Asymmetric Cryptography

presentation of a new mathematical scheme

Rémy Aumeunier
Amateur

15 Jul 2021

Asymmetric encryption appeared in 1976, with the publication of a book on cryptography by Whitfield Diffie and Mar-tin Hellman but also by Ralph Merkle at the same time. The asymmetric cryptosystem uses two keys : a public key and a private or secret key.When two people (named by convention Alice and Bob) want to exchange information via an open or public channel, Alice publishes a public key, Bob encodes his message with Alice's public key and makes the result of the encryption available to Alice.Then Alice, with her private key, retrieves the information encoded by Bob

1 State of the art

SAsymmetric cryptography algorithms can be grouped into 4 major families.The best known are the RSA type cryptograms. This algorithm has eté d written,in 1977 by Ronald Rivest,Adi Shamiret Leonard Adleman.There are also the elliptic curve cryptograms pro-posed independently,by NealKoblitz and Victor Miller in 1985. An elliptic curve is a special case of algebraic curve with which one can make an addition,which allows to define a key exchange of type Diffie-Hellman.There is also the El Gamal cipher which is an asymmetric cryptography algorithm based on the discrete logarithm problem created by the Egyptian Taher Elgamal,doctoral student of Stanford University.Then to finish there are also several cryptosystems based on the famous knapsack problem

2 Préambule

I do not claim that this proposal is secure, weak or mathematically exploitable or realistic. I wish to propose an asymmetric cryptography algorithm that the factorization of public keys does not allow to break the system

3 optional non-academic mathematics

To understand this proposal I will propose to you to leave the academic field,an integer is not just a combination of prime numbers.

$$Syn_n = \begin{pmatrix} (n)mod(2) = \{1\} \\ (n)mod(3) = \{1,2\} \\ (n)mod(5) = \{1,2,3,4\} \\ (n)mod(7) = \{1,2,3,4,5,6 \\ \cdots \\ \cdots \\ (n)mod(q_{max}) = \{1,\cdots,(q_{max}-1)\} \end{pmatrix}$$

Here I consider an integer as a container which has several values,and each different integer has its own values and properties, for example a prime number has no zero.end of this side note, but before I add a footnote.[1]

4 Asymmetric Cryptography algorithm

Alice draws an integer at random n

$$n = 12345 * 101$$

modify n to have 2 relatively close but different values.

$$n = 12345 * 101$$

$$(n+1)mod(101) = 1$$

$$(n+1)mod(97) = 8$$

here the private keys have the 2 integers $(101, 97)$,and the public key $(n+1) = 1246846$.

Bob uses the public key Alice by multiplying it to change all the values and then adds his msg and adds noise so as not to disturb his msg.

$$msg = 99, k = 5, (1246846)+msg+2\cdot3\cdot5\cdot7\cdot11...101\cdot103\cdot107\cdot109\cdot113\cdot1134564646$$

Alice finds Bob's message because

$$(2\cdot3\cdot5\cdot7\cdot11...101\cdot103\cdot107\cdot109\cdot113)mod(101) = 0$$

$$(2\cdot3\cdot5\cdot7\cdot11...101\cdot103\cdot107\cdot109\cdot113)mod(97) = 0$$

$$\frac{(publicBob)mod(97) - (publicBob)mod(101)}{(8-1)} = k$$

here and for the moment I notice that any factorization of the numbers public will not be of any use

[1] I propose you to use this representation on several different couple of twin primes and apprehend thereafter the conjecture on the twin primes

5 Academic mathematical analytical demonstration

6 author's note

No need to go further since I haven't found a quick way to generate noise yet

Références

[1] .....

[2] .....

[3] .....

[4] .....

[5] .....