IPASJ International Journal of Electronics & Communication (IIJEC)
Web Site: http://www.ipasj.org/IIJEC/IIJEC.htm
A Publisher for Research Motivation ..... Email:editoriijec@ipasj.org
Volume 6, Issue 4, April 2018 ISSN 2321-5984

# CRYPTOGRAPHIC METHODS AND MEANS PROTECTION TRANSMITTED INFORMATION IN TELECOMMUNICATION SYSTEMS

**Bayram G.Ibrahimov[1] , Ramiz T.Humbatov[2], Arif H. Hasanov[3], Rufat F. Ibrahimov[4]**
Azerbaijan Technical University[1]
Military Academy of the Republic of Azerbaijan[3]
Institute of Control Systems NASA[2, 4]

**ABSTRACT**

***Methods transmission and means cryptographic protection information from unauthorized access to the subscriber and network communication line are considered. A cryptographic method and means protecting transmitted information in telecommunication systems are proposed, which are based on the information-theoretic method coherent network coding and the method of message encryption.***

**Key words:** algorithm, cryptographic protection, coding, information protection, cryptography.

## 1. INTRODUCTION

In the modern telecommunication space, the emergence new types multimedia traffic and guaranteed quality its servicing using the architectural concept NGN requires the creation new methods and means cryptographic protection information from unauthorized access to the subscriber line in communication systems that ensure the security of the transmitted information of mixed type [1, 2].

The security modern information and communication systems is inextricably linked with algorithms that ensure the confidentiality and integrity of the stored and cryptographic stability of the transmitted information mixed type, as well as the identification and authentication functions. The cryptographic strength these algorithms is based on the computational complexity solving some problems in the telecommunications system, which is becoming increasingly important [3].

In [3-5] the classification of cryptographic methods information transformation is analyzed and attention is paid mainly to algorithmic methods protecting the transmitted information. In [ 6 - 8], the security communication systems and the protection of information from unauthorized access to the subscriber line were considered and a scheme for connecting the terminal security device "Password" with the coding of the subscriber line was proposed.

Given the foregoing studies information security, there is an important issue - the study of effective cryptographic algorithms, methods and means protection transmitted information of mixed type that provide solutions to the most important security problems in the telecommunications system. Mixed type information means documentary message, information and graphic file, voice traffic, and also facsimile messages.

In this paper, we consider the solution to the above-stated problem - the creation of a cryptographic method and a means protecting the transmitted information mixed type, which make it possible to ensure the transmission and cryptographic protection of information in telecommunication systems (TS).

## 2. GENERAL STATEMENT OF THE PROBLEM

It is known [8-10] that the task cryptographic protection transmitted information mixed type in a telecommunication system was investigated with a certain method of message transmission and with a certain scenario of hacker's actions. In all the cases described here, the telecommunication system is represented as a cyclic directed graph. In the general case, the distributed communication system and its network topology are considered, which are specified in the form of a graph:

$$Q = [V_j, E_k] \ , \quad j = \overline{1, N_{uz}} , \quad E_k = 1, 2, ..., N_k \ , \tag{1}$$

where $V_j$ – multiple nodes of the network link using dynamic routers and и $V_j = 1, 2, ..., v_j$ ; $E_k$ – a number of communication channels (CC) and и $E_k$ = (ke, kd).

IPASJ International Journal of Electronics & Communication (IIJEC)
Web Site: http://www.ipasj.org/IIJEC/IIJEC.htm
A Publisher for Research Motivation ..... Email:editoriijec@ipasj.org
Volume 6, Issue 4, April 2018 ISSN 2321-5984

On the basis the system-technical analysis, the mathematical formulation of the task of the proposed cryptographic method and the means for protecting the transmitted information from unauthorized access to the subscriber and network communication lines for evaluating the effectiveness of the cryptographic strength methods and means information protection is described by the following objective functions:

$$E_{EF} = W[\arg\max_{i}(D_{i.\max})], \quad i = \overline{1,n}\ , \tag{2}$$

under the following restrictions

$$E[T_{i.m.dt}] \le T_{i.m.dt.av}\ , C_a \le C_{a.av}\ , \eta_i \le \eta_{i.av.} \quad , \tag{3}$$

where $T_{i.m.dt.}$ – the mean delay time for the transmission of the *i*-th message stream; $D_{i.\max}$ – the maximum value of the time period necessary to perform the decryption operation by an attacker when protecting *i*-th information from unauthorized access to subscriber lines; $C_a$ – cost hardware and software cryptographic information security system; $\eta_i$ – coefficient effective use network resources of the transmission and protection information in the transmission of the *i*-th message stream; $T_{i.m.dt.av.}, C_{a.av.}$ *and* $\eta_{i.av.}$ – respectively, the permissible value of the mean delay time, the cost of hardware and software and the coefficient of effective use of network resources of the transmission and protection of information in the transmission of the *i*-th message flow

Expressions (2) and (3) define the essence of the cryptographic method under consideration and the means for protecting information in the TS and are one of the important indicators of the cryptographic strength of the system when communicating information of a mixed type through communication channels.

To solve this problem, we propose a cryptographic method and means for protecting the transmitted information mixed type in the TS, taking into account the features of the transmission methods, crypto protection algorithms, and information-theoretic methods for encoding the transmitted message over communication channels

## 3. SCHEME FUNCTIONING OF THE RESEARCHED LINK AND MEANS CRYPTOPROTECTION

Based on the system analysis [3], the process of protecting information of a mixed type from unauthorized access to the subscriber line is proposed to be carried out according to the scheme presented in Fig.1. It provides for the protection of transmitted information using an open and secret key.

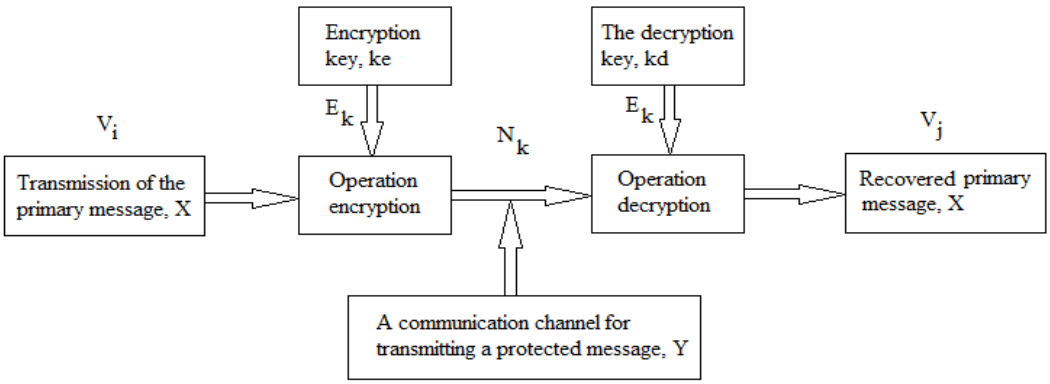


**Figure1.** Structurally functional scheme information protection from unauthorized access to the subscriber and network communication line

To ensure the secrecy-unavailability of the structure of the TS in the transmission of information over the communication channel, the most effective and promising methods are the network coding method and the encryption method [3, 6, 9, 10].

The use of public and private keys, which determine the specific secret state of certain parameters of the algorithm for cryptographic information transformation, protects the information, provides the choice of one variant from the set

IPASJ International Journal of Electronics & Communication (IIJEC)
Web Site: http://www.ipasj.org/IIJEC/IIJEC.htm
A Publisher for Research Motivation ..... Email:editoriijec@ipasj.org
Volume 6, Issue 4, April 2018 ISSN 2321-5984

of all possible for the given algorithm [3, 7]. The key used by us is usually external with respect to the algorithms for encryption and decryption of information of mixed type, which determines the specific type of encrypted message Y in the presence of this initial message X.

In the proposed scheme (figure 1), the secrecy of the telecommunications system is provided by means of an encryption key and decryption key.

It should be noted that the secrecy of modern cryptographic protection algorithms for information intended for a wide range of users is the use of a combination of numbers from the set of possible individual for each user or a pair of users, called the key [3, 8].

## 4. ANALYSIS AND CREATION OF THE CRYPTOGRAPHIC METHOD INFORMATION PROTECTION

In order to create cryptographic method and means protecting transmitted information from unauthorized access, a functional process protecting information mixed type is considered.

It follows from the algorithm figure 1 that the block diagram of the protection information from unauthorized access to the subscriber line represented by the functional unit is a cryptographic means protecting the transmitted information.

Based on the transmission and protection of information scheme, a cryptographic method for protecting transmitted messages using algorithms public key cryptographic system and the RSA method (named after the initial letters of the names its inventors Rivest, Shamir & Adleman).

On the basis figure 1, in order to use the RSA algorithm, you must first generate the public and private keys, and execute the following procedures [2, 9]: 1.Select two very large prime numbers $p$ and $q$; 2. Define n as the result of multiplying $p$ by $q$, $n = p \cdot q$ and choosing a large random number $d$. It must be relatively prime to the result $(p-1)(q-1)$ and determine the number $e$, which is true the following relation:

$$(\{1 - ed \bmod [(p-1)\cdot(q-1)]\} = 0 \quad (4)$$

Here, are the public key of the numbers e and n, and the secret key is the numbers d and n.

To encrypt the above data on the known key $E_k(e,n)$, it is necessary to break the encrypted information of the mixed type into blocks, each which can be represented as the number $M(k) = 0,1,\ 2,\ ...,n-1$. Now we can encrypt information mixed type, considered as a sequence numbers $M(k)$ by the formula [7, 8]:

$$C(k) = M(k)^e \bmod (n) \quad (5)$$

In order to decrypt this data using the secret key $E_k(d,n)$, the following calculations must be performed:

$$M(k) = C(k)^d \bmod (n) \quad (6)$$

Thus, as a result, a set numbers $M(k)$ will be obtained, which is the initial information mixed type.

To protect the message from unauthorized access, some conversion of the original message is used $X$, called an encryption operation:

$$X = D_{kd}[Y]\ ,\ \ Y = E_{ke}[X]\ , \quad (7)$$

Taking into account (7) the process restoring the original message $X$ from the encrypted message $Y$, a decryption operation using the function $D_{kd}[Y]$ is applied, such an algorithm is described as follows:

$$D_{kd}\{E_{ke}[X]\} = X \quad (8)$$

It can be seen from (7) and (8) that cryptographic protection algorithms for information consist an operation encryption, transmission and decryption message using public key. From the point view of the content of the keys $kd$ and $ke$, all cryptographic protection algorithms fall into two broad categories: symmetric algorithms and public-key algorithms.

In this method and tool, symmetric algorithms are basically used that contain the same keys for encryption and decryption: $kd = ke$. The latter means that in the general case, the key can be calculated from a known value $ke$. Such algorithms are called, in addition, single-key, or algorithms with a private key [5].

## 5. EVALUATION OF THE CRYPTOGRAPHIC STABILITY OF THE METHOD INFORMATION PROTECTION

IPASJ International Journal of Electronics & Communication (IIJEC)
Web Site: http://www.ipasj.org/IIJEC/IIJEC.htm
A Publisher for Research Motivation ..... Email:editoriijec@ipasj.org
Volume 6, Issue 4, April 2018 ISSN 2321-5984

To increase the cryptographic stability of the information protection system, it is advisable to use the information-theoretic method, which is based on the statistical independence of the transmitted information mixed type $E_{ke}[X]$ from the original message from $X$. It is assumed that the average mutual information between random data is available to the attacker.

An important condition for decoding message using public key algorithm is that the encrypted messages arriving through communication channels to the recipient do not have to match if the original source messages are different, i.e.,

$$E_{ke}[X] \neq E_{kd}[Y], \quad ke \neq kd \tag{9}$$

Expression (9) is a public-key algorithm that uses a pair $ke$ and $kd$ keys to protect the message or the transmission channel, and $kd$ can not be acceptable for a given crypto attack level. The key $kd$ is an individual key or a private part of the key.

Taking into account figure 1 and features of the information- theoretic method and means, we assume that there are several subsystems consisting channels $N_k$ in the TS under investigation and an attacker has access to one these subsystems during one of the transmissions of the message through communication channels $N_k^{at.}$. Assume that for a given attacker and a subsystem with several recipients, the set conditions can be met.

Based on the information indicator of the source of the message, the algorithm for implementing the proposed method for protecting the transmitted information mixed type, the following condition can be obtained:

$$H(K) \geq (T_{cp.з} \cdot C_{\max} / N_k^{at.} - 1)^{-1} \cdot H(X), \tag{10}$$

where $N_k^{at.}$ – the number communication channels for the transmission information mixed type that is available to an attacker; $H(K)$ – entropy of the public and private key, $K \in ke, kd$; $C_{\max}$ – the maximum value of the throughput encrypted communication channels; $T_{cp.з}$ – mean delay time for message transmission from the beginning to the end of the path (End to end), $T_{m.dt.Vi} \rightarrow T_{m.dt.Vj}$); $H(X)$ – entropy information source mixed type and according to the definition K.Shannon is expressed as follows [3]:

$$H(X) = -\sum_{i=1}^{N} p(x_i) \ell og_m p(x_i)$$

where $p(x_i)$ – the probability various messages mixed type information, the number which is equal to $N$.

The obtained condition (10) contributes to providing the required level of protection of the transmitted information and determines the crypto stability of the telecommunication system using a symmetric algorithm for transmitting a message over the CS.

Symmetric algorithms are divided into streams that perform the current operation on the current bit of the stream, and block algorithms that implement information processing, divided into groups of bits, called blocks. These means protection and methods closing information are considered cryptographic methods that are widely used to protect voice messages in the TS.

However, the latter introduce a long delay in the processed information $T_{m.dt}$, with which in a number cases it is necessary to be considered, especially in the tasks protecting information from unauthorized access to the subscriber and network communication lines in the TS in the transmission of voice traffic.

One of the important indicators of the cryptographic stability information security system in the TS is the mean delay time $E[T_{i.m.dt.}]$ in the transmission of the *i*-th traffic. Taking into account the average time of the operation by the method encryption of the message, the transmission method and the particularity of the information-theoretic method network coding, mean delay time $E[T_{i.m.dt}]$ in general form can be determined by the following expression [11]:

$$E[T_{i.m.dt.}] = \frac{1}{N_{uz}} \sum_{j=1}^{N_{uz}} E[T_{ij.m.dt}(\lambda)] \leq T_{i.m.dt.av.}, \quad i, j = \overline{1, N_{uz}}, \tag{11}$$

где $N_{uz}$ – the total number j-th block-modular transmission systems in the information protection scheme; $\lambda$ – the intensity incoming transmitted voice traffic; $E[T_{i\,j.m.dt.}(\lambda)]$ – the mean time of the weighted delay from *i*-th to *j*-th

module-block transmission systems in the information protection scheme; $T_{i\,j.m.dt.av}$ – the allowable value is the mean delay time for the transmission voice messages and is equal $T_{i.m.dt.av} = (150,...,300)$ ms (on the Recommendation ITU-T, G.826).

In the information protection system, the random value of the delay time $T_{i.m.dt}$, taking into account all possible cryptographic operations, including the reliability of the transmission of voice traffic [3, 11], on one cycle should not exceed $T_{m.dt.av}(t_{\text{VT}})$, i.e.

$$P_{BER}\{[T_{m.dt}(t_{\text{VT}}) \le T_{\text{m.dt..av.}}(t_{\text{VT}})] \le 300\,ms\} \le (10^{-4},...,10^{-7}), \quad (12)$$

where $P_{BER}(\bullet)$ – bit error probability in the information security system during the transmission voice of traffic.

Expression (11) characterizes the cryptographic stability of the information protection system and the quality of the operation communication channels with wire-tap channel.

## 6. Conclusions

As a result of the research, a cryptographic method and a means protecting the transmitted information mixed type in telecommunication systems are proposed, using algorithms for the operation cryptographic encryption and network coding of the message.

A structural-functional scheme for protecting information from unauthorized access is proposed, which provides cryptographic stability of the information security system and high reliability the communication channel during encryption and coding of the voice message.

The conditions and analytical expressions are obtained, allowing to estimating the cryptographic stability of the information protection system in telecommunication systems.

## References

[1] Laqutin V.S., Petrakov A.P. Protection of the subscriber's teletraffic. M.: Energo-atomizdat. 2007. - 528 p.
[2] Olifer V.G, Olifer N.A. Computer networks. Principles, technologies, Protocols. Textbook for High Schools .- St. Petersburg .: Peter, 2011. - 958 c.
[3] Ryabko B. Y., Fionov A. N. Cryptographic methods of information protection. M .: Hot line - Telecom, 2014. – 229 p.
[4] Sovetov B.Y., and others.Cryptography.-SPb.:Publishinghouse"Lan",2001.-224 p.
[5] Periti Lambha. AN Innovative Methodology of High Performance and Information Security for Gratis House Optical Communication// International Journal of Electronics & Communication.Vol. 5, Issue 8, 2017. – pp.15–17.
[6] Gabidulin, E.M., et al., Network coding, Trudy MFTI. T. 1, No. 2. - 2009. - pp.3-28.
[7] Tikhonov, S.V. Universal method of protection of block ciphers from side attacks on power circuits / / Problems of information security. Computer system. - No. 3.- pp.48-55.
[8] Fragouli C, Soljanin E. Network coding. Foundations and Trends // Networking.V.2,No.1. 2007. -pp.1–134.
[9] Ibrahimov B.G., Ismaylova S.R.The Effectiveness NGN/IMS Networks in the Establishment of a Multimedia Session //American Journal of Networks and Communications. Vol. 7, No. 1. 2018. - pp.1-5.
[10] Shafali Agarwal. Image Encryption Techniques Using Fractal Function: A Review// International Journal of Computer Science & Information Technology. Vol 9, No 2, 2017. – pp.53-68.
[11] Ibrahimov B. G. The Study and Estimation of the Performance Attributes of Terminal Hardware for a Link in a Multiservice Communication Network//Automatic Control and Computer Sciences.USA. 2010. Vol. 44. No. 6.– pp.359 - 363.