УДК 004.057.4
Rudyk O.F. student of group 125-22-2
(Dnipro University of technology, Dnipro, Ukraine)

METHODS OF ENSURING DATA PROTECTION AGAINST BRUTE FORCE CRYPTOGRAPHIC ATTACKS

Currently, due to the rapid development of computer technology and open networks, there are more threats and vulnerabilities associated with the risks of loss, disclosure or modification of user information. Cryptographic methods play a key role in data protection, but even the most advanced cryptographic algorithms can become the target of attacks. The classification of modern cryptanalysis methods is shown in fig. 1.

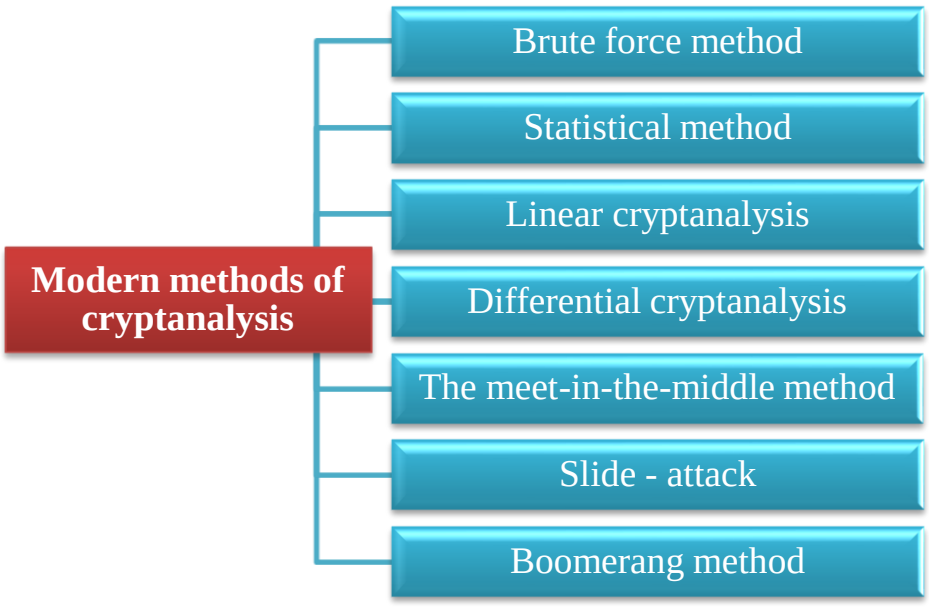

Figure 1 – Classification of modern cryptanalysis methods

One of the most common threats is brute force attacks. Brute force is a technique used in cybersecurity to crack encrypted messages or passwords by systematically trying all possible combinations until the correct one is found. This method is based on the assumption that the encryption algorithm used is known, but the key or password is unknown. The use of these methods is relevant when solving security aspects of problems in sources [3-4], using the algorithms described in [1-2].

In the case of using a brute-force method to decrypt text protected by a symmetric key, the level of complexity of information disclosure can be relatively low, especially if the key is short or not sufficiently complex. If an 8-bit key is used, there are 2^8, or 256, possible keys. Therefore, it will take at most 256 tries to find the correct key, with a 50 percent chance of finding the right key after half of the tries. If the key length is 56 bits, then there are 2^56 possible keys. If a computer can check a million keys per second, it will take an average of 2,285 years to find the right key.

Methods of protection. One of the key measures is the use of longer and more complex cryptographic keys or passwords, which significantly complicates the process of their selection due to an increase in the number of possible combinations. A strong password must contain:

1. The length of the key is at least 16 characters.
2. Combinations of upper and lower case letters.
3. Numbers and special characters.

The reliability of such a key is shown graphically in fig. 2.

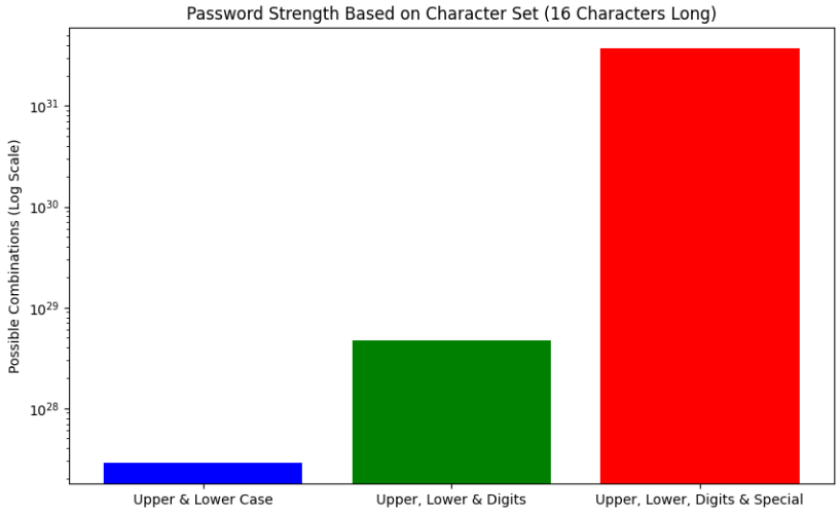

Figure 2 - Password strength based on character set

Also an important aspect is the implementation of account lockout mechanisms after a certain number of failed authentication attempts, which reduces the probability of a successful brute force attack. In addition, the use of modern cryptographic algorithms, resistant to such attacks, provides an additional level of protection, because they are optimized to counter attempts at key manipulation.

In conclusion, it can be noted that effective protection against brute force attacks requires a comprehensive approach. Although cryptographic methods remain one of the most important data protection tools, no algorithm is completely secure.

REFERENCE

1. Khabarlak, K. S. (2022). FASTER OPTIMIZATION-BASED META-LEARNING ADAPTATION PHASE. *Radio Electronics, Computer Science, Control*, (1), 82. https://doi.org/10.15588/1607-3274-2022-1-10

2. K. Khabarlak, "Post-Train Adaptive U-Net for Image Segmentation," Information Technology: Computer Science, Software Engineering and Cyber Security, no. 2, pp. 73--78, 2022, https://doi.org/10.32782/IT/2022-2-8

3. Олішевський І.Г. Автоматизована методика розрахунку параметрів для нетрадиційних технологій опалення та кондиціонування будівель/ І.Г. Олішевський, Г.С. Олішевський // Електротехніка та електроенергетика. / Запорізький нац. ун-т «Запорізька політехніка». – Запоріжжя, 2021. – № 3. – С. 40-47. https://doi.org/10.15588/1607-6761-2021-3-4

4. Олішевський І. Г. Обгрунтування методу утилізації теплоти системи кондиціонування для теплонасосної системи опалення / Г. С. Олішевський, І. Г. Олішевський // Інформаційні системи, механіка та керування / НТУУ «Київський політехнічний інститут». – Київ. – 2017. – № 17. – С. 86 – 94. DOI: http://dx.doi.org/10.20535/2219-3804172017102874