# A NEW CHARACTER ENCRYPTION ALGORITHM

**SCRIPCARIU Luminița[1]*, FRUNZĂ Mircea Daniel[1]**

[1]Communications Department, Technical University "Gh.ASACHI", Iaşi, ROMANIA
Bd. Copou 11, CP 700506, E-mail: luminita.scripcariu@gmail.com

## ABSTRACT

Secure communications involves the use of different cryptography methods [1]. A new, fast and secure character encryption algorithm (CEA) is proposed in this paper. CEA uses polynomial invertible functions defined on Galois Fields (GF) [2], with encryption keys as long as the message itself generated from chaotic signals [3]. Simulations are made and the performances of the CEA are analyzed based on the Matlab version of CEA.

**Key words**: cryptography, algorithm, encryption key, chaos, security.

## INTRODUCTION

Special encryption algorithms could be designed exclusively for text transmission.

The character encryption algorithm CEA can be applied for text encryption in different digital communication systems (i.e. encoding the short written messages SMS transmitted on digital mobile phones). The coding rate is 1:1 and the transmission rate is not modified.

The user password, consisting in a short string of $N$ characters, is the secret key used to initialize the chaotic system which generates the encryption key. The same password must be introduced by the receiving person for message decryption.

The encryption key is randomly generated, without any periodicity, as long as the message, using the following logistic function for the chaotic number generator [3]:

$$x_{k+1} = Rx_k(1 - x_k), k = 0,1,2\ldots, x_k \in (0,\ 1),\ R \in (0,\ 4), x_0 \neq 0. \quad (1)$$

The initial decimal value could be any number between 0 and 1. It results by decimal-to-binary conversion of the 8-bit ASCII (American Standard Code for Information Interchange) code user password:

$$x_{0(2)} = \overline{0, p_0 p_1 \ldots p_{8N-1}},\ p_i \in \{0;1\}, i = \overline{0,\ 8N - 1} \rightarrow x_{0(10)} \in (0,\ 1). \quad (2)$$

The chaotic signal is sampled with a sample period of $T$ samples and quantized on the necessary number of levels in order to obtain the key-sequences ( $k_1, k_2, k_3$ ) as integer strings.

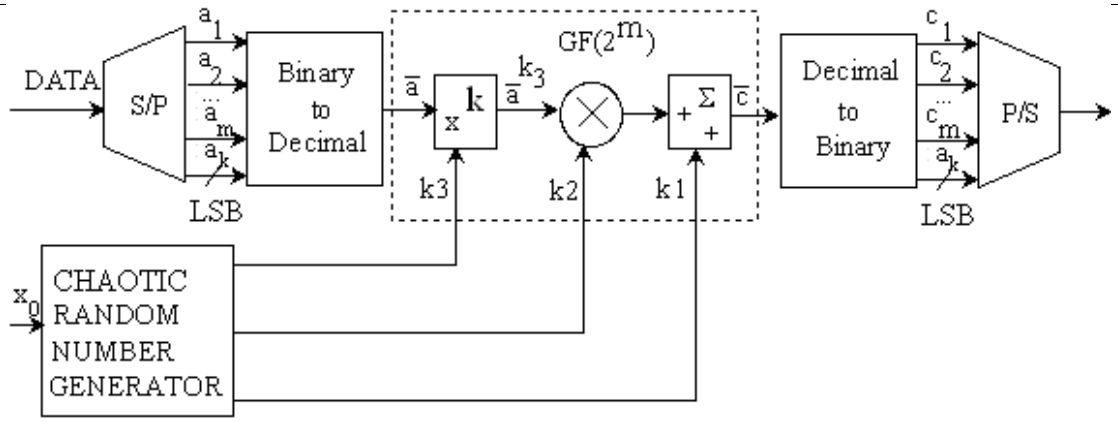


Figure 1. The principle of the Encryption Method

Each character is selectively encoded on the *m* most significant bits (MSB) of its 8-bit ASCII code ($a_1, a_2 \ldots a_m$). The least significant bits (LSB) are transmitted without being coded. The resulting data vector $\bar{a} = \overline{a_1 a_2 \ldots a_m}$ is an element of the definition field GF ($2^m$).

A class of 3-parameters polynomial invertible functions defined on a GF, with *m*-bits symbols [2], is applied on each data block with a special set of parameters (Figure 1):

$$E_{\bar{k}}(\bar{a}) = \bar{c} = k_1 + k_2 \bar{a}^{k_3}, k_2 \neq 0, k_3 \neq 0 \ , \ k_3 \neq 2^m - 1, \bar{k} = [k_1, k_2, k_3]. \quad (3)$$

The inversed functions, defined on the same GF, have the following expression:

$$E_{\bar{k}}^{-1}(\bar{c}) = \left| k_1^{-1}(\bar{c} + k_0) \right|^q \quad (4)$$

The inverse key component *q* verifies two conditions:

$$(\bar{a}^{k_2})^q = \bar{a} \ ; \quad (k_2 \cdot q) \bmod (2^m - 1) = 1 \quad (5)$$

The element *q* exists for all $k_2$ values if and only if *m* and $2^m$-1 are prime numbers.

## EXPERIMENTAL

We implemented the CEA in Matlab and used it to encrypt different texts, with the following parameters: $N = 6, m = 3, R = 3.9, T = 100.$ The plain text is processed as a serial decimal data stream. The most significant *m* bits of each 7-bit character code are converted binary-to-decimal to obtain the element $\bar{a}$ of the GF and the chaotic system generates the encryption function parameters-vector $\bar{k}$. The polynomial function is applied on $\bar{a}$ using the arithmetic operations (addition, multiplication) defined on the GF. The encoded bits are concatenated with the LSB bits of the original character in the binary codeword. Finally, the binary-to-character conversion is made and the encrypted text results.

## RESULTS

Some 8-bit ASCII encoded texts are used for algorithm testing. Different parameters of the original text and of the encrypted one are considered: the total number of characters (L), the mean value (M), the standard deviation (STD), the maximum value of the process histogram (HIST.MAX) and the maximum value of the normalized cross-covariance function between the plain text and the encrypted one (XCOV.MAX) (Table I).

TABLE I. ALGORITHM TEST RESULTS ON DIFFERENT TEST-FILE

| File Name | L | Plain Text | | | Encrypted Text | | | XCOV. MAX |
|---|---|---|---|---|---|---|---|---|
| | | M | STD | HIST. MAX | M | STD | HIST. MAX. | |
| File_E.txt | 15381 | 91.83 | 31.99 | 2389 | 124.87 | 73.37 | 128 | 0.0331 |
| File_R.txt | 13982 | 87.15 | 35.31 | 1863 | 126.26 | 73.36 | 103 | 0.0422 |
| File_E.doc | 49152 | 53.92 | 68.39 | 22876 | 127.11 | 74.42 | 145 | 0.0097 |
| File_R.doc | 99840 | 39.51 | 64.08 | 56724 | 127.37 | 74.23 | 196 | 0.0115 |

The histograms of the original and the encrypted character strings of the test file *File_E.txt* are represented in figure 2.

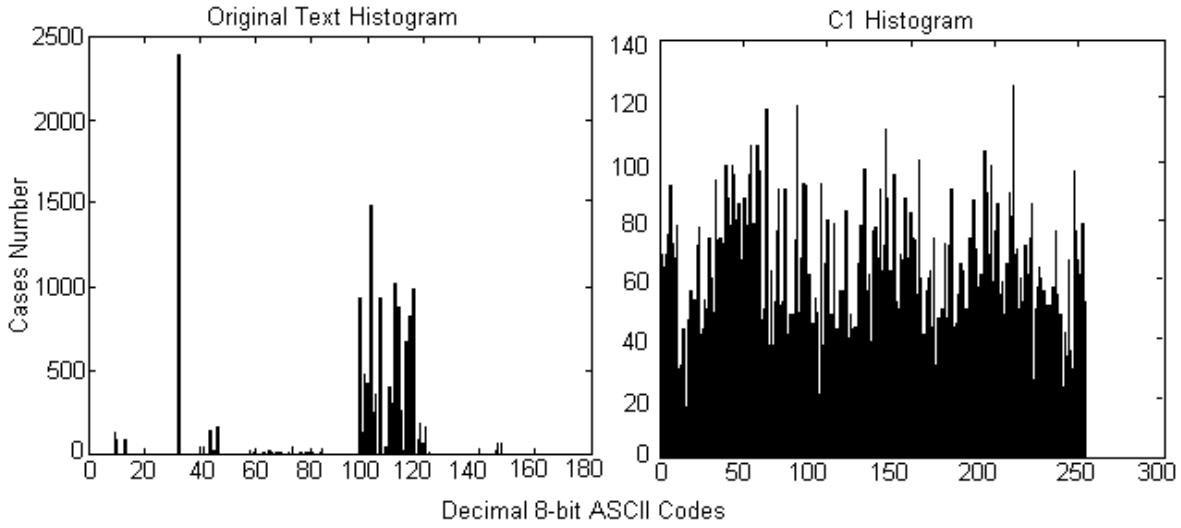


Figure 2. Original and Encrypted Text Histograms for File_E.txt

## DISCUSSION

The proposed encryption algorithm modifies the probabilistic distribution of the initial character set. Near-uniform distributed characters in the encrypted frame result. The mean and the standard deviation values of a uniform distributed 7-bit ASCII codes are equal to 127.5 and 74.045. The maximum values of the cross-covariance between the original and the encrypted vectors are very small.

The same chaotic random number generator is used for decryption. The chaotic system is very sensitive to the initial state so any unmatched character string will not be able to decrypt the

message. The tests reveal that the CEA is secure and fast. It works with a reduced capacity of memory and a great diversity of encryption keys.

## CONCLUSIONS

CEA is comparable as robustness with the classical encryption systems. The encoding time is hardly decreased using a chaotic system to generate the encryption keys. This algorithm is deduced from the more complex image encryption algorithm (IEA) [4] also based on polynomial invertible functions defined on GF. The robustness of CEA is ensured by the high diversity of the encryption key which is as long as the message itself and by great sensitivity of the chaotic random number generator to the initial condition deduced based on the secret user password. The CEA algorithm could be implemented using different programming languages such as C++ or Java.

## ACKNOLEDGMENT

This paper is a result of the research grant accorded by CNCSIS-MECT (Romania): "Development of new data encoding algorithms to increase the security and ensure the information integrity on digital communication networks"(2005).

## REFERENCES

[1] Schneier B. 1996, "Applied cryptography", second edition, NY: John Wiley & Sons, Inc.
[2] Scripcariu L. and Duma P. (2004), "Analysis of Simple Invertible Functions Defined on Galois Fields for Cryptography Use", Trans. on Electronics and Communications, Vol. 49 (63), Fasc. 2, 2004, ISSN 1583-3380, Ed. POLITEHNICA Timisoara (Romania), pp.55-59.
[3] Luca A. and Vlad A. 2005, "Generating Identically and Independently Distributed Samples Starting from Chaotic Signals", In Proc. of the Intern. Symposium on Signals, Circuits and Systems ISSCS 2005, July 14-15, 2005, Vol.1, Iasi, Romania, pp. 227 - 230.
[4] Scripcariu L. and Frunza M.D. 2005, "A New Image Encryption Algorithm Based on Invertible Functions Defined on Galois Fields", In Proc. of the Intern. Symposium on Signals, Circuits and Systems ISSCS 2005, July 14-15, 2005, Vol.1, Iasi, Romania, pp. 243 - 246.