УДК 378.4

UPDATED CRYPTANALYSIS

Mokliak Alina

National Aviation University, Kyiv

Scientific supervisor: V.I. Trofymenko, Ph. D, Associate Professor

Keywords: cryptanalysis, algorithm, methods, system, machine

Every day there are more and more scientific articles and research in the field of cryptology and cryptanalysis, as the topic of solving complex cryptographic systems spreads through the information space, capturing the attention of future professionals in this field. Research and development of the cryptanalysis system are important both for the protection of human life and for the promotion of security information systems through the constant threat of cyber-attacks and robberies.

Cryptanalysis is based on finding the key of the cipher without the possibility of access to it, is developing methods of breaking the code and methods of finding vulnerabilities in the cryptographic algorithm. Over time, cryptanalysis techniques evolved from the use of only pens and paper by linguists to the widespread use of computing power by mathematicians. Cryptanalysis turns to the human brain even in informational situations when it seems that it is not able to solve the problem on a par with software. Well-known evidence of this is the deciphering of the Enigma machine during World War II and the deciphering of all military messages by American geneticists during World War I.

Today, linear cryptanalysis (to use you need to have a large number of pairs of plaintext / encrypted text obtained using the same encryption key) along with differential (to use you need to be able to encrypt any text in any number) is one of the most common methods of breaking block (a kind of symmetric) ciphers. Both types of cryptanalysis, as well as its entire space, are closely related to the mathematical field, namely, probability theory and mathematical statistics. Probability, in particular, is used to determine the fairness of the ratio for arbitrarily selected bits of plaintext, cipher text and key, as well as to characterize the differences in the received cipher texts.

Cryptanalysis itself takes place in two steps: the first - building relationships between plaintext, cipher text and key, which are fair with a high probability; the second is to use these relationships together with known plaintext cipher text pairs to obtain key bits.

The meaning of this algorithm is to obtain relations of the following type:

$$P_{i1} \oplus P_{i2} \oplus ... \oplus P_{ia} \oplus C_{j1} \oplus C_{j2} \oplus ... \oplus C_{jb} = K_{k1} \oplus K_{k2} \oplus ... \oplus K_{kc}$$

Fig.1 Example of a linear equation

where Pn, Cn, Kn - n-and bits of text, cipher text and key.

The data of this ratio are called linear approximations. For arbitrarily selected bits of plaintext, cipher text and key, the probability of the validity of the ratio "P" is approximately 1/2. If the probability of the ratios differs markedly from the value of 1/2, then this makes it possible to use them to reveal the algorithm. Linear cryptanalysis has one very useful property - under certain conditions it can be reduced to the equation of the form:

$$C_{j1} \oplus C_{j2} \oplus \ldots \oplus C_{jb} = K_{k1} \oplus K_{k2} \oplus \ldots \oplus K_{kc}.$$

Fig. 2 Example of a linear equation without bits

There are no plaintext bits in this type of equation, ie you can build an attack based on cipher text only. Such an attack is actually the most practical.

In conclusion can be summed that cryptanalysis is a difficult and complex research activity that involves all modern mathematical and technological capabilities to ensure confidentiality and integrity, as well as the protection of information and information resources. The future of cryptanalysis will be closely and even inextricably linked with nanotechnology, as quantum devices for technological calculations such as P. Shore's algorithm-machine are already being developed today. However, it should be noted that sometimes the use of conventional and perhaps somewhat outdated crypto analytical systems is more rational, as unjustified and costly one-time decryption methods are not cost-effective. Choosing the necessary level of protection is a search for a compromise between the level of security and the cost of ensuring it.

References:

1) Модель криптоалгоритму підвищеної стійкості до часової атаки. Поровозник В. Інтернет джерело. [Режим доступу] http://dspace.wunu.edu.ua/bitstream/316497/40525/1/%D0%BF%D0%BE%D0%B2%D0%BE%D1%80%D0%BE%D0%B7%D0%BD%D0%B8%D0%BA_%D0%9C%D0%A0_2020.pdf
2) Криптоаналіз,: вчора ,сьогодні, завтра. Інтернет джерело. [Режим доступу]]https://www.osp.ru/os/2009/03/8120956
3) https://ru.wikipedia.org/wiki/Линейный_криптоанализ
4) https://studopedia.su/15_68118_postroenie-lineynih-uravneniy.html