V. A. Luzhetskyi, Dr. Sc. (Eng), Prof.; A. V. Dmytryshyn

ALTERNATIVE MODES OF BLOCK CIPHERING

There had been analyzed the operation of basic modes of block ciphering with the observation of their construction peculiarities. On the basis of the received results there had been developed the new schemes of block ciphering operation mode which enable to improve cryptographic stability of the ciphering process.

Key words: *information protection, symmetrical block ciphers, modes of block ciphering, block ciphering keys, stages of subkeys modification.*

Introduction

One of the efficient methods of information cryptographic protection is the use of symmetrical block ciphers. Symmetrical ciphers is the class of cryptographic algorithms which use sets of identical primitive operations with the same key for both enciphering and deciphering. There are two types of symmetrical ciphers: stream cipher and block cipher. The process of open text one element ciphering (symbol or one bit) which is practically reduced to the process of gamma xoring is performed by stream symmetrical ciphers and each element of the open text shall be enciphered independently. In symmetrical block ciphers unlike in stream once the groups of open text elements (data blocks) are subject to processing. During such ciphering each data block to be processed first of all undergoes transformations within some rounds, which, in turn, causes the avalanche effect. Secondly, each element of the data block depends on all elements of this block.

Symmetrical ciphers are used for the confidential data holding on storage media and information ciphering during the process of network transfer.

But in case of using symmetrical block cipher without supplementary cryptographic transformations such ciphering would suffer from some drawbacks. Particularly in such cases it is impossible to conceal information structure which is under protection due to using blocks of fixed size and the same secret key during ciphering. Therefore to remove negative ciphering peculiarities and depending on the branch, there is introduced a range of basic block ciphering modes which are standardized by National Institute of Standards and Technology:

- Electronic Codebook (ECB)
- Cipher Block Chaining (CBC)
- Cipher Feedback (CFB)
- Output Feedback (OFB)
- Counter Mode (CTR)

Besides the mentioned above modes there had been developed a range of new ciphering modes [2 – 8] which may be used during information protection, particularly the CTR mode [2] had been introduced as addition to the standard «NIST Special Publication 800-38A 2001 Edition – Recommendation for Block Cipher Modes of Operation. Methods and Techniques» [1].

The purpose of this paper is to improved the stability of ciphering with the use of symmetrical block ciphers due to using new schemes of mode operation of block ciphering.

The main tasks of the research is the following:

1. Analysis of block ciphering basic modes which are used in schemes of symmetrical block ciphering.
2. Development of the approach for using new schemes of block ciphering mode operation which enables to improve cryptographic ciphering stability.

Analysis of basic block ciphering modes

1. Mode of electronic code book

The first and the very easy block ciphering mode is the mode of electronic code book (ECB) [1].

Using this mode, the open text shall be divided into n-bits blocks and each block shall be enciphered independently. The process of enciphering and deciphering is described by the following formulas:

$$C_i = E_K(P_i),\ P_i = D_K(C_i), \tag{1}$$

where E, D – correspondently, functions of enciphering and deciphering;

P_i, C_i – i^{-th} n-bits block of open and enciphered text correspondently, i=1, 2, 3, ...;

K – n-bits secret ciphering key.

The main advantage of ECB mode is the possibility of simultaneous ciphering range of data blocks and self-synchronization support, e.g. the damage of i-enciphered text block influences only the same deciphered block.

However such ciphering process has a number of disadvantages:

- the same blocks of open text causes the appearance of the same blocks of enciphered text;
- permutation of enciphered text blocks causes the permutation of correspondent open text blocks, which results in disturbance of information integrity;
- it is impossibility to conceal information structure which is to be protected.

Some block ciphering basic modes, particularly ECB mode, are vulnerable to attacks based upon pair of known and enciphered texts and to attack called "birthday". Besides, it is well known that when the large volume of information is enciphered with the same secret key, the enciphered block text contains the information on open text. The paper [3] mentions this fact.

If open text blocks accept a random form, which meets the Law on Equal Distribution, and are enciphered with the same secret key, the information drain on open text in the enciphered text takes place with the following value of probability:

$$p_s = 1 - \left(1 - 2^{-n}\right)^{s(s-1)/2}, \tag{2}$$

where $s = 2^{(n+1)/2}$, p_s≈0,63.

According to the paradox "birthday" there is a pair $C_i = C_j$ with probability p_s for ECB mode, for s n-bits blocks of enciphered texts C_1, …, C_s. Thus the first of disadvantages of ECB mode becomes a serious barrier for this mode usage, since a malefactor can immediately find out that $P_i = P_j$.

2. The mode of enciphered text blocks concatenation

In the mode of enciphered text blocks concatenation [1], i-open text block and (i-1)- of enciphered text block are concatenated with modulo two addition, before the enciphering process which is conducted in the following way:

$$C_i = E_K(P_i \oplus C_{i-1}),\ P_i = D_K(C_i) \oplus C_{i-1},\ C_0 = IV, \tag{3}$$

where ⊕ – modulo two addition; IV – initialization vector.

The advantage of CBC mode is the absence of disadvantages which are of ECB character, namely the support of the open text structure concealment and absence of possibility for transference of blocks of enciphered text, which are attained due to the fact that each following block of enciphered text depends on previous blocks. But in its turn, this does not allow the simultaneous enciphering several open text blocks.

Besides the advantages mentioned above it is worth to state that this mode allows to multisequence the deciphering enciphered text blocks and supports self-synchronization. Provided during data transferring or data recording i-enciphered text block had been damaged, only i and (i+1) open text blocks would be damaged within deciphering.

Similar open text blocks cause appearance of different enciphered text blocks, this fact in its turn makes impossible to use the enciphered text blocks transposition for open text content modification in contrast to ECB mode. Due to this CBC ciphering mode also can be used as a medium for providing information integrity and protection from falsification.

But for the CBC mode, as well as for ECB mode there are *s* *n*-bits enciphered text blocks C_1, ..., C_t such, that $C_i = C_j$ with probability p_s [3]. That is $P_i \oplus C_{i\text{-}1} = P_j \oplus C_{j\text{-}1} \rightarrow P_i \oplus P_j = C_{i\text{-}1} \oplus C_{j\text{-}1}$. In case an assaulter has the access to several sets of enciphered texts C^1, …, C^t, where each set C^l consists of s_l enciphered text blocks, the general sample volume, the malefactor works with, equals to:

$$s = \sum_{l=1}^{t} s_l \ . \tag{4}$$

Thus using the paradox "birthday", the malefactor may substitute the pair of enciphered text blocks ($C_{i\text{-}1}$, C_i) for ($C_{j\text{-}1}$, C_j) regardless that the open text blocks $P_{i\text{-}1}$ and $P_{j\text{-}1}$ will not be reliable to receive the rest of the open text blocks during deciphering, which would be equivalent to the original blocks. Furthermore the malefactor having several enciphered text sets may substitute the whole groups of enciphered text ($C_{i\text{-}1}$, …, $C_{i\text{-w}}$) for ($C_{j\text{-}1}$, …, $C_{j\text{-w}}$), if $C_i = C_j$ и $C_{i\text{-w}} = C_{j\text{-w}}$.

In the same way as mentioned in the papers [7, 9] ciphering basic functions in CBC mode may be attacked with pair of known open text. That is, then input value which is supplied into the enciphering function is calculated with modulo two addition of current open text block to the previous enciphered text block and the ciphering output is a current enciphered text block.

3. Enciphered Text Feedback Mode

In the enciphered text feedback mode the open text blocks are modulo two added to gamma blocks. The first gamma block is formed with n-bits initial vector ($1 \le n \le b$), which is recorded in low *n*-bits of *b*-bits input block I_l, which together with the secret key *K* are fed for ciphering function. *n*-high bits of ciphering output data block act as gamma, which is modulo two added to open text block that results in enciphered text block. The input the j^{-th} block I_j is a concatenation result of low (*b-n*)-bits of previous input block $I_{j\text{-}1}$, which are recorded to high (*b-n*)-bits of *b*-bits input block I_j and *n*-bits of the enciphered text block $C_{j\text{-}1}$, which are recorded to low *n*-bits of *b*-bits input block I_j etc.

The process of open text block enciphering and enciphered text blocks deciphering is performed in the following way:

$$I_1 = IV\ ,\ I_j = \left(I_{j-1} << n\right) \| \, C_{j-1}\, ,\ O_j = E_K\left(I_j\right),$$

$$C_j = P_j \oplus \left(O_j >> \left(b-n\right)\right),\ P_j = C_j \oplus \left(O_j >> \left(b-n\right)\right). \tag{5}$$

where I_j – *b*-bits input block ; O_j – *b*-bits output block;

>>, << – operations of dextral and sinistrial shift correspondingly.

The possibility to conceal the open text structure and synchronization support is considered to be the positive peculiarities of CFB mode, i.e. if 1 bit of any enciphered text block would be lost, in addition *b*/*n* open text blocks will be damaged during enciphering. As in the CBC mode, deciphering may be multisequenced but enciphering may not, since each following enciphered text block depends on all previous blocks.

CFB mode suffers from the same drawback under "birthday" attack, as CBC mode. That means, that such enciphered text pairs, that C_i = Cj, exist with the possibility p_s. From this $P_i \oplus (O_i >> (b\text{-}n)) = P_j \oplus (O_j >> (b\text{-}n)) \rightarrow P_i \oplus P_j = (O_i >> (b\text{-}n)) \oplus (O_j >> (b\text{-}n)) \rightarrow P_i \oplus P_j = C_{i\text{-}1} \oplus C_{j\text{-}1}$.

In particular, ciphering basic function attack in CFB mode may be fulfilled with the attack based upon the known open text pairs [7]. Besides the input value may be calculated on the basis of information on previous enciphered text blocks, and ciphering output is calculated as modulo two addition of current open text block to the correspondent enciphered text block.

4. Output Feedback Mode

Output feedback mode is a confidential mode, in which a sequence of n-bits output blocks *Oj* are generated from the initial vector *IV* , they are modulo two added to open text blocks *Pj* for obtaining enciphered text blocks and vice versa.

Ciphering and deciphering is performed in the following way:

$$I_1 = IV\,,\ I_j = O_{j-1}\,,\ O_j = E_K\left(I_j\right),\ C_j = P_j \oplus O_j\,,\ C_N^* = P_N^* \oplus \left(O_j >> (n-u)\right),$$

$$P_j = C_j \oplus O_j\,, P_N^* = C_N^* \oplus \left(O_j >> (n-u)\right), \tag{6}$$

where I_j – n-bits input block;

P^*_N, C^*_N – last u-bits blocks of open and enciphered text correspondently.

If last open text block P^*_N consists of u-bits, this open text block is modulo two added to u of the most significant bits of the last output block. Furthermore, the initial vector *IV* must be unique for each message ciphered with the set key. The possible methods for initial vector *IV* generation are described in [1].

The main OFB mode advantage, in comparison with modes, is that damage of one bit of the enciphered text influences the same bit of the open text. Also there is a possibility to conceal the open text structure. However OFB mode suffers from the following drawbacks:

- absence of possibility to overlap enciphering and deciphering several data blocks in time;
- necessity to resynchronize periodically;
- vulnerability to modification of separate bits of enciphered text.

In OFB mode, as in the previous modes, ciphering may be cracked with the attack based upon known text pairs [7]. It means, if open text and enciphered text are known it is considerably easy to find output as well as input blocks of ciphering function.

5. “Counter” mode

CTR mode is similar to previous mode. But in the “counter” mode not the previous output of ciphering function is subject to ciphering, but the counter value Tj, which is multiplied by a certain constant number at every step. Ciphering process is described by the following formulas [1]:

$$O_j = E_K\left(T_j\right)_,\ C_j = P_j \oplus O_j{}_,\ C_N^* = P_N^* \oplus \left(O_j >> (n-u)\right)_,$$

$$P_j = C_j \oplus O_j{}_,\ P_N^* = C_N^* \oplus \left(O_j >> (n-u)\right)_. \tag{7}$$

Positive peculiarities of CTR mode are the following [2]:

j-enciphered text block Cj may be enciphered in a random way;

- enciphering and deciphering may be multisequenced;
- information structure that is under protection can be concealed.

Negative peculiarities of CTR mode are the following drawbacks:

- error in one bit of enciphered text influence only correspondent bit of the open text;
- it is necessary to resynchronize counter periodically;
- mode is vulnerable to modification of separate bits of enciphered text.

If in this mode the “weak” block cipher is used a counter periodicity may be taken for differential crypto analysis attack [2].

The above drawbacks of basic ciphering modes and specificity of its use creates conditions for alternative ciphering modes developing.

Nowadays alternative modes’ schemes for block ciphering are created:

- on the basis of the open and enciphered text block concatenation, particularly such methods are described in the papers [3], [8], [10] etc.;
- on the basis of counter mode modifications [7];
- on the basis of modifications of the mode of back action along enciphered text [11];

- with matrix ciphering, when one data sub block is ciphered within different data blocks [6];
- on the basis of Feistel cipher [4, 5].

The above basic and alternative ciphering modes fulfill binding at the level of open and enciphered text blocks, which have both advantages and disadvantages.

However there is another approach to creating text block ciphering modes based upon the usage of different ciphering keys for each data block. This approach was realized in the key feedback mode [12]. Such a mode is similar to OFB mode but feedback is organized not along an output, but along a key.

Authors of this paper suggest an approach, which allows to fulfill binding at the level of key decompression procedures.

Keys Concatenation modes

Each symmetrical block cipher is described by two main components: key decompression procedure and ciphering procedure. Key decompression procedure is used to form sub keys set for the following usage in ciphering procedure. Ciphering procedure fulfills immediate data transformation, i.e. data blocks enciphering and deciphering. Depending on functional purposes, key decompression procedures are divided into two groups [13].

The first group consists of keys decompression procedures, which form the sub keys for data block sequences. Key decompression procedures, which form the sub keys for one data block ciphering rounds refer to the second group and include three basic stages of key modification [14]: initial, main and final.

Initial stage of key modification is intended for performing an initial secret key transformations and forming an input set for main stage of key processing. At the second stage sub keys set is formed from received data for its further using at the final stage of modification. The following requirements to transformations of this stage are set:

- restoring the ciphering key K based upon specified sub key must be quite difficult;
- every bit of input ciphering key must influence each sub key.

At the stage of final key modification, the sub key set is transformed into the form applicable to be used in ciphering procedure.

The mentioned above stages of key modification are used to obtain sub keys sets for the rounds of first data block$\{S\}_1$ ciphering, in fact this block is the first block key from the secret ciphering key *K*. The authors of this paper suggests the following modes of block log in concatenation.

1. Iterative sub keys concatenation mode. To form sub keys set $\{S\}_i$ ($i=\overline{2,N}$, where N – quantity of sub keys sets) the following transformations are fulfilled:

$$S_{1,i} = f_t\left(S_{k,i-1}\right),\ S_{j,i} = f_t\left(S_{j-1,i}\right), \tag{8}$$

where $S_{j,i}$ – the j^{-th} *m*-bits sub key of the i^{-th} block key , $j=\overline{1,k}$, *k* – Sub keys number in a set ; f_t – random reflection function *m*-bits in *m*-bits, in of case ciphering *t* fulfillment , $t=\{e,\ d\}$, *e* – enciphering operations , *d* – deciphering operation; *m* – sub keys digit.

During the execution of this mode for the formation of the first set of subkey $\{S\}_{1,}$ the secret ciphering key *K* is used. To obtain the first sub key of the i^{-th} block key the k^{-th} sub key of the $(i\text{-}1)^{-th}$ block key is transmitted to function f_t. To form the j^{-th} sub key of the i^{-th} block key (*j*-1)-sub key of *i*-block key is transmitted to function f_t etc. (fig. 1).

For this mode it is impossible to multisequence the process of sub keys reevaluation, since to reevaluate the j^{-th} sub key the value of the $(j\text{-}1)^{-th}$ sub key is used and to reevaluate the i^{-th} block key the $(i\text{-}1)^{-th}$ block key is used.

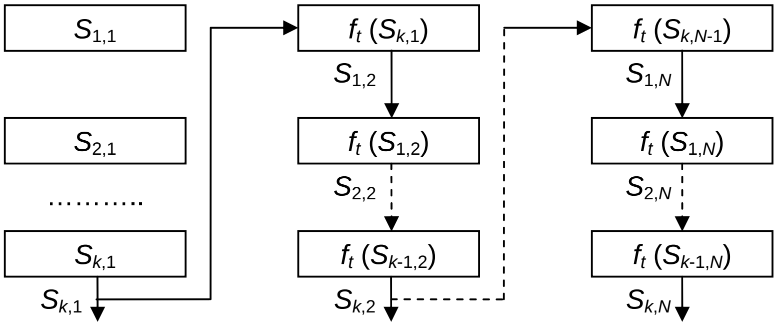

Fig. 1. Scheme of iterative sub keys concatenation mode

2. Sub keys concatenation consequent mode is used to form sub keys set $\{S\}_i$ following this rule

$$S_{j,i} = f_t\left(S_{j,i-1}\right). \tag{9}$$

As in the previous mode secret ciphering key K is used to form the first block key $\{S\}_1$. In the obtained sub keys set $\{S\}_1$, each sub key independently on each other comes to function f_t, which output results in forthcoming block key $\{S\}_2$ etc. (fig. 2).

Since the j^{-th} and the $(j\text{-}1)^{-th}$ sub keys of the i^{-th} block key are not linked together, for the defined mode the process of parallel sub key computation may be organized.

3. Combined mode. This mode consists in simultaneous use of both, previous concatenation modes and may be described by the following formula:

$$S_{1,i} = g_t\left(S_{k,i-1}, S_{1,i-1}\right),\ S_{j,i} = g_t\left(S_{j-1,i}, S_{j,i-1}\right), \tag{10}$$

where g_t – function of arbitrary displaying $2m$-bits as m-bits.

Thus, the process of the second block key obtaining consists in fulfillment of one steps. Firstly the first $S_{1,i\text{-}1}$ and the last $S_{k,i\text{-}1}$ sub keys of the $(i\text{-}1)^{-th}$ block key are transmitted to function g_t , to obtain the first sub key of the i^{-th} block key. Secondly, the obtained sub key and the second sub key of the $(i\text{-}1)^{-th}$ block key participates in forming the second sub key $S_{2,i}$ of the second block key that are coming to function g_t. Transformations that form the j^{-th} sub key of the i^{-th} block key are conducted in accordance with formula (10) (fig. 3). The first block key is identified following the rules stipulated for in the ciphering key (K) decompression procedure.

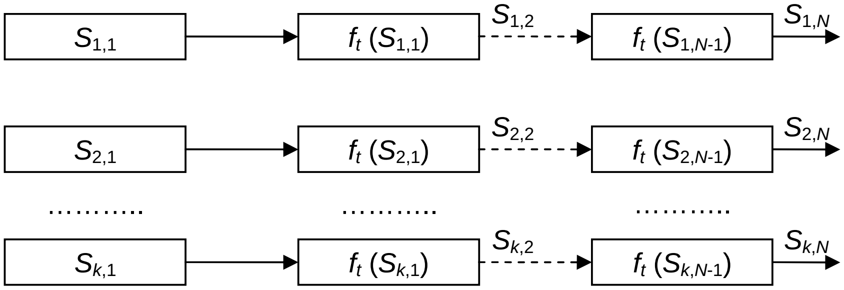

Fig. 2. Scheme of sub keys concatenation consequent mode

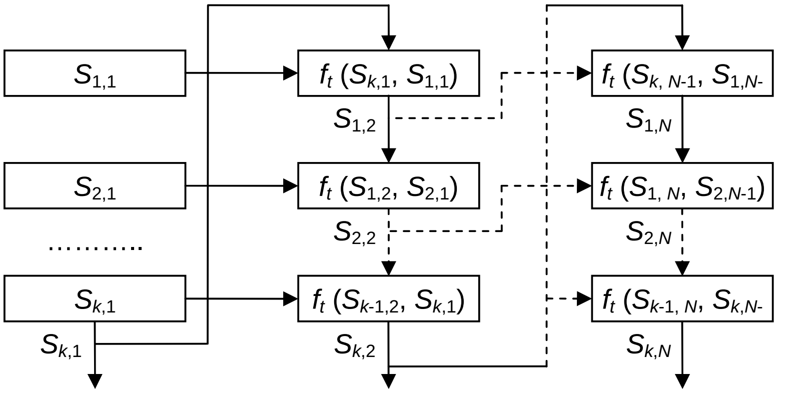
$S_{1,1}$
$S_{2,1}$
……….
$S_{k,1}$
$S_{k,1}$
$f_t\ (S_{k,1}, S_{1,1})$
$S_{1,2}$
$f_t\ (S_{1,2}, S_{2,1})$
$S_{2,2}$
$f_t\ (S_{k\text{-}1,2}, S_{k,1})$
$S_{k,2}$
$f_t\ (S_{k,\ N\text{-}1}, S_{1,N\text{-}}$
$S_{1,N}$
$f_t\ (S_{1,\ N}, S_{2,N\text{-}1})$
$S_{2,N}$
$f_t\ (S_{k\text{-}1,\ N}, S_{k,N\text{-}}$
$S_{k,N}$

Fig. 3. Scheme of sub keys concatenation combined mode

Combined mode does not support the multisequent computation of sub keys for the i^{-th} block key, since the $(j\text{-}1)^{-th}$ sub key of the current block key participates in forming the j^{-th} sub key of the same block key.

Since in some symmetrical block ciphers [15] key decompression time substantially exceeds enciphering/deciphering one data block, therefore for using key decompression modes mentioned above it is necessary to observe the following requirement: sub key decompression time must be less enciphering/deciphering time of one data block.

The following drawback, that diminish the attractiveness of using key decompression modes, consists in ciphering total time increase. Even if key decompression time would not exceed the data ciphering time, the total time will be doubled. However, considering modern trends of development of microprocessor-based technique we may conclude that every personal computer will be multinuclear in the nearest future. Therefore the processes of keys decompression and data ciphering can be simultaneous.

The keys formed in the key decompression mode provide for the following:

- identical open text blocks correspond with the different enciphered text blocks;
- possibility to conceal open the text structure;
- possibility to identify the fact of message integrity disturbance in case of text block permutation;
- ciphering procedure does not require the initialization vectors;
- possibility of simultaneity of block key identification and data block ciphering;
- absence of errors spreading (error in one block of enciphered text causes the mistaken deciphering of only the block).

The drawback of using key decompression mode consists in impossibility of simultaneous ciphering several data blocks.

The key decompression modes also allow to increase the block ciphering resistibility to “birthday” attack due to using block keys. Consequently if $C_i = C_j$, $P_i \neq P_j$. Furthermore for ECB, CBC and CFB modes the malefactor with several enciphered text sets may substitute the whole groups of enciphered text blocks ($C_{i\text{-}1}$, …, $C_{i\text{-w}}$) to ($C_{j\text{-}1}$, …, $C_{j\text{-w}}$), if $C_i = C_j$ and $C_{i\text{-w}} = C_{j\text{-w}}$. In case of using the key decompression modes, this substitution is impossible, since the open text after deciphering will be distorted.

Depending on the used keys decompression mode, the period of block key formation may change. This period will be determined by function of key sequence formation, which must:

- be easy in realization in software as well as in hardware-based realization, not to increase essentially ciphering time;
- make quite difficult the restoration of the $(i\text{-}1)^{-th}$ block key value in case of the i^{-th} key is known;
- the function has to ensure the sufficiently long period of T key sequence, which allows to cipher the texts of any volume.

Conclusions

Part of basic block ciphering modes, particularly ECB, CBC and CFB modes, are vulnerable to "birthday" attack, with the help of which, using the same secret key, it is possible to obtain information on open text and disturb the open text integrity.

The above drawbacks of block ciphering basic modes and specificity of its use creates conditions for alternative ciphering modes search, modes which are based upon modification of symmetrical block ciphering basic modes and fulfill binding at the level of open and enciphered text blocks.

However, there is the other approach to block ciphering modes construction, based upon different ciphering keys use for every data block, which also increases cryptographycal ciphering resistance, particularly this approach was realized in the key feedback mode.

This paper has suggested exactly this approach, when different block keys are used for every data block. The suggested modes ensure personal block key formation for every data block, that increases cryptographycal ciphering resistance with holding majority of basic ciphering modes' advantages. Thus, for instance, the malefactor should look through enciphered/deciphered text pairs in T times more than in basic ciphering modes.

References

1. NIST Special Publication 800-38A 2001 Edition – Recommendation for Block Cipher Modes of Operation. Methods and Techniques // Computer Security Division Information Technology Laboratory National Institute of Standards and Technology, Gaithersburg, MD 20899-8930. December 2001.

2. Lipmaa H. CTR-mode encryption / H. Lipmaa, Ph. Rogaway and D. Wagner // Submission of modes of operation, 2001. – P. 4. – Режим доступу до ресурсу: http://csrc.nist.gov/groups/ST/toolkit/BCM/documents/proposedmodes/ctr/ctr-spec.pdf.

3. Knudsen L. R. Block chaining modes of operation / L. R. Knudsen // Reports in informatics No 207, October 2000. – P. 16. – Режим доступу до ресурсу: http://csrc.nist.gov/groups/ST/toolkit/BCM/documents/proposedmodes/abc/abc-spec.pdf.

4. Brier E. BPS: a format-preserving encryption proposal / E. Brier, Th. Peyrin and J. Stern – P. 11. – Режим доступу до ресурсу: http://csrc.nist.gov/groups/ST/toolkit/BCM/documents/proposedmodes/bps/bps-spec.pdf.

5. Bellare1 M. The FFX Mode of Operation for Format-Preserving Encryption. Draft 1.1. / M. Bellare1, Ph. Rogaway and T. Spies // February 20, 2010. – P. 18. – Режим доступу до ресурсу: http://csrc.nist.gov/groups/ST/toolkit/BCM documents/proposedmodes/ffx/ffx-spec.pdf.

6. Belal A. A. 2D-Encryption mode. / A. A. Belal, M. A. Abdel-Gawad // March, 2001. – P. 32. – Режим доступу до ресурсу: http://csrc.nist.gov/groups/ST/toolkit/BCM/documents/proposedmodes/2dem/2dem-spec.pdf.

7. Головашич С. А. Безопасность режимов блочного шифрования / С. А. Головашич // Радиотехника: Всеукр. межвед. научн.-техн. сб. – Х.: ХНУРЭ, 2001. – Вып. 119. – С. 135 – 145.

8. Дмитришин О. В. Режим керованого зчеплення блоків зашифрованого тексту / О. В. Дмитришин, В. А. Лужецький // Вісник ВПІ. – Вінниця, Видавництво Вінницького національного університету, 2009 – № 1. – С. 34 – 36.

9. Biham E. Differential cryptanalysis of Feal and N-hash / E. Biham, A. Shamir // Advances in Cryptology Proceedings Eurocrypt'91, LNCS 547, D.W. Davies, Ed.,Springer-Verlag, 1991. – pp. 1 – 16.

10. Gligor V. D. On Message Integrity in Symmetric Encryption / V. D. Gligor, P. Donescu // November 10, 2000. – P. 41. – Режим доступу до ресурсу: http://csrc.nist.gov/groups/ST/toolkit/BCM/documents/proposedmodes/ige/ige-spec.pdf.

11. Mattsson Ul. T. Format-controlling encryption using datatype-preserving encryption / Ul. T. Mattsson // June 30, 2009. – P. 46. – Режим доступу до ресурсу: http://csrc.nist.gov/groups/ST/toolkit/BCM/documents/proposedmodes/fcem/fcem-spec.pdf.

12. Hastad J. Key Feedback Mode: a Keystream generator with Provable Security / J. Hastad, M. Naslund // October 11, 2000. – P. 23. – Режим доступу до ресурсу: http://csrc.nist.gov/groups/ST/toolkit/BCM/documents/proposedmodes/kfb/kfb-spec.pdf.

13. Лужецький В. А. Процедури розгортання ключів для блокових шифрів на основі арифметичних операцій за модулем / В. А. Лужецький, О. В. Дмитришин // Інформаційні технології та ком'ютерна інженерія. – Вінниця, Видавництво Вінницького національного університету, 2009 – № 2. – С. 69-74.

14. Коркішко Т. Алгоритми та процесори симетричного блокового шифрування / Коркішко Т., Мельник А., Мельник В. – Львів: Бак, 2003. – 168 с.

15. Горбенко І. Д. Аналіз властивостей алгоритмів блокового симетричного шифрування (за результатами міжнародного проекту NESIE) / І. Д. Горбенко, Г. М. Гулак та інші // Радиотехника: Всеукр. межвед. научн.-техн. сб. – Х.: ХНУРЭ, 2005 – № 141. – С. 7 – 24.

Volodymyr Luzhetskyy – Doctor of Science(Eng.), Professor, Head of Department for Information Protection.

Olexandr Dmytryshyn – Master on Information Security, Post Graduate Student with the Department for Information Protection.

Vinnytsia National Technical University.