2. Гончар С.Ф. Дослідження проблеми кіберживучості Об'єднаної енергосистеми України / Гончар С.Ф., Герасимов Р.П., Ткаченко В.В. // Електронне моделювання. – 2019. – Т.41. – №1. – С.43-53. https://doi.org/10.15407/emodel.41.01.043
3. Komarov, M., Honchar, S., & Dimitriieva, D. (2021). Дослідження проблеми кіберживучості об'єктів критичної інформаційної інфраструктури. Ядерна та радіаційна безпека, 1(89), 59-66. https://doi.org/10.32918/nrs.2021.1(89).07

Marharyta Ihorivna Popp, the student of English Language and Applied Linguistics Department,
Zhytomyr Ivan Franko State University, Zhytomyr, Ukraine

THE ENCRYPTION ALGORITHMS

Cryptography is the method of converting data into an unencrypted format so that only authorised users can access the information. There are two main types of encryption: symmetric and asymmetric.

The method of symmetric encryption contains one cryptographic key to encrypt and decrypt data. Using the same key for both operations makes the process simple. The most popular example of symmetric encryption is the "Caesar cipher".

Modern encryption methods are based on very complex mathematical functions that are almost impossible to uncrack. There are hundreds of symmetric algorithms, but AES, DES and 3DES are the most common of them.

DES (data encryption standard) is the older symmetric method of encryption, developed by IBM to secure confidential government data and then used by federal agencies in the United States of America. DES converts 64-bit data blocks to encrypted text by splitting them into two separate 32-bit blocks, applying the encryption process to each of the parts separately. This algorithm includes 16 cycles of various processes, through which data passes in encrypted form, such as expansion, permutation, replacement and so on. In 2005, however, DES was declared obsolete and replaced by the AES encryption algorithm.

3DES, also known as TDEA (triple data encryption algorithm) is an updated version of the DES algorithm. The new algorithm applied DES cycles three times to each data block. As a result, 3DES was much harder to crack than its DES predecessor. TDEA has become a widely used in

payment systems and other technologies in the financial industry. In 2019 National Institute of Standards and Technology has officially announced the aging of the algorithm. Therefore, the usage of 3DES must be abolished in all new applications after 2023.

AES (advanced encryption system) was developed as an alternative to DES and after the approval of NIST in 2001 became a new encryption standard. AES works by substitution and permutation methods. First, unencrypted data is converted into blocks, and then encryption is applied using a key. The encryption process consists of various processes, such as shifting rows, mixing columns, and adding keys. Depending on the length of the key there can be 10, 12 or 14 transformations and the last round of transformation is different from previous ones and does not include the subprocess of mixing.

Asymmetric encryption includes several keys that are mathematically related to each other to encrypt and decrypt data. One of the keys is known as "public key" and the other one – "private key". In this method, the public key, which is publicly available, is used to encrypt the data, while the decryption of the data is performed using a private key and that ensures the data from attacks. There are two main types of asymmetric encryption: RSA and ECC algorithms.

In 1977 the RSA asymmetric encryption algorithm was invented by three scientists from the Massachusetts Institute of Technology: Ron Rivest, Adi Shamir and Leonard Adleman. This method is efficient as two different random primes of a given size are selected and multiplied to create another giant number. The task is to determine the original primes from the multiplied giant. It turns out that this puzzle is almost impossible to be solved for modern supercomputers, let alone humans.

In 1985, two mathematicians named Neil Koblitz and Victor Miller proposed the use of elliptic curves in cryptography. Almost two decades later, their idea came true and the ECC (Elliptic Curve Cryptography) algorithm began to be used in 2004-2005. In the ECC encryption process, the elliptic curve represents a set of points that represent the mathematical equation ($y^2 = x^3 + ax + b$). The number that symbolizes a point on the curve is multiplied by another number and gives another point on the curve so that you have to find a new point on the curve to break this puzzle. It is built in such a way that it is almost impossible to find a new point, even if you know the starting one.

There is also the hybrid method of encryption that includes symmetric and asymmetric ones. The idea of hybrid encryption was born when it became critical to encrypt data at high speed while providing identity verification. The hybrid encryption method is used in SSL / TLS certificates during serial communication between servers and clients in a process known as a "TLS handshake". First, the identity of both parties is verified using a private and public key. After that, the data is encrypted using symmetric encryption using an ephemeral key. This ensures the fast transfer of large amounts of data that we send and receive on the Internet every minute.

Each of the encryption algorithms has pros and cons, but most modern SSL certificates use a hybrid method: asymmetric encryption for authentication and symmetric encryption for privacy.

References:

1. Stephens Rod Essential Algorithms: A Practical Approach to Computer Algorithms/ R. Stephens. – Indianapolis, Indiana, 2013. – 624 p. Retrieved from: https://doc.lagout.org/science/0_Computer%20Science/2_Algorithms/Essential%20Algorithms_%20A%20Practical%20Approach%20to%20Computer%20Algorithms%20%5BStephens%202013-08-12%5D.pdf
2. Fouché Gaines, Helen Cryptanalysis: A Study of Ciphers and Their Solution/ H. Fouché Gaines. – New York: Dover Publications Inc., 1956. – 259 p. Retrieved from: https://archive.org/details/cryptanalysis00hele/page/n5/mode/2up

Кравченко Валерій Іванович, к. т. н., доцент,
Стукалова Юлія Анатоліївна, асистент,
Зубрицький Олексій Олександрович, студент групи КН 20-МН
Донбаська державна машинобудівна академія, Краматорськ

МОДЕЛЮВАННЯ СИСТЕМИ ПОШУКУ ШКІДЛИВОГО ПЗ У ВИКОНУВАНИХ ФАЙЛАХ OS WINDOWS

Збільшення кількості програмного забезпечення (ПЗ) постійно породжує різні проблеми особливо актуальною з яких є захист інформації в інформаційно-комунікаційних системах. Використання виконуваних файлів заражених вірусами, може призвести до різних