Gulnur Zhangissina, Dr. Sc. (Vice-Prezident,
International Academy of Informatization, Kazakhstan, Almaty),
Ahmad Djoan, Kim Ilya., Toleuhan Tomas, Kairat Ruslan,
Amanbaev Tair, Kleymenova D., Vilkovitskay Sofa, Birzhanov Alibi,
Bulgusheva Toma, Kadirov Asman (Kazakhstan, Almaty)

Cryptographic methods of information protection

This article describes the basic cryptographic methods of information security. Objectified an advantage and disadvantages of cryptographic methods: symmetric cryptography key, public cryptography key, encryption.

Cryptography - the science of protecting information from unauthorized reading it. Protection has achieved by encryption, transformation that make protected inputs difficult Rusk undermines the input data without the knowledge of a special key Institute formation - key. Easily understood by the key variable part cryptosystem storing in secret and determines which of the possible transformation of ciphering performed in this case. Cryptosystem - a family selected by a reversible transformation key transformations that convert plaintext into protected cryptograms and back.

It is desirable that the encryption methods had at least two properties:

- Legitimate recipient will be able to convert back and decrypt the message;

- Crypto analyst enemy interception of communications, couldn’t restore it to the original message without such time and resources that will make this work inappropriate.

Cryptographic transformation - the transformation of information, based on some algorithm that depends on the parameter to be changing (usually called the private key), and having the property that it is impossible to restore the original information on the transformed, without the knowledge of the current key with complexity less than a predetermination

The main advantage of cryptographic methods is that they provide a high resistance guaranteed protection, which can be calculated and expressed in a numerical form (the average number of operations and the time needed for disclosing the encrypted information or the key calculation).

The main drawbacks of cryptographic techniques include:

• significant resource costs (time, CPU performance) to perform cryptographic transformations of information;

• difficulty sharing encrypted (signed) information related to key management (generation, distribution, etc.);

• high demands on the safety of secret keys and public key protection against spoofing.

Cryptography was divided into two classes: symmetric key cryptography and public-key cryptography.

Cryptography with symmetric keys In symmetric key cryptography (classical cryptography) subscribers used the same (common) key (secret element) for both encryption and decryption of data. It will highlight the following advantages cryptography with symmetric keys:

• relatively high performance algorithms;

• high resistance cryptographic algorithms per unit length of the key. The disadvantages of symmetric-key cryptography include:

• the needing to use complicated key distribution mechanism;

• technological difficulties ensuring non-repudiation. Public-key cryptography

To solve the problems of key distribution were used ideas asymmetry change and public distribution of Hellman. The result was a public-key cryptography, which uses more than one secret, and a pair of keys: open (public) and private key (personal, individual) key known only to one side of interacting. Unlike the secret key, which must be kept secret, the public key can be distributed publicly. Encryption

Implementation circuit connected with a digital signature by calculating the hash function (digest) of the data, which is a unique number obtained from the raw data by compressing (convolution) with a complex but well-known algorithm. A hash function is a unidirectional function, i.e. on its hash value is impossible to recover the original data. A hash function is sensitive to all sorts of corruption. Additionally, very difficult to find two data sets having the same hash value.

Cryptography today - is the most important part of information systems: from email to cellular network access from the Internet to electronic cash. Cryptography ensures accountability, transparency, accuracy and privacy. It prevents fraud attempts in e-commerce and provides a legally binding financial transactions. Cryptography helps to establish your identity, but also provides you with anonymity.

Cryptographic methods of information protection against unauthorized access, alteration or deletion of important commercial and personal data stored on your computer. In the world of modern commerce, information is one of the most important elements, and the main part of this important information is stored and processed electronically, so reliable methods of protecting computer information - is the best way to prevent deliberate or accidental leak it. And in the future, as commerce and communications are all closely connected with computer networks, cryptography becomes vital.

But participants in the market do not provide cryptographic the level of protection that is promised in the advertisement. Most products are developed and applied not in cooperation with the cryptographers. Engineers were engaged, for which cryptography - just another component of the program. But cryptography - it is not a component.

Can not ensure the security of the system, "inserting" cryptography after its development. At every stage, from conception to installation, you must realize that you are doing and why.

In order to properly implement your own cryptosystem is necessary not only to get acquainting with other errors, and understand the reasons for which they have occurred, but perhaps special secure programming techniques and specialized tools.

On computer security spend billions of dollars, with much of the money thrown away on worthless products. Two Crypto Pack for e-mail have a similar user interface, but of this ensure the safety and the second allow eavesdropped. Comparison may indicated similarities of the two programs, but one of them security while gaping hole which devoid of another system. Experienced cryptographer can tell the difference between these two systems. The same can be done and the attacker. The date, of Computer security - is a house of cards, which at any moment could fall apart. Too many weak products didn’t of them because they are little used. Once they become widespread, they will become a magnet for criminals.

Press immediately give publicity to these attacks, undermining public confidence in these cryptosystems. Writing this work, we can draw the following conclusions:

- Cryptoalgorithms undoubtedly the "heart" of cryptographic systems, but their direct application without any modifications to encode large amounts of data is not actually very acceptable.
- Reasonable choice of a protection system in general should be based on some performance criteria.
- We recommend using some integral indicators, taking into account the characteristics of the system.

But in any case, the selecting set of cryptographic methods will combine as convenience, flexibility and efficiency of use, and protection from intruders circulating in the system information.

Recent advances in the field of cryptography was the development of a cryptographic system, based on the properties of quantum particles. Some of the parameters of quantum particles can not be predicted, and they are used for key generation. Parameters of a quantum particle distorted when you try to copy it, so the fact of listening to the information once it becomes known to the recipient. In the market of information security software was expected to appear commercial quantum cryptosystems.

As shown, in the presence of systems such as AES or RSA, the weak point in the security of information is often not the cipher strength, and other factors, such as errors in the implementation of the algorithm, security holes in software equipment and human factors.

The effectiveness of modern cryptographic systems and their resistance to decipherment is so high that in some countries the using of powerful algorithms prohibited because it does not decrypt the information even possible for the authorities that can be used for criminal purposes. The restrictions imposed on the possibility of cryptographic systems to resist the business community - in fact anyone who needs numbers that can easily be hacked competitors.

In Kazakhstan, and other countries, there are strict limits on the using of cryptography. Almost all the activities associated with obtaining information requires encryption state license. Availability resistant to breaking cryptographic systems, however, is one of the important factors for the development of e-business. Hopefully, with time the situation in Kazakhstan will free development and use of strong cryptographic systems that will undoubtedly have a positive impact on the electronic market of the country.

References

[1] Shangin V.G. Protection of information in computer systems and networks. - DMK-Press, 2012, 592 p.

[2] Domarev V.V. Safety of information technology. The systems approach. / V. Domarev - K.: TID Dia Software Ltd., 2004. - 992 p.

[3] Zegzhda D.P. Fundamentals of Information Systems Security / DP Zegzhda, A.M.Ivashko - Moscow Hotline - Telecom, 2000. 452 p.

[4] Zhangissina G., Kuldeev E., Shauhanova A., Data protection from network attacks.. - Bezpeka ìnformacìì, 2013. – 21 p.

[5] Zhangissina G., kasabekov S., Munalbaeva N. About cryptographic methods of information protection. USA, 2016.