Construction of Absolutely Failure-free Minimal Data Transmission Systems on Railway Transport

N. V. Medvedeva[a] and S. S. Titov[b]
Ural State University of Railway Transport, Yekaterinburg, Russia

Keywords: Information protection, absolutely failure-free data transmission systems, perfect ciphers.

Abstract: One of the main tasks of the critical infrastructure process control system is information protection. Information security is important for the transport system, including the railway one. The paper proposes a graph approach to the construction of absolutely failure-free data transmission systems by creating ciphers that do not disclose any information about encrypted texts. A class of minimal perfectly secure Shannon ciphers is considered, in which for each pair of ciphertexts and ciphervalues, (x, y) respectively, there are at most two keys on which x is encrypted into y. For ciphers of this class, a graph is defined on a set of keys, namely: two different keys are connected by an edge if there is such a pair (x, y) that on both of these keys the ciphertext x is encrypted into a ciphervalue y. Within the framework of this approach, the necessary and sufficient minimality condition for the inclusion of perfect ciphers is proved. The minimality criterion for the inclusion of perfect ciphers is formulated. Examples illustrating the concepts used and the theoretical statements obtained are constructed. The tables of encryption of perfect ciphers are given, which ensure data protection when they are transmitted over a communication channel on transport.

1 INTRODUCTION

The problem of transmitting short and important messages that are absolutely resistant to a cipher-text attack, due to the specifics of data transmission on transport, is solved by using perfect (according to Shannon) ciphers. In the continuation of research (Medvedeva, 2015; Medvedeva, 2016; Medvedeva, 2019; Medvedeva, 2020; Medvedeva, 2021) of the problem of describing Shannon-perfect ciphers in the framework of the probabilistic cipher model Σ_B (Shannon, 1963), we consider an arbitrary perfect cipher. According to (Alferov et al., 2001, Zubov, 2003), a cipher on a set of ℓ-grams is given by the probability distribution of keys at $\ell = 1$. Similarly (Medvedeva, 2015; Medvedeva, 2016; Medvedeva, 2019; Medvedeva, 2020; Medvedeva, 2021), let $X = \{x_1, x_2, ..., x_\lambda\} = \{1, 2, ..., \lambda\}$ be the set of ciphertexts; $Y = \{y_1, y_2, ..., y_\mu\} = \{1, 2, ..., \mu\}$ – a set of ciphervalues with which some substitution cipher operates; $K = \{k_1, k_2, ..., k_\pi\}$ – a set of keys. By condition $|X| = \lambda > 1, \quad |Y| = \mu \geq \lambda, \quad |K| = \pi \geq \mu.$ This means that open $x = x_{i_1} x_{i_2} ... x_{i_\ell}$, $x_{i_j} \in X$, $j = 1, 2, ..., \ell$ and encrypted $y = y_{i_1} y_{i_2} ... y_{i_\ell}$, $y_{i_j} \in Y$ texts are represented by words (ℓ-grams, $\ell \geq 1$) in alphabets X and Y respectively. In accordance with (Alferov, 2001; Zubov, 2003), a cipher Σ_B will be understood as a set of sets of encryption rules and decryption rules with specified probability distributions on sets of plain texts and keys. Ciphers for which a posteriori probabilities $p(x \mid y), \quad x \in X^\ell, \quad y \in Y^\ell$ of open texts coincide with their a priori probabilities $p(x)$, are called perfect (Alferov, 2001; Zubov, 2003).

In (Medvedeva, 2016) it is shown that the problem of describing ciphers in a probabilistic model Σ_B leads to the problem of describing a convex polyhedron (Nosov, 1983) in a π-dimensional space R^π, where $\pi = \pi_{\max} = \mu \cdot (\mu - 1) \cdot ... \cdot (\mu - \lambda + 1)$,

[a] https://orcid.org/0000-0002-9736-5481
[b] https://orcid.org/0000-0003-0427-9048

Medvedeva, N. and Titov, S.
Construction of Absolutely Failure-free Minimal Data Transmission Systems on Railway Transport.
DOI: 10.5220/0011579100003527
In *Proceedings of the 1st International Scientific and Practical Conference on Transport: Logistics, Construction, Maintenance, Management (TLC2M 2022)*, pages 73-77
ISBN: 978-989-758-606-4

each point is a probability distribution of the P_k keys $k \in K$ of a particular cipher. To solve this problem in the work (Medvedeva, 2020) based on the equivalence relation on the set of keys, sufficient conditions are obtained for the absence of non-endomorphic ($\lambda < \mu$), endomorphic ($\lambda = \mu$) perfect ciphers of Latin rectangles, squares, respectively, in the encryption tables.

In this paper, the problem of constructing (describing) ciphers that do not disclose any information about open texts is investigated. A graph approach to solving the problem is proposed. A minimality criterion for the inclusion of non-endomorphic (endomorphic) perfect ciphers is obtained. Examples containing tables of encryption of perfect ciphers are constructed, ready for use when organizing a communication channel on transport.

2 MAIN RESULTS

Consider the definitions.

Definition 1 (Medvedeva, 2020). The keys k' and k'' are equivalent in ciphertext x_i, if x_i the keys k' and k'' are encrypted into the same ciphervalue, i.e.

$$k' \underset{i}{\equiv} k'' \Leftrightarrow e_{k'}(x_i) = e_{k''}(x_i),$$

in this case, a bijection is used in the notation for the equivalence of keys: $i \leftrightarrow x_i$.

Definition 2 (Medvedeva, 2020). Pairwise different keys $k_1, k_2, k_3, ..., k_{n-1}, k_n$ form a cycle of length n, if the conditions are met

$$k_1 \underset{i_2}{\equiv} k_2 \underset{i_3}{\equiv} k_3 \underset{i_4}{\equiv} ... \underset{i_{n-1}}{\equiv} k_{n-1} \underset{i_n}{\equiv} k_n \underset{i_1}{\equiv} k_1,$$

where $i_2 \neq i_3, i_3 \neq i_4, ..., i_{n-1} \neq i_n, i_n \neq i_1$.

We distinguish a class of minimal ciphers by inclusion, in which for each pair (x, y) of ciphertext x and ciphervalue y there are at most two keys k, on which the ciphertext x is encrypted into y. Then, in each column of the encryption tables of such ciphers, each cipher value y occurs, respectively, no more than twice. For ciphers of this class, it is natural to define a graph (Ore, 1980; Harari, 1973) on a set of keys. According to (Medvedeva, 2021), two different keys k' and k'' (corresponding to different injections $e_{k'}$ and $e_{k''}$ encryption, where $e_k : X \to Y$, $k \in K$) connect with an edge, if there is such a pair (x, y) of ciphertexts x and cipher values y that on both of these keys the ciphertext is x encrypted in y, i.e. equality $e_{k'}(x_i) = e_{k''}(x_i)$ is fulfilled.

Example 1. Consider an endomorphic cipher, for which $X = \{x_1, x_2, x_3, x_4, x_5\} = \{1, 2, 3, 4, 5\}$ there is a set of ciphertexts; $Y = \{y_1, y_2, y_3, y_4, y_5\} = \{1, 2, 3, 4, 5\}$ – a set of cipher values; $K = \{k_1, k_2, k_3, k_4, k_5, k_6, k_7, k_8, k_9\}$ – a set of keys. Here in the encryption table (Table 1) of a perfect endomorphic cipher with $\lambda = \mu = 5$ and key probabilities $P_1 = 0{,}2$ and $P_2 = P_3 = ... = P_9 = 0{,}1$ there are no Latin squares.

Table 1: Encryption table.

K	x_1	x_2	x_3	x_4	x_5	P_k
k_1	1	2	3	4	5	0,2
k_2	2	3	4	5	1	0,1
k_3	2	5	1	3	4	0,1
k_4	3	4	5	2	1	0,1
k_5	3	1	2	5	4	0,1
k_6	4	5	1	3	2	0,1
k_7	4	3	5	1	2	0,1
k_8	5	1	4	2	3	0,1
k_9	5	4	2	1	3	0,1

The graph corresponding to the cipher with the encryption Table 1 is shown in Figure 1. In this graph, the key k_1 with probability $P_1 = 0{,}2$ is an isolated vertex of the graph.

Note that in the graph shown in Figure 1, the keys k_2, k_3, k_5 form a cycle of length three: $k_2 \underset{1}{\equiv} k_3 \underset{5}{\equiv} k_5 \underset{4}{\equiv} k_2$, and the keys k_2, k_4, k_5, k_9, k_8 form a cycle of length five: $k_2 \underset{5}{\equiv} k_4 \underset{1}{\equiv} k_5 \underset{3}{\equiv} k_9 \underset{1,5}{\equiv} k_8 \underset{3}{\equiv} k_2$.

The incidence matrix corresponds to this graph (Ore, 1980, Harari, 1973), namely a binary matrix I of size 9×20:

$$I = \begin{bmatrix} 0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0 \\ 1&1&1&1&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0 \\ 0&0&0&0&1&1&1&1&1&0&0&0&0&0&0&0&0&0&0&0 \\ 0&0&0&1&0&0&0&0&0&1&1&1&1&0&0&0&0&0&0&0 \\ 0&0&1&0&0&0&0&0&1&0&0&0&1&1&1&0&0&0&0&0 \\ 0&0&0&0&0&1&1&1&0&0&0&0&0&0&0&1&1&0&0&0 \\ 0&1&0&0&0&0&0&0&0&0&0&1&0&0&0&1&1&1&0&0 \\ 1&0&0&0&0&0&0&0&0&0&1&0&0&0&1&0&0&0&1&1 \\ 0&0&0&0&0&0&0&0&0&1&0&0&0&1&0&0&0&1&1&1 \end{bmatrix}.$$

The necessary and sufficient condition for the minimality of the cipher on inclusion is valid.

Statement. A cipher is minimal in inclusion if and only if there is an odd-length cycle in some non-element connected component of the graph corresponding to it.

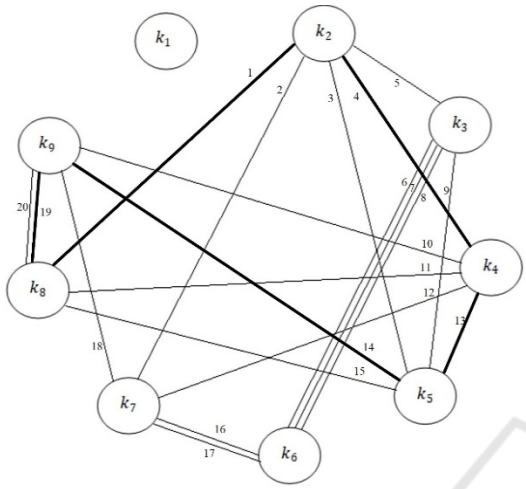

Figure 1: Graph.

Proof. Let the key k is not an isolated vertex of the graph. This means that there is a partition $\{X_1, X_2, ..., X_s\}$ of a set X and a set $\{k_1, k_2, ..., k_s, k\}$ of different keys such that

$$e_k(x) = e_{k_t}(x) \Leftrightarrow x \in X_t \ (t = 1, 2, ..., s).$$

It is clear that $s \geq 2$. Since otherwise equality would be fulfilled $e_k(x) = e_{k_1}(x)$ for all $x \in X$. Therefore, the valence s of each non-isolated vertex is greater than one.

Let's assume that the cipher is not minimal, and you can zero the probability P_k of the key k. Then the probabilities P_{k_t} of the keys k_t $(t = 1, 2, ..., s)$ in the resulting (residual) cipher should be put equal $1/\mu$, since otherwise the transitivity of the cipher will be violated. However, it follows that it is necessary to put the probabilities of keys $k' \neq k$, connected by an edge with one of the vertices $k_1, k_2, ..., k_s$, equal to zero from the condition of perfection of the cipher with equally probable cipher values.

Continuing to track the probabilities of vertices when moving along the edges of a connected component containing k, we get: if $k, k^{(1)}, k^{(2)}, ..., k^{(r)}, ...$ – the path in this graph, then the probabilities $P_k = 0$, $P_{k^{(2)}} = 0$, and generally $P_{k^{(l)}} = 0$ for even l, but $P_{k^{(1)}} = 1/\mu$, and generally $P_{k^{(r)}} = 1/\mu$ for odd r, since the sum of

Table 2: Encryption table.

K	x_1	x_2	x_3	x_4	x_5	x_6	P_k
k_1	1	2	3	6	5	4	1/18
k_2	1	4	6	3	2	5	1/18
k_3	1	6	2	5	4	3	1/18
k_4	2	4	1	5	3	6	1/18
k_5	2	1	6	4	3	5	1/18
k_6	2	5	4	3	1	6	1/18
k_7	3	5	4	1	2	6	1/18
k_8	3	4	6	2	1	5	1/18
k_9	3	2	5	4	6	1	1/18
k_{10}	4	5	3	1	6	2	1/18
k_{11}	4	1	5	6	3	2	1/18
k_{12}	4	6	1	2	5	3	1/18
k_{13}	5	1	3	6	2	4	1/18
k_{14}	5	6	4	3	1	2	1/18
k_{15}	5	3	2	1	6	4	1/18
k_{16}	6	3	2	5	4	1	1/18
k_{17}	6	3	5	2	4	1	1/18
k_{18}	6	2	1	4	5	3	1/18

Table 3: Matrix A.

$$A=\begin{bmatrix}
1&0&0&0&0&0&0&1&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&1&0&0&0&0&1&0&0&0&0&1&0&0\\
1&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&1&0&0&1&0&0&0&0&1&0&0&0&0&0&0&0&0&1&0\\
1&0&0&0&0&0&0&0&0&0&0&1&0&1&0&0&0&0&0&0&0&0&0&1&0&0&0&0&1&0&0&0&0&1&0&0&0\\
0&1&0&0&0&0&0&0&0&1&0&0&1&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&1&0&0&0&0&0&0&0&0&1\\
0&1&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&1&0&0&0&1&0&0&0&0&1&0&0&0&0&0&0&0&1&0\\
0&1&0&0&0&0&0&0&0&0&1&0&0&0&0&1&0&0&0&0&1&0&0&0&1&0&0&0&0&0&0&0&0&0&0&1\\
0&0&1&0&0&0&0&0&0&0&1&0&0&0&0&1&0&0&1&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&1\\
0&0&1&0&0&0&0&0&0&1&0&0&0&0&0&0&0&1&0&1&0&0&0&0&1&0&0&0&0&0&0&0&0&0&1&0\\
0&0&1&0&0&0&0&1&0&0&0&0&0&0&0&0&0&1&0&0&0&0&1&0&0&0&0&0&0&0&1&1&0&0&0&0&0\\
0&0&0&1&0&0&0&0&0&0&1&0&0&0&1&0&0&0&1&0&0&0&0&0&0&0&0&0&0&1&0&1&0&0&0&0\\
0&0&0&1&0&0&1&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&1&0&0&1&0&0&0&0&1&0&0&0&0\\
0&0&0&1&0&0&0&0&0&0&0&1&1&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&1&0&0&0&1&0&0&0&0\\
0&0&0&0&1&0&1&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&1&0&1&0&0&0&0&0&0&0&1&0&0&0\\
0&0&0&0&1&0&0&0&0&0&0&1&0&0&0&1&0&0&0&0&1&0&0&0&1&0&0&0&0&0&0&0&1&0&0&0&0\\
0&0&0&0&1&0&0&0&1&0&0&0&0&1&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&1&0&0\\
0&0&0&0&0&1&0&0&1&0&0&0&0&1&0&0&0&0&0&0&0&0&1&0&0&0&0&0&1&0&0&1&0&0&0&0&0&0\\
0&0&0&0&0&1&0&0&1&0&0&0&0&0&0&0&1&0&0&1&0&0&0&0&0&0&0&0&0&1&0&0&1&0&0&0&0&0\\
0&0&0&0&0&1&0&1&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&1&0&0&1&0&0&0&0&1&0
\end{bmatrix}.$$

Table 4: Matrix $\overline{A}$.

$$\overline{A}=\begin{bmatrix}
1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1
\end{bmatrix}.$$

the probabilities of keys connected by an edge is $1/\mu$. And since the probabilities of keys do not depend on the path in the graph, we get that this component is a bipartite graph, all cycles of which are of even length, and the probabilities of vertices in the fraction containing k, can be put equal to zero, and in the other fraction equal $1/\mu$, i.e. we get a contradiction with the fact that k – an uninsulated vertex of the graph.

The minimality condition formulated above for the inclusion of a perfect cipher satisfies the criterion.

Minimality criterion for the inclusion of perfect ciphers. Let be given an encryption table of a perfect cipher Σ_B with $|X|=\lambda>1$, $|Y|=\mu\geq\lambda$, $|K|=\pi\geq\mu$.

1. Let's break each of λ columns $x_1, x_2, ..., x_\lambda$ by μ columns, numbering all the resulting columns with indexes (i, j), where $i=1,2,...,\lambda$, $j=1,2,...,\mu$.

2. Let's construct (0,1) matrix A with π rows and $\lambda\mu$ columns corresponding to this encryption table as follows: at the intersection of the row k $(k=1,...,\pi)$ and the column (i, j), we will put one if and only if, $e_k(x_i)=y_j$, i.e. if the ciphertext x_i on the key k is encrypted into a cipher value y_j. Otherwise, we set zero.

Then the set of cipher keys is minimal if and only if the rank of the matrix A maximal, equal to π.

Let us illustrate the application of this criterion to the determination of minimality by the inclusion of a given perfect cipher by an example.

Example 2. Consider an endomorphic cipher with a set of six ciphertexts. Let $X = \{x_1, x_2, x_3, x_4, x_5, x_6\} = \{1,2,3,4,5,6\}$ – a set of ciphertexts; $Y = \{y_1, y_2, y_3, y_4, y_5, y_6\} = \{1,2,3,4,5,6\}$ – a set of cipher values; $K = \{k_1, k_2, k_3, ..., k_{18}\}$ – a set of keys. Encryption table of a given perfect endomorphic cipher with $\lambda = \mu = 6$ and key probabilities $P_k = 1/18$ $(k = 1,2,...,18)$ – is this Table 2.

For this cipher, we will create a binary (0,1) matrix A of 18 rows and 36 columns (Table 3).

In the matrix A, for example, the first column (column (1,1)) in the first three rows contains units since in the encryption Table 2, the ciphertext is $x_1 = 1$ encrypted on the keys k_1, k_2 and k_3 in the cipher value 1. The remaining elements of the column (1,1) are zero. The remaining columns of the matrix A are filled in the same way.

The matrix A is equivalent to the matrix $\overline{A}$ (Table 4) and its rank by rows (Gantmacher, 1967) equal to 18, i.e. equal to the number of keys specified in the encryption table. This, according to the criterion, means that the cipher with the encryption Table 2 is minimal in inclusion.

Consequences of the minimality criterion for the inclusion of perfect ciphers:

1. For the minimality of the set of cipher keys, it is necessary to perform an inequality $\pi \le \lambda\mu$.

2. For an endomorphic minimal perfect cipher, the inequality holds $\pi \le \lambda(\lambda - 1)$.

3 CONCLUSIONS

Thus, the paper considers a graph approach to the construction of absolutely failure-free data transmission systems. Within the framework of this approach, a necessary and sufficient condition for the minimality of a perfect cipher by inclusion is proved.

A minimality criterion for the inclusion of non-endomorphic (endomorphic) perfect ciphers is obtained. Examples illustrating the concepts used, obtained theoretical statements and constructions of perfect ciphers are constructed. In addition, the paper presents tables of encryption of perfect ciphers that ensure the protection of the communication channel in transport.

REFERENCES

Medvedeva, N. V., Titov, S. S., 2015. Non-endomorphic perfect ciphers with two ciphertexts. *Applied discrete mathematics. Appendix*. 8. pp. 63-66.

Medvedeva, N. V., 2016. On analogs of the Shannon's theorem for perfect ciphers. *CEUR Workshop Proceedings*. 1825. pp. 232-239.

Medvedeva, N. V., Titov, S. S., 2016. Geometric model of perfect ciphers with three ciphertexts. *Applied discrete mathematics. Appendix*. 12. pp. 113-116.

Medvedeva, N. V., Titov, S. S., 2020. Constructions of non-endomorphic perfect ciphers. *Applied discrete mathematics. Appendix*. 13. pp. 51-54.

Medvedeva, N. V., Titov, S. S., 2021. To the task of describing the minimum on the inclusion of perfect ciphers. *Applied discrete mathematics. Appendix*. 14. pp. 91-95.

Shannon, K., 1963. Communication theory in secret systems. *Works on information theory and cybernetics*. pp. 333-402.

Alferov, A. P., Zubov, A. Yu., Kuzmin, A. S., Cheremushkin, A. V., 2001. *Fundamentals of Cryptography*. p. 479.

Zubov, A. Yu., 2003. *Perfect ciphers*. pp. 160.

Nosov, V. A., Sachkov, V. N., Tarakanov, V. E., 1983. Combinatorial analysis (Non-negative matrices, algorithmic problems). *Results of science and technology. Ser. of Theor. of Prob. of Mat. Stat. Theor. Cybernet*. 21. pp. 120-178.

Ore, O., 1980. *Graph Theory*. pp. 336.

Harari, F., 1973. *Graph theory*. p. 300.

Gantmacher, F. R., 1967. *Matrix Theory*. pp. 575.