MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE
SUMY STATE UNIVERSITY
UKRAINIAN FEDERATION OF INFORMATICS

PROCEEDINGS

OF THE V INTERNATIONAL SCIENTIFIC CONFERENCE

ADVANCED INFORMATION SYSTEMS AND TECHNOLOGIES

AIST-2017

(Sumy, May 17–19, 2017)

SUMY
SUMY STATE UNIVERSITY
2017

Verification of Cryptosystems Sustainability as the Main Criterion for Development of Common Information Security Policy

Andrii Boiko[1], Vira Shendryk[1], Lina Cherednichenko[2]
[1]Sumy State University, 2, Rymskogo-Korsakova st., 40007 Sumy ,Ukraine
[2]George Brown College, Toronto, Canada

Security of data resources has become one of the main issues of modern society. Encryption is one of the most reliable ways to protect data from unauthorized disclosure. One of the key factors that influenced the formation of a new approach to information security is a significant growth of distributed-processing systems and use of computer networks for communication between users. It is a key reason to develop an information security policy.

Keywords – symmetric cryptosystem, information security policy, public key cryptosystems, requirements for cryptosystems, Kerckhoffs' principle.

I. INTRODUCTION

The processes that take place today in the world directly have influence on the information security of any company. At the same time there are new factors which need to be considered while verifying the actual state of information security and identifying key issues and trends in this area.

Today, one of the main parts of the overall security is the information security. The evolution dynamics of information technology in social and economic sphere requires a comprehensive approach to addressing information security. To ensure complete, accurate and timely information there is a need to provide security functions in information system as well as to secure the information resources.

Thus, the development of a comprehensive information security policy which throughout the information life cycle determines the relevance and timeliness of this study.

II. STRUCTURE OF CRYPTOSYSTEMS

The analysis of cryptosystems makes it possible to identify the main areas of their application. The main functions are:

- Provision of confidential information for further data transfer through communication channels (e.g. e-mail);
- Authenticity of transmitted messages;
- Data storage (documents, databases) on storage medium in encrypted form.

The cryptographic methods are an integral part of the information security policy. The term cryptographic methods of information protection means the special methods of encryption, encoding or other transformation of information, which makes the data content inaccessible without a key cryptograms and reverse transformation. The cryptographic method is one of the most reliable methods of security, as it secure information itself, and not access to it.

Modern cryptosystem includes four major sections:

- Symmetric cryptosystem;
- Public key cryptosystems;
- Digital signature;
- Key management.

Symmetric cryptosystems are based on such encryption methods where encryption and decryption use the same key (Fig. 1).

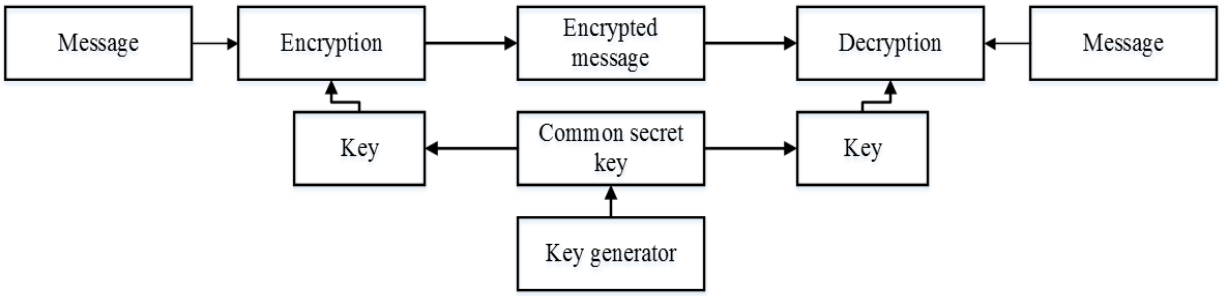

Figure 1. Symmetric cryptosystems

Public key cryptosystems use two keys: one is public key and another one is private key, these two keys are mathematically related to each other. Data is encrypted by using a public key that is available to any person and decrypted by using a private key known only to the recipient (Fig. 2).

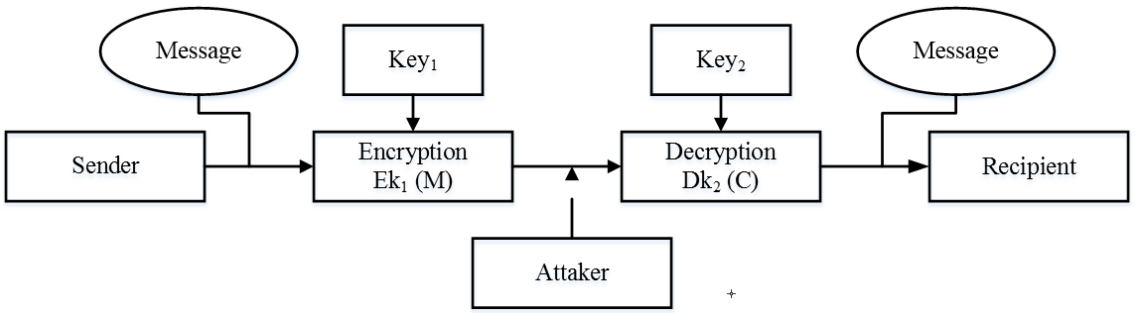

Figure 2. Public key cryptosystems

The system of digital signature is its cryptographic transformation, which are attached to the text and gives a recipient possibility to check the authorship and authenticity of the message.

The process of key management in information processing system consists of formation and distribution.

III. REQUIREMENTS FOR CRYPTOSYSTEMS

The process of cryptographic data closure can be implemented both programmatically and in hardware. Hardware implementation is significantly more expensive, but it also has advantages: high performance, simplicity, security, etc. The software implementation is more practical, allows for a certain flexibility in use. For modern cryptographic information security systems, the following requirements should be emphasized:

- The encrypted message must be readable only if there is a key;
- The number of operations necessary to determine the encryption key used for the fragment of the encrypted message and the corresponding plaintext corresponding to it should be not less than the total number of possible keys;
- The number of operations which is necessary to decrypt information by searching all possible keys must have a strict lower bound and go beyond the capabilities of modern computers;
- Knowledge of the encryption algorithm should not affect to the reliability of protection;
- A minor change in the key should lead to a significant change in the type of encrypted message, even when using the same key;
- The structural elements of the encryption algorithm must be unchanged;
- The length of the encrypted text should be equal to the length of the source text;
- Any key of the set must provide reliable protection of information.

IV. VERIFICATION OF CRYPTOSYSTEMS SUSTAINABILITY

To verify the sustainability of data security cryptosystems it is necessary to follow Kerckhoffs' principle: A cryptosystem should be secure even if everything about the system is public knowledge. Therefore, the analysis of sustainability of cryptosystem is based on the assumption that the opponent knows the detailed description of the system, statistical properties of the message language, the space of possible keys and cryptograms. Also, he may have some information about the context of the message, etc. The only thing the offender mustn't know is the secret cryptographic key used by users of secure cryptographic systems. The system of analysis of cryptographic algorithms can be divided into two subsystems:

- secure cryptographic subsystems with different classes of ciphers;
- subsystems of cryptanalysis.

Typically, different approaches are used to verify the sustainability of secure cryptographic systems; the most interesting among them are the information-theoretical, complexity-theoretic and system-theoretical approaches.

According to information-theoretical approach used to verify the sustainability of cryptographic systems, the cryptosystems can be divided into absolute stable and relatively stable. Sustainability of cryptographic systems with absolute stability does not depend on any abilities of intruder and cannot be decreased under any circumstances. Sustainability of cryptographic systems with relative stability depends on the abilities of opponent and his methods which can vary depending on various factors.

Consider the example of an arbitrary function y = f (x), which is shown graphically (Fig. 3).Suppose that we have a set X = {a, b, c, d, e} and a set Y = {1,2,3,4,5}. Note that, the function is defined by two sets X and Y, and by the rule f, which assigns one element from the set Y to each element of the set X. The set X is called the function domain, and the set Y is the value domain.

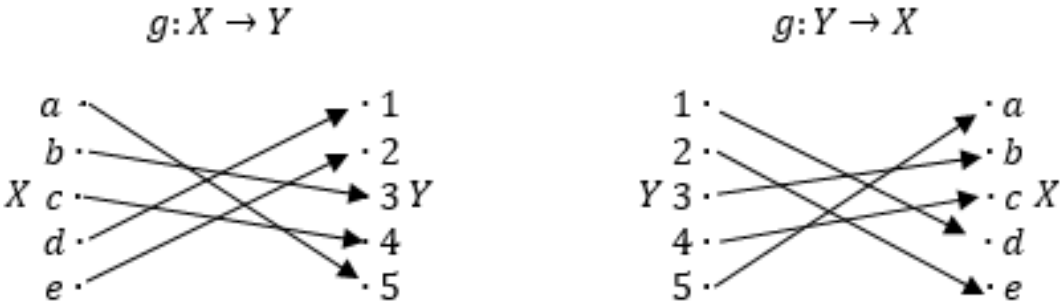

Figure 3. Bijective function f and its inverse function g= f^(-1)

The element y of the set Y is a direct image of the element x, and the element x is an inverse image of y. The mapping of elements from the set X to the set Y is written as follows: f: X → Y.

The set of all elements y having at least one inverse image is called the direct image of the function f and is denoted by Im (f).

A function is said to be single-valued function (one-to-one mapping) if every element of the set Y is the direct image of not more than one element of the set X. A function f is said to be a bijection function if it is single-valued function and Im (f) = Y. A function of the form g = f ^ (-1) is said to be the inverse function of f. Among bijective functions there is a class of functions which is called involutions which are most often used to build secure cryptographic systems.

A bijective function is called an involution if the function domain coincides with the value domain, that is, X = Y = S, and also the inverse function coincides with the function f = f -1. Fig. 3 shows an example of an involution for the set S = {1,2,3,4,5}.

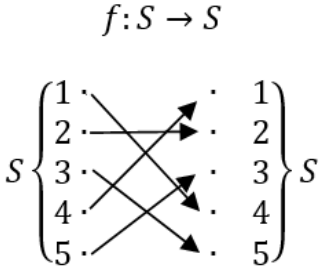

Figure 4. Involution f for the set S={1,2,3,4,5}

The existence of an inverse function is the basis for building of data encryption systems, by means of which cryptograms can be precisely decrypted into messages. Consistent application of encryption function at first, and then decryption function to an undefined message x∈S precisely restores this message: f (f (x)) = x.

V. CONCLUSIONS

The clarification of the question whether the cryptosystem is absolute or relative stable constitutes an important task of the information-theoretical approach used to verify the sustainability of data security cryptosystems. If, within the information-theoretical approach, the cryptosystem is considered as absolute stable, then the degree of its sustainability should be further verified using the complexity-theoretic and system-theoretical approaches. It should be noted that the information-theoretical approach is often referred to the class of theoretical approaches used to verify the sustainability of cryptosystems, and the rest referred to the class of practical approaches.

REFERENCES:

[1] Siponen, M. and Willison, R. (2009). Information security management standards: Problems and solutions. Information & Management, 46(5), pp.267-270.

[2] Kenkre, P., Pai, A. and Colaco, L. (2015). Real Time Intrusion Detection and Prevention System. Advances in Intelligent Systems and Computing, pp.405-411.

[3] Boiko, A. and Shendryk, V. (2017). System Integration and Security of Information Systems. Procedia Computer Science, 104, pp.35-42.

[4] Eskander, G., Sabourin, R. and Granger, E. (2014). Improving Signature-Based Biometric Cryptosystems Using Cascaded Signature Verification-Fuzzy Vault (SV-FV) Approach. 2014 14th International Conference on Frontiers in Handwriting Recognition.

[5] Chadha, R., Cheval, V., Ciobâcă, Ş. and Kremer, S. (2016). Automated Verification of Equivalence Properties of Cryptographic Protocols. ACM Transactions on Computational Logic, 17(4), pp.1-32.

[6] Zhao, T., Ran, Q., Yuan, L., Chi, Y. and Ma, J. (2016). Information verification cryptosystem using one-time keys based on double random phase encoding and public-key cryptography. Optics and Lasers in Engineering, 83, pp.48-58.