Synthesis of Quite Proof Cryptosystem with Increased Unicity Distance for Cloud Computing

Volodymyr Klimchuk[1], Eugene Samoylik[1], Viktor Gnatyuk[1], Dmytro Prysiazhnyy[2], Volodymyr Buryachok[3]

[1]National Aviation University, Kyiv, Ukraine
[2]Vinnytsia National Technical University, Vinnytsia, Ukraine
[3]Borys Grinchenko Kyiv University, Kyiv, Ukraine
v.klimchuk@gmail.com samojlikzhenya@gmail.com
viktorgnatyuk@ukr.net dimpris@gmail.com BVL-home@ua.fm

Abstract. Modern cryptosystems have a narrow application area, mainly because of a strict restriction of overrunning during the encryption of so-called unicity distance for the key. It is possible to essentially increase the unicity distance by using a synthesis of a constructed/artificial/planned language in the application area, where an alphabet of a high dimension is used. There was made a synthesis of highly secured cryptosystem. It has such feature as the security of text information with an increased unicity distance. This distance is set into a tabular form which assumes that this text information is taken from the thesaurus of predefined application area. There were gotten mathematical expressions that display the procedure of the encryption and decryption. There were considered the features of construction of the generator of pseudorandom sequences. Also, there was defined the level of security of cryptosystem with a different levels of resource capabilities. There was given a graph of correlation between the indicator of security and the code length of the encryption key. There were also defined the conditions of providing a necessary security regime in cloud systems.

Keywords: text information security, encryption, highly secured cryptosystem, unicity distance, alphabet enlargement, synthesis of cryptosystem, cloud system.

1. Introduction

As the procedure of text messages encrypting is directly connected with a usage of the alphabet symbols of any natural language, it is well known [1] that it requires a frequent change of the key information in secured cryptosystems with perfect/ideal theoretically informational security. That is determined by a short unicity distance during the encryption of such text messages. That is why these cryptosystems have such a limited application field. The paper [2] suggests a method of increasing the unicity distance by using the synthesis of the constructed language that displays the application area that includes an alphabet with a high dimension. Highly secured cryptosystems usually use the mechanism of increasing the alphabet of the display language of text messages. The value of performance indicators is much higher in such systems as compared to other methods of ensuring a perfect secrecy. The paper [2] also shows the efficiency of a method that increases the alphabet of the display language in a text messages and is compared to the efficiency of method of using one-time pads. It is important to consider the length of the key as a criterion of effectiveness while comparing those two methods:

$$Z = \frac{H_1(K)}{H(K)}, \tag{1}$$

where H(K) stands for the entropy of a system of security as a size of the key space in the cipher, which depends on the number of available cipher keys; K is stands for the available for usage number of the keys of the cipher in the security system with the integrated alphabet (H(K)= log(K)); $H_1(K)$ is entropy of the cipher key in case of using one-time pads method to secure the information in the mode of a perfect secrecy (in this case the length of a cipher key has to be equated to a length of a message [1]). The next expression (2) defines the entropy for such kind of a key:

$$H_1(K) = \log_2(B_1^{n_1}), \tag{2}$$

where n_1 stands for the length of a message, which is written by a natural language (for example, English, Ukrainian, Russian etc.), that contains an alphabet B_1 .

While the entropy of the key, which is used for the security of information when using the integrated alphabet of the display language for this exact information, is calculated as

$$H(K) = \log_2 \prod_{i=1}^{n} \left[B - (s-1)\right] \tag{3}$$

where B stands for the alphabet of a tabular form, i.e. the amount of possible combinations of table rows of a semantic dictionary, which is created artificially as a result of statistical and semantic analysis of the subject area, n is the number of rows in tabular form, and s stands for the number of columns in tabular form.

The paper [2] shows the advantages Z of using a cryptosystem with integrated alphabet in comparison with the one-time pads method. This method almost does not depend on the usage of the alphabet of natural language, and significantly depends on the length of messages that are used / available in this language. In this paper it was considered the features of quite proof cryptosystem which secures the text messages which are set into a tabular form with an extended unicity distance (EUD) with a condition that these messages are taken from the semantic dictionary of the pre-defined application area. Therefore, before the encryption procedure beginning with usage of any of quite proof cipher, it is necessary to create a semantic dictionary. Its linguistic units have to fully reflect the language space for this application area [3].

2. Features of Construction of the EUD

EUD can be implemented for different types of substitution ciphers and is mainly used in polyalphabetic ciphers, such as Vigenere cipher and Beaufort cipher [3]. They don’t mask the periodicity of appearance of the alphabetical elements on the output of the encoder. As a result these ciphers are considered as easily exposed while using the probabilistic analysis of the cipher message. Also, there is a possibility of using different options which are based on usage of pseudorandom number generators. (pseudo-random number generator (PRNG)) [7,8]. Under normal conditions such secure systems also have a certain level of security against hacking attacks [9,10]. That is because they do not provide a random substitution of the symbols in the original text message. It significantly exceed the period of generated sequence of PRNG. However, under certain conditions that are further defined in this article, EUD which are based on the usage of PRNG, are able to ensure the random substitution of linguistic units in the open text by other linguistic units which are taken from the domain vocabulary application area. Therefore, they are able to provide a certain level of security against attacks [9] that are based on probabilistic analysis of cipher telegrams.

Fig. 1 shows one of the possible schemes for the construction of the EUD, based on the synchronization of the PRNGs. They are located on the transmitting and receiving sides of the secret information exchange channel with a help of a known cipher key.

The scheme on the Fig.1 contains all main elements of a symmetric cryptosystem for security of text information. This system can function in the mode of a perfect stability under certain conditions [2, 3]. However, there is also used an additional element, which is called the subject domain dictionary (thesaurus), in which it is supposed to apply the EUD. This dictionary contains those linguistic units which can potentially be included as a part of open simple text messages. These messages are placed into a given table form by the administrator during the preparation of a table. This table needs to be transmitted through the open communication channel. If such components as dictionary, a known cipher key and a preset tabular form are available, administrator of the application system forms the initial outgoing text on the transfer side as an adjusted preset form. This specified form of a table sheet contains the elements which arrive to the encryption device (or program encoder) one row after another. The encryptor implements the mechanism of enlarging the alphabet of the display of information language which is set into a given table form, as it is shown in [2]. Every single row of the table, in particular, is presented as a separate letter of the enlarged alphabet of the display language for the table information. With the help of key information the PRNG is set into a certain initial state, and from that state it generates pseudorandom numbers at the input of the encryption device. For each row in the table there is only one pseudorandom number. The third encryptor input contains linguistic units from the subject domain vocabulary, as well as data on the sequence numbers of these units in the structure of the dictionary. The encryptor replaces the true enlarged element of the table, which is taken as a current table row, with the masking string of linguistic elements taken from the dictionary. The display/reflection of the original table has to be found in the dictionary. Also, its serial number should be determined in the structure of the dictionary. This needs to be done for every current line of the original table which is formed by the administrator. The next step is determination of the number of the table row in the structure of the dictionary. It is used as a substitute for the true row of the table.

This number is determined by using exclusive disjunction of a number of the true element and the pseudorandom number derived from the PRNG. The result of the usage of an encryption device is the ciphered text of the table, which is transmitted to the receiving side via an open communication channel.

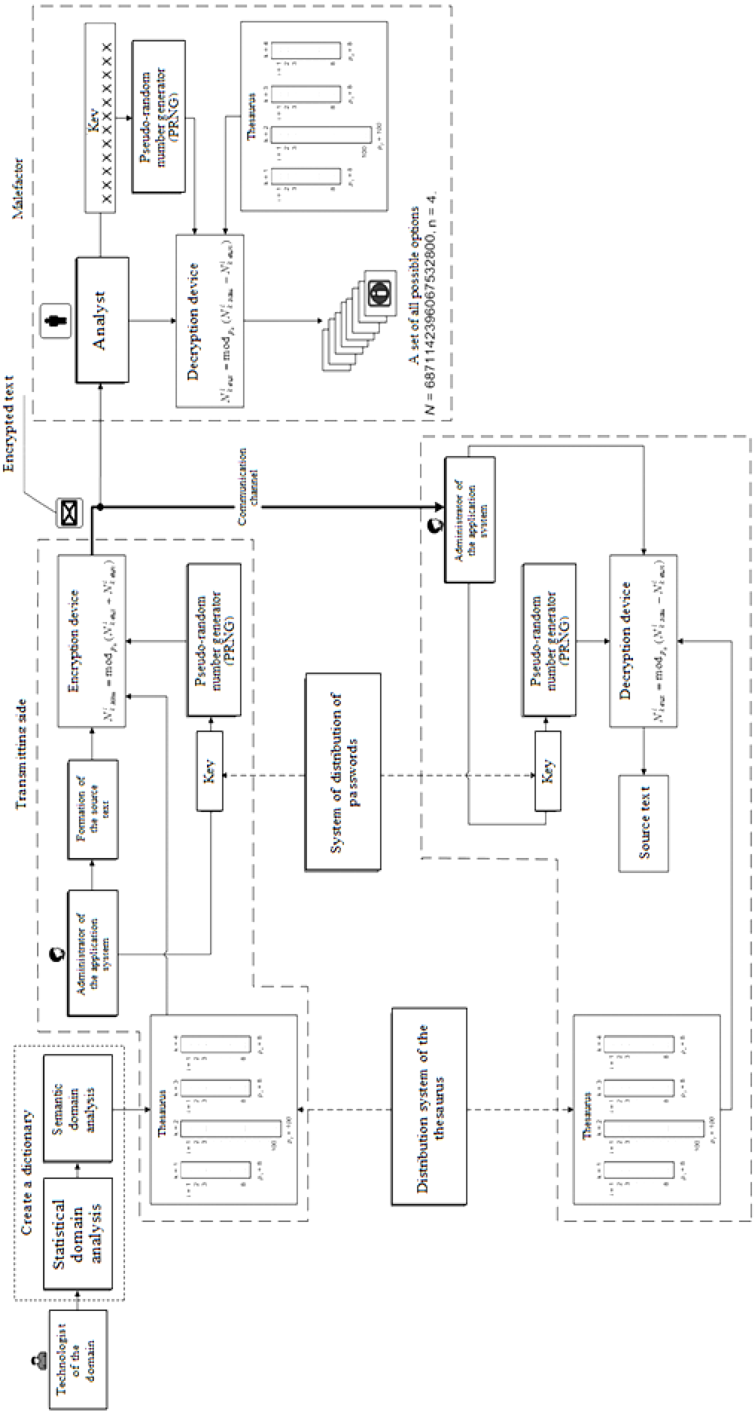
Technologist of the domain
Create a dictionary
Statistical domain analysis
Semantic domain analysis
Thesaurus
Distribution system of the thesaurus
Transmitting side
Administrator of the application system
Formation of the source text
Key
Encryption device
$N^i_{i\,shu} = \mathrm{mod}_{p_k}(N^i_{i\,ext} + N^i_{i\,dun})$
Pseudo-random number generator (PRNG)
System of distribution of passwords
Encrypted text
Communication channel
Malefactor
Analyst
Key
X X X X X X X X X X X X X X
Pseudo-random number generator (PRNG)
Decryption device
$N^i_{i\,ext} = \mathrm{mod}_{p_k}(N^i_{i\,shu} - N^i_{i\,dun})$
Thesaurus
A set of all possible options
N = 6871142396067532800, n = 4.
Receiving side
Administrator of the application system
Pseudo-random number generator (PRNG)
Key
Decryption device
$N^i_{i\,ext} = \mathrm{mod}_{p_k}(N^i_{i\,shu} - N^i_{i\,dun})$
Source text
Thesaurus

Fig.1. Variant of the flowchart of EUD construction

The application system administrator submits the received encrypted text to the decryption device on the receiving side. Also, he sets the same initial state of the PRNG as the initial state of the transmitter's generator using the known key. The decryptor does the same transformations as the encryptor. The result of the decryption device is the output table that was formed on the transmitting side.

If the characteristics of the synthesized EUD are defined as it is shown in [2], then this cryptosystem will function in the mode of quite proof.

As see, for the increase of distance of unicity the dictionary of language of reflection of information is plugged in composition of this system, linguistic units from that are placed in the set table form [2]. The structure of the dictionary is conformed to the structure of the tabular form, which contains text messages that require security. For example, if semantically connected linguistic units are displayed in the columns of the table, we should present this dictionary as a collection of *n* subdictionaries, where *n* stands for the number of columns of a given table form. Every subdictionary is used to process data from one column. Therefore, the number of thesaurus subdictionaries which are used for encryption and decryption is equal to the number of columns of a given table form.

In order to explain the mechanism of replacing the true element of the open text sequence with the masking element of the closed sequence in the encryption procedure, we have to consider the following example. Let's suppose that the dictionary of the subject area consists of *n* subdictionaries. All elements of every subdictionary are numbered. Let's also assume that the location of the first true element of the introductory sequence in the structure of the defined by the *k*-th subdictionary by encoder is of the serial number N_{inp}, and the first random number given by the generator of the PRNG is equal to N_{inp}, where $0 \le N_{ran} \le p_{\kappa}$, p_{κ} stands for the dimension (i.e., the total number of words) of the *k*-th subdictionary.

Then the ordinal location number in the structure of the *k*-th subdictionary of "not true" (i.e., masking) linguistic element, which is set as the first element in the output encrypted sequence instead of the true first linguistic element, will be equal to

$$N^{i}_{k\ \mathrm{sec}} = \mathrm{mod}_{p_k}(N^{i}_{k\ \mathrm{inp}} + \mathrm{mod}_{p_k}(N^{i}_{k\ \mathrm{ran}}) + p_k)\ . \qquad (4)$$

The expression (1) is fair only if provided by the coincidence of the dimension of the applied subdictionary with the scope of random sequences generated by the PRNG. (Scope means the difference between the maximum and minimum pseudorandom numbers in the sequence). In general, when the size of the PRNG is equal to the dimension of the largest subdictionary, the encryption equation, which in fact is a formula for determining the sequence number of the masking word placement in the thesaurus subdictionary, has the following form:

$$N_{\mathrm{sec}} = \mathrm{mod}_{p_k}(N_{\mathrm{inp}} + N_{\mathrm{ran}})\,, \qquad (5)$$

where N_{inp} stands for the serial number of the location in the *k*-th subdictionary of the *i*-th true linguistic element taken from the source that requires to be encrypted, the open sequence of linguistic units, where *i* is the sequence number of the location of this element in an open sequence; N_{sec} stands for a serial number in the *k*-th subdictionary of the masking element, which is placed into the *i*-th position (instead of the true element) of the output encrypted sequence of linguistic units; N_{ran} is a pseudorandom integer generated by a PRNG on the *i*-th step of the generation in order to encrypt the *i*-th true element with a serial number N_{inp}; p_κ is the dimension of the *k*-th subdictionary; *k* is the sequence number of the subdictionary in the dictionary of the language of the applied region.

In this case the equation of decryption of information is a formula for determining the sequence number of the location in the selected subdictionary of the *i*-th true linguistic unit placed in the output of the decrypted sequence instead of the masking linguistic unit taken from the original encrypted sequence. The decryption equation has the following form:

$$N_{inp} = \mathrm{mod}_{p_k}\,(N_{\mathrm{sec}} - N_{\mathrm{ran}})\,, \tag{6}$$

where N_{inp} stands for the serial number of the linguistic unit (according to the numeration in the *k*-th subdictionary), which is identical to the true unit reflected in the original open sequence of linguistic units; N_{sec} is a serial number of the encrypted linguistic unit (according to the numbering in the *k*-th subdictionary) taken from the encrypted sequence that is provided for processing, at the current step of the decryption procedure; N_{ran} is a pseudorandom integer generated by the PRNG to decrypt the encrypted unit with the serial number N_{sec}; p_κ is the dimension (i.e., the total number of words) of the *k*-th subdictionary; *k* is the serial number of the subdictionary which is selected at the current step of the decryption procedure.

Formula (6) is valid if the width of the PRNG is equal to the dimension of the subdictionary, which has the largest number of linguistic elements among the plurality of all subdictionaries of the used domain vocabulary.

3. Construction of the PRNG for Synthesized Cryptosystem

It should be noted that PRNGs that are used in the information security systems have to meet the following requirements: high cryptofirmness; good statistical properties, generated pseudorandom sequences, which according to their statistical properties, should not differ from truly random sequences in the uniquely determined conditions; a big period of generated random sequence; efficient hardware and software implementations.

Fig. 2 shows the scheme of work of the PRNG in the EUD.

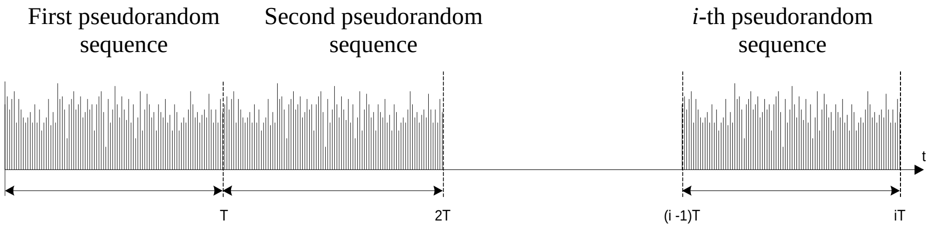
First pseudorandom sequence
Second pseudorandom sequence
i-th pseudorandom sequence
t
T
2T
(i -1)T
iT

Fig. 2. The work of the PRNG in the EUD without providing of a random way of substitution of symbols

This picture also shows that knowing the size of the period of random sequence *T*, the analyst can make a filter and “catch” symbols with a period *T*. And if you apply the encryption procedure, where each next table is encrypted from the first value of the pseudorandom sequence of numbers, then a random character of symbols substitution is not provided.

Fig. 3 shows how the PRNG provides the random way of substitution by encrypting tables with text information with a help of the EDU. In Fig. 3 there is evidence that each next table is encrypted by a sequence of pseudorandom numbers without resetting the PRNG to its initial state. The amount of pseudorandom numbers used during encryption is getting fixed after every encryption session. Also, every next table is encrypted not from the initial state of the PRNG, but from the point of the sequence where it was fixed on the previous encryption act. Therefore, the random nature of the substitution is provided and, consequently, the attack type like the probabilistic analysis of the repetition rate of the characters in the source text is neutralized [9]. To ensure the randomness of the nature of substitution, the period of PRNG *T* has to be much longer than the length of the table *n*.

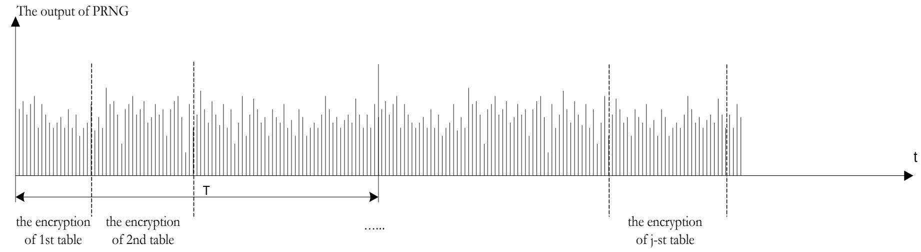
The output of PRNG
t
T
the encryption of 1st table
the encryption of 2nd table
......
the encryption of j-st table

Fig. 3. The operation of PRNG in the EUD with the provision of random substitutions

Firmness of EUD

1. Analysis of EUD security, provided that at least one sample of the output (open) text message and a sample of the correspondence with the cipher gram are known.

Initial conditions and resources of the malefactor: 1) the analyst knows at least one sample of the original open table and correspondent table encrypted in/with it; 2) the participants of the secret information exchange do not change the key of the cipher during the time when the attack occurs; 3) the analyst has the means of encryption and decryption of the EUD . He knows the structure of the key of the cipher, the structure of the given table form and the dictionary of the applied area, the structure of which is coordinated with the structure of the table form; 4) analysis of the security of the algorithm of cipher transitions on the basis of intercepted cipher grams was not conducted or did not have a positive result.

The components of the equipment that are used by the analyst to carry out an attack on the cipher under the above conditions are shown in Fig. 1. Analytics actions. An analyst decrypts the known encrypted sample of a known output table. Then he makes attempts to determine the key of the cipher by directly scanning all possible values of this key until an appropriate open output message is received. Indicator of firmness: K_1 is the maximum possible number of search for the cipher key (which is equal to the number of possible values of the cipher key).

$$K_1 = x^k \ , \tag{7}$$

where x is the basis of the language alphabet of the cipher key, k is the code length of the cipher key.

Conclusion regarding the above attack model: the analyst has the opportunity to determine the fact of successfully completing the attack by comparing the decrypted sample of the known cipher gram with its open source output message; in this case the observance or non-observance of restrictions on the unicity distance does not affect the security of the EUD, and the security of the coincides with the security of the algorithm of cipher transformations that were used in accordance with the scheme shown in Fig. 1.

2. Analysis of EUD security in the absence of correspondent samples of output and encrypted text messages and non-compliance with restrictions on the unicity distance

Initial conditions and resources of the malefactor: a) an analyst is provided with a sufficient volume of intercepted ciphertext (which was obtained at intervals when the key of the cipher was not changed) to make reasonable statistical conclusions about the probability of the appearance of its individual elements; b) the absence of any corresponded pair of samples of the source and encrypted information, i.e. the analysis of firmness can only be performed with the help of intercepted ciphertext; c) an analyst has the ability to determine that the condition of observing the distance of unity is not fulfilled, and, therefore, the attack on the cipher does not lose its meaning; d) the scheme of the generator of pseudorandom sequences (PRNG) provides the random way of substitution; e) the possibility to get information about the statistical properties of the dictionary of the application area, which is consistent with the structure of the given table form; f) the analyst has the PRNG encryption and decryption means, as well as the dictionary of the applied area. He also knows the structure of the cipher key and the structure of the tabular form.

The flowchart of equipment used to carry out an attack on the code in the above conditions is similar to that shown in Fig. 1, but the amount of work that the analyst has to perform is much wider.

Analytics actions

Preparatory stage. 1) Pre-receiving of information about the statistical properties of secret data exchange, which consists of: a) obtaining a statistically complete sample of cipher grams on a problem within the given thesaurus of the applied area; b) processing of the sample in order to obtain an ideal statistical function of the distribution of semantic units, which make up the information of secret exchange to solve a problem.

Attack stage. 1) decryption of intercepted samples of encrypted text by the direct search of all values of the cipher keys until all samples of the distribution function of the probability of appearance of speech elements at the output of the decoder are obtained. 2) received samples of the distribution function are compared to the function that was gotten at the preparatory stage. The next step is making the decision about the most likely variant of the key. Firmness indicator is statistical:

$$K_2 = K_1 \times V \ , \tag{8}$$

Where K_1 stands for the index of algorithm security, V is the size of the statistical information of a secret exchange.

Conclusion regarding the above attack model: The firmness of the EUD is V times higher than the firmness of the used cipher transformation method and is statistical unit of measurement. Let's consider the graph of the dependence of security the parameter K on the key of the cipher k to the two above-mentioned attack models (Fig. 4).

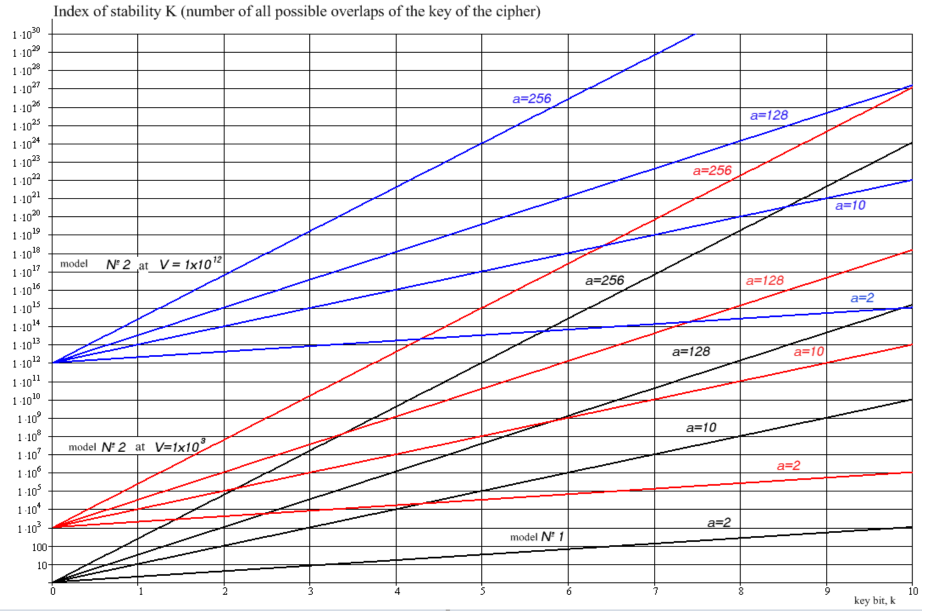

Fig. 4. The graph of the dependence of security the parameter of EUD on the bit rate of the cipher key

Firstly, it leads to a trivial result: with the length of the cipher key always rising, the stability of the security system is increasing. Secondly, in any case, the stability of the EUD for attacks of type № 1 is much lower than the security of this system comparing to type of attacks №2. Thirdly, the sustainability of the EUD is increasing with the increase in the sample size (which is marked with a symbol V).

Let's consider the dependence of the stability parameter K on the parameter a, where a is the basis of the alphabet of the key language of information. According to the graph on the Fig. 4, we can see that the increasing of the value of parameter a leads to the increasing of the index of stability K with a constant (unchanged) value of the code length of a cipher key k. For example, if we consider the group of curves in relation to the attack model №1, then we can see that with the bit rate k = 8, the firmness index is equal to the following values: K = 256 for a = 2, $K = 1 \cdot 10^8$ for a = 10, $K = 1{,}4064 \cdot 10^{12}$ for a = 128, $K = 1{,}8447 \cdot 10^{19}$ for a = 256. Therefore, it is recommended to increase the basis of the alphabet of the language of the key information.

4. Terms of Providing a Quite Proof Security

Initial conditions and resource possibilities of the malefactor (that case when the EUD parameters provide conditions for maintenance of a perfectly secret system): 1) the analyst has the means of encryption / decryption of the EUD , including dictionary of the applied area, but there is no possibility of intercepting the amount of cipher grams that exceed/overrun the unity distance, because the security system satisfies the conditions of quite proof; 2) the absence of any a priori information about the original text information and encrypted text which is correspondent with this information; 3) there is no need to obtain any priori information about the statistical properties of confidential data (because the conditions for maintaining a perfectly secret system are provided).

The attack model (if the EUD`s parameters match the conditions of a perfectly secret system) - does not need to be defined. Stability indicator is not defined, since there are no conditions for determining the moment of successful completion/ending of the attack. In this case, the distance of unity *U* is used as an efficiency indicator of the EUD.

The criterion for the correct functioning of the constructed EUD is the observance of the unicity distance (the condition that the amount of cipher encrypted with the same key will not exceed the unicity distance), which is defined as [2,11].

$$U = \frac{\log_2(K)}{D}, \tag{9}$$

where *U* stands for the unicity distance, *K* is the maximum number of ciphers variations, D is the redundancy of accepted language for displaying messages.

To fulfill the condition of observing the distance of unity, it is necessary to correctly determine the length of the key *k* in the correlation with the length of the message *n*, considering that [4,12].

$$k = \log_2 N, \tag{10}$$

where *k* stands for the code length of the key, *N* is the number of possible values/meanings of the message with the length *n*. So the dependence of the entropy (the length of it in bits) of the cipher key on the length of the message can be written as (3) (the output of the formula was given in [2,13]).

Conclusion regarding the above attack model: EUD has the properties of an absolutely secret system if all the above written conditions were performed.

5. Conclusions

1. In this paper a cryptosystem was synthesized that executes the offered method [2] of constructing a quite proof system of security against violations of the confidentiality of textual information. It is taken from the thesaurus of a predetermined application area and placed into a given table form. The method is based on the application of the mechanism of enlarging the alphabet of the display language of textual information. The thesaurus of the application area uses this information and considers the structure of the table form. As a result of the enlargement of the alphabet, the so-called unicity distance, which was firstly considered in the works of C. Shannon [5,6], increases and is the main threshold

indicator of the cryptosystem belonging to a class of quite proof systems of security with a theoretically proved ideal and informational firmness. The small values of the unicity distance while encrypting messages composed of alphabets of natural languages, cause the need for constant/regular changes in key information. It is a big problem for many applications. The synthesized cryptosystem is largely devoid of this disadvantage and, as a result, can be used in the wider application areas.

2. Mathematical expressions that represent the encryption / decryption procedures are valid if the dimension of the applied subdictionary coincides with the scope of random sequences generated by the PRNG. The encryption equation is a formula for determining the serial number of the masked word placement in the *k*-th thesaurus subdictionary. The decryption equation is a formula for determining the ordinal number of the location in the selected subclass of the *i*-th true linguistic unit placed in the output decrypted sequence instead of the masking linguistic unit that was taken from the original encrypted sequence.

3. There were also considered some features of construction of the pseudorandom sequence generator. Each next table was encrypted by a sequence of pseudorandom numbers without resetting the PRNG to its original state. Thus, the random nature of the substitution was provided. Therefore, attacks like the probabilistic analysis of the frequency of the characters repeats in the source text are neutralized.

4. It was determined the firmness of this cryptosystem for the different resource possibilities of the malefactor. If at least one sample of the output (open) text message and a sample of the correspondent cipher gram with it are known, then the firmness of the synthesized cryptosystem coincides with the firmness of the algorithm of the cipher transformation. In the absence of correspondent samples of source as well as encrypted text messages and non-compliance with the restrictions of the unicity distance, the firmness of the cryptosystem is statistically significant and is V times higher than the stability of a used method of the cipher transformation, where V is the volume of the statistical sample of secret information. As the sample size V increases, the firmness of the cryptosystem also increases.

5. There were gotten mathematical expressions and there was given the graph of dependence of the firmness index on the code length of the cipher key. With the length of the cipher key always rising, the firmness of the security system increases too. When the basis of the alphabet of the language of key information is increasing, then the index of firmness of the cryptosystem also significantly increases with a value of the code length of the cipher key stays constant.

6. There were determined formal conditions for the correct functioning of the built cryptosystem (with the abidance of the unicity distance) and the code length of the cipher key in correlation with the length of the closing messages. It was shown that the developed cryptosystem has the properties of quite proof system.

7. The efficiency of the suggested method for constructing a quite proof cryptosystem, if the unicity distance is chosen as the criterion of efficiency, is characterized by much higher levels in comparison with the efficiency of other methods (for example, the method of one-time pad) providing a regime of perfect secrecy.

References

1. Sushko. S., Kuznetsov. V., Fomicheva. L., Korablev. A.: Mathematical foundations of cryptanalysis. National Mining University, 465 (2010)
2. Samoylik, Ye. Efficiency of quite proof cryptosystems with megascopic distance of unicity, Zahist informacii, Vol.19, №2, Kyiv, p. 184-192 (2017)
3. Shyrokov, V., Bugakov, O., Gryaznukhina, T. Cabinet-type linguistics, Kyiv, Dovira, 471 p. (2005)
4. H.C.A. X.K.A. Van, Tilborg, Encyclopedia of cryptography and security, New York, Springer, 684 p. (2005)
5. Shannon, C. A Mathematical Theory of Communication, Bell System Technical Journal, Vol. 27, № 4, pp. 379-423, 623-656 (1948)
6. Shannon, C., «Predication and Entropy in Printed English», Bell System Technical Journal, Vol. 30, № 1, pp. 50-64 (1951)
7. Gnatyuk, S., Kovtun, M., Kovtun, V. et al. Search method development of birationally equivalent binary Edwards curves for binary Weierstrass curves from DSTU 4145-2002. In: Proceedings of 2nd International Conference on the Problems of Infocommunications, Science and Technology, Kharkiv, Ukraine, October 13-15, pp. 5-8. (2015)
8. Gnatyuk, S., Okhrimenko, A., Gancarczyk, T. et al. Method of Algorithm Building for Modular Reducing by Irreducible Polynomial. In: Proceedings of the 16th International Conference on Control, Automation and Systems, October 16-19, Gyeongju, Korea, pp. 1476-1479 (2016)
9. Hu, Z., Gnatyuk, S., Kova,l O. et al. Anomaly Detection System in Secure Cloud Computing Environment. International Journal of Computer Network and Information Security, Vol. 9, № 4, pp. 10-21 (2017)
10. Hu, Z., Gnatyuk, V., Sydorenko, V. et al. Method for Cyberincidents Network-Centric Monitoring in Critical Information Infrastructure, International Journal of Computer Network and Information Security, Vol. 9, № 6, pp. 30-43 (2017)
11. Vajda, I. Computational Independence in the Design of Cryptographic Protocols, International Journal of Computer Network and Information Security, Vol.8, №10, pp.1-11 (2016) DOI: 10.5815/ijcnis.2016.10.01.
12. Goyal, R., Khurana, M., Cryptographic Security using Various Encryption and Decryption Method. International Journal of Mathematical Sciences and Computing, Vol.3, №3, pp. 1-11 (2017) DOI: 10.5815/ijmsc.2017.03.01.
13. Vajda, I. On Classical Cryptographic Protocols in Post-Quantum World. International Journal of Computer Network and Information Security, Vol.9, №8, pp.1-8 (2017) DOI: 10.5815/ijcnis.2017.08.01.