The quantitative comparison between the integer splitting cipher and the traditional gamma cipher

Amanie Alhussain [1] and Vadim L. Stefanuk [1 2]

[1] *Peoples' Friendship University of Russia, Miklukho-Maklaya Street 6, Moscow, 117198, Russia*
[2] *The Institute for Information Transmission Problems of Russian Academy of Sciences, Bolshoy Karetny pereulok 19, Moscow, 127051, Russia*

Abstract

The symbolic integer splitting cipher is a special mathematical method that is proposed by the authors and it can be considered as a generalization of a modular arithmetic operation. In this cipher, each text's symbol is represented as an integer in accordance with the selected code table after that this integer is replaced on the base of another number with a sequence of *k* integers (*k*-splitting level). This study is conducted from the point view of the possible hacker's attack. Two lemmas, which are related to the unauthorized access to the information transmission channel, were proven in this article; the first lemma is related to the probabilistic analysis of unauthorized restoration of the plaintext based on the gamma cipher while the second lemma studied the probabilistic analysis of unauthorized restoration of the plaintext processed by integer splitting cryptosystem. After that a quantitative comparison is performed based on these two lemmas. In the result of our study a conclusion was made that the effectiveness of the splitting cryptosystem supersedes essentially the traditional gamma cipher and also the increase in splitting level leads to greater protection of information and greater level of safety.

Keywords

Integer splitting cipher, gamma cipher, unauthorized plaintext recovery, the level of splitting, probability theory

1. Introduction

The integer splitting method is a certain generalization of the modular arithmetic operation and may be used for as a symmetric encryption method that was described in details in the authors' publication [1].

This method is defined as follows: consider two integers r and a satisfy the inequality $r > a > 0$.

Definition 1. The integer splitting of the number a on the basis of r is the representation of a as a sequence of numbers $a_1, a_2, a_3, \dots, a_{k-1}, a_k$ in which

$$a_1 = \delta^{(2)}, \text{ where } \delta^{(2)} = r \bmod a,$$

$$a_2 = \delta^{(3)}, \text{ where } \delta^{(3)} = r \bmod q^{(2)}, \ q^{(2)} = \left\lfloor \frac{r}{a} \right\rfloor,$$

$$a_3 = \delta^{(4)}, \text{ where } \delta^{(4)} = r \bmod q^{(3)}, \ q^{(3)} = \left\lfloor \frac{r}{q^{(2)}} \right\rfloor,$$

$$\dots\dots \qquad (1)$$

III International Workshop on Modeling, Information Processing and Computing (MIP: Computing-2021), May 28, 2021, Krasnoyarsk, Russia
EMAIL: amanie.alhussain@mail.ru (Amanie Alhussain); stefanuk@iitp.ru (Vadim Stefanuk)
ORCID: 0000-0002-3838-4260 (Vadim Stefanuk)

$$a_{k-1} = \delta^{(k)}, \text{ where } \delta^{(k)} = r \bmod q^{(k-1)}, \ q^{(\text{k-1})} = \left\lfloor \frac{r}{q^{(k-2)}} \right\rfloor,$$

$$a_k = q^{(k)}, \text{ where } q^{(k)} = \left\lfloor \frac{r}{q^{(k-1)}} \right\rfloor,$$

where, δ – is the remainder of the integer division r/a, q – is the integer part of this division, and the symbol $\lfloor \ \rfloor$ means rounding down to the nearest integer. The natural number k is called the splitting level.

Gamma cipher which will be studied in this article can be executed using several mathematical formulas. For example, the encryption process can be performed by the following formula [3, 4]:

$$\text{C= P} \oplus \text{K} \tag{2}$$

where, C, P, K – ASCII codes of the ciphertext, plaintext and gamma, respectively, $\oplus$ – bitwise operation - "exclusive or". The decryption process (plaintext restoration) is performed similarly by using the following formula [3, 4]:

$$\text{P= C} \oplus \text{K}. \tag{3}$$

The suggested integer splitting cryptosystem can be considered as an upgraded version of the traditional gamma cipher which will provide more secrecy based on the selected level of splitting and has the advantage of hiding the length of original plaintext. This cryptosystem performs two steps during the encryption process. The first step will encrypt the plaintext M according to the splitting cipher mentioned in definition 1, and as a result the sender at this step will obtain the intermediate ciphertext $\tilde{C}$ as shown in the following expression:

$$\tilde{C} = \begin{cases} r_i \oplus a \quad npu \quad k = 1 \\ \delta^{(2)}, \delta^{(3)}, \delta^{(4)}, ..., \delta^{(k-1)}, \delta^{(k)}, q^{(k)} \quad npu \quad k > 1 \end{cases} \tag{4}$$

The second step of the encryption process of the splitting cryptosystem will apply the gamma cipher on the intermediate ciphertext $\tilde{C}$ in order to provide more protection of information and as a result we will obtain the final ciphertext C that will be sent to the receiver side, as shown in the following expression:

$$C = \begin{cases} \delta^{(j)} \oplus r_{i+j-1} \quad , \textit{где} \quad j = 2, 3, ..., k \quad npu \, k > 1 \\ q^{(k)} \oplus r_{i+k} \end{cases} \tag{5}$$

At the receiver side, the decryption process will be executed, i.e., the splitting cryptosystem will perform the steps in an inverse order to obtain the plaintext M. So, the first step of the decryption process will apply the gamma decryption model on the received ciphertext C, and as a result the intermediate ciphertext $\tilde{C}$ will be obtained at this step, as shown in the following formula:

$$\tilde{C} = \begin{cases} \delta^{(j)} \oplus r_{i+j-1} \quad , \textit{где} \quad j = 2, 3, ..., k \quad npu \, k > 1 \\ q^{(k)} \oplus r_{i+k} \end{cases} \tag{6}$$

The second step of the decryption process of the splitting cryptosystem will apply the splitting decryption process on the intermediate ciphertext $\tilde{C}$ in order to obtain the original plaintext M, as shown in the following expression:

$$\begin{cases} r_i \oplus \tilde{C} \quad npu \quad k = 1 \\ \dfrac{\left(r_i - \delta^{(j)}\right)}{q^{(j)}} \quad , \textit{где} \quad j = k, k-1, ..., 3, 2 \quad npu \, k > 1 \end{cases} \tag{7}$$

This article will study the quantitative comparison of the integer splitting cryptosystem from the point view of the hacker. It is important to notice that in the article [3] a qualitative comparison was conducted between the symbolic integer splitting method over both synchronous stream ciphers and perfect secrecy ciphers, but in this article the quantitative comparison of the proposed cryptosystem and the gamma cipher will be studied and show how the proposed cryptosystem increases the level of security.

2. Formulation of the main lemmas and their proofs

To perform the quantitative comparison between the gamma cipher and the splitting system we need to prove the following lemmas:

Lemma 1. The probability of a successful unauthorized restoration of the plaintext M from the ciphertext C by applying gamma decryption process is defined by the following formula:

$$\Pr_G(M \mid C,1) = \left(L^N\right)^{-1} \tag{8}$$

where N – is the size of the ciphertext C, which is created for the plaintext M based on the gamma cipher, and L – is the number of all possible events during the search in the key space R, which is used by the attacker and consists of random integers $\{\tilde{r}_1, \tilde{r}_2, ..., \tilde{r}_L\}$.

Proof.

It is assumed that the attacker obtains the ciphertext by simply intercepting the message in the communication channel and also, he knows both the rule of decryption presented in the formula (3) and the ciphertext C, consists of integers $\{c_1, c_2, ..., c_N\}$ with size N, which for him looks like a random sequence of integers. But he does not know the keys (gammas) that were used during the encryption process, so he will be forced to generate a set of independent random integers, which will be formed the space $R = \{\tilde{r}_1, \tilde{r}_2, ..., \tilde{r}_L\}$ with size L, where $L > N$ and he will try to recover the original plaintext M by using this space. The attacker will use a brute force search.

In an attempt to extract the ciphertext C the attacker must perform these steps:

First step: the attacker will begin to perform the brute force search on the space R with repetition. From formula (2), we conclude that each integer, located in the ciphertext C, is calculated using one value $\tilde{r}_i$, where $i = 1, 2, 3, ..., L$. So, the attacker will search with repetition N elements from the set R with size L. The number of all possible outcomes is given by the following expression [5, 6, 9, 10]:

$$n_1 = L^N \tag{9}$$

The second step consists in an attempt to extract the plaintext M by using the rule, which is described in formula (3), with the help of the ciphertext C and the generated set of keys R obtained in the first step.

Consider the event $\Pr_G(M \mid C,1)$ – The probability of a successful unauthorized restoration of the plaintext M from the ciphertext C by applying gamma decryption process, and it is determined by the following formula:

$$\Pr_G(M \mid C,1) = \frac{p_1}{s_1} \tag{10}$$

where, p_1 – is the number of all attempts to restore a meaningful plaintext M, s_1 – is the total number of all possible attempts to restore the value of the plaintext M.

First, let's find s_1 – the total number of all possible attempts to get the plaintext M. From formula (9), the number s_1 is determined by the following expression:

$$s_1 = L^N \tag{11}$$

Second, let's find p_1 – the number of meaningful restoration events of the plaintext M.

Of all the attempts to restore the plaintext M, only one case will give a meaningful plaintext that matches what is encrypted by the sender. This is a situation where the selected keys on the attacker's side match the same keys that were used by the sender during the encryption process of the plaintext [6,8]. So, this leads to the fact that the number of correct extractions of a meaningful text, which meets the plaintext, is equal to one.

$$p_1 = 1. \tag{12}$$

Replacing the values of s_1 and p_1, from equations (11) and (12) in the formula (10), we obtain the result:

$$\Pr_G(M \mid C,1) = \frac{1}{L^N} = \left(L^N\right)^{-1} \tag{13}$$

The proof of Lemma 1 is complete.

Lemma 2. The probability of a successful unauthorized restoration of the plaintext M based on the result of splitting cryptosystem C decreases exponentially with increasing the level of splitting k according to the expression:

$$E\,\Pr_{S\cap G}(M \mid C,k) = \left(L^N \sum_{i=2}^{k} (L-N)^{\left\lfloor \frac{N}{i} \right\rfloor} \right)^{-1} \tag{14}$$

where, N – is the size of the ciphertext C created for the plaintext M based on the splitting cryptosystem, and L – is the number of all possible events in the keys' space R, which is consisted of random integers $\{\tilde{r}_1, \tilde{r}_2, ..., \tilde{r}_L\}$ used by the hacker during the brute force search.

Proof.

It is assumed that the attacker obtains the ciphertext C by simply intercepting the message in the communication channel (attack based on ciphertext).

In this case, the attacker knows the ciphertext C, which represents a sequence of integers and also, he knows the rules of restoration the symbol stated in equations (6) and (7). But the level of splitting k is assumed to be unknown to him. In addition, the gammas that were used during the encryption are also unknown, so the attacker will be forced to generate a set of random integers R and try to recover the plaintext.

Thus, the attacker has a set of integers $C = \{c_1, c_2, ..., c_N\}$ with size N, which for him looks like a random sequence of integers. The attacker knows the encryption methods of the splitting cryptosystem that are used in the formulas (4) and (5) and also, he knows the decryption process of the splitting cryptosystem that are shown in formulas (6) and (7), so he will first build a set of independent random integers

$$R = \{\tilde{r}_1, \tilde{r}_2, ..., \tilde{r}_L\} \text{ of size } L \text{ where } L > 2N. \tag{15}$$

The method that is used by the attacker will be based on a brute force procedure.

Since the attacker does not know the value of k, he will try different values of the splitting level k, starting with $k = 2$.

a. Assessment the probability of unauthorized recovery of the plaintext at the splitting level $k = 2$

In an attempt to retrieve the plaintext M at level $k = 2$, the attacker must follow the outlined steps in the following formula:

$$\Pr_{S\cap G}(M \mid C,2) = \Pr_{S/G}(M \mid \tilde{C},2) \times \Pr_G(\tilde{C} \mid C,1) \tag{16}$$

where, $\Pr_{S\cap G}(M \mid C,2)$ – is the probability of a successful unauthorized recovery of the plaintext M from the result of splitting C at $k = 2$ by applying the splitting decryption process and gamma decryption process successfully, $\Pr_{S/G}(M \mid \tilde{C},2)$ – is the probability of a successful unauthorized recovery of the plaintext M from the intermediate ciphertext $\tilde{C}$ at $k = 2$, on condition, that the event of a successful unauthorized recovery of the intermediate ciphertext $\tilde{C}$ from the result of splitting cryptosystem C by applying the gamma decryption process has occurred successfully, $\Pr_G(\tilde{C} \mid C,1)$ – is the probability of a successful unauthorized restoration of the intermediate ciphertext $\tilde{C}$ from the result of splitting cryptosystem C by applying gamma decryption process.

First step: calculating the probability of a successful unauthorized restoration of the intermediate ciphertext $\tilde{C}$ from the result of splitting system C by applying gamma decryption process, i.e. $\Pr_G(\tilde{C} \mid C,1)$.

From Lemma 1, we have:

$$\Pr_G(\tilde{C} \mid C, 1) = \left(L^N\right)^{-1} \tag{17}$$

Second step: calculating the probability of a successful unauthorized recovery of the plaintext M from the intermediate ciphertext $\tilde{C}$ at $k=2$, on condition, that the event of a successful unauthorized recovery of the intermediate ciphertext $\tilde{C}$ by applying the gamma decryption process has occurred successfully, i.e., $\Pr_{S/G}(M \mid \tilde{C}, 2)$.

Sub-step 2.1: splitting the obtained ciphertext $\tilde{C}$ into pairs of two integers. Each symbol is represented by two elements in space $\tilde{C}$ at $k=2$. As a result, the number of pairs, studied by the attacker, will be equal to

$$N_2 = \left\lfloor \frac{N}{2} \right\rfloor \tag{18}$$

Sub-step 2.2: the attacker will start a brute force search on the elements of the space R with a repetition. From equation (4), we conclude that in the case of splitting at $k=2$, each pair of two elements is calculated using one value $\tilde{r}_i$ from the space R , which is at this step consisting of $L-N$ elements. At this stage, the attacker will enumerate the values from $\left\lfloor \frac{N}{2} \right\rfloor$ elements with repetition from the values of the set R with the size $L-N$. The number of all possible outcomes is given by the following expression [2, 5-10]:

$$n_2 = (L-N)^{\left\lfloor \frac{N}{2} \right\rfloor} \tag{19}$$

Sub-step 2.3: consists of trying to extract the plaintext M by applying the rule (7) by using both the built pairs of numbers obtained in sub-step 2.1 and the sets of numbers (keys or gammas) obtained in sub-step 2.2.

Consider $\Pr_{S/G}(M \mid \tilde{C}, 2)$ – the probability of a successful unauthorized restoration of the plaintext M based on the intermediate ciphertext $\tilde{c}$ at the level of splitting $k=2$. The probability $\Pr_{S/G}(M \mid \tilde{C}, 2)$ is determined by the following formula:

$$\Pr_{S/G}(M \mid \tilde{C}, 2) = \frac{p_2}{s_2}, \tag{20}$$

where, p_2 – is the number of attempts to restore of a plaintext M meaningfully by the attacker at the level of splitting $k=2$; s_2 – the total number of all possible attempts to restore the value of the plaintext M at $k=2$.

First, let's find s_2 – the total number of all possible attempts to get the plaintext M at the splitting level $k=2$. From formulas (18) and (19), the number s_2 is determined by the following expression:

$$s_2 = (L-N)^{\left\lfloor \frac{N}{2} \right\rfloor}. \tag{21}$$

Now let's find p_2 the number of the events that restore a plaintext M meaningfully.

Of all attempts to recover the plaintext, only one case will produce a meaningful plaintext that matches what is encrypted by the sender. This is a case when the selected gammas on the attacker's side match the same gammas that are used by the sender's side when encrypting the plaintext [6, 8]. This leads to the fact that the number of correct extractions of a meaningful plaintext corresponding to the original one is equal to one.

$$p_2 = 1. \tag{22}$$

Replacing the values of s_2 and p_2, from equations (21) and (22) in formula (20), we obtain the result:

$$\Pr_{S/G}(M \mid \tilde{C},2)=\frac{1}{(L-N)^{\left\lfloor \frac{N}{2}\right\rfloor}}=\left((L-N)^{\left\lfloor \frac{N}{2}\right\rfloor}\right)^{-1}. \tag{23}$$

The third step: calculating $\Pr_{S\cap G}(M \mid C,2)$ – the probability of a successful unauthorized recovery of the plaintext M from the result of splitting C at $k=2$ by applying the splitting decryption process and gamma decryption process successfully.

Replacing the values $\Pr_G(\tilde{C} \mid C,1)$ and $\Pr_{S/G}(M \mid \tilde{C},2)$, from equations (17) and (23) in formula (16), we obtain the result:

$$\Pr_{S\cap G}(M \mid C,2)=\Pr_{S/G}(M \mid \tilde{C},2)\times\Pr_G(\tilde{C} \mid C,1)=\left((L-N)^{\left\lfloor \frac{N}{2}\right\rfloor}\right)^{-1}\times\left(L^N\right)^{-1}$$

$$\Pr_{S\cap G}(M \mid C,2)=\left(L^N\times(L-N)^{\left\lfloor \frac{N}{2}\right\rfloor}\right)^{-1} \tag{24}$$

b. Assessment the probability of unauthorized recovery of the plaintext at the splitting level $k=3$

The attacker will start extracting the plaintext at $k=3$, if he fails to extract the correct meaningful plaintext at $k=2$. In an attempt to retrieve the plaintext M at $k=3$ the attacker should follow the outlined steps in the following formula:

$$\Pr_{S\cap G}(M \mid C,3)=\Pr_{S/G}(M \mid \tilde{C},3)\times\Pr_G(\tilde{C} \mid C,1), \tag{25}$$

where, $\Pr_{S\cap G}(M \mid C,3)$ – is the probability of a successful unauthorized recovery of the plaintext M from the splitting system C at $k=3$ by applying both the splitting decryption process and gamma decryption one successfully, $\Pr_{S/G}(M \mid \tilde{C},3)$ – is the probability of a successful unauthorized recovery of the plaintext M from the intermediate ciphertext $\tilde{C}$ at $k=3$, on condition, that the event of a successful unauthorized recovery of the intermediate ciphertext $\tilde{C}$ from C by applying the gamma decryption process has occurred successfully, $\Pr_G(\tilde{C} \mid C,1)$ – is the probability of a successful unauthorized restoration of the intermediate ciphertext $\tilde{C}$ from the result of splitting cryptosystem C by applying gamma decryption process.

First step: calculating $\Pr_G(\tilde{C} \mid C,1)$.

From Lemma 1, we have:

$$\Pr_G(\tilde{C} \mid C,1)=\left(L^N\right)^{-1} \tag{26}$$

Second step: calculating $\Pr_{S/G}(M \mid \tilde{C},3)$.

Sub-step 2.1: splitting the obtained ciphertext $\tilde{C}$ into a combination of three integers. Each symbol is represented by three elements in space $\tilde{C}$ at $k=3$. As a result, the number of combinations, studied by the attacker, will be equal to

$$N_3=\left\lfloor \frac{N}{3}\right\rfloor. \tag{27}$$

Sub-step 2.2: the attacker will start a brute force search on the elements of the space R with a repetition. But the space R in this step will consist of $L-N$ elements, because N elements were correctly selected in the previous step in order to get the ciphertext $\tilde{C}$ correctly from C by applying gamma decryption process. From equation (4), we conclude that in the case of splitting at $k=3$, each combination of three integers is calculated using one value $\tilde{r}_i$ from the space R , which at this step is consisting of $L-N$ elements. At this stage, the attacker will enumerate the values from $\left\lfloor \frac{N}{3} \right\rfloor$ elements with repetition from the values of the set R with the size $L-N$. The number of all possible outcomes is given by the following expression [2, 5-10]:

$$n_3 = (L-N)^{\left\lfloor \frac{N}{3} \right\rfloor} \tag{28}$$

Sub-step 2.3: consists of trying to extract the plaintext M by applying the rule (7) by using both the built combinations of numbers obtained in sub-step 2.1 and the sets of numbers obtained in sub-step 2.2.

Consider $\Pr_{S/G}(M \mid \tilde{C}, 3)$ – the probability of a successful unauthorized restoration of the plaintext M based on the intermediate ciphertext $\tilde{c}$ at the level of splitting $k=3$. The probability $\Pr_{S/G}(M \mid \tilde{C}, 3)$ is determined by the following formula:

$$\Pr_{S/G}(M \mid \tilde{C}, 3) = \frac{p_3}{s_3}, \tag{29}$$

where, p_3 – is the number of attempts to restore the plaintext M meaningfully by the attacker at the level of splitting $k=3$; s_3 – the total number of all possible attempts to restore the value of the plaintext M at $k=3$.

First, let's find s_3 – the total number of all possible attempts to get the plaintext M at the splitting level $k=3$. Since the attacker was obviously unable to extract the correct meaningful plaintext at the previous level ($k=2$), then s_3 is given by the following expression:

$$s_3 = n_2 + n_3, \tag{30}$$

where, n_2 – is the total number of all possible attempts to get the plaintext at the level $k=2$ and n_3 – is the total number of all possible attempts to get the plaintext at the current level $k=3$.

Substituting the values n_2 and n_3 from equations (19) and (28) into expression (30), we obtain the following expression:

$$s_3 = (L-N)^{\left\lfloor \frac{N}{2} \right\rfloor} + (L-N)^{\left\lfloor \frac{N}{3} \right\rfloor} = \sum_{i=2}^{3} (L-N)^{\left\lfloor \frac{N}{i} \right\rfloor}. \tag{31}$$

Now let's find p_3 the number of the events that restore a plaintext M meaningfully.

As discussed previously, only one case will produce a meaningful plaintext that matches what is encrypted by the sender. This is a case when the selected gammas on the attacker's side match the same gammas that are used by the sender's side when encrypting the plaintext [6, 8]. So

$$p_3 = 1. \tag{32}$$

Replacing the values of s_3 and p_3, from equations (31) and (32) in formula (29), we obtain the result:

$$\Pr_{S/G}(M \mid \tilde{C}, 3) = \frac{1}{\sum_{i=2}^{3} (L-N)^{\left\lfloor \frac{N}{i} \right\rfloor}} = \left(\sum_{i=2}^{3} (L-N)^{\left\lfloor \frac{N}{i} \right\rfloor} \right)^{-1}. \tag{33}$$

The third step: calculating $\Pr_{S \cap G}(M \mid C, 3)$. Replacing the values $\Pr_G(\tilde{C} \mid C, 1)$ and $\Pr_{S/G}(M \mid \tilde{C}, 3)$, from equations (26) and (33) in formula (25), we obtain the result:

$$\Pr_{S \cap G}(M \mid C, 3) = \Pr_{S/G}(M \mid \tilde{C}, 3) \times \Pr_G(\tilde{C} \mid C, 1) = \left(\sum_{i=2}^{3} (L-N)^{\left\lfloor \frac{N}{i} \right\rfloor} \right)^{-1} \times \left(L^N\right)^{-1}$$

$$\Pr_{S\cap G}(M \mid C,3) = \left(L^N \times \sum_{i=2}^{3} (L-N)^{\left\lfloor \frac{N}{i} \right\rfloor} \right)^{-1} \tag{34}$$

c. Assessment the probability of unauthorized recovery of the plaintext at the splitting level k.

The attacker will start extracting the plaintext at a level k if he cannot extract the correct meaningful plaintext from all previous levels of splitting.

In an attempt to retrieve the plaintext M at k level, the attacker must follow the outlined steps in the following formula:

$$\Pr_{S\cap G}(M \mid C,k) = \Pr_{S/G}(M \mid \tilde{C},k) \times \Pr_G(\tilde{C} \mid C,1) \text{ ,} \tag{35}$$

where, $\Pr_{S\cap G}(M \mid C,k)$ – is the probability of a successful unauthorized recovery of the plaintext M from the result of splitting C at k by applying both the splitting decryption and gamma decryption successfully, $\Pr_{S/G}(M \mid \tilde{C},k)$ – is the probability of a successful unauthorized recovery of the plaintext M from the result of splitting method $\tilde{C}$ at k, on condition, that the event of a successful unauthorized recovery of the intermediate ciphertext $\tilde{C}$ from C by applying the gamma decryption has occurred successfully, $\Pr_G(\tilde{C} \mid C,1)$ – is the probability of a successful unauthorized recovery of the intermediate ciphertext $\tilde{C}$ from the result of splitting system C by applying gamma decryption.

First step: calculating $\Pr_G(\tilde{C} \mid C,1)$. From Lemma 1, we have:

$$\Pr_G(\tilde{C} \mid C,1) = \left(L^N\right)^{-1} \tag{36}$$

Second step: calculating $\Pr_{S/G}(M_k \mid \tilde{C},k)$.

Sub-step 2.1: splitting the obtained ciphertext $\tilde{C}$ into combinations of k integers. Each symbol is represented by k elements in space $\tilde{C}$. As a result, the number of combinations, studied by the attacker, will be equal to

$$N_k = \left\lfloor \frac{N}{k} \right\rfloor. \tag{37}$$

Sub-step 2.2: The attacker will start a brute force search of the values in the set R with a repetition. The space R in this step will consist of $L-N$ elements, because N elements were correctly selected in the previous step in order to get $\tilde{C}$ correctly from C by applying gamma decryption. From definition 1, we conclude that in the case of the splitting level k, each combination of k integers is calculated using one value $\tilde{r}_i$ from the space R, which is consisting of $L-N$ elements in this step. The attacker will enumerate the values from $\left\lfloor \frac{N}{k} \right\rfloor$ elements with repetition from the values of the set R with the size $L-N$. The number of all possible outcomes is given by the following expression:

$$n_k = (L-N)^{\left\lfloor \frac{N}{k} \right\rfloor} \tag{38}$$

Sub-step 2.3 is trying to extract the plaintext using the rules (7), using combinations of numbers constructed in sub-step 2.1 and combinations of integers obtained in sub-step 2.2.

Consider $\Pr_{S/G}(M_k \mid \tilde{C},k)$ – The probability of a successful unauthorized restoration of the plaintext M based on the intermediate ciphertext $\tilde{C}$ at the level of splitting k, it is determined by the following formula:

$$\Pr_{S/G}(M \mid \tilde{C},k) = \frac{p_k}{s_k} \text{ ,} \tag{39}$$

where, p_k – is the number of attempts to restore of a plaintext M meaningfully by the attacker at the level of splitting k ; s_k – the total number of all possible attempts to get the plaintext M at the splitting level k.

First, let's find s_k. Since the attacker was obviously unable to extract the correct plaintext from all previous levels of splitting, then s_k is given as following:

$$s_k = n_2 + n_3 + ... + n_k \tag{40}$$

where, n_2 – is the total number of all possible attempts to get the plaintext at the level $k = 2$, n_3 – is the total number of all possible attempts to get the plaintext M at the level $k = 3$, and n_k – is the total number of all possible attempts to get the plaintext M at the current level k.

Substituting the values n_k, n_3 and n_2 from equations (38), (28) and (19) into expression (40), we obtain the following expression:

$$s_k = (L-N)^{\left\lfloor \frac{N}{2} \right\rfloor} + (L-N)^{\left\lfloor \frac{N}{3} \right\rfloor} + ... + (L-N)^{\left\lfloor \frac{N}{k} \right\rfloor}$$

Or

$$s_k = \sum_{i=2}^{k} (L-N)^{\left\lfloor \frac{N}{i} \right\rfloor} \tag{41}$$

Similar of what was discussed in the section (a) and (b) the number of correct extractions of the meaningful text, which meets the plaintext M , is equal to one.

$$p_k = 1. \tag{42}$$

Replacing the values of s_k and p_k, from equations (41) and (42) in formula (39), we obtain the result

$$\Pr_{S/G}(M \mid \tilde{C}, k) = \frac{1}{\sum_{i=2}^{k} (L-N)^{\left\lfloor \frac{N}{i} \right\rfloor}} = \left(\sum_{i=2}^{k} (L-N)^{\left\lfloor \frac{N}{i} \right\rfloor} \right)^{-1} \tag{43}$$

The third step: calculating $\Pr_{S \cap G}(M \mid C, k)$.Replacing the values of $\Pr_G(\tilde{C} \mid C, 1)$ and $\Pr_{S/G}(M_k \mid \tilde{C}, k)$, from equations (36) and (43) in formula (35), we obtain the result:

$$\Pr_{S \cap G}(M \mid C, k) = \Pr_{S/G}(M \mid \tilde{C}, k) \times \Pr_G(\tilde{C} \mid C, 1) = \left(\sum_{i=2}^{k} (L-N)^{\left\lfloor \frac{N}{i} \right\rfloor} \right)^{-1} \times \left(L^N \right)^{-1}$$

$$\Pr_{S \cap G}(M \mid C, k) = \left(L^N \times \sum_{i=2}^{k} (L-N)^{\left\lfloor \frac{N}{i} \right\rfloor} \right)^{-1} \tag{44}$$

The equations (24), (34), and (44) lead that Lemma 2 is valid for any natural number k. Lemma 2 is proved.

For example, if we choose the values $N = 9$ and $L = 24$ in accordance with the proven formulas for Lemma 1 and Lemma 2 we obtain the Figure 1: which shows a graph for the behavior of formulas (8) and (14) for the probabilities of unauthorized recovery of the plaintext at the various level of splitting k.

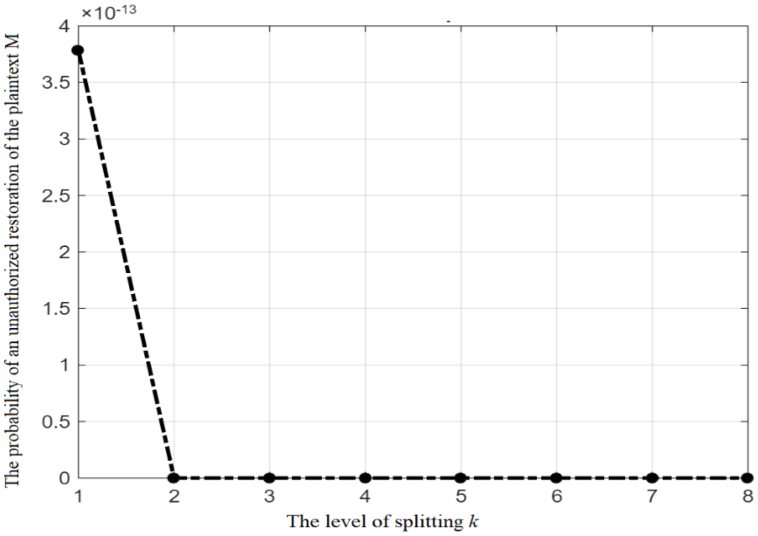

Figure 1: Example of the probability's behavior of an unauthorized recovery of the plaintext at different level of splitting k

Table 1 shows the numerical values of the probabilities' behavior of an unauthorized recovery of the plaintext in case of splitting cryptosystem and gamma cipher for the same values of the graph presented in Figure 1:.

Table 1
The quantitative comparison of the probabilities' behavior of an unauthorized recovery of the plaintext in case of splitting cryptosystem and the gamma cipher

Symbolic splitting cryptosystem		Gamma cipher
k=2	$7.4771*10^{-18}$	$3.7853*10^{-13}$
k=3	$7.0098*10^{-18}$	
k=4	$7.9807*10^{-18}$	
k=5	$7.9788*10^{-18}$	
k=6	$7.9768*10^{-18}$	
k=7	$7.9749*10^{-18}$	
k=8	$7.9730*10^{-18}$	

Table 1 shows the probabilistic analysis when using the gamma cipher at $k = 1$, and when using the splitting cryptosystem at $k > 1$ for the same plaintext. We can conclude that the secrecy of splitting system increases with the level of splitting k. Notice: in the Table 1 in spite that there are little differences in the probabilities at the splitting level $k >= 5$, but we cannot skip these values because of the butterfly effect concept especially in case of applying the splitting system in other fields.

Definition 2. We say that a method that depends on a parameter k has asymptotic secrecy if it satisfies the following condition:

$$\text{when } k \to \infty \text{, then it is executed } \Pr(M \mid C, k) \to 0. \qquad (45)$$

3. Conclusion

This article presents the effectiveness and importance of the splitting cryptosystem over the gamma cipher and what makes it special is its ability to change its level of protection of information by changing the level of splitting. A Lemma was proved that the splitting secrecy of the cryptosystem increases with increasing the splitting level, which allows us to speak about the asymptotical secrecy obtained by the splitting cipher.

4. Acknowledgements

This work was supported by RFBR №18-07-00736A and №17-29-07053. I wish to extend my special thanks to both professor Stefanyuk Vadim Lvovich and professor Orlov Yuri Nikolaevich at the information technology department, Peoples' Friendship University of Russia, Moscow, Russia.

5. References

[1] V. L. Stefanyuk, A. H. Alhussain, "Symmetric Encryption on the Base of Splitting Method" Bulletin of PFUR, Series Mathematics, Information Sciences, Physics 2 (2016) 53-61.

[2] J. C. Skaff Stephanie, Probabilistic and Statistical Methods in Cryptology: An Introduction by Selected Topics, Naval Postgraduate School, (2009)137.

[3] A. Alhussain, The effectiveness of symbolic integer splitting method over both synchronous stream ciphers and perfectly secret ciphers, Journal of Physics: Conference Series 1687 (2020) 012006 1-8. doi:10.1088/1742-6596/1687/1/012006.

[4] D. Melnikov, V. Fomichev, Cryptographic methods of information security, 2, Systemic and applied aspects, Litres, (2021) 243.

[5] E. P. Paul, Concepts of Probability Theory: Second Revised Edition, Courier Corporation (2013) 416.

[6] L. Lester, Introduction to Probability Theory with Contemporary Applications, Courier Corporation (2012) 368.

[7] E. Biham, A. Shamir, Differential Cryptanalysis of the Data Encryption Standard, Springer Science & Business Media (2012), 188.

[8] A. H. Alhussain, "Asymptotic secrecy of the information protection by the usage of simple integer splitting method", IOP Conference Series: Materials Science and Engineering 862 (2020) 1-7. doi:10.1088/1757-899X/862/5/052032.

[9] K. Achim, Probability Theory: A Comprehensive Course, Springer International Publishing (2020) 716.

[10] K. Achim, Probability Theory: A Comprehensive Course, Springer International Publishing (2020) 716.