

1 Asymmetric Cryptography  
2 presentation of a new mathematical scheme

3 Rémy Aumeunier  
4 Amateur

5  
6  
7  
8  
9  
10  
11  
12  
13  
14 15 Jul 2021

Asymmetric encryption appeared in 1976, with the publication of a book on cryptography by Whitfield Diffie and Martin 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

15 **1 State of the art**

16 Asymmetric cryptography algorithms can be grouped into 4 major fami-  
17 lies. The best known are the RSA type cryptograms. This algorithm has été  
18 d written, in 1977 by Ronald Rivest, Adi Shamir et Leonard Adleman. There are  
19 also the elliptic curve cryptograms proposed independently, by Neal Koblitz and  
20 Victor Miller in 1985. An elliptic curve is a special case of algebraic curve with  
21 which one can make an addition, which allows to define a key exchange of type  
22 Diffie-Hellman. There is also the El Gamal cipher which is an asymmetric cryp-  
23 tography algorithm based on the discrete logarithm problem created by the  
24 Egyptian Taher Elgamal, doctoral student of Stanford University. Then to finish  
25 there are also several cryptosystems based on the famous knapsack problem

26 **2 Préambule**

27 I do not claim that this proposal is secure, weak or mathematically exploi-  
28 table or realistic. I wish to propose an asymmetric cryptography algorithm with  
29 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.

$$Syn_n = \left( \begin{array}{l} (n)mod(2) = \{0, 1\} \\ (n)mod(3) = \{0, 1, 2\} \\ (n)mod(5) = \{0, 1, 2, 3, 4\} \\ (n)mod(7) = \{0, 1, 2, 3, 4, 5, 6\} \\ \dots \\ \dots \\ (n)mod(q_{max}) = \{0, \dots, (q_{max} - 1)\} \end{array} \right)$$

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.<sup>1</sup>

### 4 Asymmetric Cryptography algorithm

Is under development but the general scheme is as follows, Alice draws an integer at random n

$$n = 12345 \cdot 101$$

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

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

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.

$$msg = 99, k = 5, (1246846 \cdot k) + msg + 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \dots 101 \cdot 103 \cdot 107 \cdot 109 \cdot 113 \cdot 1134564646$$

Alice finds Bob's message because

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

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

## 49 5 Academic Mathematical Démonstration

$$Pgcd(PublicKeyAlice, PublicKeyBob) = 1$$

50

$$(2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \dots \cdot P_n) \bmod (PrivateKeyAlice) = 0$$

51

52

53

## 54 6 Author's note

55 No need to go further since I haven't yet found a fast way to generate noise,  
56 if the private keys have the 2 integers of value  $2^{512}$ .

## 57 Références

58 [1] .....

59 [2] .....

60 [3] .....

61 [4] .....

62 [5] .....