International Journal of Computer Science
and Engineering (IJCSE)
ISSN(P): 2278-9960; ISSN(E): 2278-9979
Vol. 4, Issue 3, Apr -May 2015, 9-10

International Academy of Science,
Engineering and Technology
Connecting Researchers; Nurturing Innovations

PROTECTION INFORMATION DES ALGORITHM

ZHANGISSINA G. D[1]. & SHANKIVAEV B. N[2]

[1]Vice-Rector, PhD, Professor, Central-Asian University, Almaty, Kazakhstan

[2]Vice-Rector, PhD, Professor, Central-Asian University, Almaty, Kazakhstan

ABSTRACT

In this paper we will be consider organization of protection information by DES algorithm. This is important problem in the field of Security information in the enterprise. We will be consider DES algorithm.

KEYWORDS: Sequrity, Information, Protection, Protection, Information, DES Algorithm

INTRODUCTION

Popular DES data encryption algorithm used by the US government as a standard since 1977. For encryption algorithm uses a 64-bit key data block and a 64-bit and 16 and passes (cycles). This algorithm is fast and effective. However, in its original form, this standard is not enough kriptostability, to direct attacks with search keys occupy, at the present level of technology, a reasonable time. Therefore, currently used all kinds of modifications thereof, such as 3-DES and cascaded 3-DES.

By making additional changes to the algorithm (such as the introduction of additional or redundant feedback keys), these modifications are much more resistant to direct attack. The main disadvantage of this system is that it uses a so-called symmetric keys: encryption and decryption of messages using the same secret key. Therefore, a prerequisite for the successful use of this system is the existence of a secret secure channel for key transfer. If an attacker intercepts the encryption key, then he can easily by using the same key to implement decoding secret messages. If a secure channel exists, then it is reasonable to transfer and message on the same channel, without resorting to the procedure of encryption.

State Standard GOST 28147-89 was approved in 1989 as a means of security, which is the standard for government agencies. Although he is not the main kriptomeans secure government communications lines, but this is the only more or less an open standard for this type of research and the use of the widest range of people. Despite the fact that the Russian guests to play the same role as that of DES in the United States, this standard began to be used in other countries. For example, a popular encryption algorithm ARJ archivers built just on the use of algorithms GOST.

GOST is very similar to DES. It uses the same 64-bit blocks. Nevertheless, there are some differences, for example, guests make 32 passes instead of 16, and the key is much longer, and consists of 256 bits, and so on.. In general, among the experts considered that it outperforms DES. Currently, however, and its interpretation is in the range of modern technology. And just as he has all the disadvantages of algorithms using symmetric keys.

DES algorithm has long been criticized for a number of drawbacks, including too small key length - only 56 digits. In addition, in January 1999 by DES encoded message has been hijacked by a connected via the Internet into a single network of 100 thousand. Personal computers. And it took less than 24 hours. In this regard, it became apparent that in the next few years, given the emergence of cheaper and more efficient equipment, des algorithm would be insolvent.

To solve this problem, in 1997 NIST released a request for comment RFC (Request For Comment), which describes the alleged "Advanced Encryption Standard» AES (Advanced Encryption Standard), which is to replace the standard des. In 1998, NIST (National Institute of Standards and Technology), which was the forerunner of the modern National Institute of Standards and Technology, announced a competition to create an algorithm that meets the requirements set by the Institute:

- The use of one or more open encryption algorithms;
- Accessibility and lack of royalties;
- The use of symmetric encryption;
- Support for the minimum block size of 128 bits and key sizes of 128, 192 and 256 bits;
- Free distribution throughout the world;
- Acceptable performance for different applications.

Prior to the first round of competition at NIST received 21 proposals, of which 15udovletvoryali extended criteria. This was followed by studies of these decisions, including those related to decoding and verification of performance and obtain expert judgments in cryptography.

As a result, as the standard algorithm was selected Rijndael, designed by two Belgian scientists, experts in cryptography. The US government announced that the authors of the most promising of the encryption algorithm was John Diemen from the company Proton World International and Vincent Ridzhmen, an employee of the Catholic University.

The algorithm Rijndael block cipher is unconventional because it is not used for kriptotransform Feyshtelya network. It represents each block of the encoded data in a two dimensional array of bytes table size 4 * 4 * 4 * 4, 6 or 8, depending on the fixed length block. Next, in respective steps or transformations are made independent columns or rows of independent, general or individual bytes in the table.

CONCLUSIONS

We considered Popular DES data encryption algorithm which used by the US government as a standard since 1977.

REFERENCES

1. Zhangissina G. D., Kasabekov S. A., Dzhusubalieva D.M., Munalbaeva N. About problems of specialists training on Informatics in Higher Education Institutions of Kazakhstan. International Journal of Educational Science and Research (Impact Factor: 3,9678). India. 28.02.2015. - p.9-14.