THE LATEST METHODS OF CRYPTOGRAPHIC PROTECTION OF INFORMATION RESOURCES.

Valentina Della[1], Lucía fare Melchor[2] , Phot Tangi[3*]

1Department of Public Finance, College of Business, Feng Chia University, Taiwan
2 Research scholar, University of Hyderabad, India
3 University of Lorraine, France
** Corresponding author: tangi.photi@gmail.com*

Abstract

The development of modern information technology (IT) has led to the widespread use of satellite communication channels for high-quality and reliable processing of digital images. This trend establishes the need for reduction or compression information flows of data on the condition of compliance with the technical requirements and capabilities of communication channels.

Introduction

The constant increase in the number of transmitted satellite images and their confidentiality and value, in terms of quality management decisions, has led to the need to use and develop modern dual-use systems. These systems, along with methods of compact data representation, should use modern methods of cryptographic protection of information resources. Aviation, rescue and military services are especially in need of such systems. Thus, the solution of the double problem is relevant:

- Compression of information data flows without loss of quality;
- Encryption of the specified streams on the basis of new methods of cryptosecurity of information resources of communication channels.

The growing need to address information security issues leads to the constant development of such a science as cryptography. The development of information technology (IT) has led to a separate section of cryptography, block encryption. Most existing algorithms are quite versatile and can encrypt any type of data (in terms of their structure and statistical characteristics), but with the growing number of classes of satellite images, there is a need to develop new algorithms and encryption methods that would be very narrow and optimal adapted to their class and thus quite stable.

Formulation of the problem

The use of such narrowly focused algorithms has its advantages in encrypting information data streams in satellite communication channels. Example:

- □□□□□□ cipher key should not be static, as when encrypting standard text;
- □□□□□□ encryption algorithm itself does not necessarily have to have high stability, which means a large key size.

It is clear that the implementation of a consistent procedure of image compression and encryption, further provides the stability of ciphertext, against modern methods of decryption. Thus there is a completely different section of cryptography - image encryption.

The aim of the article *is to* develop and study modern methods of formation of cryptoprotection systems of information flows of data of satellite communication channels on the basis of image compression procedures from the conditions of increasing cryptographic stability of ciphertext.

Analysis of modern approaches to the formation of stable ciphertexts

Modern cryptography solves the problem of encrypting plaintext with the key *K (key),* used in encryption and decryption functions, and can take any value and be selected from a large set, which is called the *key space* .

The idea of public key cryptography is very closely related to the idea of one-sided functions, ie such functions $f\ (x)$, which according to the known *x, is* quite simply the value of $f\ (x)$, while the definition of x from the function $f\ (x)$ *is* difficult to sense of theory.

Now consider an example of a cryptographic system with a change in the length of the key (system with a dynamic key). A typical cryptographic system with the principle of public key transmission, ie: to encrypt the message *m* uses the encryption key *e,* which are combined in the function *E (m)* and form ciphertext *c,* which is transmitted by the communication channel. On the other hand, the recipient of the message decrypts the message c using the function D (c) and the decryption key d , and receives the message m . Let both keys e and d belong to the key space$K$, ie e K and d K . You can then create two

∈ ∈

pairs of corresponding procedures: one for encryption and one for decryption

∈ ∈

$\{E\ (\ m\ ):\ e\ K\}$ and $\{D\ (\ c\ ):\ d\ K\}$.

Then d is actually a hint or a loophole. Unlike a public key cryptographic system, a dynamic key cryptographic system has no clues. Instead, the principle of generating a key based on the main message and embedding this key in ciphertext is used. That is, there is a function $f\ (x,\ k\ (x))\ =\ c$, which can be easily found for a known x , but the function

$f\ (c)\ =\ x\ +\ e$, if e is a key, then $k\ (x)\ =\ e$ *is the* function of forming the key e based on the known x, ie the function

$f\ (c) = x + k\ (x)$.

In this case, the very need to use hints disappears, because it is directly present in a certain functional dependence. In the block diagram shown in Fig. 1 , shows a general diagram of the algorithm with a dynamic key.

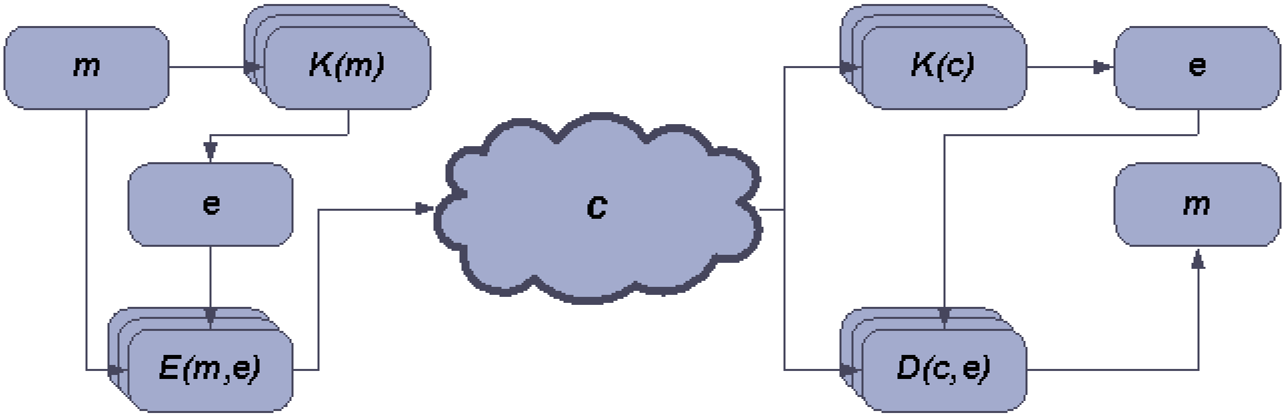

Fig. 1 Block diagram of a cryptographic system with a dynamic key

As can be seen from the diagram, the algorithm has changed slightly. Now to send the message m , you must first get the key e using the function $K\ (\ m\ )$. The next step is to perform the function $E\ (\ m\ ,\ e\ )$, which encrypts the message itself and the key with which the message was encrypted. After the message is delivered, the function $K (c)$ is executed , which retrieves the key e from the ciphertext c . Then the key e is passed to the function $D (c , e)$, which performs the final decryption of the message and issues a message m . That is, we can define the following pairs of encryption and decryption procedures :

$\{ K (m), E (m , e): e\ K \}$ and $\{ K (c), D (c, e): e\ K \}$ $\in$ $\in$

Conclusions

Summing up from all the above, we can conclude that cryptographic protection systems with a dynamic key in combination with image compression systems without loss of quality - can form a fairly stable ciphertext. The cryptographic strength of such a system will depend on many parameters, such as:

□□ Length of the encryption key;
□□□□□□□ degree of image compression;
□□ Type of encrypted image;
□□ Type of image compression algorithm;
□□ Sequence of execution of algorithms of cryptographic system, etc.

With different indicators of these parameters, it is possible to effectively adjust both the cryptographic stability of the system and the compression ratio of the image, to achieve optimal values of cryptographic resistance and compression for each class of images.

References

1. Ryabko B.Ya., Fionov AN Fundamentals of modern cryptography for information technology professionals. M .: Nauchnyi mir, 2004. ISBN 5-89176-233-1 .
2. 2. Yudin OK Coding in information and communication networks: - Monograph. - К .: НАУ, 2007.-308с
3. 3. Varfolomeev AA, Zhukov AE, Pudovkina MA Current cryptosystems. Basic properties and methods of resistance analysis. M .: PAIMS, 2000.

4. 4. Bruce Schneier. Applied cryptography. Protocols, algorithms, source texts in C language. M.: Triumph, 2002. ISBN 5-89392-055-4 , ISBN 0-471-11709-9 .
5. Armstrong .M. & Taylor .S. (2014) *Armstrong's Handbook of Human Resource Management Practice.* (13th Edition). London, Kogan Page Publishers.
6. Bendix, S. (2011). Industrial relations in South Africa; commonality, conflict and power in collectivebargaining. Available:
7. DeGennaro, William, and Kay Michel Feld. (2006),"Joint Committee take the Rancor out of Bargaining with our Teachers". The American School Board Journal 173 (2006): 38-39.
8. Gall, G. (2007). Turning full circle? Changing industrial relations in the magazine industry in Britain. Personnel Review, 36. 1, 91- 108.
9. Gwisai, M. (2006)Labour and Employment Law in Zimbabwe: Relations of work under Neo-colonial capitalism.Harare: Zimbabwe Labour Centre.
10. Herman, Jerry J. (2003),"With Collaborative Bargaining, you work with the Union-not Against it". The American School Board Journal 172 (2003): 41-42, 47. Huber, Joe, and Jay Hennies. "Fixon these five guiding lights, and emerge from the Bargaining fog". The American School Board Journal 174 (2007).
11. Hitt MA, Ireland RD, Hoskisson RE. (2014) Strategic management: Competitiveness and globalisation. 10th ed. Mason: South- Western, Cengage Learning.
12. Howell.C. (2005). Trade Unions and the State: The Construction of Industrial Relations Institutions in Britain, 1890-2000.
13. Wenbo Mao. Modern Cryptography: Theory and Practice = Modern Cryptography: Theory and Practice. - M .: «Williams» , 2005. - P. 768. - ISBN 0-13-066943-1