CONTINUOUS ENCRYPTION ALGORITHMS AND THEIR CRYPTANALYSIS

Obidova Dilafruz Faxridin qizi
Termez State University, 2nd-level graduate student, majoring in computer systems and their software

https://doi.org/10.5281/zenodo.7390863

Abstract. *Information technology has irreversibly entered the daily activities of every person - the life of an ordinary person cannot be imagined without various gadgets. Most homes use embedded operating system devices (other than regular personal computers) that can connect to the Internet and even wirelessly. Everywhere people are surrounded by various terminals, readers, sensors, etc. This proliferation of smart technologies raises the issue of data security. However, it is currently not possible to propose a cryptographic primitive that can be implemented on all types of target devices. This article discusses continuous encryption algorithms and their cryptanalysis.*

Keywords: *Continuous encryption, algorithm, program, code, cryptanalysis, open code, closed code.*

АЛГОРИТМЫ НЕПРЕРЫВНОГО ШИФРОВАНИЯ И ИХ КРИПТАНАЛИЗ

Аннотация. *Информационные технологии необратимо вошли в повседневную деятельность каждого человека – жизнь обычного человека невозможно представить без различных гаджетов. В большинстве домов используются устройства со встроенной операционной системой (кроме обычных персональных компьютеров), которые могут подключаться к Интернету и даже по беспроводной сети. Повсюду людей окружают различные терминалы, считыватели, датчики и т. д. Такое распространение умных технологий поднимает вопрос безопасности данных. Однако в настоящее время невозможно предложить криптографический примитив, который можно было бы реализовать на всех типах целевых устройств. В данной статье рассматриваются алгоритмы непрерывного шифрования и их криптоанализ.*

Ключевые слова: *Непрерывное шифрование, алгоритм, программа, код, криптоанализ, открытый код, закрытый код.*

INTRODUCTION

Protection of information by means of cryptographic modification consists in changing its components (words, letters, syllables, numbers) with the help of special algorithms or hardware solutions and key codes, that is, making it secret. To get acquainted with the encrypted data, the reverse process is used: decoding (decoding). The use of cryptography is one of the common methods that significantly increases the security of data transmission in computer networks, data stored on remote storage devices, and data exchange between remote objects.

For conversion (encryption), usually some algorithm or device is used that implements a certain algorithm, which can be known to a wide range of people. The encryption process is controlled by a key code that changes from time to time, which ensures the original appearance of the data using the same algorithm or device every time. Knowing the key makes it easy and secure to decrypt the text. However, without knowing the key, this procedure may be practically impossible even with a known encryption algorithm. Even simple alteration of information is a very effective means of hiding its meaning from most unskilled violators.

LITERATURE ANALYSIS AND METHODOLOGY

Encryption algorithms are designed to solve the problem of data privacy. Currently, cryptographic methods are intensively used to hide information. Encryption has been and remains the most effective form of protection since ancient times.

Encryption refers to the mutual transformation of unprotected (open) data into an encrypted (closed) form - ciphertext, in which an attacker cannot fully access it. Encryption uses keys, the presence of which indicates the ability to encrypt and/or decrypt data. It should be noted that the encryption method itself does not need to be kept secret, since knowing it alone does not allow decryption of the ciphertext.

Modern cryptosystems can be clearly divided according to the way they use keys into cryptosystems with a secret key (symmetric) and cryptosystems with a public key (asymmetric). If the same key is used for encryption and decryption, such a cryptosystem is called symmetric.

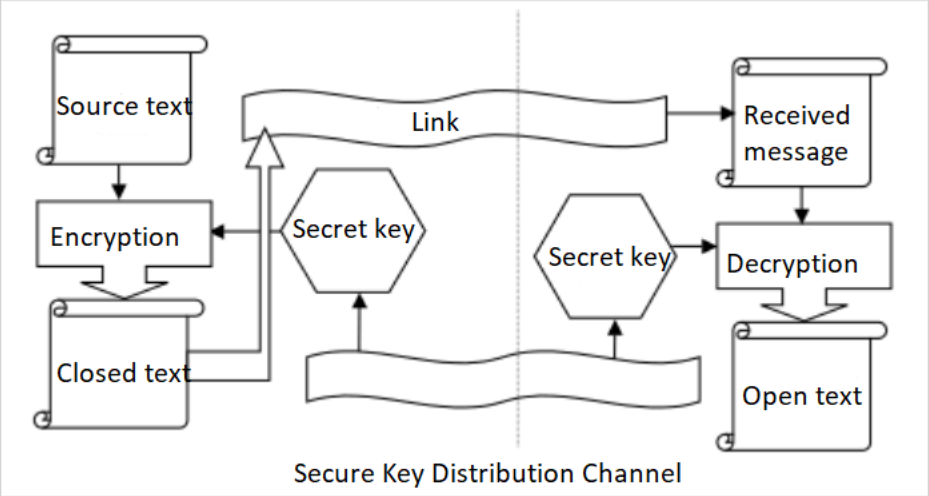

Figure 1. Scheme of construction of symmetric cryptosystems.

RESULTS

An encryption algorithm is considered strong if it is impossible to obtain information about public data, having access to private information and knowing the secret key. It has been proven that it is impossible to create an absolutely secure cipher, except when the size of the secret key is equal to (or larger than) the size of the data to be encrypted. This is difficult to do in practice, because cryptographic defenses use real-world and commercially available ciphers, for which the task of recovering plaintext from private text is difficult to compute, i.e., it requires such large resources that the attack is economically unfeasible.

Among the symmetric ciphers, the following are known and often used (the block size in bits is determined by b, the number of cycles is r, and the key length is determined by l):

DES is a US government standard (β = 64, ρ = 16, λ = 56). Currently, DES has been shown to be insufficiently resistant to brute force attacks.

Triple DES and DESX (b = 64, r = 16, λ = 168;112) - sequential application of the DES algorithm with different keys, which has a significant resistance to tampering.

IDEA - (b=64, r=8, l=128). An active study of its power has revealed a number of weak keys in it, but the probability of their exploitation is insignificant.

RC5 is a parametrized cipher with variable block size (b I), number of cycles (r 255) and number of key bits (l 2040). A study of its security showed that for β = 64 it is not available for differential cryptanalysis with r 12 and linear cryptanalysis with r 7.

GOST 28147-89 - Russian data encryption standard (b = 64, r = 32, l = 256). Many weak keys have been found for GOST, which significantly reduces its effective strength in normal encryption modes. GOST's cryptographic strength assessment is hampered by the fact that the most important part of the algorithm - substitution nodes, or S-boxes in the terminology of the DES cipher - is not described in the standard, and the laws of its creation are also unknown. At the same time, it has been proven that the probability of obtaining weak substitution nodes is high, which simplifies the cryptanalysis of this cipher.

Blowfish is a 64-bit block cipher developed by Schneier in 1993, which is implemented by key-dependent permutations and permutations. All operations are based on XORs and additions to 32-bit words. The key is of variable length (maximum 448 bits) and is used to create multiple subkey arrays. The cipher is designed specifically for 32-bit machines and is significantly faster than DES.

CONCLUSION

Currently, symmetric algorithms (Triple DES and IDEA, etc.) with a key length of more than 100 bits are not broken. The local GOST algorithm, in comparison with them, is characterized by an increase in complexity both in the creation of switching nodes and in the creation of keys. Also, in some encryption modes for the GOST algorithm, there is a high probability of generating an unstable key that reduces its effective key length from 2^{256} to 2^{62}.

Triple DES is more proven and provides acceptable performance than the IDEA algorithm. Triple DES algorithm - Applying the DES algorithm to the same data three times, but with different keys.

REFERENCES

1. Shannon C.E. Communication Theory of Secrecy Systems. Bell Systems Technical Journal 28, 1949, p. 656 - 715.
2. Federal Information Processing Standards Publication 46-2. Data Encryption Standard (DES). NIST, US Department of Commerce, Washington D.C, 1993.
3. ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования.
4. Bruce Schneier, Applied Cryptography: Protocols, Algorithms and Source Code in C. John Willey & Sons, 1994.
5. Nechvatal James. Public-Key Cryptography. NIST, Gaithersburg, 1990