Journal of Computer Virology and Hacking Techniques (2024) 20:277–293
https://doi.org/10.1007/s11416-023-00481-2

ORIGINAL PAPER

Historical notes on Russian cryptography

Anna Epishkina[1,2] · **Sergey Zapechnikov**[1] · **Anna Belozubova**[1]

Received: 3 October 2022 / Accepted: 27 April 2023 / Published online: 15 May 2023

Abstract
The article is devoted to the main milestones in the development of encryption techniques and mathematical methods of cryptography in Russia from the period of ancient Russia up to the nowadays. We break down the history of Russian cryptography into several periods and highlight the periods of cryptography development, analyze the most notable achievements and summarize the main results and applications of each period. The review of scientific research and standardization of cryptography in modern Russia is given. The progress of related areas is briefly analyzed: steganography and protection against falsification of documents.

Keywords Information security · Cryptography · Cipher · Encryption machine · Encryption · Decryption · Cryptographic algorithm

1 Introduction

The history of Russian cryptography is an important part of the history of world cryptography. It covers a long time period from the XII century. Since the ancient period, it is rich of bright ideas, its applications are quite wide in the realm of state documents, religious writings and private letters of highly educated people. Starting from the since the 18th century, the history of Russian cryptography includes a lot of science, which, albeit with some time lag, is increasingly being used to protect information. In the XX century, Russian cryptography, like everywhere else in the world, is becoming a strict scientific discipline. Extensive research is being conducted, state standards are emerging, and cryptography is widely used in computer information systems.

There are a number of books and articles devoted to the history of Russian cryptography, such as [1–7]. However, almost all of them either cover a limited time interval, or with great attention consider only one aspect of cryptography and pay much less attention to other issues. Besides, almost all of these works are in Russian. Of particular note is such an extensive work as a book [8].

✉ Anna Epishkina
avepishkina@mephi.ru

[1] National Research Nuclear University MEPhI (Moscow Engineering Physics Institute), Moscow, Russia

[2] Peoples' Friendship University of Russia (RUDN University), Moscow, Russia

In this regard, the authors of this article have attempted to present their own view of the history of Russian cryptography, paying approximately equal attention to all historical periods and different aspects of practical application and scientific research in the field of cryptography. The article provides an overview of the main stages of the development of Russian cryptography, highlights the main periods of its development and the most significant achievements of each period. The article has the following structure.

Section 2 is devoted to ancient Russian cryptography (before the XVII century). Section 3 examines pre-scientific cryptography in Russia in the second half of the XVI – early XVIII centuries, up to and including Peter the Great period, shows the awareness of the need to use cryptography for sovereign affairs. Section 4 provides an overview of cryptography in the service of the state and diplomacy in the period after Peter the Great till to Catherine II. Section 5 is dedicated to Leonhard Euler, his followers in Russia and their contribution to the development of the mathematical foundations of modern cryptography. Section 6 describes the cryptographic service in Russia in the early – mid-XIX century, including the creation of the first encrypted communication network. Section 7 provides an overview of cryptography in Russia at the turn of the XIX – XX centuries, during the First World War and the 1917 year Revolution. Section 8 is devoted to Russian cryptography during the Civil War and the first Soviet years (before 1941). Section 9 briefly describes Soviet cryptography during the Second World War. Section 10 tells

about cryptography in the USSR in the period 1945 – 1991, including the creation of the first national standards. Finally, section 11 is about modern research in the field of cryptography in Russia (1991 – 2022). In conclusion, the results of the study of the history of Russian cryptography are summarized.

2 Ancient Russian secret writings

The array of written sources that make up the literary heritage of Ancient Russia is huge. It is generally recognized that ancient Russian literature belongs to the most valuable world cultural heritage. Unfortunately, it is difficult for the modern reader, accustomed to working with a different kind of literature, to imagine the volume of this array of literary texts, as well as the variety of their forms and genres. Such famous Russian scientists as academicians Vasiliy Istrin, Nikolay Gudziy, Dmitriy Likhachev and professor Mikhail Speransky devoted their lives to the study of ancient Russian literature.

The volume of ciphertexts in the general array of literary sources of Ancient Russia is negligible: sometimes they are only individual words and sentences in a large text, sometimes larger documents. But their rarity does not detract from the importance of understanding and solving problems related to cryptography.

As the analysis of the samples of the secret texts given in the [9–11] shows, the form of the ciphertexts found in various sources differs significantly [12]. Differences are observed in the following main features:

- the volume of texts: from individual words and even parts of words to multi-page documents;
- external features of documents, namely, fonts, the method of drawing symbols, the quality of the text, the safety of the material carriers of texts, the degree of legibility and the possibility of unambiguous interpretation of the text;
- configuration of the text on the medium: traditional lowercase order of writing, curly writing, ornamentation;
- the form of speech captured in the text: prose or poetic;
- the presence or absence of an illustrative series.

The content of the ciphertexts is very diverse. Basically, as the analysis shows, it includes the following:

- the names of authors, compilers, copyists of texts, sometimes their customers;
- dates of creation, rewriting of texts, as well as dates of events mentioned in the texts;
- magic formulas, spells;
- parables and hints;
- rhetorical statements or appeals of critical or ironic content to the state authorities or influential people;
- apocrypha and heretical from the point of view of the Orthodox Church texts of religious content;
- diplomatic correspondence;
- numerical data characterizing the state structure, the number of people of various professions and resources serving the state interests, including soldiers and weapons.

Let us now consider the techniques found in ancient Russian manuscripts for converting a traditional text written in Cyrillic alphabet into cryptic texts.

1. Methods based on the replacement of alphabet characters:

1.1) replacing some Cyrillic letters with other Cyrillic letters:

- "simple litorea", or "gibberish alphabet" is the replacement of some consonant letters with others, while the vowels remain unchanged;
- "wise litorea" assumes some more complex substitution rules. Substitutions of whole groups of letters are used, as well as numerical combinations: a number is assigned to each consonant letter, and then arithmetic operations are performed on the resulting sequence of numbers (for example, a certain key constant is added to all);
- "numerical cryptography", i.e. replacing some sequences of letters with others with the same summar numerical value (as is known, in ancient Russia, the letters of the Slavic alphabet with titles above them were used to record the numbers);
- "cryptography in squares", i.e. replacement by a key written in the form of a square table;

1.2) replacement of Cyrillic letters with letters of other alphabets of natural languages: Glagolitic alphabet, Greek script, Latin script, ligature with vowel letters up per line;

1.3) replacement of Cyrillic letters with other artificial symbols:

- an "intricate" or "closed" letter in specially constructed alphabets invented by scribes, monks, diplomats, the tsar or other persons interested in secret correspondence (an example is the Perm alphabet, invented by Stefan Permsky at XIV century);
- a half-word (tachygraphy), i.e. changing the shape of letters by erasing or adding extra strokes to each of the Cyrillic letters;

1.4) mixed substitution of letters, for example, replacement of Cyrillic alphabet with a combination of letters of Slavic and Greek alphabet.

The technigues listed in 1.1 are essentially substitution ciphers with the same plaintext and ciphertext alphabets, and

in 1.2 – 1.4 are substitution ciphers with ciphertext alphabets other than the plaintext alphabet.

2. Techniques based on the permutation of alphabet characters:

2.1) writing the entire text from back to front (from the last letter to the first) with the treatment of the sequence of words and sentences;

2.2) writing each word from back to front while preserving the order of words and sentences.

3. Elements of steganography:

3.1) techniques based on the introduction of redundancy into the text with the "dissolution" of the source text in excess:

- acrostic, or edge-hiding of the plain text in the initial letters of the verse lines;
- ciphertexts in the form of parables, literary and artistic works, in which plaintext books are inserted in certain, naturally located positions, and the ciphertext masks the original;

3.2) concealment of inscriptions in drawings, geometric figures and ornaments;

3.3) charades and riddles, the solution of which is the hidden plaintext.

It is worth noting that most of them were known yet in Byzantium [13]. So, they were borrowed during the Russian-Byzantine relations. However, despite their simplicity, they cannot be considered primitive, since they fully corresponded to their purpose.

The main purpose of using cryptography is to destroy the semantics of the text. How is this achieved when using the techniques listed above? Obviously, the phonetic structure of the text is completely transformed: it becomes indistinct, and most often unpronounceable. But the limits of the conversion of phonetic units of the text in all known examples pass along morphological and (or) syntactic boundaries. This allows us to draw a very significant conclusion that, although cryptographic operations are performed on the recorded text, but exactly the units of the language are transformed: phonemes, morphemes, words, sentences. This is a fundamental difference from modern cryptographic methods that are independent of the content of the processed text. At the same time, the syntactic division of Old Russian texts, especially of the pre-Moscow period, was much weaker in itself: words were written in a row, without spaces, or separated by dots in a line.

As it was noted, the transformations of language units in the vast majority of cases are quite simple. Can this circumstance also be explained on the basis of linguistic factors? It is quite possible that those who are well acquainted with the secret script "book people" could read such a secret text "from a sheet", mentally translating it into natural language, as we do quite easily after some training, reading a Russian-language text subjected to Latin transliteration. Under these conditions, cryptography became primarily a means of masking the text from the uninitiated and a way of "hiding evidence": the storage of meaningless text could no longer be considered the same guilty act as the storage, for example, of a text of divisive content.

Let us now consider the functions of secret writing from the standpoint of the history of the Russian literary language. With a certain degree of conditionality, one can hypothesize that the history of ancient Russian cryptography is a chain of attempts to create and apply a special, third, "secret" language that was intended to function in parallel with the traditional bilingualism of Ancient Russia (spoken Russian and Church Slavonic book languages), but would remain understandable and, accordingly, would serve the interests of only a select group of people who considered themselves to be "wise" or "philosophers".

In general, the functions performed in the literary language by typescript texts, as well as any texts in natural languages, can be divided into communicative and memorative. However, among these obvious broad functions, a narrower range of functions can be outlined that determine the specific features of the functioning of the cryptography. It seems that the main of these functions are as follows:

- concealment of names, dates and magic formulas for mystical reasons, as well as for reasons of shyness, fear of the author, etc.;
- creation of riddles and charades for the reader, demonstration of their high mental abilities, higher educational level compared to others, compilation of "messages to descendants", etc.;
- compilation of secret texts as a means of engaging in special types of literary creativity – compilation of parables, "weaving of words", versification;
- concealment of the content of non-canonical or heretical religious texts (in order to avoid persecution for "ideological" reasons;
- the classification of information about the state structure, the disclosure of which in the face of any social group (for example, boyars) could lead to an unstable position of the current government;
- classification of information about the terms of agreements with foreign sovereigns, about the state of affairs in Russia or in foreign countries (diplomatic secret writing).

Thus, the function of the cryptographic text described here – the expression of the implied symbol by a conventional sign, but not generally understandable, but accessible to a limited circle of people – can be compared with one of the main functions of modern cryptosystems – ensuring confidentiality.

Is it possible to identify functions in the considered forms of cryptography that are comparable to other basic functions of modern cryptosystems: ensuring integrity and authenticity? It seems that the answer should be positive, although with certain reservations.

The authenticity of the cryptographic text is ensured (of course, not with such a degree of reliability as in modern cryptosystems) by the very fact of using cryptography, which already confirms the fact that the author belongs to the group of "initiates" and that he has an "educational qualification". Thus, by the very fact of using cryptography, the authenticity of the text is ensured up to the author's belonging to a separate group. But the authenticity of the author's identity among this small group in the conditions of existence of exclusively handwritten texts, apparently, was established by the individual features of the author's handwriting known to the reader or by hidden non-linguistic features introduced into the document. Important state documents were certified with the wax seal of the tsar or senior officials. This method was also borrowed from Byzantium.

Finally, the integrity of certain types of texts could be controlled in two ways: both by means of the cryptography itself, and by means external to it, which remained unchanged in our time, for example, by page numbering. Let's focus on the possibilities of integrity control by means of cryptography. It was carried out by introducing redundancy into the text. The forms of such conversion of plaintexts into ciphertext, which introduce redundancy into the text, include acrostic and masking of plaintext in the ciphertext of new content with the letters of the original plaintext placed in it. The acrostic is especially remarkable in this respect, since versification generally refers to the oldest ways of fixing the most significant texts of historical, sacred and religious content for the people's memory. A poetic text that has rhythm, and most often rhyme, is much easier to remember than prose. Thus, the poetic form of presentation contributes to the preservation of the integrity of the text, of course, not with such a degree of reliability as modern methods, but only preserving the general meaning of the text, but perhaps allowing inaccuracies or even errors in particulars.

3 Pre-scientific cryptography in Russia in XVI – XVIII Centures

Methods of protecting written information have always been highly dependent on the means of communication. Until the end of the XV century, messages were sent mainly by a special courier – messenger. Since the beginning of the XVI century, the horse-based postal service began to spread. However, secret letters were still sent most often with special messengers.

The earliest known use of cryptography was diplomatic correspondence. The first of the international acts on the transportation of correspondence concluded between Russia and a foreign state was the agreement between Moscow and Warsaw in 1634. In 1665, an international postal service was organized between Moscow and Riga. Later, a similar agreement was signed with Sweden. Wax seals were used to confirm the integrity of these messages. However, neither the physical protection of messengers nor special seals could guarantee the secrecy of correspondence, so cryptographic methods of information protection were used more and more actively.

The first cryptography specialists in public service appeared in Russia in 1549, when the Embassy Order was formed. It carried out the overall management of the country's foreign policy. The staff of the Embassy Order consisted of persons who knew how to create ciphers. In addition to protecting mail correspondence, since the end of the XVI century, Russian ambassadors abroad have been receiving ciphers in the form of replacement tables or memorizing them.

With the beginning of the reign of the Romanovs' dynasty in 1613, when Patriarch Filaret concentrated the supreme secular and spiritual power in his hands for a time, he personally managed foreign affairs and developed secret alphabets. At that time, the ciphers used were of the simplest kind: these are ciphers of simple substitution and permutation. During the reign of Tsar Alexei Mikhailovich from 1629 to 1676, ciphers became even more widespread. Even the tsar himself uses ciphers in his private correspondence. Diplomatic secrecy is also developing. During this period, all ambassadors in foreign countries were necessarily provided with ciphers for correspondence with the Embassy order.

However, the first of the Russian sovereigns who very clearly realized the importance of encryption and the development of encryption for the state security was Peter the Great. At the very beginning of the XVIII century, Peter the Great established a Field Embassy office, in which all political correspondence was concentrated. The need to create it was caused by Peter's frequent trips. The Field Embassy office was engaged in processing the correspondence of the emperor. From here came his most important order for all branches of management. Cases from all departments flocked here to his decision. However, the main function of the Field Embassy office was to conduct diplomatic affairs. By 1757, the permanent Embassy office was established in St. Petersburg and turned from a temporary institution into a long-term one. All work on processing encrypted correspondence of Peter the Great and his associates with various correspondents, as well as the creation of ciphers and recommendations for their use, is concentrated here.

In the conditions of Peter the Great's intense activity related to reforms and wars, it was necessary to establish permanent Russian diplomatic missions abroad, as well as reciprocal Western European embassies in Russia. It is known that already in 1701 Russia had 6 permanent diplomatic missions in Europe, and subsequently their number only increased. They were the first correspondents of the encrypted communication network created in Russia. All of them necessarily had ciphers for correspondence with the Tsar and the Embassy Office.

It should be noted that already at that time all organizational procedures for handling ciphers were worked out at a high level. In particular, the ciphers were sent to the Board of Foreign Affairs in envelopes sealed with state sealing wax seals or personal seals of the compilers. The transfer of ciphers was performed quite often, since their validity period was limited. New ciphers were prepared and sent to the addressees in advance. Even short-term diplomatic missions were accompanied by the delivery of a cipher to a person who was sent from Russia abroad.

The encrypted diplomatic correspondence of the early 18th century provides rich material for study. Russian encrypted alphabets and keys created in 1700-1723 are mainly substitution ciphers. It is known that the texts to be encrypted were written in Russian, French, German and Greek. Separate letters, words and standard phrases were used as plaintext units during encryption. As a rule, Cyrillic, Latin, Glagolitic letters, numbers, as well as specially designed symbols, combinations of two, three letters or alphanumeric combinations were used as ciphertext alphabets. Often, dummy characters are introduced into ciphertexts, that is, such ciphertext characters that do not correspond to any plaintext character. Sometimes dummy characters were put in place of punctuation marks in the plaintext. These dummies broke the linguistic connections of the plaintext, to some extent changed statistical patterns, changed the length of the transmitted message, which greatly hindered the manual decryption of such ciphers. In general, the combination of techniques used in ciphers made them quite resistant for their time. It is known that the first Russian cipher was decrypted by the British only in 1725.

In addition to diplomatic applications, ciphers were used for other purposes. Thus, it is known about the use of ciphers by highly educated persons of that time in private correspondence. The cipher, created by the famous poet and diplomat Dmitry Kantemir, has been preserved. The highest command staff of the Russian army and navy also had ciphers for correspondence with the tsar. Ciphers were also given to persons who received special one-time orders from the tsar. In particular, the encrypted correspondence of Peter the Great and Field Marshal A.D. Menshikov has been preserved in the archives. Encrypted military correspondence was also accompanied by a conditional alarm, which was supposed to confirm the fact of receiving and reading the message. In particular, it is known that this was done before the Battle of Poltava.

4 Cryptography serving the state and diplomacy

The development of cipher systems in the XVIII century is closely related to practical tasks. The main area of application of ciphers remains diplomacy. With the beginning of the reign of Catherine I, Count Andrei Ivanovich Osterman became the Vice-chancellor of Russia and the head of its cryptographic service. In 1720, the Board of Foreign Affairs was formed under the leadership of A.I. Osterman. The Board of Foreign Affairs continues its activities in accordance with established traditions. At the same time, the search for new types of ciphers is underway.

During the XVIII century, at least three types of ciphers were used in Russia. The first type is the ciphers of old samples, in which there is an alphabet, and the ciphertext is represented only by numbers, letters or specially designed symbols.

The second type has been used since the 1730s. It is characterized by the use of a non-alphabetic encoding method along with alphabetic. In these ciphers, dictionary values were placed in several sections: alphabet, syllables, supplement, abacus, months. The alphabet in these ciphers could be Russian or Latin. Syllables are constant and characteristic of each language. Therefore, these cipher sections were the same for each language. The other sections could be different. The supplement is a dictionary that included the names of kings, statesmen and geographical names, as well as some commonly used words. The abacus section was intended for encrypting numeric values. The months were listed in a special section. With rare exceptions, the ciphertext was represented by arabic numerals. Ciphers have a large number of dummies introduced in order to complicate them. Already during this period, the compilers of ciphers knew that the frequency of use of vowel letters in the language is higher than consonants. Therefore, in the new ciphers, vowel letters necessarily correspond to several possible designations, while consonants have one or two designations. The introduction of many dummies testifies to the understanding by the compilers of ciphers of the influence that the frequency of the use of the same letters has on the disclosure of the ciphertext.

The third type of ciphers has been used since the late 1740s – early 1750s. It remains predominant until the end of the XVIII century. Dictionaries of these ciphers have a volume from 400 to 1200 values and include letters, syllables, the most commonly used vocabulary in correspondence, geographical names, names, months and numbers. The ciphertext consists almost exclusively of digits. Vowels

necessarily correspond to several symbols in the ciphertext. The number of dummies in ciphers becomes even larger and is measured in thousands. In addition, various other "tricks" are used, which are described in detailed and voluminous rules. For example, special signs are introduced that separate false sections of the ciphertext from the useful ciphertext. Such sections should not be taken into account when decrypting.

Another area of application of cryptography was related to intelligence activities, namely, the extraction of information from secret correspondence of foreign states. For this purpose, a perlustration service was established in the 1740s. The leading role in the creation of this service belongs to A.P. Bestuzhev-Ryumin, appointed in 1742 as the chief director of the post office. The so-called "black cabinets" are being established10 This is a service in which foreign diplomatic correspondence was secretly opened, copied and decrypted. The work of perlustration was very difficult. Envelopes should be opened carefully, if possible, without violating their integrity. Diplomatic letters were usually placed in an envelope, which was stitched with thread and sealed. The message packed in this way could be enclosed in another envelope, also stitched and sealed. The letters were opened and sealed personally by the director of the "black cabinet". They were copied by a special secretary, translated by a special translator. Since the letters had to be given their original appearance, that is, sealed, stitched with thread and sealed with exactly the same seals as they were sealed before opening, the skill of the person who made the seals was of great importance. The master of seal carving was also kept on the staff of the "black cabinet". The results of this work were regularly reported to A.P. Bestuzhev-Ryumin, and, if necessary, to Empress Elizabeth Petrovna. Copies of letters of foreign diplomats taken in "black cabinets" have been presented to Elizabeth Petrovna. All of them are sewn into thick folders and provided with translation, some of them have notes indicating that the Empress has familiarized herself with the contents of these letters. Elizaveta Petrovna closely followed the perlustration of documents and delved into details, trying to protect the state interests as much as possible. The very fact of perlustration was kept in the deepest secret. It should be noted, however, that the first perlustration services appeared in European countries about 200 years earlier than in Russia.

At first, when perlustrating letters, their encrypted parts were simply skipped and not even copied. However, it is gradually being discovered that the most important and interesting information is usually contained in the encrypted parts of the letters. This circumstance caused the need to create a service for decrypting foreign ciphers.

The first stages of the activity of this service were associated with the famous mathematician Christian Goldbach. Christian Goldbach worked closely with Leonhard Euler from 1729 until the end of his life and conducted regular correspondence with him. Goldbach did not achieve success in his activities immediately, but only a year after the start of his activity.

The first letter decrypted by Russian cryptographers was shown to Empress Elizabeth Petrovna on June 16, 1744. Since the main suppliers of encrypted correspondence for the decryption service were "black cabinets", and copying ciphertexts for accurate decryption had to be done very carefully and error-free, this work was entrusted to mathematicians. During his work, Goldbach developed a system of techniques and methods that allowed him to succeed and decipher letters for an average of two weeks. Empress Elizabeth Petrovna began to actively use the information received to conduct foreign and domestic policy. Success in decrypting foreign ciphers has revealed to the Empress of Russia the possibility of obtaining additional knowledge that has long been a completely different content of political activity. In particular, it is known that the decryption of the correspondence of the French ambassador to Russia marquis de la Chétardie even led to a diplomatic scandal in 1744. The ambassador was expelled from Russia, which led to a temporary cooling of relations between Russia and France. In addition to Christian Goldbach, Franz Ulrich Aepinus, as well as Yerofey and Fyodor Korzhavins made a great contribution to the decryption activity.

Under Empress Catherine II, the Russian network of diplomatic encrypted correspondence is developing. In 1779, she approved the staff of the foreign institutions of the Board of Foreign Affairs. Russian representatives abroad had the rank of ambassadors or ministers of the second rank. All correspondence of these persons was encrypted and kept strictly secret. The same cipher could be used for correspondence of the Board not with one, but with several diplomatic representatives. Such ciphers were called general. A significant number of general ciphers are known from archive documents for different languages: Russian, French, German, Italian and others. On average, they were used for two years, after which, as a rule, they were replaced. Different ciphers were used in different regions.

Much attention in the Board of Foreign Affairs was paid to the secrecy regime. The Board kept a careful record of all ciphers. A list of ciphers, lists of persons to whom they were sent, lists of incoming and outgoing encrypted correspondence in different languages and other necessary information were entered into special ledgers. If a copy of the general cipher was lost by one of the correspondents or compromised, an imperial decree was immediately issued to remove this cipher from use and replace it with another. This decree was sent out to all the correspondents who were part of the communication network. Count Nikita Ivanovich Panin played a major role in the creation of the general ciphers. He put the creation of new ciphers on stream. On average, it took about two weeks to develop a new cipher in that time. To conduct

encrypted correspondence, all major political and military figures in Russia had a special staff of clerical workers. The encryption and decryption of the message texts was carried out by special secretaries-translators, each of whom spoke two or three foreign languages. As an additional measure of protection, a letter in invisible ink was sometimes used between the lines of another, masking text. The appearance of a text written in such invisible ink immediately indicated that the letter had been read by outsiders.

5 Leonhard Euler and the development of the mathematical foundations of modern cryptography

One of the brightest pages in the history of Russian and world mathematical science is associated with the name of Leonhard Euler (1707 – 1783). Most of his life he lived and worked in Russia (1727 – 1741, 1766 – 1783). In 1731, Euler received the vacant position of professor of physics at the St. Petersburg Academy. He works a lot and hard, doing both important government tasks and a number of initiative studies, gives lectures, makes reports at academic conferences. His authority among Russian and European scientists was indisputable. The most important feature of Euler's works and at the same time their most important contribution to science is that all his activities were aimed not just at establishing single scientific facts, but at building a system of new scientific knowledge with a core in the form of a system of mathematical tools.

A versatile scientist who worked in a variety of fields of knowledge: fundamental and applied mathematics, mechanics, hydrodynamics, optics and many others – he made a particularly great contribution to the development of number theory. Number theory has become the foundation of modern cryptography and cryptanalysis. A lot of methods of number theory are now classical tools for designing and analyzing cryptographic security mechanisms.

Leonhard Euler is one of those people without whom there would be no cryptology in its modern form [14]. The first thing a researcher pays attention to when trying to evaluate L. Euler's contribution to science is the exceptionally high quality of his scientific results.

Almost all of L. Euler's results, belonging to those areas of mathematics that form the mathematical foundations of modern cryptology, are concentrated around number theory. We will list only his most significant achievements in this field. Euler is the founder of analytical number theory, he proved and generalized Fermat's small theorem, first hypothesized the validity of the quadratic reciprocity law, introduced a number of arithmetic functions, including the famous zeta function (although today it is known as the Riemann zeta function), introduced the concept of a primitive root, proved numerous theorems, lemmas, statements, derived formulas that named after L. Euler. In total, more than 120 works of Euler are devoted to the theory of numbers. P.L. Chebyshev wrote: "Euler was the beginning of all the research that makes up the general theory of numbers." Euler's number-theoretic works have been considered in detail by historians of mathematics, so we will focus only on those works that later came in handy in cryptography. Euler continued the number-theoretic research of Christian Goldbach, who served as a cryptographer at the Ministry of Foreign Affairs in Moscow.

The most importany Euler's contribution to number theory is twofold.

1. Testing numbers for primality. Primality tests are widely used in generating parameters of asymmetric cryptosystems, and the results obtained by Euler are extremely important for constructing algorithms for testing numbers for primality.

2. Computationally infeasible problems of number theory. The most important areas of Euler's work: the study of the properties of quadratic residues, the theory of primitive roots – turned out to be closely related to three computationally complex problems of number theory, which are now the basis of the most commonly used asymmetric cryptosystems, namely, the RSA problem, the problem of quadratic residues and the problem of discrete logarithm. The results formulated by Euler are the theoretical platform that makes possible the practical use of computationally infeasible problems and one-way functions based on them in cryptography.

The considered examples are quite sufficient to conclude that the results obtained by L. Euler are of fundamental importance for modern cryptological science. With all this, history has disposed in such a way that the most important results, which seemed to many during Euler's lifetime to be a kind of "numbers game", became in demand by science and, moreover, formed the mathematical basis of asymmetric cryptography two hundred years after the death of L. Euler.

It should be noted that despite Leonard Euler's close acquaintance with Christian Goldbach, there is no historical evidence that Leonard Euler was aware of Goldbach's activities in the field of decryption and encryption techniques in general.

The significance of Euler's research in the field of number theory lies in the fact that, although they were of almost exclusively theoretical interest in his time, they laid the foundation for knowledge that three hundred years later became crucial for cryptography and other areas of applied mathematics. The Euler's investigations were later continued by his followers Nikolay Fuss, Mikhail Golovin, Anders Lexell and others.

6 Cryptographic service in Russia up to the middle of the XIX century

The beginning of the XIX century was marked by turbulent political and military events. First of all, these are the wars in Europe and Russia's war with Napoleon's army in 1812. At the beginning of the XIX century, as a response to the turbulent military and political events in Russia, the reorganization of the supreme state administration was carried out, which throughout the XVIII century maintained collegial principles. The manifesto of Emperor Alexander the First in 1802 established ministries instead of colleges. The Ministry of Foreign Affairs has become one of the most important Russian ministries.

Due to the aggravation of the military-political situation at the beginning of the XIX century, a reform of the cryptographic service was required. Three secret departments were formed (the so–called expeditions) as part of the Office of the Ministry of Foreign Affairs: encryption, decryption and perlustration service. The first expedition included also lithography.

In addition, at the beginning of the XIX century, the so-called digital committee was organized in the Ministry of Foreign Affairs, which included the most experienced and qualified cryptographers. The tasks of the committee included the analysis and introduction of new encryption systems, monitoring their correct use and storage of keys, decommissioning outdated or compromised ciphers, compiling reports and reports for the heads of the Ministry of Foreign Affairs and the Emperor on encryption and decryption. The information obtained by decrypting the correspondence continued to serve as the most important source of information for the Ministry of Foreign Affairs and the Military Department of Russia. Russian decryptionists played a significant role in the defeat of Napoleon's army, which was invincible until then. This is evidenced by the fact that Alexander the First, in his memoirs of the war of 1812, personally quoted the correspondence of Napoleon's generals, which is sometimes decoded by the Russian cryptographic service. As in the eighteenth century, encrypted correspondence in the XIX century was conducted on political, military, economic and other important state issues. First of all, the correspondence was with Russian diplomatic missions abroad. There were 21 such representative offices at the beginning of the XIX century. By 1825, there were 24 of them. They were mainly located in European countries, but some of them were in the Middle East and Asia.

In addition to protecting international correspondence with Russian embassies abroad, domestic political correspondence between the Asian Committee of the Ministry of Foreign Affairs and the eastern regions of Russia was also protected. This was due to the great dangers of intercepting correspondence on the long distances and long time of its delivery.

The constant increase in the number of correspondents of the encrypted communication network and the growth in the volume of encrypted correspondence have led to the urgent need to find a new way to quickly reproduce encryption documents. This method was found. This event was associated with the name of the outstanding scientist and inventor Baron P.L. Schilling von Kunstadt. The main merits of Baron Schilling were as follows.

Firstly, under his leadership, the technology of reproduction of documents and drawings using lithography was mastered. It was used, among other things, to copy both encryption tables and documents and letters decrypted by cryptanalysts.

Secondly, Schilling was one of the first to put into practice the electromagnetic telegraph apparatus in Russia, which was soon introduced in the Ministry of Foreign Affairs, and this made it possible to speed up the transmission of messages over long distances many times.

Thirdly, Schilling became the inventor of bigram type ciphers. The dictionary of the bigram cipher consisted of two-digit combinations of letters of the Latin alphabet. Thus, the set of bigrams was about a thousand units. The code designations for them were two-, three- and four-digit numbers. Externally, such a cipher was a dismountable table, with instructions for using the cipher. The peculiarity of the cipher was that it was not consecutive plaintext bigrams that were encrypted, but letters located on adjacent lines. To do this, the text was written letter by letter in a special table called a transparency. They took the first letter vertically from the top row, the second from the next row below it. The probabilistic characteristics of such simple replacement ciphers, of course, do not obey a uniform law, but for their time their decryption was of considerable complexity, although from modern positions such a cipher cannot be considered cryptographically stable at all. The correspondence was conducted mostly in French, however, similar bigram ciphers for the Russian language was later introduced into the Russian army.

Baron Schilling made a significant contribution to the development of Russian cryptography. He was patronized by both the Emperor Alexander I and the Foreign Minister Count Nesselrode.

Thus, the first half of the 19th century was marked mainly by the growth of the practical application of already known ciphers, the contribution to the progress of cryptographic science at this stage was relatively small.

7 Cryptography in Russia at the turn of the XIX–XX centuries

In the second half of the XIX century, the cryptographic service of Russia underwent a significant reorganization, as a result of which it ceased to be a privilege of the Ministry of Foreign Affairs, but was created in two more departments: the military and the Ministry of Internal Affairs, which indicates the growing importance of cryptography in the activities of state bodies and a significant expansion of its use.

The development of external and internal communication networks, the growth in the volume of encrypted correspondence led to an increase in the number of ciphers and codes being put into operation [15–17, 20]. Ciphers began to be divided primarily according to the linguistic principle. Depending on the language of the encrypted information, Russian, French, German, English and other ciphers appear. According to their branch purpose, they are divided into ciphers of the Ministry of Foreign Affairs, ciphers of the military department, including imperial ciphers, ciphers of the gendarmerie and the Police Department belonging to the Ministry of Internal Affairs. Also, some ciphers were used by civilian agencies, for example, the Ministry of Finance. Separately, it is possible to distinguish agent ciphers designed to communicate with intelligence agents and agents.

Let's consider the ciphers used in the historical period under consideration [16–18]. In the Ministry of Foreign Affairs, bigram ciphers were actively used, and in 1872 some improvement was introduced into their structure. It was proposed to significantly reduce the number of letters of the Latin alphabet and punctuation marks in the plaintext, as used in biclavic ciphers, so that Latin bigrams and letters could be used as cipher symbols. The principle of the system of these ciphers is bigram, with the only difference that two letters of the text are transmitted not by three numbers, as in bigrams, but by two letters, and when encrypting two-letter combinations are not made up of the letters of two rows of the text rewritten for this purpose according to a known transparency, but from the extreme letters of each line of the text rewritten according to the transparency, moving from two ends to the middle. The latest improvement also carried some cryptographic load. Since by that time it became clear that the enemy knew the principle of encryption on this system, it was advisable to introduce some changes to this principle, which, of course, complicated the work of the decryptors. Russian Russian bigram ciphers are the second group of bigram ciphers, according to which messages written in Russian were encrypted. These ciphers were intended for both internal and external correspondence. Since the number of bigrams in the Russian language exceeded the number of three-digit numbers, the compilers of ciphers replenished the missing number of cipher values with single-digit, two-digit and four-digit numbers.

A biclavic cipher is a multi-valued substitution cipher consisting of 26 different simple substitutions with a rather complex choice of substitution for each character of the plaintext, determined by two keys. In this case, two characters of the ciphertext correspond to separate characters of the plaintext. Thus, the length of the ciphertext does not correspond to the length of the plaintext. The cipher is based on a briefcase with 24 movable strips — the main part of the double key, two tables (encryption and decryption) — the second part of the double key and a calendar of typing and parsing. Each strip is a random set with repetitions of 20 letters of the Latin or French alphabet of 26 letters. Thus, each strip can contain 20 or less Latin letters. For convenience, they are written in groups of four letters each with omissions. Each strip has its own number, indicated by a number or letter. The encryption table is a 26x26 square, the rows of which are indicated by 23 letters of the Latin alphabet (without the letters k, w, y) and three punctuation marks (dash, comma and dot) and the columns of which are indicated by all 26 letters of the Latin alphabet. Each column of this table is filled in randomly without repetition with 26 characters, 17 letters of the Latin alphabet and nine digits from 1 to 9 were used. The encryption process is carried out as follows. The plaintext is written on a banner, each line of which contains 24 cells. The text is written in four characters with gaps in one cell. Thus, 20 characters are written in each line of the banner, the form of the record corresponds to the form of the encrypted strip. If the text does not end at the end of the line, then the word "end" and any other arbitrary characters are added. Each banner contains eigth horizontal lines, and a long message can be written on several banners. When writing the encrypted text to the banner, it was recommended to first make all possible abbreviations of the text that do not change the meaning of the message. Next, three letters and some punctuation marks were replaced with signs included in the intermediate text. After the message is recorded on the banner, encryption is performed. From 24 strips, eight strips are selected in a strictly defined order according to the daily key. The markant of this key is the date of encryption, which is placed at the beginning of the message. The first strip is substituted for the first line of the message. The text signs with the letters of the strip form vertical bigrams that define the inputs of the cipher table (the coordinates of the cipher text). The next 20 characters are encrypted using the next strip, determined by the daily key, and so on. If the encrypted text exceeds 160 characters, the encryption procedure is repeated, starting from the first strip. The decryption of the message is performed in reverse order, and it is obvious that the open message is restored unambiguously if the correspondent has the appropriate keys. From the described encryption procedure, it is clear that the cryptographic strength of this cipher is based on the filling of strips unknown to the enemy, determining the choice of the sequence of 26 substitutions, and the

daily key. Although this number is quite large, nevertheless, the cryptographic strength of this cipher system cannot in any way be based on this daily key, since it allows sequential testing of cipher strips one after another. The main weakness of this cipher is the relatively short period of this cipher, equal to 160 letters, and the absence of a one-time key. However, that in those days, as a rule, no more than one message from a particular correspondent was encrypted per day. For this reason, there was no need to introduce additional one-time keys. The messages themselves were also not long enough, so deep overlaps of the cipher were not expected here. It is no coincidence, therefore, that ciphers of this very original type have been used along with bigram ciphers for almost forty years.

Encryption codes continued to be actively used in the XIX century. They were of different types, gradually modified and improved both operationally and cryptographically. The volume of codes varied from 300 to 10,000 dictionary values. By the end of the XIX — beginning of the XX century, codes with a volume of 10,000 dictionary values or more appeared, and by 1917, codes of this volume were the most widespread. Practically from the very beginning of the use of codes, they had code values in which several dictionary values corresponded to one code designation, on the one hand, and, on the other hand, several code designations corresponded to the same dictionary value, the most commonly used one. This was the most important condition for increasing the cryptographic strength of the code, observed in Russia, as in all other advanced countries of the world. The same purpose was served by the presence of an alphanumeric syllabic table, which, in addition, indefinitely expanded the vocabulary capabilities of the code. Variants of code designations achieved relative alignment of frequencies of occurrence in cryptograms of cipher meanings, made it difficult to decrypt. The second important condition for the code is the need for dummy zeros, i.e. code designations that do not correspond to any dictionary values. Such pacifiers should have been randomly scattered throughout the text of the cryptogram. This measure of increasing the strength of the cipher had great efficiency and was successfully used in the practice of cryptography in Russia since the first quarter of the XVIII century, having migrated to codes for a certain period of time. Nevertheless, these tricks were not able to completely make the ciphertexts of messages equally probable. Sooner or later, with the accumulation of cipher material, frequently occurring code designations corresponding to the most commonly used vocabulary values are gradually revealed. This moment is the starting point for decrypting messages and has been successfully used by decryption specialists both in Russia and in other countries.

In the second half of the XIX century. in Russia, the weaknesses of the use of codes in their pure form, without complications, especially the weaknesses of alphabetic codes, were already well understood. In the instructions to the ciphers of the Ministry of Foreign Affairs and the Ministry of War of Russia, it was repeatedly recommended to use various ways to increase resistance. These methods included: timely change of keys and codes, and the use of several codes at the same time in places where there was such an opportunity, and the use of various kinds of techniques such as the use of different variants of code designations, and, finally, the use of various methods and systems of re-encryption. The parallel application of several codes required large expenditures for the compilation and publication of a large number of them and therefore did not receive wide distribution. In Russia, as in many other countries, various types of code reencryptions were used: with the help of column substitution, gamming and permutations.

8 Russian cryptography during the civil war and the first Soviet years

After the October Revolution of 1917, the fate of Russia changed dramatically. The need to organize a new system of public administration required a radical restructuring of all public services and institutions. The cryptographic service of Russia was no exception. The White armies inherited encryption and radio equipment from the Tsarist army. The cadres of experienced specialists of the cryptographic service of tsarist Russia, mostly turned out to be on the side of the whites. Due to the fact that most of the cryptographers and cryptographers of tsarist Russia went over to the side of the whites, the encryption business in the white armies was at a higher level than in the Red Army. The Ministry of Foreign Affairs of the Kolchak government included a digital department that retained its name, traditions, and the technical base of the tsarist cipher service. The Whites widely used ciphers and codes developed before the revolution, but they also created new ciphers. To encrypt messages, the White Guards used alphanumeric-syllabic ambiguous substitution tables. The validity period of such ciphers was determined in six months. As you know, their cryptographic strength is low. Such ciphers are revealed on the material of several dozen characters. In addition, the white armies used codes with a volume of several thousand dictionary values. The codes were mostly alphabetic, rarely used non-alphabetic small volume, which had a certain number of pacifiers. Even if all the rules of use are followed, such codes do not have high durability and can be disclosed on a material of sufficient volume. With the organization of regular interception, their disclosure became a relatively simple task. Decryption was also facilitated by the fact that often not the whole telegram was encrypted, but only its individual pieces, although even during the First World War this was strictly prohibited.

As agent ciphers, White used permutation ciphers, namely, slogan ciphers of vertical permutation.

The Bolshevik leaders, including V.I. Lenin, paid special attention to the organization and security of communications [17, 18]. Many of them got acquainted with cryptography during their underground work. The management insisted that the government communication functioned smoothly in all situations, was of high quality and, most importantly, ensured the secrecy of negotiations. To fulfill these requirements, the following principles were put into the basis of the organization of communication: providing communication by wire; special selection of service personnel; establishment of a strict procedure for the use of communication means; the use of ciphers and conditional signals. Since the main part of cryptographers after the revolution went over to the side of the opponents of the Soviet government, the winners were forced to use the ciphers of pre-revolutionary Russia, or previously developed underground ciphers. Both ciphers were well known to the cryptographers of tsarist Russia who worked for the whites. Now let's consider the ciphers used on the communication lines of the Soviet Republic. Ciphers of simple and proportional substitution were mainly used. For example, the Vigener cipher was used with alternating letters of the alphabet inside the square in accordance with the slogan key. The situation with the decryption of foreign and military correspondence was extremely bad. There was no organized decryption service in the Red Army, since the cipher groups created at the headquarters had the main task of creating ciphers and protecting secret correspondence with them. We can say that there was practically no decryption service. At that time, the Soviet side did not have the forces and means to successfully carry out such work. The Soviet side experienced an acute shortage of radio interceptors and their equipment, although military formations intercepted radio conversations conducted along the communication lines of front-line and divisional formations of the white armies. However, both Soviet radio intelligence and cryptanalysts achieved success.

The organization and activity of the cryptographic service of Russia in the early years of Soviet period is of considerable interest to specialists in various fields both from the point of view of studying the formation of the special service of the Soviet state at the initial stage, and from the point of view of generalizing historical experience in its various aspects. It was at this time that the origin of scientific methods of cryptographic analysis, the development of radiotelegraphic encrypted communication and radio interception belonged. During this period, a critical understanding of the state of security of domestic communication lines and the definition of the forms of the country's future encryption service began.

A Special Department was formed under the All-Russian Extraordinary Commission, whose activities included the issues of setting up encryption, in particular, the scientific development of encryption issues, the analysis of all existing and existing Russian and foreign ciphers, the creation of new cipher systems, the compilation of cipher descriptions and instructions on encryption and the use of ciphers. Special attention was also paid to the examination of all existing ciphers, the processing of instructions on encryption and the use of ciphers and the development of rules for the work of cipher agencies, the distribution of newly developed cipher systems among all departments, the organization of the training unit, the creation of a school of cryptographers.

9 Soviet cryptography during the second world war

In 1938-1939, a laboratory for classifying telegraphic and telephone information was organized under the leadership of V.A. Kotelnikov, the author of fundamental works in the field of radio engineering, the theory of noise-resistant communication, radar, radio astronomy. Under his leadership, in the 1930s, the first domestic devices for encrypting a speech signal were created. This work continued during the Great Patriotic War. In parallel with K. Shannon, V.A. Kotelnikov mathematically formalized the requirements for the strength of ciphers. Kotelnikov, for the first time in the USSR, developed the principles of constructing telegraphic secret equipment, implemented in the Moscow equipment, by superimposing cipher signs on messages. The scheme proposed by V.A. Kotelnikov for applying a cipher to an open text turned out to be very attractive, and was used for a long time in the equipment of the next generations. The encoder itself was complex, cumbersome, it was designed on electromechanical nodes. The design was based on a drum filled with balls. When the drum was rotated through a system of pins and slots, the balls randomly rolled down six vertical tubes onto two moving telegraph tapes, which were superimposed on each other through a carbon paper. As a result, the same pattern was obtained on both tapes – tracks of randomly located spots. Then the tapes were perforated according to these marks. These tapes formed a random key and were sent to the equipment installation points. The cipher was read from the key using photoelectronic elements. In 1939, V.A. Kotelnikov was entrusted with the solution of an important state task – the creation of an encoder for classifying speech signals with increased resistance to decryption. In addition to V.A. Kotelnikov, A.L. Mints, K.P. Egorov, V.K. Vitorsky took part in the work on secret telephony [17, 19, 21].

A system based on quasi-random (known only to the recipient) permutations of time segments and two-frequency bands with inversion of the speech signal was proposed. The control of frequency and time permutations on transmission and reception was carried out by an encoder that generated 5 bits of gamma 10 times per second. The development of the

encoder was of defensive importance, and was completed by the autumn of 1942. During the Great Patriotic War, developed under the leadership of V.A. Kotelnikov and tested back in 1938, the complex secret equipment C-1 Sobol was widely used in the active army. The first apparatuses were immediately sent to Stalingrad to connect the Headquarters of the Supreme High Command with the headquarters of the Transcaucasian Front, the wired connection between which was destroyed during the fighting. At that time, in the army, wired telephone lines were mainly used for communication of this level, and Sobol-P allowed communication via a radio channel. As veterans of the Great Patriotic War recalled, the use of Kotelnikov encoders during the decisive battles on the Kursk Bulge largely determined the successful outcome of the battle. They provided a speech coding system for closed-circuit radio communications, which was practically unbreakable.

In the USSR, the theoretical basis for the creation of encryption technology, radically different from foreign samples, was first proposed in 1930 by a talented engineer I.P. Volosok, who became the leading designer of many samples of Russian encryption technology of the pre-war and post-war periods. The principle he used of superimposing a random sequence of gamma characters on combinations of plaintext characters created an unreadable cryptogram with guaranteed resistance against decryption by opponents. The physical carrier of the signs of a random scale was a punched tape.

The M-100 cipher machine consisted of three main components – a keyboard with contact groups, a tape drive mechanism with a transmitter and a device mounted on a typewriter keyboard and seven additional blocks. The total weight of the kit reached 141 kg. Only one battery for autonomous power supply of the electrical part of the car weighed 32 kg.

In 1937, under the leadership of V.N. Rytov, a mock-up of a small-sized disk encoder was created, designed to replace manual ciphers in the operational control unit. A multialphabetic substitution cipher found use in it. It was a fairly compact device packed in one box weighing 19 kg. In 1939, this cipher machine called K-37 "Crystal" was put into serial production. In total, by the beginning of the Great Patriotic War, over 150 sets of K-37 and 96 sets of M-100 were adopted by the USSR cipher organs. This technique made it possible to increase the processing speed of cipher telegrams by 5-6 times, while maintaining the stability of the transmitted messages.

But despite the fact that domestic cipher machines were actively and effectively used at the front, manual ciphers were the main type of encryption for the majority of the Soviet military. The most common encryption system of the Soviet armed forces during World War II were re-encrypted codes. For the first time in the USSR, a stable encryption system with a one-time scale was developed in the early 1920s. The active use of a one-time scale in diplomatic correspondence began in 1927. A little later, the one-time gamma began to be used to re-encode codes in the Red Army and Soviet special services.

It is impossible not to note the contribution of Soviet radio intelligence and cryptanalysts to the victory in the Great Patriotic War. For example, very valuable information was obtained from the decrypted diplomatic correspondence of Japan. The most valuable information was obtained from decrypted messages of representatives of Germany's allies in Helsinki, Finland, and important information came from Bucharest, Romania's capital. Soviet decryption specialists made a great contribution to the victory near Moscow. During the war, the Soviet decryption services provided the political and military leadership of the USSR with a large amount of important information. This information was received during all the most important battles and contributed to our victories. Soviet cryptanalysts opened manual and machine ciphers of foreign countries. During the war, it was possible to decrypt a number of German encoders, but not Enigma.

10 Cryptography in the USSR (1945-1991)

In the post-war years, several dozen types of encryption technology were developed. The letter T began to denote the technique of linear encryption, and M stood for the technique of preliminary encryption [17, 22–24].

In 1945, the encryption machine M-102 "Malachite" was developed, in 1946M-150 "Rubin", in 1952 the production of encryption machines M-152 (A and B) "Granite", M-103 "Malachite–2M" was mastered, in 1955M-153 "Amethyst-A" was propodes. This was followed by the M-161 "Apatit", M-111 "Marble" in 1967. Under the leadership of N.M. Sharygin, the M-120 "Pearl" disk machine was developed. The SM-1 "Cornflower" and SM-2 "Lilac" took their place in this row.

Specialized encryption equipment was also produced, for example, the M-130 "Coral" encryption machine, designed to close meteorological information. On the keyboard of this machine there were only 10 significant keys corresponding to the numbers from zero to nine.

In the 1980s, the USSR Armed Forces began to receive encryption machines of the 3rd generation M-200 "Uran", the automated workstation of the cipher operator "Tobol" and other equipment.

However, for many years, almost until the end of the existence of the Soviet Union, the basis of the machine park of the encryption services of the USSR were the coding machine M-125 "Violet" and the encryption machine M-105 "Agat".

Created in the second half of the 50s, the M-125 "Violet" coding machine was one of the most common products of this class in the Soviet Union, it was widely used not only

in the Armed Forces, but also in industrial enterprises, the merchant fleet. "Violet" was repeatedly upgraded to improve cryptographic strength and operational characteristics, modifications were made adapted to the languages of foreign customers. The cryptographic system of the machine consisted of a set of cipher disks (rotor) and a switch. This machine originally used ten cipher disks with a fixed internal desoldering. Thirty input contacts are connected to thirty output contacts in a certain order and its change in the field is not possible. Each disc had an external adjustable ring with thirty possible positions. There was a wiring module inside the disk, which could also be fixed in thirty different positions. The wiring modules were interchangeable and could be used in each disk. Cipher disk sets (rotors) were manufactured in various series with unique internal desoldering schemes. The most important advantage of this machine was the ability to use one-time general communication keys to establish secret communication with almost any correspondent who has the same machine and the corresponding key documentation.

The M-105 "Agat" encryption machine was developed in the second half of the 60s to replace the largely identical M-104 "Amethyst". Nevertheless, "Amethyst" continued to be used in some networks for quite a long time. Structurally, the M-105 was an adder of plaintext characters with signs of the external scale, the carriers of which were cipher tapes. Agat implemented the Vernam cipher. In compliance with the requirements for the scale and the rules of operation, guaranteed durability was provided. The machine had three modes of operation "O" — plaintext, "Z" — encryption and "R" — decryption. The source text could be entered both from the keyboard and from the punched tape. In the same way, information was output from the machine - printing on paper or punched tape.

By the mid-60s of the last century, due to the development of computer technology, it became clear that electromechanical machines would not be able to provide the necessary degree of protection of transmitted information in the foreseeable future. One of the ways to solve the problems that arose was the creation of an encryption/encoding technique with an electronic encoder. In the late 70s/early 80s, a number of samples of special equipment of the third generation were developed (M-200, M-201, M-204, M-464, etc.). The M-205 was chosen as the main encryption machine designed to replace the M-105 "Agat", for the first time introduced in 1983.

We must not forget that in the USSR cryptography was a completely closed discipline, which was used exclusively for the needs of defense and state security, and therefore there was no need for public coverage of achievements in this field. It was only in the late 1980s and early 1990s that significant changes took place. So, in 1989, the first domestic encryption standard GOST 28147-89 was adopted [25]. This is a 64-bit block algorithm based on the Feistel scheme, with a 256-bit key. During the operation of the algorithm, a simple encryption algorithm is performed sequentially, for 32 rounds. Decryption is carried out in the same way with inverting the order of the plug-ins. The procedure for generating S-boxes is not defined in the standard. Since the standard uses a 256-bit key and S-blocks can be secret, the durability of this algorithm is great and it is quite reliable. It, having a structure similar to that of DES algorithm, and having twice as many rounds, nevertheless demonstrates a performance an order of magnitude higher than the performance of DES.

We should mention that until 2010 it practically did not attract the attention of foreign cryptographers. The situation changed dramatically after the appearance of the work [26] in which the authors demonstrated that the GOST28147-89 version they considered can be used as a lightweight block cipher with much better parameters than most known low-resource ciphers.

In connection with the subsequent attempt to promote GOST 28147-89as an international standard, in 2010-2020 a huge number of works on cryptanalysis of GOST 28147-89 appeared. As a result, some weaknesses were found in the algorithm that reduced its theoretical stability. However, the estimates of some authors are greatly exaggerated. For example, Courtois says that “clearly GOST is deeply flawed, in more than one way, and GOST does not provide the security level required by ISO… It is for the first time in history that a major standardized block cipher intended to provide a military-grade level of security and intended to protect also classified and secret documents, for the government, large banks and other organisations, is broken by a mathematical attack…»” [27]. Such an assessment is overly emotional, since the proposed attacks cannot be implemented in practice, as evidenced by a much more balanced assessment given by the famous Israeli cryptographer Adi Shamir: “Consequently, we are concerned about the demonstrated weaknesses in the design of GOST (especially in its simplistic key schedule), but do not advocate that its current users should stop using it right away” [28].

11 Modern cryptographic research in Russia

In this section, we will consider the achievements of Russian cryptographers in the late XX – early XXI centuries.

One of the important tasks is to increase the performance of cryptographic transformations when implementing strong block ciphers, since the use of such transformations should not reduce the performance of computer and telecommunications systems operating in secure mode. One of the ways to solve this problem is to use flexible operations based on permutations performed depending on the transformed data and on the secret key. N.Gut, A.Moldovyan, N.Moldovyan

suggested using managed double operations implemented by non-standard managed operating units [29–31]. The combination of controlled permutations and controlled two-place operations makes it possible to significantly expand the class of microelectronic encryption devices that provide encryption speeds of more than 1 Gbit/s. Strength of such ciphers is based on the dependence of conversion operations on the data being converted and the dependence of conversion operations on the secret key. Two types of controlled adders with a large number of unique transformation modifications are proposed. The implementation of adders has a low circuit complexity, which makes it possible to develop inexpensive high-speed hardware ciphers based on them. Two block iterative cryptosystems using controlled permutations and controlled summation operations are proposed, and the choice of specific modifications at this current conversion step is carried out depending on the input data and on the secret key. The advantage of the proposed cryptosystems is that nonlinear transformations are performed on large data subblocks, which determines their high resistance to all known methods of cryptanalysis.

Among the encryption algorithms developed by Russian cryptographers, it should be noted the encryption algorithm used in the SPECTR-Z cryptosystem, which has high resistance to attacks based on both known and specially selected texts [32]. This is a 512-byte block encryption algorithm consisting of three rounds, the encryption key is formed at the stage of pre-calculations in a pseudo-random way from the password entered by the user. The encryption procedures are arranged in such a way that the sub-keys do not participate directly in the equation linking the ciphertext and the plaintext, when encrypting two different texts, differences appear that increase avalanche-like, the value of the variable by which the plug-ins are sampled at the current step depends on all previously converted words, when converting words, a cyclic shift operation is used, depending on the text being converted. The SPECTR-Z crypto algorithm is resistant to known cryptanalytic attacks, including linear and differential cryptanalysis. The strength of the cryptoalgorithm is provided not by the number of rounds of encryption, but by the very structure of the conversion procedures. This algorithm is also resistant to attacks based on the generation of random hardware errors.

Consider the algorithm WICKER-98 (A.Volchkov, N. DeMonderik, A. Lebedev) [33]. This algorithm is similar to RC-5 and RC-6, but the fundamental difference between the algorithm of WICKER-98 from these algorithms is the absence of context-dependent shift of operands: all cyclic shift operations in WICKER-98 are specified explicitly. This at least leads to greater performance of the algorithm, especially on low-bit processors and specialized chips, where such a shift simply corresponds to a fixed jumper between adjacent parts of the conveyor. On the other hand, the absence of a context-dependent shift leads to less dependence of arguments on this operation and it is necessary to specially select and analyze fixed parameter shifts in order to ensure the complete dependence of each output bit on all input bits and key bits. At the same time, the linear and differential analysis of the algorithm is correspondingly complicated. Fixing the shift does not allow us to make assumptions about its possible coincidence with the required value and cost simple differentials on this basis, as is the case for RC-6, where differential analysis turned out to be the most powerful tool for a violator. In other words, the WICKER-98 algorithm requires a more scrupulous selection of cyclic shift values, but it provides a greater counteraction to linear and differential analysis than RC-5 and RC-6. The WICKER-98 has about the same number of cycles as the RC-6, each of which consists of four iterations. A cycle means a conditionally repeating segment of calculations taking into account the arguments involved, and an iteration means without taking them into account. In each iteration, WICKER-98 changes two registers, as in RC-6, but in fact, the number of iterations doubled compared to PC-6 leads to a doubled frequency of register conversions. Each iteration in WICKER-98 actually consists of two independent parts, which allows them to be executed in parallel on two processor pipelines. Unlike WICKER-98 in RC-6, each iteration contains two multiplications and its complete parallelization is not achieved and this leads to the fact that the RC-6 cycle exceeds the WICKER-98 cycle in duration. Thus, the WICKER-98 algorithm, having approximately the same number of cycles as the PC-6, works faster, while performing almost twice the number of iterations and, as a result, twice the number of register conversions, although each of these operations is somewhat simpler.

R. Abdrakhmanov and A. Zhukov proposed a data encryption method such that blocks are transformed and rearranged inside a larger array depending on the current state of the working key and the encrypted data, such that blocks are transformed and rearranged inside a larger array depending on the current state of the working key and the encrypted information [34]. The cipher combines elements of block ciphers, stream ciphers and permutation ciphers. To reduce the correlation between the plaintext and the ciphertext, a gamma is superimposed on the text, for initialization of which an additional input array of arbitrary length is used. Initialization of the gamma array is carried out once at the initial stage of the algorithm, unidirectional functions are used during initialization. The resulting ciphertext depends on the plaintext, the key, and the gamma array. The algorithm can operate with blocks of any size, the performance and mixing characteristics of the algorithm depend on the block size. The peculiarity of this algorithm is that during its operation, key information is constantly changing in the process of its use, depending on the encrypted data: the secret key changes depending on the plaintext, the key itself and the gamma

array. Together with the ciphertext, it is necessary to store or transmit the information necessary to restore the decryption key, the role of which is performed by the key value at the end of the algorithm. As such information, you can use the sum of the secret key and the decryption key.

In 2015, a new Russian Kuznechik cipher was developed, which is part of the GOST R 34.12-2015 encryption standard [35]. Algorithm is based on substitution-permutation network. Such cipher receives a block and a key as input and performs several alternating rounds consisting of substitution stages and permutation stages. In the Kuznechik cipher, nine complete rounds are performed, each of which includes three consecutive operations: the operation of superimposing a round key or bitwise XOR from the key and the input data block, a nonlinear transformation, which is a simple replacement of one byte with another according to the table, a linear transformation consisting in the fact that. Each byte from the block is multiplied in the Galois field by one of the coefficients of the series, depending on the byte sequence number, the bytes are added together modulo 2, and all 16 bytes of the block are shifted towards the lowest digit, and the resulting number is written to the place of the read byte. The Kuznechik cipher is a block algorithm, it works with data blocks of 128 bits long, the key length is 256 bits. Round keys are obtained by certain transformations based on the master key. This process begins with splitting the master key in half, so the first pair of round keys is obtained. To generate each subsequent pair of round keys, eight iterations of the Feistel network are used, in each iteration a constant is used, which is calculated by applying a linear transformation of the algorithm to the value of the iteration number. The Cipher has several modes of operation: Electronic Codebook, Counter, Output Feedback, Encryption Block Chain, Cipher Feedback, Message Authentication Code, defined in the GOST R 34.13-2015 standard [36]. This standard also defines the Magma cipher, which is similar to the previous GOST 28147-89 encryption standard, but differs from it in that it has fixed replacement blocks and the reverse order of these blocks.

In addition to encryption standards, Russia has standards for the processes of forming and verifying a digital signature [37]. The first edition of the standard was adopted in 1994 (GOST R 34.10-94), the scheme was based on the complexity of discrete logarithm in a finite simple field, new algorithms are based on the mathematical apparatus of elliptic curves (GOST R 34.10-2001 and GOST R 34.10-2012) [38]. The durability of a digital signature depends not only on the signature algorithm itself, but also on the hash function used. Among the Russian cryptographic standards there is a standard for the hashing function, the first edition of the standard was also adopted in 1994 (GOST R 34.11-94), the current one – in 2012 (GOST R 34.11-2012) [39]. The algorithms GOST R 34.10-94 and GOST R 34.10-2001 use the hash function according to GOST R 34.11-94, the hash function standard GOST R 34.11-2012 was developed for the new digital signature algorithm. The first hashing function standard used a 256-bit hash value, the current standard allows one to create both 256-bit and 512-bit hash values, which undoubtedly increases the reliability of the hash function. The main difference between the current digital signature standard and the 2001 standard is the availability of additional options for parameters of the algorithm.

Russian scientists are also actively engaged in post-quantum cryptography, first of all, it should be noted the works of A. Stolbunov and A. Rostovtsev devoted to the study of supersingular isogeny-based cryprography, a family of quantum-resistant algorithms [40]. They also proposed the adaptation of the ElGamal cryptosystem to the isogeny of elliptic curves [41].

Among the developments of cryptographic primitives, it is necessary to note the work of B. Sukhinin, in which he presented a stream cipher based on a cellular automaton [42]. The practical implementation of the cipher on the Altera Cyclone II platform at a clock frequency of 149 MHz showed a performance of 35.5 Gbit/sec.

The work [26], which put GOST 28147-89 on a par with the best lightweight algorithms, as well as the works that appeared after it, which revealed some weaknesses of GOST 28147-89, caused the appearance of the work [43] in which a low-resource version of GOST 28147-89 (750 GE) with a modified order of using cyclic keys is announced. The last change is due to the fact that most attacks that weaken GOST 28147-89 are based on symmetry in the key schedule. The new key schedule assumes the impossibility of carrying out such attacks.

The topic of cryptography is very popular in Russia, many universities graduate specialists in this field who are widely in demand in government agencies and in commercial firms performing works related to the production and distribution of cryptographic tools. Among the universities that train specialists in the field of information security, it should be noted National Research Nuclear University MEPhI (Moscow), Lomonosov Moscow State University, The Bauman Moscow State Technical University, Moscow Institute of Physics and Technology, Russian State University for the Humanities (Moscow), The Peter the Great St.Petersburg Polytechnic University, Novosibirsk State Technical University, Tomsk State University of Control Systems and Radioelectronics. In Russia, there is a technical committee for standardization "Cryptographic Protection of information" (TC 26), which has standardization objects related to information encryption methods, methods of their implementation, as well as methods for ensuring the security of information technologies using cryptographic transformation of information, including authentication and digital signature.

Currently, a number of conferences on cryptography are being held in Russia. Among the most significant it should be

noted RusCrypto Conference (annually since 1999), Conference on Methods and technical means of information security (annually since 1999), International Conference "Siberian Scientific School-seminar" Computer security and cryptography (SIBECRYPT) (annually since 2002), PKI-Forum Conference on public key infrastructure and electronic signature (annually since 2002), Workshop on Current Trends in Cryptology (CTCrypt) (annually since 2012), however, most of the results, in addition to those given in this section, are devoted to the analysis of existing structures, and not to the presentation of new cryptographic schemes or primitives.

12 Conclusion

The article analyzes various epochs of the development of cryptography in Russia, ranging from ancient Russian types of cryptography to modern ciphers. Cryptography has played a significant role in strengthening various states and its role cannot be underestimated in modern history. With the development of methods and means of encryption and decryption, increasing the cryptographic strength of ciphers, the task of ensuring the security of the state by cryptographic methods is becoming more complex, its solution can be effective with the involvement of other methods — counterintelligence, organizational, engineering and others. History holds many examples when the oblivion or underestimation of cryptographic work by the top leadership of the state (led the respective countries to negative results, and it took many years to eliminate their consequences. History, especially the twentieth century, has clearly shown that in no way should major theoretical studies aimed at the future, studies that are now commonly classified as fundamental, be ignored. It is large-scale research that from time to time gives rise to such unpredictable outputs that give rise to fundamentally new areas of cryptography and have a revolutionizing effect on all subsequent cryptographic activities.

Acknowledgements This work was supported by the Ministry of Science and Higher Education of the Russian Federation (state task Project No. FSWU-2023-0031).

Declarations

Conflict of interest All authors declare that they have no conflicts of interest.

References

1. Babash, A.V., Baranova, E.K., Larin, D.A.: History of Information Protection in Russia, p. 736. Publisher Center EAOI, Moscow (2012). (**in Russian**)
2. Larin, D.A.: Cryptographic Service of Russia. Essays on History, p. 384. Helios-ARV, Moscow (2017). (**in Russian**)
3. Nikonov, V., Stolpakov, B.: Historical Evidence of the Beginning and Development of Russian Cryptography (XVI–XVII Centuries), p. 254. Media Group “Avangard,” Moscow (2016)
4. Tokareva, N.N.: On the history of cryptography in Russia. Prikl. Diskretn. Mat. **4**(18), 82–107 (2012). (**in Russian**)
5. Babash, A.V., et al.: On the development of cryptography in the XIX century. In: Information Protection, No. 5 (2003) (**in Russian**)
6. Astrakhan, V.I., Gusev, V.V.: Formation and development of government communications in Russia, 1996 (**in Russian**)
7. Zapechnikov, S., Tolstoy, A., Nagibin, S.: History of cryptography in syllabus on information security training. In: IFIP Advances in Information and Communication Technology, vol. 453, pp. 146–157 (2015). https://doi.org/10.1007/978-3-319-18500-2_13
8. Soboleva, T.A.: The History of Encryption in Russia, p. 511. Olma-Press-Obrazovaniye, Moscow (2002). (**in Russian**)
9. Speransky, M.N.: The Secret Writing in the South Slavic and Russian Monuments of Writing, 2nd edn. Book House “Librocom,” Moscow (2011). (**in Russian**)
10. Shchepkin, V.N., Nauka, M.: Russian paleography, p. 225 (1967) (**in Russian**)
11. Shamin, S.M.: Unknown cryptographic alphabet from the archive of the order of secret affairs. Ancient Russia. In: Questions of Medieval Studies, no. 2 (40), pp. 103–106 (2010) (**in Russian**)
12. Zapechnikov, S.: From the history of cryptography: cryptography as a phenomenon of the Ancient Russian literary language (XII–XVII centuries). Inf. Technol. Secur. **18**(2), 116–123 (2011). (**in Russian**)
13. Zapechnikov, S.: From the history of cryptography: document protection, cryptography and secret communications in Byzantium (IV–XV centuries). Inf. Technol. Secur. **19**(2), 49–61 (2012). (**in Russian**)
14. Zapechnikov, S.: From the history of cryptography: Leonhard Euler’s contribution to the formation of the mathematical foundations of modern cryptology. Bull. Russian State Univ. Ser. Doc. Arch. Stud. Comput. Sci. Inf. Prot. Inf. Secur. **14**(94), 29–52 (2012). (**in Russian**)
15. Nikonov, V., Stolpakov, B.: Historical evidence of the beginning and development of Russian cryptography (XVI–XVII centuries) (2016)
16. Tokareva, N.N.: On the history of cryptography in Russia. Prikl. Diskretn. Mat. **4**(18), 82–107 (2012)
17. Babash, A.V., Baranova, E.K., Larin, D.A.: History of information protection in Russia (2012) (**in Russian**)
18. Soboleva, T.A.: The history of encryption in Russia (2002) (**in Russian**)
19. Larin, D.A.: Cryptographic service of Russia. In: Essays on History (2017) (**in Russian**)
20. Kahn, D.: The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet. Simon and Schuster, New York (1996)
21. The encryption business of the Soviet Union. Part 1. Military Review (2018)
22. Babash, A.V., et al.: On the development of cryptography in the XIX century. Information Protection, No. 5, 2003.
23. Astrakhan, V.I., Gusev, V.V.: Formation and development of government communications in Russia (1996)
24. Encryption machines of the USSR 1931–1991. (Review) 18.11.2020 (Section 9). Prisma. The army and the military-industrial complex. http://prizmablog.ru/
25. Schneier, B.: Applied Cryptography. Protocols, Algorithms, and Source Code in C. Wiley, London (2015)
26. Poschmann, A., Ling, S., Wang, H.: 256 bit standardized crypto for 650 GE—GOST revisited. In: Mangard, S., Standaert, FX. (eds.) Cryptographic Hardware and Embedded Systems, CHES 2010. CHES 2010. Lecture Notes in Computer Science, vol. 6225.

Springer, Berlin (2010). https://doi.org/10.1007/978-3-642-15031-9_15
27. Courtois, N.T.: Security evaluation of GOST 28147-89 in view of international standardisation. Cryptology ePrint Archive, Report 2011/211 (2011). http://eprint.iacr.org/
28. Dinur, I., Dunkelman, O., Shamir, A.: Improved attacks on full GOST. In: Canteaut, A. (eds.) Fast Software Encryption. FSE 2012. Lecture Notes in Computer Science, vol. 7549. Springer, Berlin (2012). https://doi.org/10.1007/978-3-642-34047-5_2
29. Moldovyan, A.A., Moldovyan, N.A.: Flexible algorithms for information security in automated control systems. Autom. Telemech. **8**, 166–176 (1998). (**in Russian**)
30. Gut, N.D., Moldovyan, A.A., Moldovyan, N.A.: Flexible hardware-oriented ciphers based on controlled adders. In: Rroceedings of RusCrypto-1999 (1999)
31. Moldovyan, A.A., Moldovyan, N.A. High-speed ciphers of a new generation. In: Rroceedings of RusCrypto-1999 (1999) (**in Russian**)
32. Alekseev, L.A., Alekseev, L.E.: Transformation of information in the SPECTRUM-Z system. In: Proceedings of RusCrypto-1999 (1999) (**in Russian**)
33. Volchkov, A., De-Monderik, N.Y., Lebedev, A.N.: Algorithm WICKER-98. In: Proceedings of RusCrypto-1999 (1999) (**in Russian**)
34. Abdrakhmanov, R.G., Zhukov, A.E.: Substitution-permutation ciphers. In: Proceedings of RusCrypto-2000 (2000) (**in Russian**). https://www.ruscrypto.ru/accociation/archive/rc2000.html
35. GOST R 34.12-2015: Information technology. In: Cryptographic Data Protection. Block Ciphers (2015) (**in Russian**)
36. GOST R 34.13-2015: Information technology. In: Cryptographic Data Security. Block Ciphers Operation Modes (2015) (**in Russian**)
37. Komarova, A.V., Menschikov, A.A., Korobeinikov, A.G.: Analisys abd comparison of digital signature algorithms GOST R 34.10-94, GOST R 34.10-2012. In: Cybersecurity Questions, No. 1(19) (2017) (**in Russian**)
38. GOST R 34.10-2012: Information technology. cryptographic data security. generation and verification processes of electronic digital signature (2012) (**in Russian**)
39. GOST R 34.11-2012: Information technology. Cryptographic data security. Hash-function (2013) (**in Russian**)
40. Stolbunov, A., Rostovtcev, A.: New cryptosystems against quantum attacks. In: Proceedings of Science Week (2004) (**in Russian**)
41. Stolbunov, A., Rostovtcev, A.: Public-key cryptosystem based on isogenies. In: IACR Cryptology ePrint Archive (2006) (**in Russian**)
42. Sukhinin, B.M.: Development and research of high-speed generators of pseudorandom uniformly distributed binary sequences based on cellular automata: dissertation ... candidate of Technical Sciences: 05.13.19—Moscow, 2011, p. 224. Russian State Library, 61 11–5/3554 (**in Russian**)
43. Dmukh, A.A., Dygin, D.M., Marshalko, G.B.: A lightweight-friendly modification of GOST block cipher. Math. Asp. Cryptogr. **5**(2), 47–55 (2014)