Available online at www.scientiaresearchlibrary.com

Scientia Research Library

ISSN 2348-0424
USA CODEN: JETRB4

Journal of Engineering And Technology Research, 2022, 10 (2):15-19

(*http://www.scientiaresearchlibrary.com/arhcive.php*)

CRYPTOGRAPHIC PROTECTION RELIABILITY

Minamatov Yusupali Esonali o'g'li

Fergana polytechnic institute, Fergana, Uzbekistan

Correspondance email: minamatovyu@gmail.com

ABSTRACT

As a result of our research, we developed an algorithm and programs for encrypting and decrypting text using a dynamic crypto-algorithm. To prove the authenticity of the encryption algorithm, we have come up with mechanisms for encryption-based software protection. We have reviewed cryptographic security enhancements and their application.

Keywords: encryption; block algorithm; cryptographic analysis; key length.

INTRODUCTION

The relevance of information security can be explained by the fact that information is a strategic resource. Modern state infrastructure is created by telecommunication and networks, various information systems, information technology and technical tools are widely used in various spheres of society. Everything has changed dramatically over the course of several decades, and the information has gained its value and became a widespread product.

The current risk is to steal or copy confidential information and documents, whereas the current threat is to use a set of computer data, electronic data, and electronic media without asking for permission from the owner. In addition, the desire for material gain has also grown.

MATERIALS AND METHOD

A cryptographic algorithm is considered computationally robust if it cannot be cracked using the available (both now and in the future) computing resources. "The strength of cryptosystems is quantified as the number of computer operations *W*, a cryptanalyst needed to open a key (or source text). "

The computational complexity of the algorithm is expressed through the symbol *O* and an indication of the order of magnitude of the computational complexity.

Currently, estimate of complexity (cryptographic strength) are obtained for all known cryptographic systems. According to the complexity theory, symmetric cryptosystems belong to the class of exponential algorithms: resistance DES cryptosystem rated as $O\ (2^{256})$, algorithm strength TDEA -

O (2 ^{168}), cryptosystems IDEA - *O (2^{128}).*

The most robust systems today are public-key cryptosystems (with a sufficient key length). However, public key encryption methods are fundamentally vulnerable, since all the mathematical methods underlying them are based on the so-called NP- complete problems that are conditionally intractable. In addition, for many NP- complete problems are constructed effective approximate algorithms (for example, a simplex method in the linear programming problem), which give exact solutions in real time. Moreover, all NP- complete problems are reducible to one another, that is, if a non-decoupling solution is found for at least one of them, then the entire class will be solved.

However, it should be noted that the computing power of computers is constantly growing, parallel computers and distributed computing technologies are successfully used to solve many cryptanalytic tasks. “For these reasons, declaring an algorithm reliable only because it is not easy to crack using modern technology is debatable at best. Therefore, when creating good cryptosystems that are resistant to cracking, the prospects for the development of computational tools for many years to come are taken into account. ”

Undoubtedly, the persistent encryption method Bruce Schneier (B.Schneier), an independent consultant and a recognized expert in the field of cryptology, calls only a single method - the one-time paid method. "Information Theory asserts the possibility of hacking all cryptographic algorithms (except for one-time notebooks)."

In practice, the following mechanisms are used to protect programs based on encryption:

- Encryption of the program code (in open form the program code is found only during the execution of the program);
- encryption of the program fragment (section) (most often, the critical section of the program is chosen);
- data encryption (a strong implementation by experts is cipher data directly in the source code of the program).

In practice, both static and dynamic encryption With static encryption, all code (code fragment) are encrypted / decrypted once. In encrypted In this form, the code is permanently stored on an external medium, in open form it is present in RAM. When dynamic scry encryption are sequentially encrypted / decrypted individual fragments or critical sections of the program.

Cryptographic protection is implemented in practice using software or software and hardware. When using software and hardware cryptographic operations are performed using a special computing device. Hardware implementation has a significant cost, however, increases the performance and reliability of the cryptosystem. Software implementation is universal, flexible and easy to use and update. However, it is low-speed and allows for easy modification (manipulation) of the algorithm.

To enhance encryption-based security, the following techniques are used.

Block decryption. The decoding of the program code is performed in stages in order to ensure that the executable code is not completely in memory in open form.

Encryption with feedback. A scheme is implemented in which the key for decrypting code fragments changes dynamically and depends on previously obtained values or conditions, for example, it is calculated as the value of a certain function from the previous block.

The check some of the executable code is used to decrypt the code fragment. Part of the protection mechanism is issued in the form of a resident module, the task of which includes, for example, prohibiting writing to a disk for some time or monitoring the segment registers for changes.

Combining cryptographic methods with compression (in this case, a copy of the decoded section cannot be entered in the same place).

Experts have studied enough the issues of the unreliability of cryptographic protection systems. Among the main reasons, researchers cite restrictions on the use of robust cryptoalgorithms, incorrect implementation and use of cryptoalgorithms, as well as the human factor.

Limit the use of robust cryptoalgorithms to their low speed; export restrictions (for example, from the USA export of cryptoalgorithms with a key length of more than 40 bits is prohibited);the use by developers of the protection systems of their own cryptoalgorithms, which, as a rule, do not possess sufficient cryptostoxicity.

In addition to errors in the software implementation and the presence of hatches (which are intentionally or intentionally left by the developers of the protection system), the following errors are examples of incorrect implementation.

- Reduced cryptographic strength during key generation. This refers to the mechanisms in which the security system either reduces the user's key length or generates a key from it that has a shorter length.
- Lack of verification for weak keys. For many cryptoalgorithms there are so-called weak keys, using which the cryptoalgorithm does not have enough power.
- Insufficient security from the so-called destructive software, that is, programs that can intercept the secret key or unencrypted data and even replace the cryptographic algorithm.
- The presence of dependencies in the key processing time. The point is that the cryptosystem can process different input data (key and / or directly encrypted data) for unequal periods of time. The burglar, measuring the processing time of various data, has the ability to select the key.
- Disadvantages of a random number generator. Pseudorandom number generators are often used to create a key. The resistance of the mechanism in this case is influenced by the initialization of the generator, a small period and a poor scatter of the generated numbers.
- Incorrect use of cryptographic algorithms include small key length, as well as key storage along with data.

RESULT AND DISCUSSION

A special role in the use of cryptographic protection systems is played by the human factor. In any system, user errors are the most common, but here the correct user experience with the security system is of great importance. For example, a user choosing a short or meaningful password crypto-resistant algorithm will reduce to zero.

To date, developed and successfully implemented mathematical methods of cryptanalysis. The basic principles used in solving problems of cryptanalysis were developed, the types of crypto-attacks were determined, a classification of cryptanalysis methods was given.

Attacking a cryptosystem, it is accepted to call cryptanalysis attempt. There are four main types of cryptanalytic attacks:

1) Attack based on ciphertext only.

Known: $C_1 = E_k(P_1)$, $C_2 = E_k(P_2)$, ..., $C_i = E_k(P_i)$.

Define: either $P_1, P_2, ..., P_i, K$, or recovery algorithm P_{i+1} of $With_{i+1} = E_k(P_{i+1})$.

2) A clear text attacks.

Known: $P_1, C_1 = E_k(P_1), P_2, C_2 = E_k(P_2), ..., P_{i,I} = E_k(P_i)$.

Define: either K, or recovery algorithm P_{i+1} of $With_{i+1} = E_k(p_{i+1})$.

3) Attack based on matched plain text.

Known: $P_1, C_1 = E_k(P_1), P_2, C_2 = E_k(P_2), ..., P_{i,I} = E_k(P_i)$,

whereby the cryptanalyst can choose $P_1, P_2, ..., P_i$.

Define: either K, or recovery algorithm P_{i+1} of $With_{i+1} = E_k(P_{i+1})$.

4) Attack based on adaptively matched plaintext.

This is a special case of attack using matched plain text. A cryptanalyst can not only choose the encrypted text, but also refine his subsequent choice based on the previously obtained encryption results.

For crypto-attacks of asymmetric cryptosystems, also used attack based on selected ciphertext:

Known: $C_1, P_1 = D_k(C_1), C_2, P_2 = D_k(C_2), ..., C_i, P_i = D_k(C_i)$.

Define: K.

The analysis of crypto-analytical attacks used in practice for decrypting computer programs shows that the encrypted source codes of programs, as well as executable program codes, are particularly vulnerable to attacks using known plaintext and selected plaintext. Cryptanalis is enough produce these types of attacks based on the assumption that the source code of the program uses known keywords and standard identifiers known string messages, and executable program codes contain known command codes, function calls, and much more.

A radical method of attack on a cryptosystem is the method of full brute force encryption keys. The time required to complete a bust depends on two parameters: the number of keys tested and the duration of each test. The time complexity of the brute force method is equal to $O(2^n)$, Where n - key length.

CONCLUSION

It should be noted that a few years ago the power of computers made possible the statements of the authors of the protection systems that a complete brute force encryption keys is impossible due to the huge number of possible keys. Even now, to demonstrate the effectiveness of the protection system, the power of multiple keys (passwords) is given, and the reliability is confirmed by the key length. But modern computer power and the latest computing technology allow for a complete exhaustive search of even sufficiently long keys within an acceptable period. of time.

In addition, to increase the search speed, effective search and comparison algorithms (usually based

on formal logic and using set theory, probability theory, and other areas of mathematics) have already been proposed and can be improved. The task of complete enumeration is solved using parallel processors. Each processor tests a particular subset of the key space. At the same time, it is essential that there is no need to exchange messages between processors, one single message of success is enough; no shared memory is required. In special cases it is possible to use specialized equipment that performs the search function.

A variation of the key brute force method is the method by which reveal a meaningful password, the so-called dictionary attack. Programs that perform a dictionary attack work quite quickly, because they implement efficient search and comparison algorithms. Many of them do not even contain a database of words, but use dictionaries embedded in common text editors.

REFERENCE

[1] Lecture of the Associate Professor of the Department of ICT of the Grodno State University Cand. tech. Sciences Livak Elena Nikolaevna

[2] Niels Ferguson, Bruce Schneier. Practical Cryptography = Practical Cryptography: Designing and Implementing Secure Cryptographic Systems. —M. : Dialectics, **2004**. — 432 с. — 3000 Copies. — ISBN 5-8459-0733-0, ISBN 0-4712-2357-3.