# Twincodes, A New Encryption Algorithm

A. Hemmati

Cryptography, maybe a familiar but is specialized word that have you heard even been for once in your life. A science that you use it hundreds of times a day without knowing it in the background of your daily life, and perhaps our everyday life is somehow affiliated with it. Bank cards, social networking messages, computer systems and cell phones that fit in our hands for hours, and much other of our digital life, all have a very strong affiliation to cryptography. Cryptography means science and art turning and hiding information.

Until today, many cryptographic algorithms have been developed to protect our digital life, but only a small number of them are standardized and used. The design of cryptographic algorithms is a topic for mathematical professionals and is created based on mathematical techniques. Although is a specialized area with complex terms and concepts, but understanding them is not so difficult and impossible too.

Claiming the creation of a new cryptographic algorithm without a general criticize and review is difficult and in vain. Therefore, in this essay, we present a new cryptographic algorithm that outside of specialized and complex discussions in the form of a mathematical game and minimalist form, is presented in several stages.

The algorithm can encrypt all digital data inside a hard disk (beyond its type and format) over the following 10 steps. Regardless of the very limited specialized discussions, it is very easy that with follow the steps, test the algorithm on a paper based on fictitious binary information, which is more like a mathematical game than a complex mathematical formula.

1. Recall the desired file from the hard drive and extract it as binary

2. arranging the extracted bits in groups of 10 members, it is normal that the last group will not have two modes more, or 10 or fewer than 10 members

3. Formation Table 1 consists of 1026 columns:

twincodesworld

3.1. The column header of the first column, with the name of the steps, will show the number of each step

3.2. 1024 The next column contains 2^10 modes of a combination of 10 bits, each of which is written in a column header

3.3. The last column corresponds to the last group, in the second stage

4. Formation Table 2 consists of 1025 columns:

4.1. The column header of the first column, with the name of the steps, will show the number of each step

4.2. 1024 The next column can be either similar to Table 1 or any header columns numbering with 1 to 1024, each with its own advantages as described below

5. At this stage, the groups created in Step 2 are arranging respectively in Table 1. Of course, the first group will be list in Table 1, because is not the duplicate group.

To do this, the members of the group are compared to the columns in Table 1 and the group 1 is marked under the same column, with the number 1.

The subsequent groups are also compared in this way and listing from 2 to 1024 below each column.

The duplicate groups will be registered in Table 2, and so, we will only record 1024 non-repetitive first groups at this stage. We will not do anything (for now), with groups beyond 1024th non-repetitive group, except the last group.

The last group, as mentioned, has 10 or fewer members. If the group was complete, the last column (1026th column) will be empty but if it was less than 10, exactly the members of this group would be registered under 1026th column.

6. As mentioned in Step 4, the table can have two modes. If the table is like Table 1, the duplicate groups that we had between non-repetitive groups in Step 5 are recorded based on the position number in Step 2. (Similar to step 5, the members of the groups are compared to the columns and its numbers will be recorded under the same column. Obviously, each column may contain several numbers that must be separated by commas.)

If the second mode is selected, the table 2 will be dependence to Table 1, and the numbers from 1 to 1024 will be the numbers of same non-repetitive groups as

twincodesworld

those listed in Table 1. Therefore, duplicate groups should be arranged according to Table 1 and recorded in Table 2, in the same way as mentioned above.

7. Up to this stage, we have produced 2 keys, which are same the tables 1 and 2. At this point, we continue with the remaining groups after the 1024th non-repetitive group. Of course, all the remaining categories are duplicate, so each of them in Table 1 has a number that has already been registered. Instead of each group, the corresponding number is replaced.

The alternate numbers are separated by a comma and stored in a text file at the specified location of the hard drive.

Regardless of the type and file encoding, these numbers are very important in the decryption stage.

8. Re-run the seven previous steps for the new saved file (in step 7), with this difference that new tables 1 and 2 are not created and only one new row is added to the existing tables

9. This repeat loop continues until we cannot create 1024 non-repetitive groups. At this point, the numbers obtained in the last possible loop from step 7 without a comma between them are stored in a file and released as the final file. The position of the deleted commas as the 3rd key is stored in a separate file.

10. The process of return or decryption is also very simple, and it is sufficient that respectively from the last step, replace the keys to restore the original file (The steps are easily and completely reversible, so there is no need to explain). Pay attention that the file format and the original file name must be recorded from the beginning to be retrieved at the end, because the final file format result from encryption will completely different from the original file.

This algorithm is very flexible and can be generated with n-bit combinations. This means that instead of using 10 bits, you can use any number in the bits grouping. So, both the algorithm itself and the final file can be considered as a key.

Although the world of encryption algorithms is a world full of mystery and complexity, but the current algorithm, out of all the complexities of this virtual world, is trying to join the world in a simpler way and play a role. As a result, though, this algorithm may not be as powerful as the other existing algorithms,

twincodesworld

but it can provide the flexibility and complexity of cryptography with proper development. It is hoped that criticism and attention will be made and its bugs and possible errors will be resolved.

**http://www.twincodesworld.com/**

twincodesworld