The fundamental point that emerges from newspapers is that security would be guaranteed by the inclusion in the algorithm of mathematical problems that are extremely difficult to solve even with Quantum Computers.

I am a mechanical engineer who worked for 20 years as an analyst-programmer in a large ICT company. The mental approach of an engineer is significantly different from that of a mathematician. So let's see why I believe that predictions about the non-solvability of complex mathematical problems cannot be trusted.

I remember that when SuperEnalotto was created, many mathematicians declared that this game would never have a winner given the very low probability of winning. Winners of huge sums laugh at such predictions. But returning to encryption systems, after the Second World War it became mandatory to adopt the RSA system of public key and private key. Here too the mathematicians have failed. The connection between public key and private key is based on very large prime numbers whose decomposition into factors was not possible with current computers at the moment.

In reality the theory spoke of random numbers which do not exist in computer science, there are pseudo-random numbers generated by an algorithm whose identification leads to the identification of the keys. It appeared already in 2012 in the Italian newspaper Repubblica that a group of researchers managed to identify 5 percent of the keys, with computers from 12 years ago.

Furthermore, the public key, which is very slow and only serves to transmit the private key, is managed by a company that issues a certificate of authenticity. The possibility of fake certificates significantly compromises the security that is still bandied about today. Then there is the problem of the Backdoor whereby Someone wants to read the encrypted texts.

However, this is a future where it is said that we will have security equal to the current AES 256 or lower.

We, however, with our product patented in Italy and working which we called CRIPTEOS 3001, have solved all these problems. With an extension of this product we have created the REAL CBDC digital currency which has zero energy costs.Come funziona?

It is a dimensional extension of the square table of Vigenere, which had perfected the cryptography of Julius Caesar. We encrypt two characters at a time, with very high speed, and therefore the key that we generate algorithmically and insert into memory for processing would need 65536 characters. That is 256 squared.

But cryptanalysts in the Italian Renaissance were able to identify messages by knowing only the language of the message, for example Italian, Latin, French. It was known that for a fairly long message there is a hierarchy of frequency of the letters of the alphabet. The most frequent letter in Italian is E, followed by A and the others. Then, having identified the most frequent encrypted characters and replaced them with E, then A etc., the message was decoded.

Therefore there must not be a one-to-one correspondence between the plaintext character and the encrypted character. We solved this by mandating that the encrypted character was a function of the plaintext character and its position in the text. F= f1 (character) + f2 (position).

Since we have a movement given by f2, the table becomes double, i.e. 128 Kilobytes. For technical reasons and to safely separate the clear text from the encrypted text, there are two keys of 131 thousand characters and therefore two tables in memory. This was created with a PC costing 300 euros.

In the case of the REAL CBDC digital currency we have three 40 megabyte keys and we had to buy a PC costing 800 euros. Backdoor issue also resolved. The third key of 40 megabytes allows you to customize the algorithm so that each customer has his own algorithm.

The verification of the REAL CBDC digital currency will be done by the Customer simply by decoding the message, given that, unlike HASH encryption, which is not reversible, our encryption is completely reversible.

A further point to our advantage is that we know how long it takes to encrypt, how long does the super-complex algorithms of mathematicians take to encrypt? posterity will judge.

The extreme future? We will be able, with enormous computers already available, to deal with two characters at a time, three characters at a time, with keys a few Gigabytes long, or four characters at a time, with keys a few Terabytes long. I called the software CRIPTEOS 3001 because in 3001, if there is still humanity, perhaps valid competitors will arrive. Never say never.

All the best

XEROMER SRL