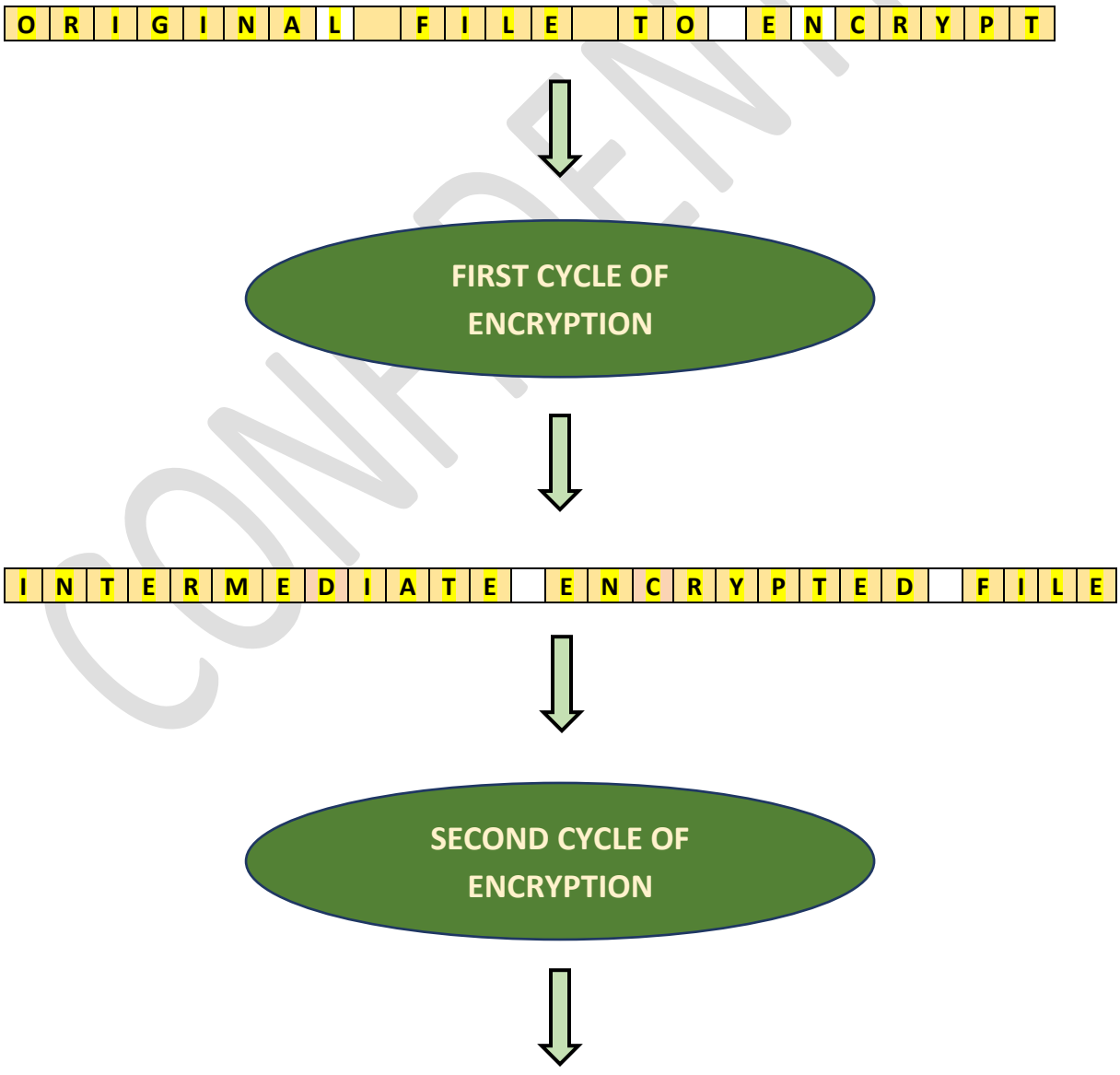
The future of encryption is our present

Panama, April 2020

OPERATING DIAGRAM OF CYPHERTOP

ENCRYPTION PROCESS

Cyphertop is an encryption meta-algorithm of two cycles. The general process of encryption is presented here, in its two cycles:



F	I	N	A	L		E	N	C	R	Y	P	T	E	D		F	I	L	E

FIRST CYCLE OF ENCRYPTION

Suppose that you want to encrypt the following file (10 characters):

M	i		a	r	c	h	i	v	o

Cyphertop encryption contains two main parts:

HEADER	MESSAGE/ENCRYPTED TEXT

The header of the first cycle is built like this:

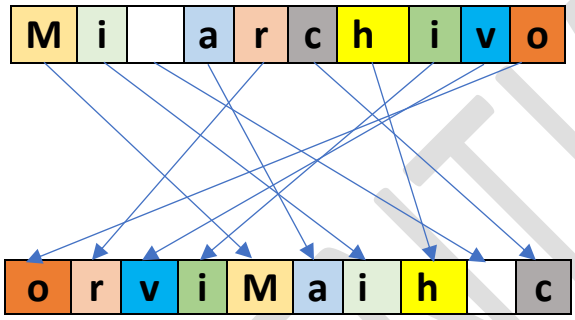
Garbage	CT1	CT2	(CI) = Field of garbage bytes that serves to insert the Modifying numbers	Garbage	Length of file
N bytes			**1.000** bytes	**K** bytes	

Steps:

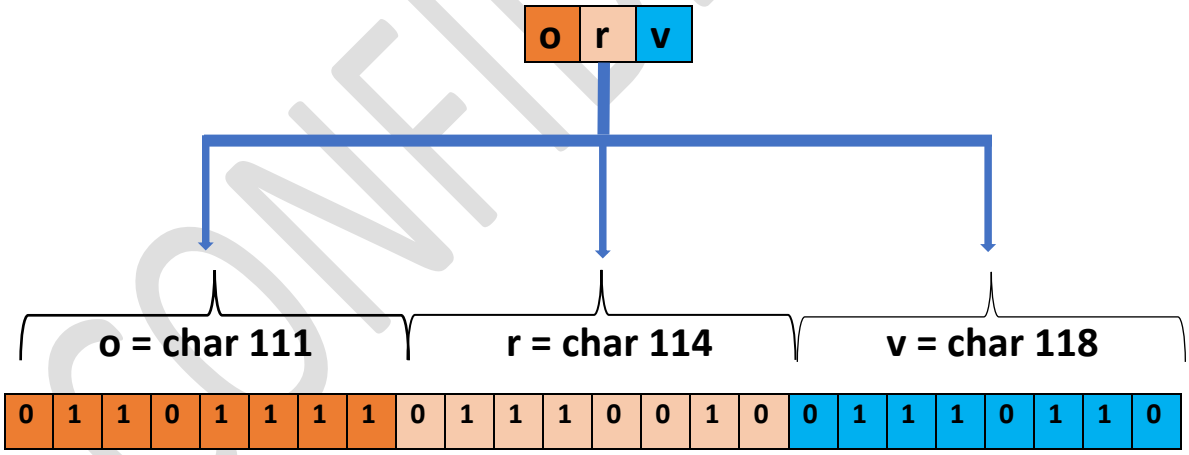
1. **N** bytes (**N** is a number dependent on the DNA used) of garbage information are inserted. That is, bytes produced randomly.
2. Next, fields CT1 and CT2 are inserted which are the tridimensional locks and are the ones that contain information that will help to insert the first five modifying numbers within the next field (**CI**).
3. Field CI is composed of 1.000 or more bytes of garbage information that will be used to insert the first five modifying numbers in them.

4. Then **K** Bytes of garbage information is inserted, where **K** is a value that depends on the information that has been introduced previously in the field **CI**.
5. Finally, the length of the name of the original file to be encrypted is inserted.

Once the header is built the name of the file is encrypted, and added after the header, and the information of the file must be encrypted, in this case, it is "**Mi archivo**" and for this, a scattering process of the respective bytes of the file is applied, ending with their positions changed (transposition) as follows:

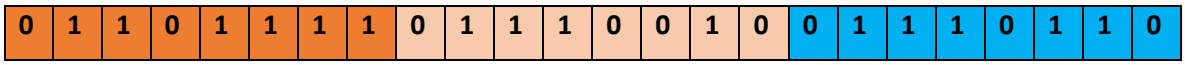


Then, every byte is divided into bits as follows:

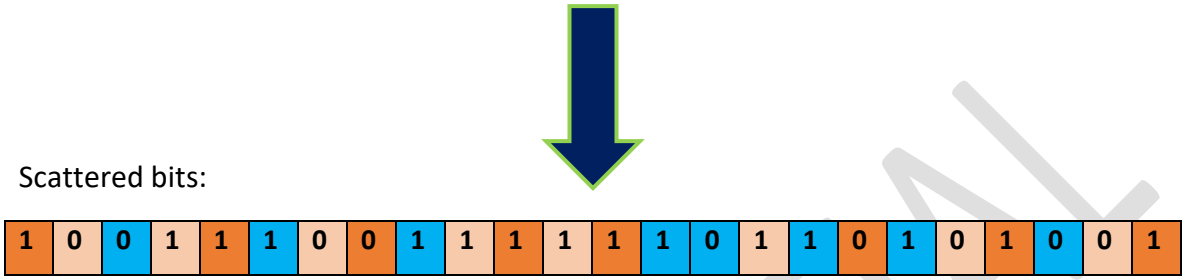


Then, the bits are scattered (transposed). For this, blocks of 4000 bits (500 bytes) are selected and 96 bits (12 bytes) of garbage randomly produced are added. Such blocks of 4096 bits (512 bytes) are stirred up internally through the use of recombinant mini algorithms that are nothing more than scattering tables of bits, 4096 positions each one. Usually, more than 1.000 scattering tables of bits (recombinant mini algorithms) are produced for each encryption cycle. When bits are scattered, a result similar to this is produced:

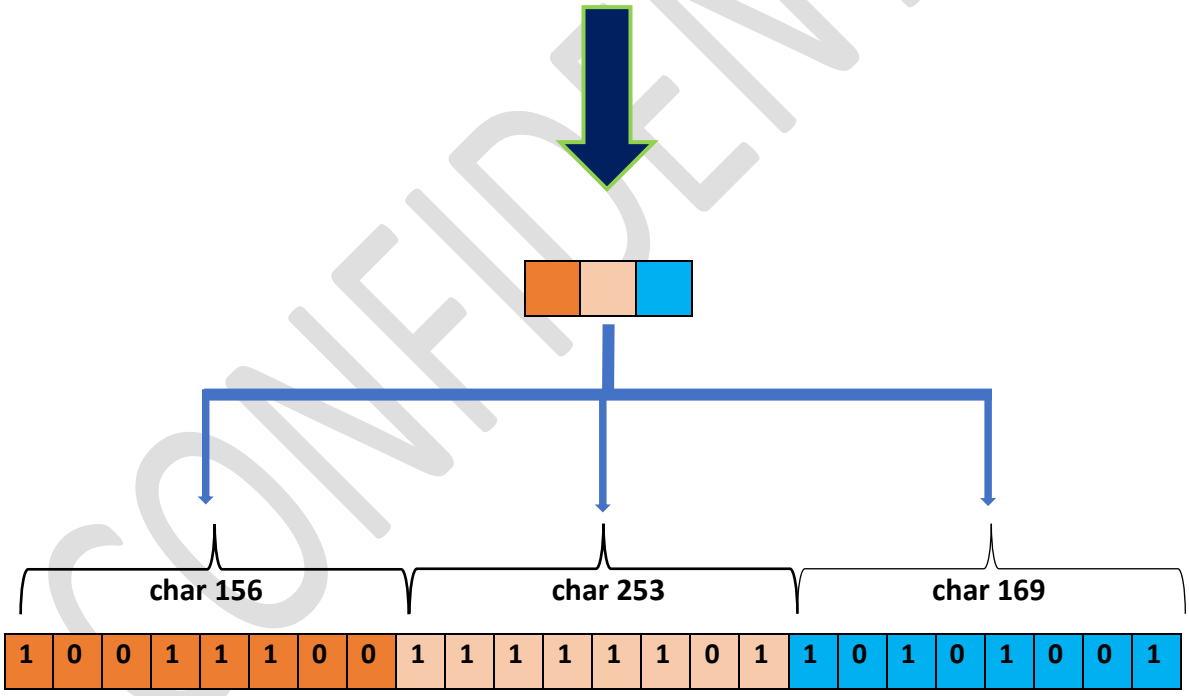
Bits to be scattered:



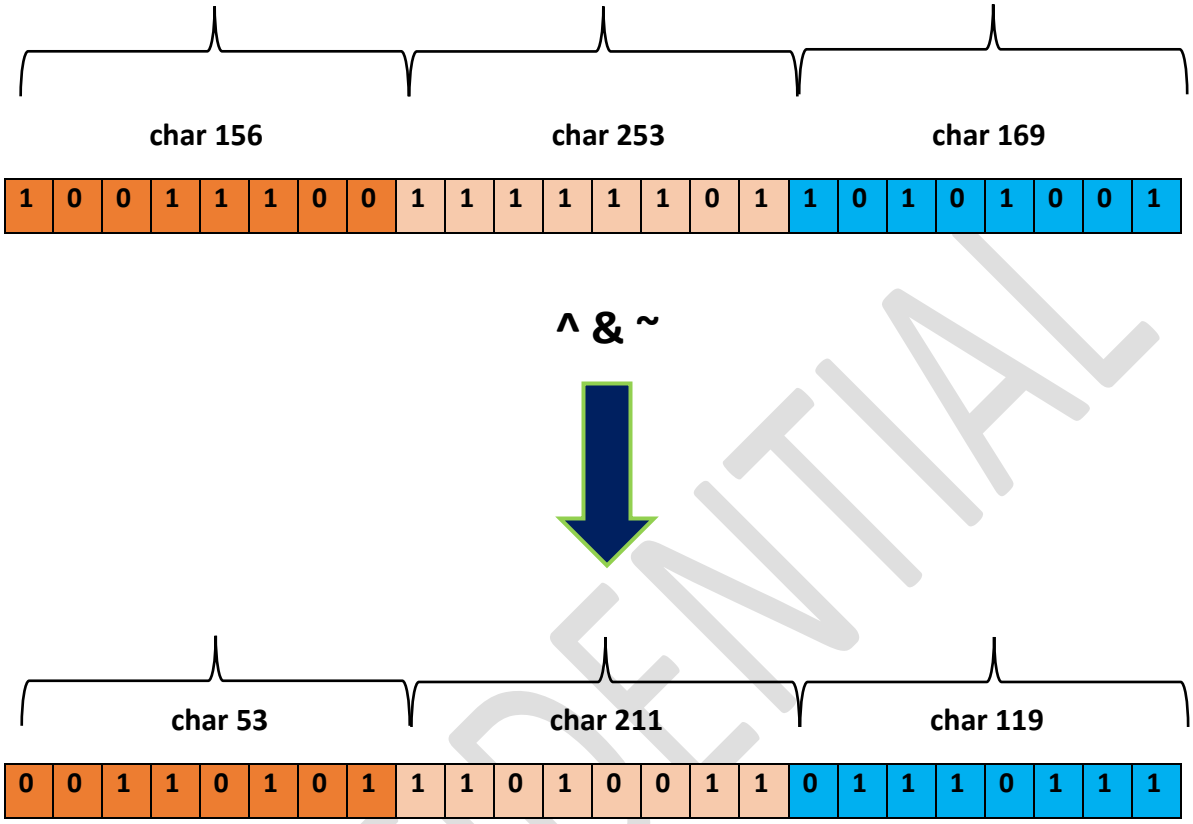
Scattered bits:



Once the bits are stirred by blocks, the information is changed into bytes again and we would have:



Finally, these characters are subjected to an XOR operation, with tables constructed through modifying numbers for each occasion of encryption. Also complement operations are applied on some of these characters. The information of the previous vector could end up like this:



When this process ends, an amount of "garbage" bytes is added whose length comes indicated by the modifying numbers. It is kind of a queue which serves to hide the end of the coding of the first cycle.

SECOND CYCLE OF

In the second cycle, what was executed in the first cycle is essentially repeated, only that the Header includes an additional field that is used so that the receiving user (decoder) can validate the DNA with which the file is coded.

Thus, for example, the header used in the first cycle:

Garbage	CT1	CT2	(CI) = Field of garbage bytes that serves to insert the Modifying numbers	Garbage	Length of file

If would end up like this:

Garbage	CT1	CT2	(CI) = Field of garbage bytes that serves to insert the Modifying numbers	Field for Validation Through hash	Garbage	Length and name of the file
N bytes			**1.000** bytes		**K** bytes	

Several changes operate here:

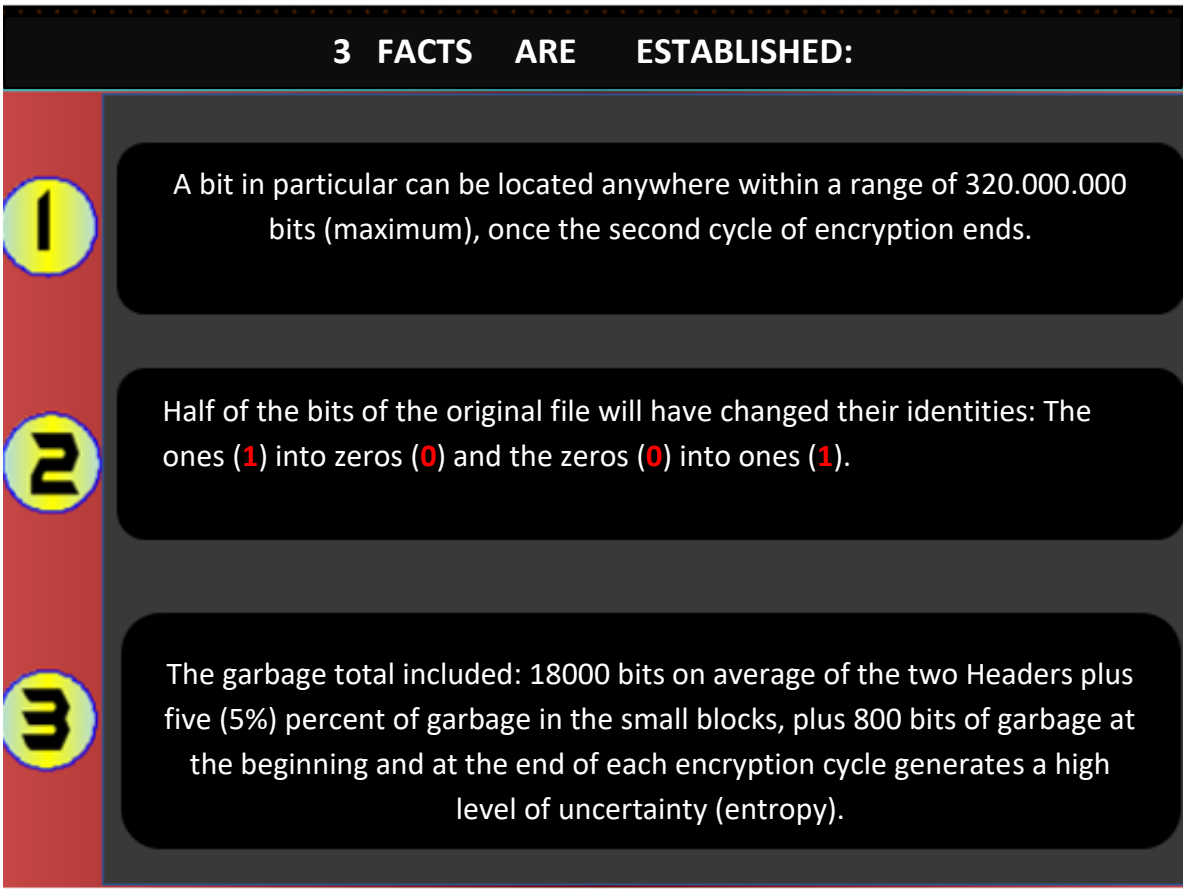
- In the beginning, the word "**CYPHERTOP**" is inserted which will function as a file identifier to avoid being catalogued by the network servers as a possible container of viruses or malwares, this word is overwritten over the initial "garbage".
- The field for the validation of the DNA is added, through which the decoding routine of Cyphertop certifies that the correct DNA will be used.
- In the last field of the Header apart from the length of the file to be processed in this cycle, the original name of the file that is being coded is included.

Thus, the five general steps that are performed in the first cycle become seven:

1. **N** bytes (**N** is a number dependent on the DNA used) of garbage information are inserted. That is, bytes produced randomly.
2. The first nine bytes of the garbage are overwritten with the word "CYPHERTOP".
3. Next, fields CT1 and CT2 are inserted which are the tridimensional locks and are the ones that contain information that will help to insert the second five modifying numbers within the next field (**CI**).
4. Field CI is built which is composed of 1.000 or more bytes of garbage information that will be used to insert the second five modifying numbers in them.
5. The result of a hash practiced over the DNA is inserted with which it is being encrypted, so that the receiver (decoding routine of Cyphertop) can validate such DNA and avoid a decoding process with the wrong DNA.
6. Then **K** Bytes of garbage information is inserted, where **K** is a value that depends on the information that has been introduced previously in the field **CI**.
7. Finally, the length of the resulting file of the first cycle of encryption and the original name of the file that is being encrypted is inserted.

It is worth noting that each encryption is different in length and content because of the action of the modifying numbers which, as the name indicates, modify the DNA of the pair of users that are sharing it (connection point), each time a file is encrypted. Quality that makes CYPHERTOP the only non-automorphic algorithm in time, or seen another way: that develops different encryptions for the same original file, which is equivalent to producing the results of applying different encryption algorithms on each occasion that the same file in encrypted. (Encryption meta-algorithm).

To conclude:



ADVM Security Software S.A. Panamá City, Panamá.