IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 22, Issue 5, Ser. I (Sep. – Oct. 2020), PP 55-58
www.iosrjournals.org

To A Differential Attack for Symmetric Block Cipher

Juraev G.U.[1], Djabborov A.Kh.[2]
[1](*Department of Information Security, National University of Uzbekistan named after Mirzo Ulugbek, Uzbekistan)*
[2](*Department of mathematical modeling, Samarkand state university, Uzbekistan)*

Abstract:
This article discusses in detail the issues related to the effective conduct of differential cryptanalysis for modern symmetric block data encryption algorithms. For this purpose, an additional stage is introduced to organize a differential attack for symmetric block ciphers. As the first stage of a differential attack, it is proposed to build an attack model, in this case, an action model, which will allow for a reasonable time and an acceptable number of cleartext - ciphertext pairs to calculate the encryption subkey used.

Key Word*: plaintext, ciphertext, symmetric block ciphers, differential attack, differential cryptanalysis, transformation, strength, differential characteristics.*

Date of Submission: 20-09-2020 Date of Acceptance: 05-10-2020

I. Introduction

As known, ensuring the confidentiality of information when transmitting messages over an insecure communication channel is a traditional task of cryptography. For this purpose, symmetric and asymmetric ciphers are now successfully used.

Symmetric ciphers have high encryption rates and are also much easier to implement in both software and hardware, for example the symmetric block cipher DES is about 1000 times faster than the asymmetric cipher RSA. For this reason, symmetric encryption is often used to encrypt messages with a longer length than asymmetric encryption.

Symmetric ciphers are divided into two categories: stream and block ciphers [1]. It should also be noted that some classifications do not distinguish between block and stream encryption, considering that stream encryption is encryption of blocks of unit length.

Stream ciphers are needed primarily in cases where information cannot be divided into blocks. For example, a data stream, each character of which must be encrypted and sent somewhere, without waiting for the rest of the data sufficient to form a block. For this reason, stream encryption algorithms encrypt data bit by bit or character by character [1]. Basically, stream ciphers are implemented in hardware in wireless data networks due to the need to immediately transfer data as it arrives. Therefore, stream ciphers are very efficient, they are often used to encrypt audio and video information [2].

Modern symmetric block data encryption algorithms encrypt an m-bit block of plaintext and decrypt an m-bit block of ciphertext. The same key is used for encryption and decryption, or the decryption key is easily calculated from the encryption key and vice versa. As a result, the decryption algorithm must be the inverse of the encryption algorithm.

According to the Kerchhoff principle, the encryption and decryption algorithms must be fully known to the cryptanalyst, i.e. the secrecy of the cipher must be ensured by the secrecy of the encryption key. Only in some cases, for example, for military and intelligence purposes, the essence of the cryptosystem is kept secret.

Symmetric block ciphers have the following basic requirements:

• sufficient cryptographic strength;
• fast encryption speed;
• simplicity of encryption and decryption procedures.

The general principles of building block ciphers have been defined by K. Shannon [3,4], on the basis of which it is necessary to use in the block cipher algorithm:

a) substitutions (nonlinear transformations);
b) permutations of symbols in blocks;
c) iterating operations a) and b) (i.e., repeating them multiple times with different keys).

Multiple application of the above algorithms, relatively simple cryptographic transformations, ensures the cryptographic strength of ciphers.

Here, cryptographic strength refers to the time required to break the cipher using the best cryptanalysis method.

From the above, it follows that the strength of the encryption algorithms depends on the complexity of the transformation used in it, as well as on the size of the key space. Research and establishment of properties of cryptographic strength of ciphers is of theoretical and practical importance.

Attack to encryption algorithm

The algorithm for finding the encryption key or round key is called an attack. An attacker attacking an encryption algorithm can have the following goals [5]:

- finding the plaintext, having it in an encrypted form, but not having a secret key;
- finding the secret key.

In the first case, an attacker can obtain an open message of the corresponding ciphertext. And in the second case, having received a secret encryption key, an attacker will be able to read all messages encrypted with this key, which can be more dangerous than others. If an attacker successfully obtains the private key, it is called cracking or fully disclosing the encryption algorithm.

An algorithm is cryptographically strong if there are no methods of breaking it, except for the brute force method, which is also ineffective for it in finding the encryption key. A cryptographically strong cipher cannot be broken in a more efficient way than a brute-force search over the entire key space.

By the nature of the applicability of the methods of cryptanalysis of block ciphers, they can be divided into universal and non-universal methods. The brute force method is a striking representative of the universal cryptanalysis methods. For this reason, Brutal-Force Attack is often used to recover the key - a brute-force attack, those brute-force search of keys. The exhaustive search algorithms can be parallelized, which can significantly speed up the key finding. If the key size is n bits, then there are 2^n key options. Finding the encryption key requires on average $2^n/2$, i.e. 2^{n-1} encryption operations.

For modern symmetric block ciphers, the use of brute force is practically not feasible. Therefore, the main goal of using any cryptanalysis methods, including differential analysis, is to improve the amount of work for a complete enumeration or improve the time / memory ratio [6]. For this purpose, in cryptography, the time of analysis using the brute-force method is considered to be the reference. This means that if there is a way to cryptanalize the encryption algorithm faster than using a brute-force attack, then this encryption algorithm is considered vulnerable.

Differential cryptanalysis

Differential cryptanalysis is believed to have been developed in 1990 by Israeli cryptographers Eli Biham and Adi Shamir [7]. However, in 1994, Don Coppersmith of IBM stated in his article that the method of differential cryptanalysis was already known to IBM in 1974, and one of the goals set in the development of DES was to protect against this method [8].

Differential cryptanalysis method is one of the main cryptanalysis methods for symmetric block data encryption algorithms. If the encryption algorithm withstands a differential attack, then it is considered strong and without any fear it can be used to transfer confidential information. Differential analysis, like linear analysis, refers to the statistical methods of cryptanalysis. This method can also be used to establish the strength of stream ciphers and hash functions [1].

To perform differential cryptanalysis, a cryptanalyst collects several texts encrypted using the same encryption key. At the same time, the corresponding open texts may not be known, and how the open texts differ from each other, the cryptanalyst knows. In the method of differential cryptanalysis, the difference between texts means the bitwise addition of texts modulo two (XOR operation). These differences are called difference or differential, and from there the name of the method is "differential cryptanalysis" or "differential analysis", which contain the English word difference - difference. Thus, the cryptanalyst chooses a pair of plain texts (X, X') with a difference $\Delta\mathrm{X} = \mathrm{X} + \mathrm{X}'$. Since the cryptanalyst knows the encryption algorithm, then he will further accumulate information about how the given difference of plain texts is manifested in ciphertexts, those. determines the difference $\Delta\mathrm{Y} = \mathrm{Y} + \mathrm{Y}'$ matching ciphertext pairs (Y, Y').

If a pair of plain texts with a difference $\Delta\mathrm{X}$ after i rounds of encryption can go into a pair of ciphertexts with a difference $\Delta\mathrm{Y}$, then a pair of differences $(\Delta\mathrm{X}, \Delta\mathrm{Y})_i$ *called* i *- th differential cipher*.

A sequence of input and output differentials that the output differential i-th round is input for $i+1$-th round is called a differential characteristic. For the analysis, those cipher differentials are used that appear with the highest probability than other possible differentials.

Information on the dependencies between the differences of plain texts and the differences of the corresponding ciphertexts can be used to break the keys of the encryption algorithm. For this, a set of pairs of

texts with a certain difference is accumulated, the analysis of which makes it possible to select a certain key or part of the key, which is the desired key either unambiguously or (in comparison with other possible keys) with the highest probability.

Differential attack building principles

Differential cryptanalysis is a selected plaintext method that is difficult to implement in practice. The principles of constructing a differential attack for symmetric block ciphers consists of the following stages:

1. Establishing an attack model (a model of an attacker's actions).
2. Determination of highly probable differential characteristics.

Using the chosen attack model, it is necessary to determine differential characteristics with a high probability - a sequence of input and output differentials on rounds, such that the output differential from one round corresponds to the input differential for the next round;

3. Revealing the correct pairs of texts using the found differential characteristics;
4. Analysis of the accumulated correct pairs of texts and keeping statistics on all possible encryption keys.

At the first stage, the attacker's task is to build an attack, i.e. an action model that will allow for an acceptable time and an acceptable number of pairs to open text - ciphertext to calculate the key used. This problem is solvable, since there is a primitive algorithm that allows you to calculate the key used. This is an enumeration over the key space K. But for modern cryptoalgorithms, the power of the key space $|K|$ - quite a large number, therefore, it is necessary to find an attack that differs significantly from brute force. For example, in [9], an approach was used - an attack is performed for one round from the beginning and a reverse attack for one round from the end for cryptanalysis of the "Grasshopper" block cipher, which is part of the Russian new cryptographic data encryption standard GOST R 34.12-2015 [10]. Thanks to the meeting in the middle, it was possible to significantly reduce the search to doable. Moreover, in the attack under development, the value of the output differential ΔY is not important, it is necessary to find out only the value of the input differential ΔX, on the basis of which pairs of known plaintext will be selected for the attack. This value should correspond to the maximum possible probability of passing the differential, because on the basis of the probability, the number of text pairs required for the attack is calculated.

At the second stage, the determination of the differential characteristics with the highest probability, according to the authors of [11], is performed only once for each block cipher and is a theoretical problem. This situation is due to the fact that the values of the differential characteristics depend on the structure of the encryption algorithm and the cryptographic operations used in it. In [12], it was possible to present the transformations of the encryption algorithm "Grasshopper" in an analytical form, with the help of which it was possible to create software to identify the most probable differentials. The description of the algorithm in an analytical form allowed 16 execution cycles of the shift register with linear feedback, in each of which 16 multiplication operations and 15 addition operations will be carried out, reduced to 16 multiplication operations and 15 addition operations.

The result of the second stage is the identification of a pair of input and output differentials $(\Delta X, \Delta Y)$, which appears with the highest probability, i.e. $p > 1/2^m$. In the next stages, all work is carried out with this pair.

At the third stage, the search for the correct pairs of texts is carried out using the found characteristics $(\Delta X, \Delta Y)$. For this purpose, many pairs of plaintext are encrypted on the same (desired) key (X, X'), for whom $X + X' = \Delta X$. If among a pair of plain texts there are pairs for which there is a high probability ΔY, then such pairs $(\Delta X, \Delta Y)$ are called right-handed pairs, otherwise they are called wrong-handed. It should be noted here that when identifying the correct pairs of texts, only the right side of the output characteristic can be taken into account ΔY, since the left side of the output characteristic is not particularly significant. This approach was tested by E. Biham and A. Shamir for the differential analysis of the DES algorithm and made it possible to improve the process of finding correct pairs of texts [13]. The right-hand pairs accumulated at this stage are used to identify the bits of the subkey or encryption key in the next step.

In the fourth step, you can start extracting the key bits. For this, the characteristics are built up to the penultimate $r-1$ round (for r round cipher). The key of the last round is always attacked. For this purpose, partial decryption is performed for each pair of ciphertexts. Search by subkey k_i^r, where *r* - round number, *i* - piece of round key, which is at a given characteristic. The search is performed over the entire range of possible values. A counter is set for each value of the desired partial subkey.

II. Conclusion

When decrypting, a part of the text is obtained on which the expected characteristic should appear. The feasibility of the characteristic is checked ΔY at ΔX. If feasible, the counter of this subkey is increased by one. The process continues for each subkey. At the end of the enumeration, the distribution of the counter values of each subkey value is displayed. The key for which the counter value at the end of the passage through all texts for the attack is the maximum is taken as a probable key K^r. Then the attack is carried out on the algorithm with $r-1$ round, after decrypting all texts to attack the truncated version with the found key. Then this process is repeated for the rest of the rounds. As a result, you can get all the key used for encryption.

References

[1]. Ivanov M.A., Chugunkov I.V. Cryptographic methods for protecting information in computer systems and networks. Moscow: NRNU MEPhI, 2012. – 400 p.: il.

[2]. Asoskov AV, Ivanov M.A., Mirsky A.A., Ruzin AV, Slanin AV, Tyutvin AN Stream ciphers. - M .: KUDITS-OBRAZ, 2003 .- 336 p.

[3]. Shannon C.E. Communication Theory of Secrecy Systems // Bell Syst. Tech. Journal. – 1949. Vol. 28.

[4]. Ojiganov A.A. Cryptography: - SPb: ITMO University, 2016. - 140 p.

[5]. Panasenko S.P. Encryption algorithms. Special reference book.. □ SPb.: BHV-Petersburg, 2009. □ 576 p: il.

[6]. Babenko L.K., Ishukova E.A. Modern block cipher algorithms and methods for their analysis. M .: Helios ARV. 2006. -376 p.

[7]. Biham E. and Shamir A. Differential Cryptanalysis of DES-like Cryptosystems //Journal of Cryptology, vol. 4, №1, pp. 3-72, 1991.

[8]. Coppersmith, Don. The Data Encryption Standard (DES) and its strength against attacks. IBM Journal of Research and Development 38 (3): 243. DOI: 10.1147/rd.383.0243.

[9]. Juraev G.U., Ikramov A.A., Marakhimov A.R. About differential cryptanalysis algorithm of block encryption Kuznyechik //International Journal of Advanced Research in Science, Engineering and Technology. Vol. 6, Issue 2, Feb 2019. –P. 8164-8169. URL: http://www.ijarset.com/upload/2019/february/26-IJARSET-gjuraev.pdf

[10]. Information technology. Cryptographic data security. Block ciphers. URL: http://www.tc26.ru/standard/gost/GOST_R_3412-2015.pdf.

[11]. Babenko L.K., Ishukova E.A. Features of the application of methods of linear and differential cryptanalysis to symmetric block ciphers // Cybersecurity issues. No. 1 (9), 2015.S. 11-19.

[12]. Juraev G.U., Marakhimov A.R. Representation of the block data encryption algorithm in an analytical form for differential cryptanalysis. IJIRIS: International Journal of Innovative Research in Information Security, volume VI, 38-42. DOI: 10.26562/IJIRIS.2019.MRIS10081.

[13]. Biham E., Shamir A. Differential Cryptanalysis of the Full 16-round DES, Crypto'92, Springer-Velgar, 1998. – P. 487. National Cholesterol Education Program (NCEP) Expert Panel on Detection, Evaluation, and Treatment of High Blood Cholesterol in Adults (AdultTreatment Panel III) Third report of the national cholesterol education

Juraev G.U, et. al. "To A Differential Attack for Symmetric Block Cipher." *IOSR Journal of Computer Engineering (IOSR-JCE)*, 22(5), 2020, pp. 55-58.