Cryptographie Asymétrique : Description d'un nouveau cryptogramme

Rémy Aumeunier
remy.aumeunier@libertysurf.fr

Amateur

Résumé En cryptographie asymétrique, l'un des principaux défis consiste à définir un point d'arrêt. Le schéma qui suit est basé sur une construction mathématique qui n'est pas utilisée, à ma connaissance, dans ce contexte.

1 Introduction

Le chiffrement asymétrique est apparu en 1976[1], avec la publication d'un ouvrage sur la cryptographie publié par Whitfield Diffie et Martin Hellman ; mais aussi par $RalphMerkle$[2] à la même époque. Le crypto-système asymétrique utilise 2 clefs : une clef publique et une clef privée, ou secrète. Lorsque 2 personnes (nommées par convention Alice et Bob) veulent échanger des informations via un canal ouvert ou public, Alice publie une clef publique, Bob code son message avec la clef public d'Alice et met à disposition d'Alice le résultat du chiffrement. Puis Alice avec sa clef privée récupère les informations codées par Bob.

1.1 État de l'art

Les algorithmes de cryptographie asymétrique peuvent être regroupés en 3 grandes familles. Les plus connus sont les cryptogrammes de type RSA. Cet algorithme a été décrit en 1977 par Ronald Rivest, Adi Shamir et Leonard Adleman. Il y a aussi les cryptogrammes à courbe elliptique proposés de manière indépendante, par $NealKoblitz$[4] et $VictorMiller$[3] en 1985. Une courbe elliptique est un cas particulier de courbe algébrique avec laquelle on peut faire une addition, ce qui permet de définir un échange de clés de type Diffie-Hellman. Enfin, le chiffrement El Gamal qui est un algorithme de cryptographie asymétrique fondé sur le problème du logarithme discret créé par l'Égyptien Taher Elgamal, doctorant de l'université de Stanford.

1.2 Préambule

Quelque relation mathematique pour n=6 par exemple

$$a^6 - b^6 = (a-b).(a^5 + b^4.b + a^3.b^2 + a^2.b^3 + a.b^4 + b^5)$$

$$b^n < (a-b) \qquad (a^n) modulo (a-b) = b^n$$

$$(b+c)^n < (a-b) \qquad (a^n).modulo(a-(b+c)) = (b+c)^n$$

$$(b+c)^6 = (b^6 + 6.b^5.c + 15.b^4.c^2 + 20.b^3.c^3 + 15.b^2.c^4 + 6.b.c^5 + c^6)$$

$$(b+c)^6 = (a^6).modulo(a-(b+c))$$

$$(b+c)^6 = b^6 + c.(\frac{a^n}{a-b}) modulo(a-(b+c))$$

2 Présentation du schéma cryptographique

Tout le cryptosystème peut se résumer par

$$(b+c)^n < (a-b) \qquad (b+c)^n = b^n + c.(\frac{a^n}{a-b}) modulo(a-b+c)$$

Alice

$$(\frac{a^n}{a-b}) \quad , \quad (a-b)$$

Bob

$$(alice) modulo(a-b+c)$$

Alice recherche par dichotomie $(b+c)^n$

$$(b+c)^n = b^n + c.bob$$

3 Unicité de la solution trouvée par Alice

Pour un b donnée il ne peut y avoir qu'un c dans

$$(b+c)^n = b^n + c.(\frac{a^n}{a-b}) modulo(a-b+c)$$

4 Etude de la sécuriter

4.1 Renforcement de la securite

Pour éviter de faire un hypothèse sur a^n
Alice

$$(\frac{a^n}{a-b}) \quad , \quad (a+m)$$

Bob

$$(alice)modulo(a+m-c)$$

Alice recherche par dichotomie $(b+m-c)^n$

4.2 Domaine d'application

Pour que le cryptograme fonctionne ,il faut que

$$(b+(m-c))^n < (a+m-c)$$

donc a et grand devant $(b+(m-c))^n$ comme par définition je ne peux pas connaitre c je peux imaginer une règles qui limite le nombre de chiffres de c par raport à a par exemple a à 10,20,30,...,100 fois plus de chiffres que c

4.3 Application numérique

Sous linux Ctrl+Alt+T exécuter bc puis un copier /coller

```
#########Alice#########
n=11
a=132135156165211321^n+3213213215615146161
y=121454784
m=515111987878
publicalice1=a^n/(a-y)
publicalice2=a+m
######################
#########Bob#########
privatebob=1544126544574
publicbob= publicalice1%(publicalice2-privatebob)
######################
#########Alice#######
c=2
r=c*publicbob+y^n-(y+c)^n
while(r>0){c=c*2;r=c*publicbob+y^n-(y+c)^n}

bornsup=c
borninf=c/2
while(r!=0)
{
c=(borninf+bornsup)/2
```

```
r=c*publicbob+y^n-(y+c)^n
if(r<0){bornsup=c}
if(r>0){borninf=c}
}
print "privatebob=";c+y+m
######################
#########Eve#########
r=1
z=0
while(r!=0)
{
    r=publicbob-publicalice1%(publicalice2-z)
    z=z+1
    print "."
}
######################
print z
```

5 Attaques possibles

5.1 L'attaques des clef *ClefPubliqueAlice*

Alice rend public deux valeurs

$$(\frac{a^n}{a-b}) \quad , \quad (a+m)$$

un attaquant peut faire une hypothèse sur n

$$(\frac{a^n}{a-b}) - (a+m)^{n-1} \approx 0$$

donc soit je considère que n et une donnée public ce qui n'est pas trés grave mais bon ...

ou alice public

$$(\frac{a^n}{a-b}) + m_1 \quad , \quad (a+m)$$

et il faut trouvé un moyen d'adapter la recherche dichotomie à

$$(\frac{a^n}{a-b}) + m_1$$

avec $m_1 > \frac{a^n}{a-b}$ ou $m_1 < \frac{a^n}{a-b}$

5.2 L'attaques de la *ClefPubliqueBob*

$$(b+c)^6 = b^6 + c.(\frac{a^n}{a-b})modulo(a-b+c)$$

$(b+c)^6 - b^6 = ((b+c)-b).(a^5+(b+c)^4.(b+c)+a^3.(b+c)^2+a^2.(b+c)^3+a.(b+c)^4+(b+c)^5)$

donc a partire de $publicbob = (\frac{a^n}{a-b})modulo(a-b+c)$

$$(\frac{a^n}{a-b})modulo(a-b+c) = (a^5+(b+c).a^4+(b+c)^2.a^3+(b+c)^3+a^2+(b+c)^4a+(b+c)^5)$$

je ne voie pas actuellement comment un attaquant qui ne connaît pas a mais (a+m) et qui ne connaitre pas b,c pourra faire cette décomposition

$publicbob = (a^5+(b+c).a^4+(b+c)^2.a^3+(b+c)^3+a^2+(b+c)^4a+(b+c)^5)$

5.3 L'attaque par force brute

Comme le décrit l'attaque cela consiste a essayer toutes les conbinaisons possibles donc plus privatebob et grand plus la recherche sera longue

```
z=0
while(publicbob-publicalice1%(publicalice2-z)!=0)
{
    z=z+1
}
```

6 Cryptanalyse

6.1 Attaque sur texte chiffré

Une attaque sur texte chiffré seulement consiste à retrouver la clé de déchiffrement à partir d'un ou plusieurs textes chiffrés

6.2 Attaque sur texte clair connu

Une attaque sur texte clair connu consiste à retrouver la clé de déchiffrement à partir d'un ou plusieurs textes chiffrés, connaissant le texte en clair correspondant

6.3 Attaque sur texte clair choisi

Une attaque sur texte clair choisi consiste à retrouver la clé de déchiffrement à partir d'un ou plusieurs textes chiffrés, l'attaquant ayant la possibilité de générer du chiffre à partir de textes en clair

6.4 Attaque sur texte chiffré choisi

Une attaque sur texte chiffré choisi consiste à retrouver la clé de déchiffrement à partir d'un ou plusieurs textes chiffrés, l'attaquant ayant la possibilité de générer du chiffre à partir de textes en clair

7 Variation possible

8 Recommandation pour une mise en oeuvre

9 Licence et droit de propriété intellectuelle

Domaine public ou libre de toute contrainte ou notion de propriété.sauf si je change d'avis

10 Mise en garde

Compte tenu du fait que la création d'un schéma de cryptographie asymétrique est l'une des choses les plus difficiles auxquelles je me suis retrouvé confronté, je vous conseille vivement la plus grande prudence. Autrement dit, je ne suis pas censé réussir à ce jeu, donc ...

Références

1. ↑ W. Diffie and M.E. Hellman, Multiuser cryptographic technics, Proceedings of AFIPS National Computer Conference, 109-112, 1976
2. ↑ A.J. Menezes, P.C Van Oorschot, S.A. Vanstone, Handbook of applied cryptography, CRC Press, 1997, p. 47
3. ↑ V. Miller, « Use of elliptic curves in cryptography », dans CRYPTO, n°85, 1985.
4. ↑ Neal Koblitz, « Elliptic curve cryptosystems », dans Mathematics of Computation, n°48, 1987, p.203–209