Panama, April 2020

CYPHERTOP

Security is priceless

How many political, military, state and private projects have failed, simply because some information about them fell in the wrong hands!

Every day you can hear of anonymous leaks or responsible persons that destroy an enterprise, business, political reputation or even government.

The common denominator is precise: Information leak. The information was not protected.

Even when the information is supposedly protected, leakage occurs with great magnitude and with considerable losses for the government, institution or person connected to it.

The WikiLeaks case illustrates a current example where the big looser is the United States. Despite the fact that more than half a million communications were protected by the ultra-famous AES 256.

What was then the real cause of this breakdown?

The key that protected those encrypted communications was in the hands of a person that is not trustworthy or what is more: It depended on the honorability of an officer.

To depend on something so volatile and difficult to evaluate in depth, as the intelligence community knows, it is imprudent, to say the least. How then can information be secured to prevent the undesirable juncture of its leak due to a human factor? The details are as follows.

Maximum security: CYPHERTOP

Cyphertop is the most powerful tool developed up to date for the protection of information.

Cyphertop advances the concept of encrypting algorithm to become the first Universal Generator of encrypting algorithms developed up to now. AND

Due to its invaluable quality, if a file is coded **n** times with Cyphertop, the coded file will have a different length and content all the **n** times. Thus making any attempt to break the code through traditional techniques used by the security agencies impossible and in general by the collectivities of hackers dedicated to the topic of cryptography.

In an attached document (Resistance of Cyphertop to computational brute force attacks), figures that demonstrate the invulnerability of Cyphertop are submitted where the following can be appreciated:

- Using all the matter available in our Universe to build the biggest grid of computers possible and

- Using the time of existence that is left to our Universe,

It is impossible to successfully attack Cyphertop.

Cyphertop as a generator of encryption algorithms makes use of several innovative concepts in the discipline of cryptography. Here they are presented in their order:

- The DNA: As in biology, where every living being possesses a specific DNA, Cyphertop assigns every pair of users a specific DNA which is constituted by several sets of numbers picked randomly. This pair of users that share such DNA is called “connection point”.

  Every time that that pair of users communicate, the random variables generated by the physical systems: computer, tablet, mobile, generate a certain amount of random figures that modify the specific DNA that is shared by this pair of users.

  With this modified DNA, Cyphertop proceeds on each occasion to generate a different pseudo random numbers generator motor that will serve as the base for the corresponding encrypted communication, be it sending files, messages, voice, image, etc.

- As it is well known, the prototype of the human DNA is quite different for example from the prototype of DNA of a horse. Within the human DNA, there is a giant quantity of DNA that we, the more than six thousand million humans that live right now, carry.

Each one of us have a different DNA but classified as “human” DNA. This same variety is observed in Cyphertop. With the same structure of DNA, it is possible to have at least 8,21479634 x $10^{60.224}$ different DNAs that allow having that same number of connection points. This set of DNA configures a UNIVERSE of Cyphertop.

Therefore, modifying the structure of DNA it is possible to generate another Universe and in fact, there can be as many Universes as the imagination allows and where the connection points of a Universe cannot communicate with those of another Universe. With that, it is possible that an organization, be it a nation, industry, internet application or any collective group can have a Cyphertop Universe for its exclusive use and maintain communications with other entities or particulars with a public version of Cyphertop.

- As it might already be inferred, randomness is one of the main elements of Cyphertop. To this purpose, Cyphertop has a three-dimensional rotational mechanism, conceptualized within its structures of information that allows it to produce a pseudorandom series of very high quality.
- Another of the prominent figures of Cyphertop is that it introduces in its encryptions an undetermined amount of “garbage” information, that is, characters produced randomly that have nothing to do with the message to be encrypted and that serve to introduce greater entropy in the final encryption.
- Finally, Cyphertop operates on a double cycle. That is to say that the file is encrypted twice consecutively. But the way in which Cyphertop does it impedes that the blocks structures used in the first cycle be preserved in the second cycle. As a consequence, it impedes segmenting the encrypted file into blocks for its analysis and attack. In addition, operating on the double cycle has the great advantage that the attacks to the final encryption only result in another encrypted text, making it even more difficult for any attack strategy that might be attempted against Cyphertop.

The design of Cyphertop was oriented so that it becomes the first personalized encryption system, as each pair of users possess a common DNA that enables the construction of a particular generator of pseudo random numbers that, at the same time, becomes the source of pseudo random numbers that allow the construction of a generator of encrypting algorithms of exclusive use for this pair of users.

This is assimilated in the fact that each pair of persons on this planet could invent an exclusive jargon for their communication and that jargon would change continuously in time. This would be the definition of Cyphertop in colloquial terms. At this point, it is relevant to say that the secure and personalized mobile, which in the markets costs more than 10.000 dollars, is an additional consequence of the novel conceptualization of Cyphertop.

Requirements and Availability

In terms of hardware requirements, Cyphertop is available for computers, tablets, mobiles and in general for any computer platform with two (2) GB of RAM memory and above.

And regarding operational platforms, it is available for Android, Windows and soon for Mac, ISO, and Linux systems (the most important implementations of Linux are included).

Parallelization and speed

Apart from the security issue, any encryption nowadays must also provide a very good speed of encrypting. In this sense, Cyphertop has been shown to be competitive in comparison with other algorithms in the market. The current speed of Cyphertop is around 50 Mbytes per second in low yield equipment. Take into account that the computer hardware, in mobiles as well as in laptops and fixed platforms advancing towards CPUs with more processors every time. This will provide Cyphertop with higher speeds of encrypting due to the effect of parallelization.

.

The impossible attack

As already said, Cyphertop is invulnerable to computational attacks of brute force. In the document “Resistance to Computational Brute Force Attacks,” the figures that back this claim are presented. Its reading is recommended for a thorough understanding of the level of security of Cyphertop.

All the information contained in this document and/or any of its annexes are considered as confidential, privileged and protected information in accordance with the applicable law. This message is directed only to the recipient. In case that you are not the recipient of this document, the reading, printing, publication distribution, copy or any other use of this message and /or its annexes is strictly prohibited. If you have received this message by error, please notify ADVN Security Sotfware C.A. immediately through the data provided above and eliminate this message as well as any other copy or back up of it.