UDK 681.5.004

S. V. Burmistrov[2], *Ph.D.,*
e-mail: burmistrovsv@rambler.ru
O. M. Panasco[1], *Ph.D., associate professor,*
e-mail: lena.pa@ukr.net
O. D. Laitarov[1], *6th year student*
e-mail: vendenta95@gmail.com
[1]Cherkasy State Technological University
Shevchenko blvd, 460, Cherkasy, 18006, Ukraine.
[2]Kiev National University of Technology and Design,
V. Chornovola str., 241, Cherkasy, 18028, Ukraine

MODERNIZATION OF SELF-MOVABLE FIXING DEVICES BASED ON VERNAM'S CIPHER ANALOGUE

In the article a functional scheme of encryption device, which is the realization of one of the variants of modernization of the Lorenz German stationary encryption machine, is developed. The device works by superposing the ciphertext on the main text of messages. It also has absolute cryptographic stability, provided that it uses conditions similar to those of the Lorentz operation, but does not use the Vernam encryption system.

The advantage of the proposed character encryption device is the much more powerful ciphertext alphabet. It consists of ***(n-1)!*** *times more characters than in Vernam's cipher. This significantly increases the cryptostability of the system.*

Unlike the Vernaim cipher, in the proposed encryption device, the ciphertext encoding does not equal the decryption ciphertext. Therefore, in order to unify the receiver and transmitting part of the device in its design, it is proposed to introduce an additional block – a block of formation of the reverse ciphertext, which automatically generates ciphertext encoding on the basis of ciphertext decoding.

The basis of this project is a special software complex designed to calculate the principle electric circuit of the block of formation of the reverse ciphertext, which automatically generates ciphertext encoding on the basis of ciphertext decoding

Keywords: *Lorentz stationary teleprinter encryption machine, Vernam system, encoding ciphertext, decoding ciphertext, a block of formation of the reverse ciphertext.*

Relevance of research. Despite the time, there is a rather solid group of enthusiasts in Europe researching encryption technology, which pays heightened attention to the devices used during the Second World War [1, 2]. Along with the well-known Enigma portable encryption device in Germany, the Lorentz stationary teleprinter encryption machine was actively used [3]. Despite the similarity of the design, the Lorentz machine was working on a different principle. The machine worked on the use of additive encryption method Teletext messages, invented in 1917 in the US AT & T staff by Major Joseph Moborn and Hilbert Vernam. Easy Vernam system [4, 5, 6] was that encoded characters were added to ciphertext symbols as the term modulo 2. Exactly the same characters as added by adding modulo 2 to the received encrypted character repeal encrypted characters and leave original message symbols that can then be printed. A significant advantage of the Vernam's cipher is that encoding ciphertext coincides with the decoding ciphertext.

The Vernam's cipher is an encryption system for which absolute cryptographic stability is proved, with the use of three critical properties – ciphertext must:

- be accidental;
- coincide in size with given open text;
- be applied only once (virtually ciphertext was made in the form of a looped notification with relatively simple periods).

The Lorenz encoding machine worked with five-digit characters, which allowed the 32-character alphabet to be served. In this encryption encoding contains the same number of characters.

The construction of digital counterparts of the Lorenz encryption machine, which would have better index of cryptostability, is **an actual task** in the development of modern digital encryption devices.

Analysis of recent researches and publications. The construction of the Lorentz stationary teleprinter encryption machine is a classic one [7, 8, 9]. It has been used for a long time as the basis for the creation and further modernization of new constructions of stationary symbolic encryption devices.

Formulating the goals of the article. The purpose of the article is to implement one of the options for upgrading the Lorentz encryption machine. It involves a construction in which ciphertext indicates a variant of combinatorial replacement of one character to another. When encoding the text for each next character, a new variant of the combinatorial character-replacement is given – a kind of analogue of the overlapping of characters of the input text with encryption coding.

Presenting main material. Setting up the task of constructing a device model: You need to get a model of an encryption device that would execute character encryption given by three-bit binary codes, using for each next character a new encryption key (example of one of the keys, see Table 1), and used the same encryption encoding both for encrypting characters and for decrypting. The alphabet of three-digit binary symbols has 8 random characters, for example, $y \in \{0,1,2,3,4,5,6,7\}$. As a result of encryption, an encrypted message is received, consisting of characters of the same alphabet.

Table 1

Example of combinatorial replacement of characters in encryption

№	Full alphabet of unencrypted text				Encrypted text				Combinatorial variant of symbols replacement
	Characters of plain text	Three-bit binary codes			Three-bit binary codes			Encrypted text characters	
1	0	0	0	0	1	1	0	6	0→6
2	1	0	0	1	0	1	1	3	1→3
3	2	0	1	0	0	0	1	1	2→1
4	3	0	1	1	1	0	0	4	3→4
5	4	1	0	0	0	0	0	0	4→0
6	5	1	0	1	0	1	0	2	5→2
7	6	1	1	0	1	1	1	7	6→7
8	7	1	1	1	1	0	1	5	7→5
		↑ a_0^{Cd}	↑ a_1^{Cd}	↑ a_2^{Cd}	↑ f_0^{Cd}	↑ f_1^{Cd}	↑ f_2^{Cd}		
		Columns unencrypted three-bit binary codes			Columns of encrypted three-bit binary codes – encryption functions				

For this method of encryption there are ***n!=8!=40 320*** variants of combinatorial replacement of symbols. That is, in other words, the ciphertext alphabet encoding consists of *40 320* characters – the current encryption keys, which is greater in ***(n-1)!*** fold compared to Vername's cipher, and, accordingly, improves the quality of encryption.

An encryption option is defined by a system of encryption functions:

$$y_{Cd} = \begin{cases} f_0^{Cd} \\ f_1^{Cd} = \\ f_2^{Cd} \end{cases} \begin{cases} F_0(a_0^{Cd}, a_1^{Cd}, a_2^{Cd}) \\ F_1(a_0^{Cd}, a_1^{Cd}, a_2^{Cd}) \\ F_2(a_0^{Cd}, a_1^{Cd}, a_2^{Cd}) \end{cases} \quad (1)$$

This encryption option (see Table 1) has a 24-bit binary number of the current encryption key, which for this case is:

$$110010010110001111000110_{BIN}=C963C6_{HEX} \quad (2)$$

The decryption operation consists in restoring the original text and is executed in inverse order (see Table 2).

The decryption option is determined by the system of decrypting functions:

$$y_{Dcd} = \begin{cases} f_0^{Dcd} \\ f_1^{Dcd} = \\ f_2^{Dcd} \end{cases} \begin{cases} F_0(a_0^{Dcd}, a_1^{Dcd}, a_2^{Dcd}) \\ F_1(a_0^{Dcd}, a_1^{Dcd}, a_2^{Dcd}) \\ F_2(a_0^{Dcd}, a_1^{Dcd}, a_2^{Dcd}) \end{cases} \quad (3)$$

Table 2

An example of combinatorial substitution of characters when decoding

No. in order	Full alphabet of encrypted text				Decrypted text				Combined variant of encryption-decryption of characters
	Encrypted text characters	Three-bit binary codes			Three-bit binary codes			Decrypted text symbols	
1	0	0	0	0	1	0	0	4	4→0→4
2	1	0	0	1	0	1	0	2	2→1→2
3	2	0	1	0	1	0	1	5	5→2→5
4	3	0	1	1	0	0	1	1	1→3→1
5	4	1	0	0	0	1	1	3	3→4→3
6	5	1	0	1	1	1	1	7	7→5→7
7	6	1	1	0	0	0	0	0	0→6→0
8	7	1	1	1	1	1	0	6	6→7→6
		↑ a_0^{Dcd}	↑ a_1^{Dcd}	↑ a_2^{Dcd}	↑ f_0^{Dcd}	↑ f_1^{Dcd}	↑ f_2^{Dcd}		
		Columns of encrypted three-bit binary codes			Columns of decrypted three-bit binary codes – decryption function				

The decryption option has a binary number – the current decryption keys (see Table 2), which for this case is:

$$10100101101100100011110 0_{BIN}=A5B23C_{HEX} \quad (4)$$

As a result, in this design, ciphertext encoding and ciphertext decoding (formulas 2 and 4) are different. In this case, the design of the device is complicated. An encryption machine must have two ciphertext at once: encoding – for encryption of texts, and decoding – for decoding texts. Between ciphertext decoding and encoding there is some combinatorial functional dependence.

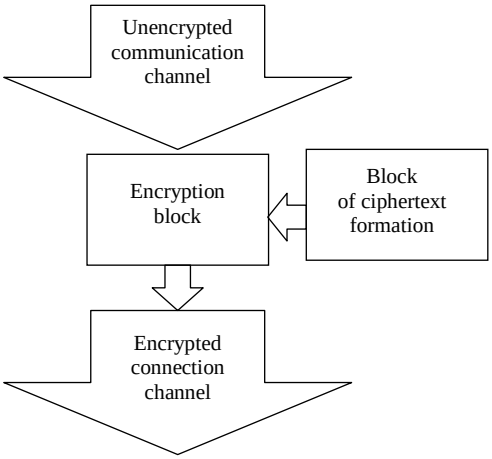

Fig. 1. Blocks for text encryption

In order to unify the blocks, the structure of the receiving and transmitting part of the device must have the same type of block. The encryption device should consist of two parts – the system of blocks for encrypting the text (see Fig. 1) and the system of blocks for decrypting the text (see Fig. 2).

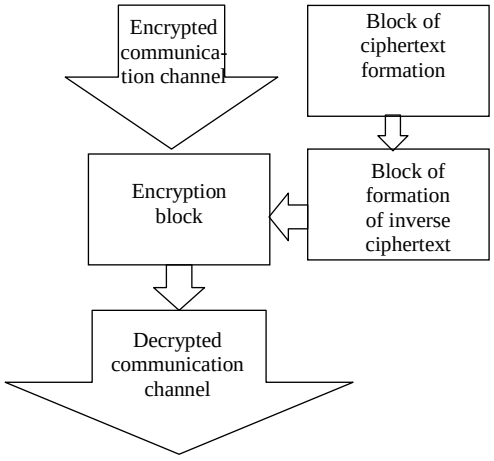

Fig. 2. Blocks for text decrypting

The difference between transmitting and receiving parts consists in the presence of the texts of the block of inverse ciphertext formation in the presence of decrypting. This block is intended for automatic generation of the current decryption ciphertext based on the current ciphertext encoding.

The purpose of this article is to develop a schematic diagram of one of the blocks of this model encryption device – ***the block of inverse ciphertext formation***.

Table 3

A truth table that describes the work of the block of inverse ciphertext formation

Line number of the truth table	Lines of arguments			Lines of functions		
	f_0^{Cd}	f_1^{Cd}	f_2^{Cd}	f_0^{Dcd}	f_1^{Dcd}	f_2^{Dcd}
	x_{24} - x_{17}	x_{16} - x_9	x_8 - x_1	y_1 - y_8	y_9 - y_{16}	y_{17} - y_{24}
0	0000 0000	0000 0000	0000 0000	**** ****	**** ****	**** ****
1	0000 0000	0000 0000	0000 0001	**** ****	**** ****	**** ****
2	0000 0000	0000 0000	0000 0010	**** ****	**** ****	**** ****
…	…	…	…	…	…	…
13198278	1100 1001	0110 0011	1100 0110	1010 0101	1011 0010	0011 1100
…	…	…	…	…	…	…
16777213	1111 1111	1111 1111	1111 1101	**** ****	**** ****	**** ****
16777214	1111 1111	1111 1111	1111 1110	**** ****	**** ****	**** ****
16777215	1111 1111	1111 1111	1111 1111	**** ****	**** ****	**** ****

The purpose of this block is to automatically receive encryption based on encryption ciphertext decoding. Between ciphertext encoding and decoding there is a clear relationship – one encoding version corresponds to one decoding version. This dependence is combinatorial. It can not be described by a mathematical formula, but it can be described by a logical formula.

If we take encoding ciphertext as an argument, and decoding ciphertext as a result, we obtain the truth table of the system of partially defined Boolean functions, which contains 24 arguments and, accordingly, 24 functions of the results.

The task of constructing a block of inverse ciphertext formation consists of several stages, the most difficult of which is minimization of the system of partially defined Boolean functions (see Fig. 3 and Table 3). To solve this problem, a special program complex has been constructed, in which method [10] is used for minimization.

The algorithm of the program complex consists of such key parts (see Fig. 3).

As a result of application of the software complex, the principle electric circuit of the block is calculated, which automatically calculates the current decoding ciphertext value based on the input current encoding value.

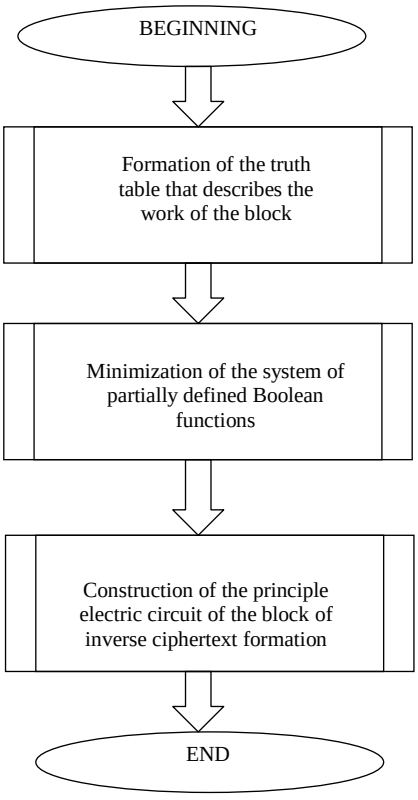

Fig. 3. Algorithm structure of the software complex for obtaining the principal scheme of the block of inverse ciphertext formation

Of the *16 777 216* lines of the truth table, there are *40 320* lines. Therefore, despite the large size of the truth table, due to the large level of minimization the result of the calculation is quite acceptable for practical implementation.

Conclusions:

For realization and achievement of the research purposes in this article the following is done:

1. The scheme of the encryption device is developed, which is the implementation of one of the variants of modernization of the Lorenz encryption machine, which works the same way, but does not use the Vernam's cipher. The developed device also has absolute cryptographic stability, subject to conditions similar to those of Lorenz.
2. The advantage of the proposed encryption device condidts in the use of a much more powerful ciphertext alphabet. It contains ***n!*** symbols of ciphertext, and not ***n***, as in the Vernam's cipher (where ***n*** is the number of characters of the main alphabet of the text). This significantly increases the cryptostability of the system.
3. In the design of the proposed encryption device, the ciphertext encoding is not equal to ciphertext decoding. Therefore, to unify receiving and transmitting parts of the device in its design, it is offered to enter an additional block – the block of inverse ciphertext formation.
4. A special program complex has been developed, on the basis of which the basic electric circuit of the block of inverse ciphertext formation is calculated.

References

1. Ulbricht, Heinz (2005) Die Chiffriermaschine Enigma — Trügerische Sicherheit: Ein Beitrag zur Geschichte der Nachrichtendienste, PhD Thesis. Online version.
2. Kahn, David (1991) Seizing the Enigma: the race to break the German U-boats codes, 1939–1943. ISBN 0-395-42739-8.
3. Davies, Donald W. (1998) The Lorenz cipher machine SZ42, (reprinted in Selections from Cryptologia: History, People, and Technology, Artech House, Norwood.
4. Fomichyov, V. M. (2013) Discrete mathematics and cryptology: course of lectures. In: N. D. Podufalov (ed.). Moscow: Dialogue-MIFI, pp. 239–246. ISBN 978-5-86404-185-7 [in Russian].
5. Gabidulin, E. M., Kshevetsky, A. S., Kolybelnikov, A. I. (2011) Information protection: a manual. Moscow: MFTI, 225 p. ISBN 978-5-7417-0377-9 [in Russian].
6. Babash, A. V., Golev, Yu. I., Larin, D. A. et al. (2004) Cryptographic ideas of the XIX century. *Information Protection.* Confidant – St. Petersburg, iss. 3 [in Russian].
7. Churchhouse, R. (2002) Codes and ciphers: Julius Caesar, the Enigma and the Internet. Cambridge: Cambridge University Press, 240 p. ISBN 978-0-521-81054-8, 978-0-521-00890-7.
8. Copeland, J. (2006) The German Tunny machine. Colossus: The secrets of Bletchley Park's code-breaking computers. Oxford: Oxford University Press, 480 p. ISBN 978-0-19-284055-4
9. Davies, D. (1998) The Lorenz cipher machine SZ42. *Selections from Cryptologia: History, People, and Technology*. Norwood: Artech House, 552 p. ISBN 978-0-89006-862-5
10. Burmistrov, S. V., Piven, O. B. (2015) Matrix method of parallel decomposition as a generalized method of minimization in an orthogonal form of representation. *Science and technology of the Air Forces of the Armed Forces of Ukraine*: sci. and tech. journal, No. 4 (21), pp. 151–157 [in Ukrainian].

С. В. Бурмістров[2], *к.т.н.,*
e-mail: sergijburmistrov@yandex.ua
О. М. Панаско[1], *к.т.н., доцент,*
e-mail: lena.pa@ukr.net
О. Д. Лайтаров[2], *студент 6-го курсу*
e-mail: vendenta95@gmail.com
[1]Черкаський державний технологічний університет
б-р Шевченка, 460, м. Черкаси, Україна, 18006
[2]Київський національний університет технологій та дизайну
вул. В. Чорновола, 241, м. Черкаси, Україна, 18028

МОДЕРНІЗАЦІЯ ПОСИМВОЛЬНИХ ШИФРУВАЛЬНИХ ПРИСТРОЇВ НА ОСНОВІ АНАЛОГУ ШИФРУ ВЕРНАМА

В статті розроблено функціональну схему шифрувального пристрою, що є реалізацією одного з варіантів модернізації німецької стаціонарної шифрувальної машини Лоренца. Пристрій працює шляхом накладання шифротексту на основний текст сповіщень. Має абсолютну криптографічну стійкість за умови використання умов, аналогічних умовам експлуатації Лоренци, але при цьому не використовує систему шифрування Вернама.

Перевагою запропонованого посимвольного шифрувального пристрою є значно потужніший алфавіт шифротексту. Він складається в ***(n-1)!*** *раз більше символів, ніж в шифрі Вернама, що суттєво підвищує його криптостійкість.*

У конструкції запропонованого шифрувального пристрою шифротекст кодування не дорівнює шифротексту декодування. Тому для уніфікації прийомної і передаючої частини пристрою в його конструкцію запропоновано ввести додатковий блок – блок формування зворотного шифротексту, який автоматично формує шифротекст кодування на основі шифротексту декодування.

Основою вказаного проекту є розроблений спеціальний програмний комплекс для розрахунку принципової електричної схеми блоку формування зворотного шифротексту.

Ключові слова: *стаціонарна телепринтерна шифрувальна машина – Лоренца, система Вернама, шифротекст кодування, шифротекст декодування, блок формування зворотного шифротексту.*