METHODS AND MEANS OF INFORMATION SECURITY IN TELECOMMUNICATION SYSTEMS

Mahambaeva I.U., Dautbaeva F.Zh.
Korkyt Ata Kyzylorda State University, Kyzylorda, e-mail: fary_95@mail.ru

The recent progressive impact of information technology on almost all spheres of human activity causes the progressive growth of the requirements for telecommunications systems and telecommunications devices. This is due to the fact that these systems are so far the primary means of information exchange and the quality of their operation is the determining factor in the effectiveness of most of information technology. The most important component of the quality of functioning of telecommunication systems is the quality of information security. Provision of this component is currently facing a number of problems, the main one being the contradiction between the potential of the existing approaches and constantly increasing requirements for data protection. The potential failure of these approaches to fulfill changing requirements explains the relevance of the search direction of research fundamentally new approaches that allow solving the mentioned problems.

Cryptographic methods of information protection – is a powerful weapon in the struggle for information security.

Cryptography is a set of data conversion methods, aimed at making the data useless to the attacker. Such transformations can solve two major issues relating to information security:

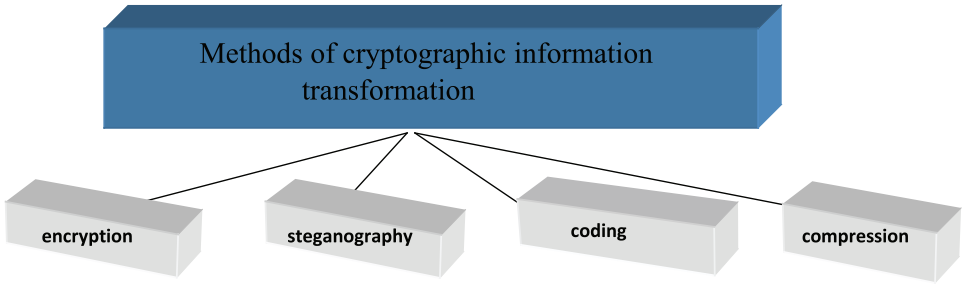
- Protection of privacy;
- Integrity protection.

Problems of protection of confidentiality and integrity of information are closely linked, so the methods of solving one of them is often applicable to other solutions.

There are different approaches to the classification of cryptographic information transformation methods. By referring to the initial exposure information, cryptographic information conversion methods can be divided into four groups.

The encryption process is to conduct a reversible mathematical, logical, combinatorial and other transformations of the initial information, as a result of which the encrypted information is a chaotic set of letters, numbers and other characters and binary codes.For the encryption algorithm used information. Typically, the encryption algorithm for a particular method is unchanged. Initial data for the encryption algorithm is the information subject to encryption and encryption key. The key contains control information that determines the choice of conversion at certain steps of the algorithm and the size of the operands used in the implementation of the encryption algorithm. Operand – a constant, variable, function, expression, and other object programming language on which operations are performed. Unlike other methods of cryptographic transformation of information, methods of steganography can hide not only the meaning of stored or transmitted data, but also the fact of storing or transmitting classified information. The basis of all methods of steganography is the masking of sensitive information among open files, i.e. hiding secret data, thus it is realistic figures that are impossible to distinguish from the real thing. Handling multimedia files in information systems has opened almost unlimited opportunities for steganography.

The graphics and audio information presented in numerical form. Thus, the graphic objects in the smallest picture element can be encoded in one byte. The lower level of certain bytes of the image according to the algorithm cryptographic transformation placed bits hidden file. If you choose the right algorithm for image transformation and against which is placed a hidden file, the human eye is almost impossible to distinguish from the original image is obtained. With steganography, tools may be masked by the text, image, voice, digital signature, the encrypted message.



Classification of cryptographic information transformation methods

Hidden file can also be encrypted. If someone accidentally discovers a hidden file, the encrypted information is perceived as a failure of the system. Integrated use of steganography and encryption greatly increases the complexity of solving the problem of detection and disclosure of confidential information.

The content of the process of encoding information is the replacement of the original meaning of the message (words, sentences) codes. The codes can be used as a combination of letters, numbers, punctuation, special tables or dictionaries are used when encoding and reverse transformation. The information networks encoding of the original message (or signal) software and hardware used to improve the reliability of the transmitted information.

Often, encoding and encryption mistaken for the same thing, forgetting that to recover the encoded message, enough to know the replacement rule, while to decrypt the message encryption in addition to knowledge of the rules, it requires a key to the cipher.

Data compression can be attributed to the methods of cryptographic transformation of information with certain reservations. The aim of compression is to reduce the amount of information. At the same time, the compressed data cannot be read or used without inversion. Given the availability of means of compression and inversion, these methods can not be considered as a reliable means of cryptographic information transformation. Even if kept secret algorithms, they can be relatively easily opened by statistical processing methods. Therefore, the compressed files of confidential information are subject to subsequent encryption. To reduce the data transmission time is expedient to combine the compression and encryption process information.

References

1. Biryukov Alex, Shamir Adi, David Wagner. Real Time Cryptanalysis of A5/1 on a PC. Prepro- ceedings of FSE'7, 2000. – P. 1–18.

2. Kwan M., PieprzykJ.. A General Purpose Technique for Locating Key Scheduling Weaknesses in DES-like Cryptosystems. Advances in Cryptology – ASIACRYPT'91, Springer-Verlag, 1993. – P. 237–246.

3. Kelsey J., SchneierB., Wagner D. Key-Schedule Cryptanalysis of IDEA, G-DES, GOST, SAFER, and Triple-DES. Advances in Cryptology – CRYPTO'96 Proceedings, Springer Verlag, 1996. – P. 237–251.

The work is submitted to the International Scientific Conference "Modern high technologies", Israel (tel Aviv), 20–27 Feb 2017, came to the editorial office on 05.04.2017.

TECHNOLOGY OF FORMATION OF THE EXTERNAL SAILING WITH THE ADVANCING EMBANKMENT AND ACTIONS FOR PREVENTIVE MAINTENANCE OF IGNITIONS OF COAL

Tsygankov D.A.

N.A. Chinacal Institute of Mining, Siberian Branch, Russian Academy of Sciences, Novosibirsk, e-mail: gallantminer@gmail.com

Prevention of coal ignition in sailings of mining enterprises has obtained a special significance in terms of strict requirements towards ecological condition of natural environment [1]. The most efficient method of avoiding fires is implementation of mining technologies that imply preventive measures against coal ignition.

The object of this research is prospecting area of a cut that carries out coal mining in conditions of sharply continental climate, defined by significant oscillation of temperature, cold and continuous winter and short, but hot summer. Snow surface preserves during five to six months. The prevailing direction of wind – West and South-West with average speed of 4,4 m/s. These aspects are considered while locating external sailings of mining enterprise and construction of dwellings [2].

The coal is presented by layers that are located in parallel at different depths and characterized by a complicated composition and low solidity. Moist content varies from 1,03 to 2,1%, actual solidity equals 1,47 t/m^3, coefficient of solidity equals 0,6-2,33, and angles of fallout – 5-80º. Quick oxidation and further ignition is typical for coal. Metane content grows along with depth of layer location and varies from 3-3,5 m^3/t to 7,5-8,2 m^3/t [2].

Uncovering and storing rocks are presented by clays, clay loam, sandstone, argillites, and aleurolites [2].

Technology of mining at a site implies facilitation of one internal and two external sailings. Transportation of uncovering rock is carried out by trucks, and their pushing and planning of sailing surface in the area of unloading – by bulldozers.

In order to improve stability of external sailing board during formation of lower level that falls down along thalweg of ravine, it is necessary to implement technological scheme of sailing formation that implies directing front of mining operations. This front must be located in perpendicular to axis of ravine thalweg, and dumping must go along its direction.

Front of dumping works is divided into three sectors. First of all, dump goes along water divisions and ravine slopes – lateral areas, characterized by lower altitude. The central area, located along ravine thalweg and defined by the greatest altitude, is dumped last. The central area of sailing is dumped with more solid rocks (sandstone, argillites, and aleurolites), and laters areas – with less solid types (clays and clay loam). No more than two sites can operate, the third site is reserved for stabilization of the emerging tension.

Formation of sailing along ravine thalweg is carried out with preliminary dump of leading embankment that is located at the same axis as the lover border of sailing. At the same time stability of the lower level in the formed sailing is regulated by height and depth of the leading embankment. Width of the leading embankment is defined via method of its construction and parameters of the aggregate that forms dumping, leading degree is defined according to width of foundation riser prism that, in its turn, is defined according to power of the weak layer. Maximum height of external sailing levels must not exceed 20 m.