УДК 004.056

L.Magas
Y.Koziuk

APPLICATION OF MATHEMATICS IN CYBER SECURITY

Vinnytsia National Technical University

Анотація
У статті розглянуто важливість математики в сфері кібербезпеки. Проаналізовано різні розділи математики які допомагають у вирішенні проблем кібербезпеки таких як: уникнень кібератак,безпечне шифрування,та загроз за допомогою різних розділів математики.
Ключові слова: *математика,кібербезпека,загрози,теорія ймовірності,шифрування,аналіз данних.*

Abstract
The article considers the importance of mathematics in the field of cyber security. Various sections of mathematics that help in solving cyber security problems such as avoiding cyber attacks, secure encryption, and threats using various sections of mathematics are analyzed.
Keywords: *mathematics, cyber security, threats, probability theory, encryption, data analysis.*

Introduction

In a world where technology is becoming more and more complex, cyber security is becoming one of the main challenges facing companies and organizations. Cyber-attacks can result in data loss, breaches of data privacy and integrity, and business and reputational damage. Ensuring cyber security is becoming an increasingly important task for many companies and organizations, and for this, tools are needed to help protect data from cyber attacks [1]. And mathematics is one of the important tools thanks to which risks and attacks can be avoided.

Basics

Mathematics is one of the key tools used to ensure cyber security. In this article, we will look at the different sections used in the protection of information.

1. Number theory: the study of the properties of numbers and arithmetic operations used in cryptography to protect data.

In general, if we talk about cryptography, we can mention the main types of cryptographic closure, such as encryption and data encoding. Modern cryptography includes four major sections: symmetric cryptosystems and electronic signature systems, control systems keys and cryptosystems with public keys. Cryptographic methods can be divided into two classes:

– information processing by replacing and moving letters, in which the amount of data does not change (encryption);

– compression of information using the replacement of individual combinations of letters, words or phrases (encoding) [2].

Cryptography is the most important part of all information systems, ensuring accountability, transparency, accuracy and confidentiality. It prevents e-commerce fraud attempts and provides legal force financial transactions. Cryptography helps establish your identity and ensures anonymity. It prevents hooligans from hacking the server and does not allow it competitors to get into confidential documents. And in the future, to the extent how commerce and communications will be increasingly linked to computing networks, cryptography will become vital [1].

2. Algebra: The study of algebraic structures such as groups, rings, and fields used in cryptography to create cryptographic protocols and encryption systems.

Algebra plays a very important role in cyber security. It is used to create cryptographic protocols and encryption systems that ensure the security of information transmitted over the network. Algebraic structures such as groups, rings, and fields are used to create cryptographic systems.

For example, the Diffie-Hellman protocol uses groups to exchange keys, while RSA uses rings and fields to encrypt and decrypt data. In addition, algebra is used to analyze cryptographic protocols and encryption systems in order to identify weaknesses and potential attacks [3]. Algebraic techniques can help identify possible ways to attack cryptographic systems and help improve their security. So, algebra in cyber security is an important branch of mathematics that ensures information security and helps avoid possible cyber attacks [2].

3. Probability Theory: The study of probability and probability distributions used in cryptography to assess the strength of cryptographic protocols and encryption systems.

A specialist should be able to:calculate the probability of an event using combinatorics formulas and rules; apply basic formulas of probability theory (formulas of addition and product of probabilities, full probability, Bayes, Bernoulli, limit theorems); find distributions of random variables and their numerical characteristics; build a state graph of the Markov process; calculate marginal probabilities and other characteristics of the Markov chain; build a geometric representation of variational series and their empirical distribution function; calculate estimates of parameters of distributions of random variables based on the results of a statistical experiment; apply the simplest statistical criteria [4, pages 55-60].

4. Information Theory: The study of concepts such as entropy and information complexity used in cryptography to determine the strength of cryptographic protocols and encryption systems.

Information theory, also called the mathematical theory of communication, focuses on the study of data transmission, data processing, and information measurement. Claude Shannon and Warren Weaver were the authors of this theory, published in 1940. The basis of his theory is represented by the sender and the receiver. As they stated, the message flows from the sender to the receiver through the channel chosen for this communication process. This theory focuses particularly on the study and measurement of information, in addition to evaluating the communication systems that exist to optimally transmit this information data.

Why do we need information theory in cyber security?

Information theory is mainly used for the following:

• It allows studying outstanding aspects in the information process. For example, communication channels or understanding of transmitted data.

• It also tries to recognize elements that may distort or prevent the message from reaching the recipient effectively. It should be noted that it is important for the recipient to be able to digest the content coming from the sender.

• It also analyzes the encoding and decoding of messages and the speed at which they are transmitted.

• Its main goal is to determine the most economical, simple and effective way to convey a message without changing it during the process [5].

5. Combinatorics: The study of concepts such as permutations and combinations used in cryptography to create cryptographic protocols and encryption systems.

Combinatorics is the science of counting things like permutations and combinations, finite geometries and configurations, and graph theory. Combinatorics can be considered a part of discrete mathematics, but in an introductory discrete mathematics course there is only time for the basic concepts [4,pages 5-15].

6. Discrete Mathematics: The study of discrete structures such as graphs and sequences used in cryptography to create cryptographic protocols and encryption systems.

Discrete mathematics is a branch of mathematics that deals with separable and distinct numbers. Combinations, graph theory, and logical statements are included, and numbers can be finite or infinite. While there are no hard and fast definitions of discrete mathematics, it's well known for the things it excludes, such as continuously varying quantities and all things related to them. Discrete mathematics is typically associated with computer science and vital to digital devices. Professionals use it to develop programs. Discrete mathematics is used when all the elements under consideration are separated from each other. This includes all finite math, which is a lot of math, as well as the study of integers. Discrete mathematics does not consider anything to do with continuity,

and it leaves out a lot of geometry and mathematical analysis. Boolean and predicate logic can be considered part of discrete mathematics because there are only two values: true and false. However, there is much more to logic, and it makes sense to see much of mathematical logic as going beyond discrete mathematics. Finite sets are discrete, so their study belongs to discrete mathematics, but again, advanced set theory should be considered a separate subject with connections to mathematical logic.

Conclusion

So, after studying various sections of mathematics that help to encrypt data, avoid threats and generally protect confidential information from intruders, we can conclude that mathematics is important in the field of cyber security.

REFERENCES

1. Shevchenko, S., Zhdanova, Y., Spasiteleva, S., Negodenko, O., Mazur, N., & Kravchuk, K. (2019). MATHEMATICAL METHODS IN CYBER SECURITY: FRACTALS AND THEIR APPLICATIONS IN INFORMATION AND CYBER SECURITY. Cybersecurity: Education, Science, Technique, (5), 31–39. URL: https://doi.org/10.28925/2663-4023.2019.5.3139

2.Панасенко С.П., Захист інформації в комп'ютерних мережах // Журнал«Світ ПК»2002 року No2.

. 3.Ковальчук М. В Методи сучасної криптографії URL: https://kovalchukmm14.wordpress.com/2014/12/16/rsa-%D0%B0%D0%BB%D0%B3%D0%BE%D1%80%D0%B8%D1%82%D0%BC/

4. C. McMullen. (2011). Probability Theory , Course Notes — Harvard University — 2011 and Rading, pages 55-60.

5.Dr.Bill Young Department of Computer Sciences,University of Texas at Austin (2020).Information Theory and Rading, pages 18-22.URL: https://www.cs.utexas.edu/~byoung/cs361/slides4-info-theory.pdf

6. Discrete Mathematics Tutorial URL: https://www.geeksforgeeks.org/discrete-mathematics-tutorial/

Магас Людмила Миколаївна–викладач англійської мови, кафедра іноземних мов, Вінницький національний технічний університет, м. Вінниця.

Козюк Юлія Юріївна– студент групи УБ-21б, Факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, м. Вінниця.

Liudmyla Mykolaivna Magas – Lecturer of English, FL department of Vinnytsia National Technical University, Vinnytsia.

Koziuk Yulia Yuriivna – student of UB-21b group, Faculty of Management and Information Security, Vinnytsia National Technical University, Vinnytsia.