exposant **e=3**,Eva intercepte trois chiffrés et connaît les clés publiques des trois destinataires

À l'instant ,on peut alors utiliser une attaque de hastad pour récupérer le message m sans factoriser N.

Afin de comprendre son principe d'attaque, on rappelle le théorème des restes chinois :

Théorème : En mathématiques, le théorème des restes chinois est un résultat d'arithmétique modulaire traitant de résolution de systèmes de congruences.

Soient n_1,n_2.....n_k,des entiers deux à deux premiers entre eux, c'est-à-dire que pgcd(n_i,n_j)=1,lors que i$\neq j, donc les entiers$(a$_1$,a_2....a_k),il existe un entier x unique module n = $\prod_{i=1}^{k} n_i$

$$\text{x} = a_1 \pmod{n_1}$$

.....

$$\text{x} = a_k \pmod{n_k}$$

Avec lemme chinoise et algo de Gauss ,Eve peut trouver la solution de x.Dans 0$\leq x<$n$_1 n_2 n_3$,on a

$$x = c_1 \pmod{n_1}$$

$$x = c_2 \pmod{n_2}$$

$$x = c_3 \pmod{n_3}$$

On sait que $m^3 < n_1 n_2 n_3$,donc x=m^3elle prend la racine cubique de xet puis elle peut obtenir le message m .

Comment prévenir et éviter cette attaque

1.Utilisez un grand exposant e, Cela rendra difficile l'utilisation de la méthode d'attaque Hastad.

2.Ajoutez quelques bits aléatoires au message, au moins 64 bits. Assurez-vous que chaque chiffré de message ajoute un nombre aléatoire différent.

3 Final

L'algorithme RSA a l'avantage d'être facile à comprendre et à utiliser, c'est donc l'algorithme à clé publique le plus étudié.Cependant, il a été progressivement accepté par des personnes avec sa propre excellence, et maintenant il est devenu l'un des plus excellents algorithmes à clé publique que les gens considèrent généralement à l'heure actuelle.

Le plan de défense ne peut pas résoudre tous les problèmes de sécurité RSA. Le système d'algorithme RSA est utilisé pour examiner attentivement les exigences de sécurité, le mettre en service et le tester en premier, et effectuer un examen complet de la sécurité du système. Diverses politiques et procédures de sécurité doivent être raisonnablement optimisées afin de réduire au maximum les risques, et l'algorithme RSA peut jouer le plus grand rôle.

Références

[1] Wikipedia. Plagiarism — Wikipedia, the free encyclopedia. 2004. [Online ; accessed 22-July-2004].

[2] Abderrahmane NITAJ. Cryptanalyse de rsa. https://nitaj.users.lmno.cnrs.fr/SlideOujda.pdf, 2009.

[3] Dan Boneh et al. Twenty years of attacks on the rsa cryptosystem. *Notices of the AMS*, 46(2) :203–213, 1999.