UDC 004.056.55 (043.2)

Rudenko M.V.
National Aviation University, Kyiv

THE MAIN FEATURES OF CRYPTOGRAPHY

The history of cryptography began in diplomatic circles thousands of years ago. For a long time, cryptography was the for the lonely people. Among them were gifted scientists, diplomats and clergymen. There were times when cryptography was considered even black magic.

Currently, in many areas, electronics replacement is increasingly used to replace paper correspondence. As a result, the amount of information available for interception becomes larger.

However, the same factors that contribute to the development of electronic means of communication, rapidly reduce the cost of cryptography. After that, there is an increasing interest in cryptography both individuals and commercial enterprises. The problem of cryptographic protection is especially acute.

Coding means a kind of cryptographic closure when data items are replaced with pre-selected codes. Sometimes the code consists of a list of words and phrases together with a letter nominal code elements. Because code groups are usually shorter than the expressions they represent codes in addition to secrecy also provide compression of information. It is divided into two groups of varieties: semantic and symbolic coding. At semantic coding the coded elements have quite definite sense. Symbol encodes each character of the protected text.

All known encryption methods are divided into five groups:

1. Substitution is a direct replacement when the letters of the encrypted text are replaced by other letters of the same or a different alphabet.

2. A permutation is an encryption process when the characters of the encrypted text are rearranged by the policies inside the encrypted block.

3. Analytical transformation is a process encryption that uses analytical transformers (for example, methods of matrix algebra).

4. Gaming is the process of encryption when the symbols of the encrypted text are consistently added up with the symbols of a special sequence called a gamma.

5. Combined encryption is the process of sequential text encryption using two or more methods to increase the robustness of encryption.

All encryption methods use a key to encrypt or decrypt messages. The key is an important component of the encryption algorithm. The encryption algorithm is as good as the business key.

There are two approaches to ensuring data security when using encryption. The first is to protect the algorithm. If the security of the encryption system depends on the secrecy of the algorithm itself, the most important guarantor is the protection of the algorithm at all costs. Every time someone learns the details of the algorithm each participating party will have to change the algorithm. This approach does not seem very reliable or manageable. The second approach is to protect the keys. Modern cryptography algorithms are generally available. Cryptographic keys view data privacy.

Cryptographic keys are passwords that are parts of the input to the encryption algorithm as well as data that requires encryption.

The more complex and longer is the algorithm, the more secure it is, but it is very resource-intensive.

There are two classes of encryption algorithms.

1. Symmetric algorithms. These algorithms use the same pre-shared key, sometimes called a pair of secret keys, to encrypt and decrypt data. Both the sender and the recipient know the pre-shared key before any encrypted message begins. Encryption algorithms that use a common key are simpler and require less processing power.

2. Asymmetric algorithms. Asymmetrical encryption algorithms use one key to encrypt data and a different key to decrypt data. One key is public and the other is private. Anyone who has a public key can encrypt a message using the public key of the receiver, and the receiver is the only one that can decrypt it using its private key. Asymmetric algorithms are more complex.

Data currently in use is a growing problem for many organizations. In its processing the data is not protected since the user needs to open and modify data. The system memory stores data that can contain sensitive data, such as an encryption key. If criminals compromise the data used, they will have access to data at rest and data in motion. That is one of the matter to which a user should pay attention to, but in general it is very helpful and convenient in operation.

Scientific supervisor: Balatska N.I.,
PhD, Senior Lecturer

UDC 11372635 (043.2)

Ryabchun D.V.
National Aviation University, Kyiv

THE CONCEPTION OF MARKETING MIX

The aim of marketing is to make marketing efforts unnecessary. Its goal is to know and understand the customer’s needs, so well that the goods or services will be exactly what the customer wants and will buy. In the defining the needs and wishes of customers, managers are using the marketing mix.

The marketing mix is a foundation model in marketing that is grounded on four main factors of marketing decision: the product, the price, the promotion, and the place (Tab. 1). The marketing mix has been determined as the set of marketing tools that the enterprise uses to pursue its marketing objectives in the target. Also, it has another name as 4Ps.

Price
Promotion
Marketing Mix
Product
Place

Tab.1 The marketing mix