FACTA UNIVERSITATIS (NIŠ)
SER.: ELEC. ENERG. vol. 16, Aug. 2003, 251-258

Novel Method of Discrete Message Ciphering with Equal Length of Message and Cryptogram

Miloš Bandjur

Abstract: Systems for ciphering contain substitution or transpositions or combination of both. The goal of the present work is to suggest the new cipher that belongs to substitutional ciphers with constant cryptogram length, where cryptogram length is equal with message length. Cipher system suggested here is new and belongs to perfect cipher class regarding the aspect of reliability, as will be shown.

Keywords: Signal processing, cryptogram, cipher system, probability of message.

1 Introduction

Since computers are taking over area of exchanging information of all kind, cipher coding of data today widely exceed it's classic manner of use and becomes highly connected with the term of human rights. Code for message enciphering must meet the following criteria:

1. Cryptogram length must not be much longer from original message,
2. Encipher and decipher must be both fast enough and
3. Anyone unauthorized who wants to discover the cipher must put a considerable amount of time and work in to that process.

Basically, cipher system can contain either substitution or transposition or combination of both [1,2,3,4,5,6].

Manuscript received February 17, 2003.
The author is with the Faculty of Technical Science, University of Priština, K. Mitrovica, Serbia and Montenegro.

2 Definition, Organization and Basic Parameters of Cipher System

Since detail analysis of cipher system parameters is subject of lot of published work [1,2,3,4,5,6,7], in present work we will introduce only the definition and meaning of those parameters that are necessary for qualitative analysis of suggested cipher system. Figure 1 shows the general structure of cipher system.

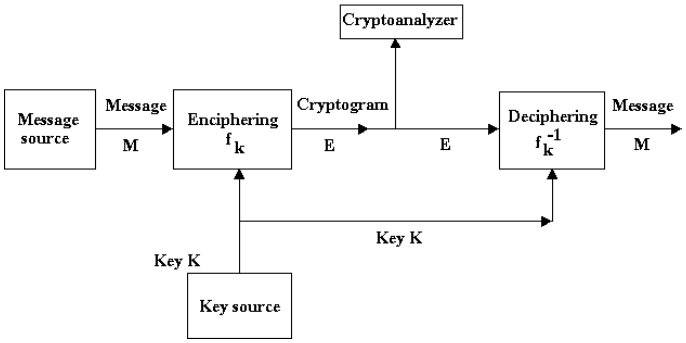

Fig. 1. General structure of cipher system.

Transmitter side generates message M. We apply encipher operator on M to obtain cryptogram E. This operator depends on additional parameter K called key so that

$$E = f_k(M) \tag{1}$$

where f_k is encipher function. We transmit cryptogram E to user who also know the key. Then user apply decipher operator f_k^{-1} to obtain M so that

$$M = f_k^{-1}(E) \tag{2}$$

Someone, who is unauthorized user, can get and analyze cryptogram. But he doesn't know the key and therefore he can't apply f_k^{-1} without determining the key K first. We assume that optional method of key determining depends only of number of cryptograms E that have been caught. In that case, key estimation $\overline{K}$ is function of E i only, and therefore message M estimation is also function of E only. So we can say that

$$\overline{M} = g(E) \tag{3}$$

where g denotes operator used for cryptogram analysis. Encipherer try to make such a system with whom he can with large probability obtain $\overline{M} \neq$

M. Cryptogram analyzer try to apply operator g, which will maximize the probability of $\overline{M} = M$.

By cipher reliability we mean:

1. how much is the system insensible to cryptanalysis if the one who is doing it has unlimited time, and all the necessary equipment,
2. can cryptanalyst, no matter of spent time, get unique solution of caught cryptogram, and if not how many logical solutions exist. Equivocal zeroes demand that one message has probability equal to one, and all the others zero, i.e. cipher system is known,
3. is there a system that never gets unique solution no matter of number of caught cryptograms.

In general case encipher is reliable if cryptogram can be revealed only after caught material (number of caught cryptograms) is considerably greater than unique distance. By unique distance we understood minimal amount of encrypt material necessary for getting unique solution of cryptogram. If caught material is of the same order or shorter than unique distance, cipher is bad. Cipher systems where the necessary number of cryptograms is greater than unique distance are: perfect cipher system, ideal cipher system and strictly ideal cipher system.

Perfect reliability of cipher is defined by condition that a posteriori of probability are equal with a priori probabilities independently of their values[7,8,9]. In this case caught cryptograms won't give any information to cryptanalyst. Necessary and sufficient condition for perfect cipher is given by following expression

$$P_E(M) = P(M) \tag{4}$$

where $P_E(M)$ is a posteriori probability of message M if cryptogram E is caught, and $P(M)$ is a priori probability of message M.

For ideal reliability $H_E(K)$ and $H_E(M)$ are not approaching to zero if $N \to \infty$, N is number of caught cryptograms.

For strictly ideal reliability, $H_E(K)$ and $H_E(M)$ remains constant if $N \to \infty$. Here $H_E(K)$ represent conditional entropy of key and $H_E(M)$ conditional entropy of the message. We agree to call these conditional entropies 'equivocal' of key and 'equivocal' of message respectively.

Ideal encode systems have following deficiencies:

1. System has to be closely adaptable to language (that demands intensive study of language structure, because changes in statistical structure in group of possible messages make system easily for analysis.

2. Structure of natural languages is extremely complex and this means complexity of required transformations for redundancies elimination.

3. Generally transformations make spreading out worse. Error in one symbol transmitting produces errors in area surrounding that symbol, which is comparable with length of statistical effects in original language.

3 Proposed Cipher System

3.1 Organization of proposed cipher system

Suppose that DSWM generates messages, where each of them is represented by n binaries symbol. All 2^n different messages that can be generated from given source, forms code ring C where messages are in optional order. To messages organized in such a way positions from 1 to 2^n are given, in manner that first position is given optionally, and the others are given rising position in clock-wise direction regarding the first one. Position of the message is written in inner band angle segment of code ring, while the corresponding content is written in the outer band of the same segment as is shown in Figure 2.

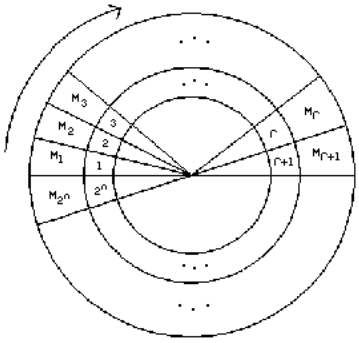

Fig. 2. Code ring C.

If we take account only mutually (relative) position of messages regardless their absolute position, described method can form N_c different code rings i.e.

$$\{Ci\}, i = 1, 2. \ldots, N_c \tag{5}$$

Each key $K_b \in \{Kb\}$, $b = 1, 2, \ldots, B$ that key source can generate, forms pseudo noise (PN) series $c_b(k)$ and group of start positions $\{P_j\}_b$ for the group of code rings $\{C_j\}_b$ which are used in encoding procedure with given key, where $\{j\} \subseteq \{i\}$ i.e. $\{C_j\}_b \subseteq \{C_i\}$.

Series $c_b(k)$ has as many different members as group $\{C_j\}_b$ has elements. Element $P_j \in \{P_j\}_b$ takes one of 2^n possible values from group $\{1, 2, \ldots, 2^n\}$, and determines the starting position on code ring C_j from $\{C_j\}_b$, while series $c_b(k)$ determines order of circle rings from group $\{C_j\}_b$, which will be used for encoding of successive generated source messages in given transmission. Figure 3 shows the proposed structure for enciphering.

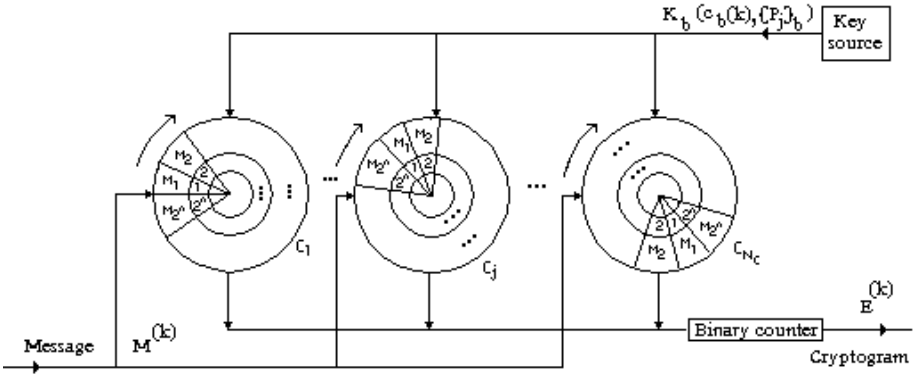

Fig. 3. The proposed structure for enciphering.

For chosen key K_b, messages encipher is performed so that message content that source generated in moment t_k, $M(t_k) = M^{(k)}$, where $M^{(k)} \in \{Mr\}$, $r = 1, 2, \ldots, 2^n$, is compared with content on starting position of code ring $C(t_k) = C^{(k)}$, $C^{(k)} \in \{Cj\}_b$, which is determined by member $c_b(t_k) = c_b^{(k)}$ of series $c_b^{(k)}$. For $C^{(k)} = C_j$, starting position is determined by P_j from $\{P_j\}_b$, in case that code ring C_j is used for the first time for encoding in current message transmission. In case that code ring C_j has already been used for encoding, starting position is one where is found content identical to content of source message in last usage of code ring in current transmission.

If $M^{(k)}$ is identical to content on starting position $C^{(k)}$ condition (state) of binary counter, that counts fail comparisons, will be unchanged, and code word contains n zeros. If mentioned contents are not identical, binary counter registers one fail comparison, and content of message $M^{(k)}$ is compared with content on following position, which is neighbor in clockwise direction. If those two contents are not identical, binary counter registers one more fail comparison and message content is compared with the follow-

ing (right one) content of the same code ring etc.; until on given code ring content is found which is identical to content of $M^{(k)}$ source message.

Code word is described by state of binary counter which registries fail comparisons. As this method presents content of $M^{(k)}$ with binary equivalent of number of fail comparisons $m^{(k)}$, that takes one of 2^n possible values from group $\{m_0 = 0, m_1 = 1, m_2 = 2, \ldots, m_{2^n-1} = 2^n - 1\}$, it is clear that message and cryptogram both have same length of n bits.

For decipher it is necessary that receiver (receiving side) has identical group of code rings $\{C_j\}_b$ (generally $\{C_i\}$, $i = 1, 2, \ldots, N_c$), identical key source K_b ($c_b^{(k)}$ and $\{P_j\}_b$), and it has to be in synchrony with transmitter (transmitting side).

For received cryptogram $E^{(k)}$, generator of pseudo noise series of receiver generates $c_b^{(k)}$, which from group $\{C_j\}_b$ activates circle ring $C^{(k)} = C_j$, identical to one which is used for message $M^{(k)}$ encoding in transmitter. Decoding (counting of positions) will start from the position on code ring from which the encoding process in transmitter began itself.

3.2 Analysis of proposed system quality

Realization of number of fail comparison $m^{(k)}$ can be described with following relations

$$\begin{aligned}
(m^{(k)} = m_0) &= (M_1, 1) + (M_2, 2) + \cdots, +(M_{2^n}, 2^n) \\
(m^{(k)} = m_1) &= (M_1, 2^n) + (M_2, 1) + \cdots, +(M_{2^n}, 2^n - 1) \\
&\vdots \\
(m^{(k)} = m_p) &= [M_1, 2^n - (p-1)] + [M_2, 2^n - (p-2)] + \cdots, \\
&\quad + [M_{2^n}, 2^n - p] \\
(m^{(k)} = m_{2^n-1}) &= (M_1, 2) + (M_2, 3) + \cdots, +(M_{2^n}, 1)
\end{aligned} \tag{6}$$

This means that $m^{(k)} = m_p$ will be realized if the content of source message $M^{(k)}$ is identical, on code ring $C^{(k)} = C_j$, with content of M_1 for starting position for comparison equal $2^n - (p-1)$; or identical with content of M_2 for start position $2^n - (p-2)$; or identical with content of M_2^n for start position $2^n - p$.

We can see that realization $m^{(k)} = m_p$ is complex event whose probability $P(m^{(k)} = m_p)$ can be described by following relation

$$\begin{aligned}
P(m^{(k)} = m_p) &= P[M_1, 2^n - (p-1)] + P[M_2, 2^n - (p-2)] + \cdots, \\
&\quad + P[M_{2^n}, 2^n - p]
\end{aligned} \tag{7}$$

$$P(m^{(k)} = m_p) = P(M_1)P[2^n - (p-1)/M_1] + P(M_2)P[2^n - (p-2)/M_2] + \cdots, + P(M_{2^n})P[2^n - p/M_{2^n}] \tag{8}$$

Since $P(1) = P(M_1)$, $P(2) = P(M_2)$, ..., $P(r) = P(M_r)$, ..., $P(2^n) = P(M_{2^n})$ if messages are equally probable we have

$$P[2^n - (p-1)/M_1] = P[2^n - (p-2)/M_2] = \cdots = P[2^n - p/M_{2^n}] \tag{9}$$

$$P(m^{(k)} = m_p) = P(M_1)\frac{1}{2^n} + P(M_2)\frac{1}{2^n} + \cdots + P(M_{2^n})\frac{1}{2^n} = \frac{1}{2^n} \tag{10}$$

Expression (10) shows that for $m^{(k)}$ all possible values of m_p are equally probable, with probability of $1/2^n$, therefore result is that proposed method belongs to perfect cipher system class, with all the attributes this class possess.

4 Conclusion

Cipher codes with constant length of cryptogram are easier for implementation, but also more easier for cryptanalysis relating to code with uneven length. Cipher code proposed and analyzed here, is not only of constant length, but also the length of cryptogram is equal to message length, and is shown to be member (concerning the aspect of reliability) of perfect cipher class.

The problem of synchronizing and practical realization of proposed method is not analyzed here, and will be subject of further research.

Acknowledgment

The author wish to thank to Dr. Milorad Mirković, professor on Faculty of Technical Science in K. Mitrovica, for his helpful suggestions in improving the paper.

References

[1] R. A. Mollin: *An Introduction to Cryptography.* Chapman & Hall, CRC Press, Boca Ration, 2001.

[2] K. H. Rosen: *Elementary Number Theory and Its Applications.* Addison-Wesley, Reading, 1993.

[3] W. Trappe, L. C. Washington: *Introduction to Cryptography with Coding Theory.* Prentice Hall, Upper Saddle River, 2002.

[4] N. Smart: *Cryptography. An Introduction.* McGraw-Hill, New York, 2002.
[5] D. R. Stinson: *Cryptography. Theory and Practice.* CRC Press, Boca Ration, 1996.
[6] N. Koblitz: *A Course in Number Theory and Cryptography.* Springer-Verlag, New York, 1995.
[7] A. Petho: *Algebraische Algorithmen.* Vieweg, Braunschweig, 1999.
[8] George I. Davida, Timothy J. Mahar, John B. Kam: *Design and Analysis of a class of ciphers.* The University of Wilkinson Milwaukee, December 1975.
[9] F.L. Bauer: *Decrypted Secrets. Methods and Maxims of Cryptology.* Springer-Verlag, Berlin, 2000.