Cryptographie Asymétrique : Description of a new cryptograme

Rémy Aumeunier
remy.aumeunier@libertysurf.fr

Amateur

Résumé The main challenge in asymetric key encryption is to define an end point. To my knowledge, the method described in this article is not used inthis case yet. This approach was discussed ans studied on a specialised forum by its web users, see newsgroup Usenet : sci.crypt

1 Introduction

In 1976, Whitfield Diffie and Martin Hellman released the first publication about asymmetric key encryption, as well as Ralph Merkle at the same period. This cryptographic system uses two keys, a public and a private secret one. To give a quick example, Alice and Bob exchange information through a non secured channel. Alice uses her private key to decrypt the encrypted message Bob sent her on the public key they share.

1.1 State of the art

There are three categories for asymmetric key encryption algorithms. First, the most know is the RSA cryptograms. This algorithm was described in 1977 by Ronald Rivest, Adi Shamir and Leonard Adleman. Second, elliptic curve cryptography is a category proposed independently by Neal Koblitz and Victor Miller in 1985. An elliptic curve is a specific algebraic curve with which addition is possible, allowing a Diffie-Hellman key exchange. Finally, El Gamal encryption system is an asymmetric key encryption algorithm based on the problem of discreet logarithm created by the egyptian Taher Elgamal, Stanford University PhD.

1.2 Foreword

Mathematical concepts and relations

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

$$b^n < (a-b) \qquad a^n \equiv b^n mod(a-b)$$

$$x = b + c \qquad y = b \qquad n = 6$$

$$x^n - y^n = (x - y).(x^5 + x^4y + x^3.y^2 + x^2.y^3 + x.y^4 + y^5)$$

$$a^n/(a - y) \equiv (x^5 + x^4.y + x^3.y^2 + x^2.y^3 + x.y^4 + y^5) mod(a - x)$$

$$x^n - y^n = (x - y).(a^n/(a - y) mod(a - x))$$

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

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

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

$$(b + c)^6 = b^6 + c.(a^n/(a - b) mod(a - (b + c)))$$

2 Cryptographic scheme presentation

The encryption system can be resumed as

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

Alice

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

Bob

$$(\frac{a^n}{a - b}) mod(a - b - c)$$

By dichotomy research Alice looks for $(b + c)^n = b^n + c.bob$

2.1 Improving the security

In order to avoid hypothesis on a^n

$$ClefPublicAlice1.ClefPublicAlice2 = \frac{a^n}{(a - b)}.(a - b)$$

Alice modifies her ClefPublicAlice1 as

$$((\frac{a^n}{a - b}) mod(a - b - c) + (\frac{a^m}{a - b}) mod(a - b - c)) mod(a - b - c)$$

$$= (\frac{a^n + a^m}{a - b}) mod(a - b - c))$$

therfore Alice shares

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

and to avoid

$$(PublicAlice1.PublicAlice2)mod(Factor_of \quad a^n) = 0$$

$$(\frac{a^n + a^m}{a-b}).(a-b)mod(a) = 0)$$

Alice introduces a light noise

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

Bob also introduces noise to enhance security, after his calculation

$$ClefPubliqueBob = ((\frac{a^n + a^m}{a-b} + bruitAlice).mod((a-b)-c) + bruitBob$$

then by dichotomy research she looks for $(b-c)^n + (b-c)^m$

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

cf. 5 Application numérique

3 Uniqueness of the solution found by Alice

For a, b et n, there can only be one value for c in because b and n are not unknown

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

or

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

in a more mathematical way

$$si \quad b^n < (a-b) \quad therefore \quad (a^n)mod(a-b) = b^n$$

cf. arithmétique modulaire is suficient to ensure the bijection

4 Scope

In order to make the cryptogram work, it must be

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

therefore a must be large compared $(b - Privatebob)^n$ As by definition PrivateBob is unknown It is possible to imagine a rule that limits the number of digits for PrivateBob regarding the public keys for example a has 10,20,30,...,100 times more digits than c

5 Mathematical application

On linux Ctrl+Alt+T execute bc then copy paste

```
#########Alice#########
 n=16
 m=14
 bruitprivatealice=2^1010-123456789
 a=1321351561652113 21^213+3213213215615146161
 b=12145478465465465463123 13

 publicalice1=(a^n+a^m)/(a-b)-bruitprivatealice
 publicalice2=a-b
 ######################
 #########Bob#########
 privatebob=12345267856
 bruitprivatebob=2^1120+1234781
 publicbob= (publicalice1%(publicalice2-privatebob))+bruitprivatebob
 ######################
 #########Alice#######
 r=1
 bornsup=publicbob
 borninf=0
 while(r!=0)
 {
 c=(borninf+bornsup)/2
 r=((c*publicbob+b^n+b^m-(b+c)^n-(b+c)^m))/bruitprivatealice+c
 if(rtmp==r){r=0}
 rtmp=r
 if(r<0){bornsup=c}
 if(r>0){borninf=c}

 }
 print "privatebob=";c
 c-privatebob
 ######################
```

6 Security Study and Possible Attacks

6.1 Attacking the *ClefPubliqueAlice*

Alice makes the results public

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

No attack have been found for the moment because *bruitAlice*

6.2 The attack of *ClefPubliqueBob*

Therefore from Bob makes public a value $ClefPubliqueBob$

$$(ClefPublicAlice1.mod(ClefPublicAlice2 - PrivateBob)) + bruitBob$$

$$ClefPubliqueBob = (\frac{a^n + a^m}{a - b} + bruitAlice).mod((a - b) - c) + bruitBob$$

no attack have been found yet because $bruitBob$

6.3 The brute force attack

As described by the attack, it consists in trying every possible combinations as I am not finding a breakpoint on the keys $ClefPublicAlice1$ and $ClefPublicAlice2$ we must cancel the noise and do a search on c in $ClefPubliqueBob$

7 Cryptanalyse

7.1 Attacking a ciphertext

Attacking a ciphertext consists in finding the decryption key from one ciphertext or more therefore

$$ClefpublicBob_1 = (\frac{a^n}{a - b})mod(a - b - c_1) + bruitBob_1$$

$$ClefpublicBob_2 = (\frac{a^n}{a - b})mod(a - b - c_2) + bruitBob_2$$

$$...$$

$$ClefpublicBob_n = (\frac{a^n}{a - b})mod(a - b - c_n) + bruitBob_n$$

for now no attacks have been found yet.Because $bruitBob_n$

7.2 Attacking a known plaintext

Attacking a known plaintext consists in finding the decryption key from one ciphertext or more by knowing the corresponding plaintext ,no attack have been found yet because $bruitBob$ and $bruitAlice$

7.3 Attacking a specific plaintext

Attacking a specific plaintext consists in finding the decryption key from one ciphertext or more, but by giving the possibility to generate encyrption from the plaintext, no attack have been found yet because $bruitBob$ and $bruitAlice$

8 Possible variation

$$ClefPublicAlice1 = \frac{a^n + a^m \pm ....}{(a-b)} + bruitAlice$$

$$ClefPublicAlice2 = (a-b)$$

9 Recommendation for implementation

evaluate the impact of the size of the noise (bruit) on the bob give but before you have to understand or apprehend the protection mechanism not very easy thing

10 Copyright

Domaine public ou libre de toute contrainte ou notion de propriété Public domain or free from any limitation or ownership.
If you liked you can donate to me via paypal or if you like the challenges and if you do not find any attaque then donate :-)

11 Warning

Considering the fact that creating an asymmetric key encryption has been one of the most difficult challenges I've faced, I totally recommand to be cautious. In other words, I am not supposed to win at this game, so...

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