ACADEMIA ONE
PEER REVIEWED JOURNALS

Diversity Research: Journal of Analysis and Trends
Volume 2, Issue 05, May 2024
ISSN (E): 2810-6393
Website: https://academiaone.org/index.php/2

Cryptography In Mathematics

Eshniyozov A. I.
Doctor of Philosophy (PhD),physical and mathematical sciences
Gulistan State University, Gulistan, Uzbekistan

Murodova N. O.
Independent searcher
Gulistan State University, Gulistan, Uzbekistan

Abstract: The article discusses the main methods of cryptography and reveals their content. The work contains a step-by-step development of cryptography over the centuries. Attention is also paid to the relevance of this science in modern times.
Keywords: cryptography, cryptographic methods, shorthand, encoding, compression, encryption.

INTRODUCTION

Cryptography is the science of mathematical methods of ensuring confidentiality, i.e. the impossibility of reading information by outsiders. With the widespread use of writing, cryptography began to emerge as an independent science. The first cryptosystems are found already in sources dating back to BC. Cryptographic systems were rapidly developed during the First and Second World Wars. From the post-war period to the present day, the advent of computing accelerated the development and improvement of cryptographic methods.

HISTORY OF ORIGINS

The history of cryptography is the same age as the history of human language. Moreover, originally, writing itself was a kind of cryptographic system, because in ancient societies it was possessed only by a select few. It is believed that the foundations of cryptography were laid by Aeneas Tacticus. Attempts to encrypt data were made in ancient India and Mesopotamia. But they were not very successful. The first reliable security system was developed in ancient China. Cryptography became widespread in the countries of Antiquity. Then it was used for military purposes. Methods of cryptography found their application in the Middle Ages, but they were already adopted by merchants and diplomats. The golden age of this science is called the Renaissance. Then the binary method of encryption was proposed, similar to which is used in computer technology today. During the First World War, it was recognized as a full-fledged combat tool. It was worth only to unravel the messages of the enemy - and you could get a stunning result.

The art of encryption and secret transmission of information was inherent in almost all states. Cryptography in the past was used primarily for military purposes. However, now, as the information society is being formed, cryptography is becoming one of the main tools to ensure confidentiality, trust, authorization, and corporate security.

ACADEMIA ONE
PEER REVIEWED JOURNALS
Diversity Research: Journal of Analysis and Trends
Volume 2, Issue 05, May 2024
ISSN (E): 2810-6393
Website: https://academiaone.org/index.php/2

The history of cryptography can be divided into several periods:

- The first period (approximately from the 3rd millennium BC) is characterized by the dominance of monoalphabetic ciphers (the basic principle is the replacement of the alphabet of the source text with another alphabet through the replacement of letters with other letters or symbols).

- The second period (chronological framework - from the IX century in the Middle East and from the XV century in Europe to the beginning of the XX century) was marked by the introduction of polyalphabetic ciphers.

- The third period (from the beginning to the middle of the XX century) is characterized by the introduction of electro-mechanical devices in the work of ciphers, while the use of polyalphabetic ciphers continued.

- The fourth period - from the middle to the 70s of the XX century - the period of transition to mathematical cryptography.

- The modern period of cryptography development (from the late 1970s to the present) is characterized by the emergence and development of a new direction - public-key cryptography. Its emergence is marked not only by new technical possibilities, but also by a relatively wide spread of cryptography for use by private individuals (in previous eras, the use of cryptography was the exclusive prerogative of the state).

TYPES OF ENCRYPTION

First a bit of terminology to get a handle on the basic concepts in cryptography.

Cipher - some system of transforming text with a secret to ensure the secrecy of the information to be transmitted.

Public text - a message to be transmitted to the addressee.

Ciphertext - a message transformed using a cipher.

Encryption - the process of transforming the plaintext.

Key - a parameter defining the rule and method of encryption.

All the variety of existing cryptographic methods can be reduced to the following classes of transformations.

Mono- and multi-alphabet substitution or replacement - the simplest type of transformation, which consists in replacing the characters of the source text with others (of the same alphabet) according to a more or less complex rule. To ensure high cryptostability requires the use of large keys.

Permutations are also an uncomplicated method of cryptographic transformation. It is used, as a rule, in combination with other methods.

Gamification - this method involves superimposing some pseudo-random sequence generated from a key on the source text.

Block ciphers are a sequence (with possible repetition and alternation) of basic transformation methods applied to a block (part) of the ciphertext. In practice, block ciphers are more common than "pure" transformations of one or another class due to their higher cryptographic strength. The Russian and American encryption standards are based on this class of ciphers.

Understanding of the mathematical nature of the problems solved by cryptography

ACADEMIA ONE
PEER REVIEWED JOURNALS
Diversity Research: Journal of Analysis and Trends
Volume 2, Issue 05, May 2024
ISSN (E): 2810-6393
Website: https://academiaone.org/index.php/2

came only in the middle of the XX century - after the works of the outstanding American scientist K. Shannon. In cryptography, all sorts of devices have always been used, both to facilitate the encoding of messages and to increase the strength of the cipher. One of the most famous devices are rotor machines. The most famous rotary device is the Enigma (Enigma). Enigma was used by the Germans in World War II. The idea itself came from Arthur Scherbius and Arvid Gerhard Damm in Europe. Many different types of ciphers are now known. Here are examples of some of them.

CAESAR'S CIPHER

The essence of this cipher is to replace one letter with another letter that is a constant number of positions to the left or right of it in the alphabet. Gaius Julius Caesar used this method of encryption when corresponding with his generals to protect military communications. This cipher is fairly easy to break, so it is rarely used.

CARDANO GRILLE

An encoding and decoding tool, which is a special rectangular (in a particular case, square) table-card with part of its cells cut out. The grid has no rigid pattern, it is made of a sheet of cardboard or parchment, or of thin metal. To mark the lines of writing, the paper is ruled, and between these lines rectangular areas are cut out at intervals of arbitrary length. The coder places the grid on a sheet of paper and writes a message in the rectangular holes, in which a single character, syllable or whole word is placed. The original message appears to be divided into a large number of small fragments. The grid is then removed and the empty spaces on the paper are filled with extraneous text so that the hidden text becomes part of another text. Such filling requires a certain literary talent. The recipient of the message must have the same grid to decipher it.

DIGITAL (NUMERIC) CODING

Coding with numbers. It probably appeared together with the first alphabet. For example, since each letter knows its place, it has a number, which means that a letter can be replaced by numbers: a - I, k - 12, o - 16, etc. In order to use the numeric code you need to learn the alphabet, but this is just very useful, especially for a future translator, scientist and in any profession related to information.

MORSE CODE

Morse code is a method of sign coding, representing letters of the alphabet, digits, punctuation marks and other symbols by a sequence of signals: long (dash) and short (dot). The duration of one dot is taken as a unit of time. The duration of a dash is equal to three dots. Pause between elements of one character - one point, between characters in a word - 3 points, between words - 7 points. Named in honor of the American inventor and artist Samuel Morse.

BRAILLE

A relief-dot tactile font, or "night font", designed for writing and reading by blind and visually impaired people. The font is actively used by visually impaired and blind people. Braille uses six dots to represent letters. The dots are arranged in two columns. When writing, the dots are pierced, and since you can only read the convex dots, you have to "write" the text from the back of the sheet. The text is written from right to left, then the page is turned and the text is read from left to right. For the reader, the dots are numbered column by column from left to right and row by row from top to bottom. For the writer on the turned page, the

ACADEMIA ONE
PEER REVIEWED JOURNALS
Diversity Research: Journal of Analysis and Trends
Volume 2, Issue 05, May 2024
ISSN (E): 2810-6393
Website: https://academiaone.org/index.php/2

numbering is different: point 1 is in the upper right corner, below it is point 2, and in the lower left corner is point 6.

THE SCITALA CIPHER

This cipher has been known since the war of Sparta against Athens in the 5th century BC. To realize it, a scitala, a rod shaped like a cylinder, was used. A narrow papyrus ribbon (without gaps and overlaps) was coiled on the scitala, and then an open text was written on this ribbon along the axis of the scitala. The tape was unwound and it turned out (for the uninitiated) that some letters were written on the tape in disorder (each of the letters across the tape). The tape was then sent to the addressee. The addressee would take the same scitala, wind the tape in the same way and read the message along the axis of the scitala.

MATRIX METHOD

In order to use the encryption method with the help of matrices, it is enough to be able to count at the 6th grade level, know the order of letters in the alphabet and remember only 8 numbers.

Specialists can decipher it only with the help of a computer. A matrix is a rectangular table made of elements of arbitrary nature. The elements of the matrix are arranged in rows and columns. A matrix that has the same number of rows and columns is called a square matrix.

CRYPTOGRAPHY IN OTHER SCIENCES.

Coding or encryption of information is used not only in mathematics or computer science, but also in other sciences. In geography, encryption is used as coordinates of the location of an object, in biology all information about a person is encrypted in the genetic code, beautiful music is encrypted in notes, artists hide information in their irresistible paintings. Some information about the properties of ciphers and their application can also be found in fiction, especially in adventure, detective and military literature. A good detailed explanation of the features of one of the simplest ciphers, the substitution cipher, and the methods of opening it, is contained in well-known works: "The Golden Beetle" by E. Poe and "The Dancing Men" by A. Conan Doyle, J. Verne's "Journey to the Center of the Earth", V. Kaverin's "Wish Fulfillment", A. S. Pushkin's "Eugene Onegin". For example, in J. Verne's novel "Journey to the Center of the Earth" in the hands of Professor Lidenbrock gets a parchment with a manuscript of signs of runic writing. Each set a consists of one element. The element of each set is chosen from a set of symbols. In A. Conan Doyle's story "The Dancing Men" each symbol depicts a dancing man in a variety of poses. In J. Verne's novel "Journey to the Center of the Earth" each runic sign was replaced by the corresponding letter of the German language, which facilitated the recovery of the open message.

CRYPTOGRAPHY IN MATHEMATICS

The methods and results of various branches of mathematics (in particular, algebra, combinatorics, number theory, algorithm theory, probability theory and mathematical statistics) are used both in the design of ciphers and in their research, in particular, in the search for methods to break ciphers. Cryptography is a rich source of difficult mathematical problems, and mathematics is one of the foundations of cryptography. History shows that sooner or later the development of mathematical methods and techniques leads to the fact that problems that seemed insoluble find a solution. Lagging behind in the creative competition between mathematicians of different countries can lead to defeats in economics, diplomacy and military

ACADEMIA ONE
PEER REVIEWED JOURNALS
Diversity Research: Journal of Analysis and Trends
Volume 2, Issue 05, May 2024
ISSN (E): 2810-6393
Website: https://academiaone.org/index.php/2

operations.

Although the methods of cryptography and cryptanalysis themselves were not closely related to mathematics until recently, many famous mathematicians have been involved in deciphering important messages throughout time. And often it was they who achieved notable success, because mathematicians in their work constantly deal with diverse and complex tasks, and each cipher is a serious logical problem. Gradually, the role of mathematical methods in cryptography began to increase, and over the last century they have significantly changed this ancient science.

Understanding of the mathematical nature of cryptography began with the works of the same K. Shannon. His work "Mathematical Theory of Cryptography" in a secret version appeared in 1945. It was declassified and published in the USA in 1949. In 1963, on the initiative of A. N. Kolmogorov, a collection of K. Shannon's works was published in Russian. Cryptographic methods and means of information protection, as well as their mathematical foundations are fundamental studies that link together the fields of mathematics, computer science and physics.

One of the sections of mathematics that is used in cryptography is combinatorics. It deals with all sorts of sets that can be formed from the elements of some finite set. Some elements of combinatorics were known in India as early as the 2nd century B.C. Indians were able to calculate numbers, which are now called "combinations". In the 12th century Baskara calculated some kinds of combinations and permutations. As a scientific discipline combinatorics was formed in the XVII century. The term "combinatorics" was used after Leibniz published in 1665 the work "Discourse on Combinatorial Art", which for the first time gave a scientific justification of the theory of combinations and permutations. The study of placements was first dealt with by J. Bernoulli in the second part of his book "Ars conjectandi" ("The Art of Prediction") in 1713. The modern symbolism of combinations was proposed by various authors of study guides only in the 19th century.

For cryptography such combinatorial algorithms as the multiplication rule, sampling and permutation are important. These algorithms are the basis for forming secret keys for symmetric ciphers.

Cryptosystems are divided into symmetric and public key (asymmetric) cryptosystems. Symmetric cryptosystems use the same key for both encryption and decryption. Public key systems use two keys, a public key and a private key, which are mathematically related to each other. Information is encrypted using the public key, which is available to everyone, and decrypted using the private key, which is known only to the recipient of the message.

CONCLUSION.

Summarizing our research the following results were obtained:
- knowledge of scientific sources on the history of cryptography was systematized;
- mathematical foundations of symmetric cryptography were analyzed;
- knowledge about the existing methods of data protection and the advantages of cryptographic protection of information was expanded.

REFERENCES

https://www.wikipedia.org/
https://habr.com/ru/all/