V. Nikonov, B. Stolpakov

Historical evidence of the beginning and development of Russian cryptography (XVI - XVII centuries).

Presentation of the book by B. Stolpakov, V. Nikonov

"... so that the content of the letter does not become known in other states"

The book is devoted to the initial period of application of cryptography serving the interests of the Russian state. The time of origin and formation of the Russian cryptographic service is the 17th century.

Back in 1853, the first study was published, specifically devoted to the use of cryptography in Russia in the 17th century. These were two articles of Corresponding Member of the Imperial Academy of Sciences A. N. Popov, published in the Notes of the Imperial Archaeological Society. A.N. Popov proposed the name "diplomatic cryptography" for the main application of cryptography in the 16th-17th centuries.

In Russia, at that time, ciphers of simple substitution were mainly used, replacing the letters of Russian alphabet with the signs of another alphabet, often of artificial origin. Such specially invented alphabets were called "new alphabets" or "tsifirnie azbuki", i.e. Cryptographic alphabets.

As the basis that holds together the mosaic of historical facts related to cryptography, the authors of the book widely use the general picture of the life of the Russian state in the XVI-XVII centuries. Diving into the details of historical events is necessary to understand how important state decisions on cryptographic issues ripened.

The historical picture of Russia's life allows us to trace the process of creating a cryptographic service as an important part of the state apparatus. In the historical context, personalities come to life: many prominent cryptographers appear to be real people with their own human interests.

In the book offered to the reader, the authors tried to systematize the available documentary evidence of the initial period of cryptographic activity in Russia. It is clear that for such a systematization the choice of the nodal time periods is important. The authors were oriented to the periods of revival of foreign policy ties. Important milestones, according to the authors, are the 90s of the 16th century, and in the 17th century - the beginning of the 30s, the reign of Alexei Mikhailovich and the 80s. The time interval of the late 20's and early 30's of the XVII century is especially important for Russian cryptography. It was at that time that Russia's final entry into the political life of Europe was celebrated by historians. It is not surprising that at that very time the first documents regulating cryptographic activity in the state appeared. The moment of their creation - August 8, 1633 deserves, according to the authors of the book, special attention and can be proposed as the date of birth of the cryptographic service as a special public service of Russia. The reader will find in the book an appropriate justification and documentary evidence.

The book reflects the results of archival research and the research of the authors made on the initial history of the cryptographic service of Russia, conducted with the support of the Academy of Cryptography of the Russian Federation. Initially, the content of the book was aimed at students-cryptographers. Suddenly, it became interesting to diplomats. O.G. Peresypkin, an outstanding domestic diplomat, helped to organize the monographic publication of the book under the title of the Diplomatic Academy of the Russian Foreign Ministry with a presentation in the assembly hall of the Academy, and wrote the foreword to the book.

The first documentary mention of the use of the Cryptographic alphabet in the diplomatic correspondence of the Moscow state is dated 1590. N. M. Karamzin pointed out in his "History of the Russian State" some details: "The courier Andrei Ivanov wrote from 1590 to Lithuania a letter, using litora (one form of old Cryptographic writing) and a new alphabet taken from the Ambassador of Austria, Nikolai Varkoch"

Varkoch passed the Cryptographic alphabet to Moscow diplomats and indicated the method of its application. Both the episode and the content of Ivanov's coded letter are reflected in the ambassadorial book on relations with Lithuania, a fragment of her page is shown in Fig. The entry reads: "A diploma from Lithuania from the bookbinder Andrei Ivanov is written with a new alphabet, which was taken from Tsesarev's ambassador Nikolai Varkoch."

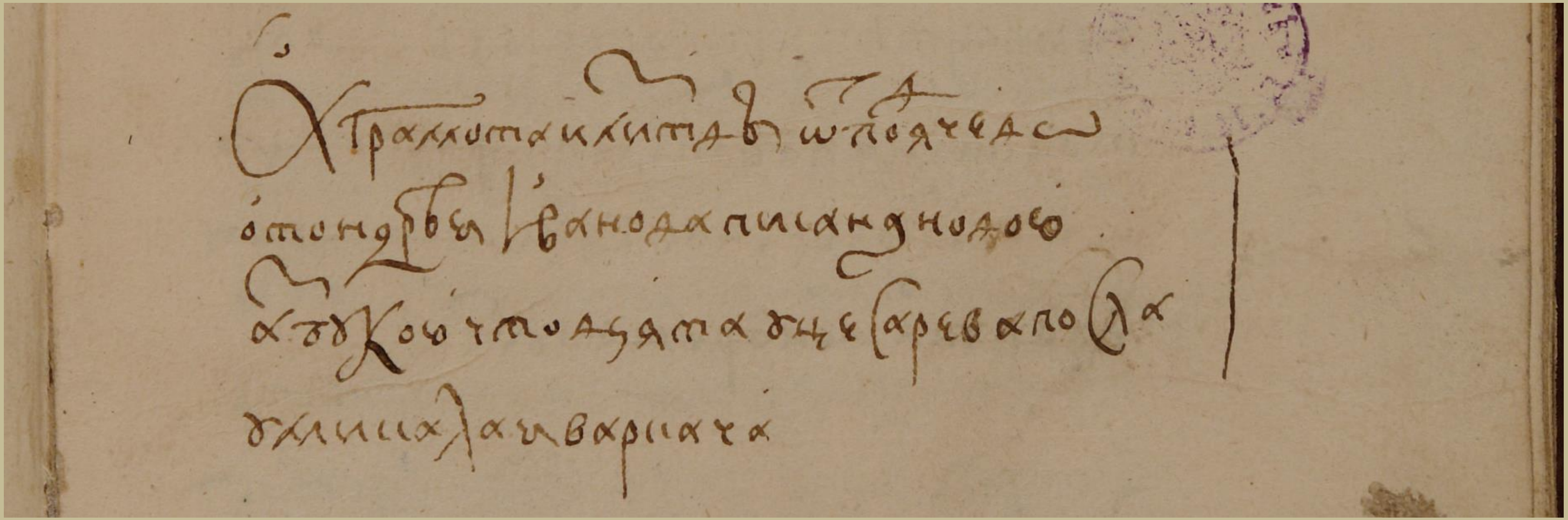


Fig.1. The entry in the Ambassadorial Book (1590)

The well-established office work of the Posolskiy Prikaz (Ambassadorial Regiment) preserved for us the name of the first Russian cipher handler who deciphered the letter in Moscow: Yakov Zaborovsky.

For us, the following fragment of Varkoch's report, written by him for the emperor after his return from Moscow, is of interest: "Godunov appointed one of his closest scribes, as well as an interpreter from the Polish language, to correspond with the emperor. Since Boris himself is familiar with Polish, he would like the encrypted news, if any, to be sent, written in Polish. "

Note that the existence of encrypted correspondence with the Austrian empire is confirmed by later documents. For example, the contents of the letter of Emperor Rudolph II dated May 23, 1600. He asked Godunov for explanations on the issue of interest to him and indicated that "he would immediately reply to Boris, either written in the Cryptographic alphabet or verbally through a special Ambassador"

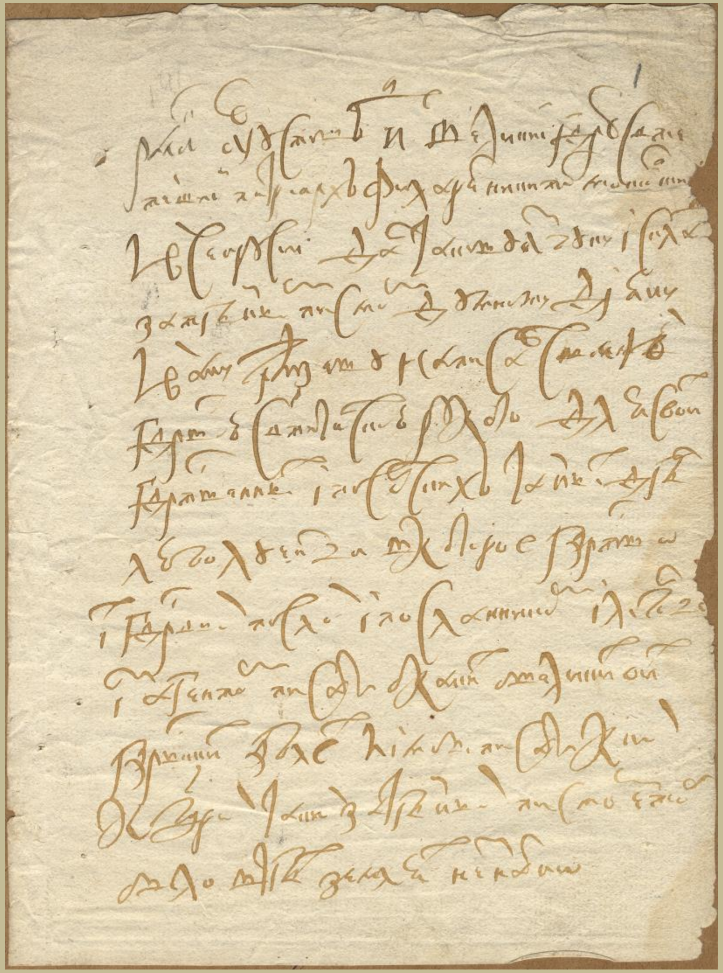
The time interval of 1628-1633 is very important for our topic. That's when the state decisions related to the organization of encryption activity ripened.

By 1626-1628 the leadership of the foreign policy of Muscovy passed to Patriarch Filaret. It was the time of the Thirty Years' War, which divided Europe into two camps. At that time, Poland was adjacent to the Austro-Spanish coalition. Opponents of this camp Denmark, Holland, England, France, Turkey, Hungary, especially Sweden, actively tried to attract the Moscow state to their side. They needed Muscovy and as a supplier of grain. By 1626, Western European prices for bread increased 10 times, and by 1628 - 20 times.

According to the opinion of B. Porshnev, "in the depths of the Posolsky Prikaz (Ambassadorial Regiment), a great deal of painstaking work was already done to gather information from residents and all kinds of informants from all parts of Europe."

Muscovy from the 30-ies of the XVII century had to take its place in the European diplomatic system. If earlier the main tasks of Russian diplomacy were the control and supervision of relations with foreign countries, now the task was to develop them in the interests of the state. The transition to a new diplomatic system necessitated the creation of permanent foreign missions and the organization of encrypted communications with them. And soon there were corresponding orders. It is important that these decisions were simultaneously supported by measures to implement them. In its significance, the document is dated August 8, 1633. It is shown in Fig

Modern reading of the contents of the document: "On August 8 (according to the old style, according to the new style on August 18), 1633, the Great Sovereign Patriarch of Moscow and Russia Filaret Nikitich gave the encrypting alphabet written by his hand and an example of its use to the Duma deacon Ivan Gryazev (the head of the Posolsky Prikaz). The Sovereign Saint wrote a cryptographic alphabet for state and embassy secret affairs. If it was necessary for state ambassadors, envoys or agents to write about important state affairs, then they should have written to the Sovereigns (the tsar and the patriarch) by an encrypted letter, so that the content does not become known in those states. "



Given the actual role of Patriarch Filaret in the governance of the country, one should recognize the patriarchal indication as a document of high state significance. This is the first of the time known documents that regulate cryptographic activities in Russia.

It seems that the instruction of Patriarch Filaret was a logical step in the expansion of the use of cryptography in diplomacy, military affairs, intelligence and counterintelligence that began in the early 1630s.

It was the first domestic textbook on cryptography. It is important to note that the instruction of Patriarch Filaret was certainly carried out. Already in 1634 the patriarchal cryptographic alphabet was given to a nobleman Dmitry Franzbekov, sent to Sweden by a permanent diplomatic representative.

Before the trip he practiced in the encryption case in the Posolsky Prikaz. This was evidenced in the documents placed in one archival file with the indication of the patriarch. The entire set of documents contained in this case is an original textbook on cryptography, probably the first in domestic practice. It includes:

1. Directions of Patriarch Filaret.

2. Two Cryptographic alphabets, showing a variety of means for their compilation. Examples of the use of these alphabets for encryption are given.

3. A practical but simplified example of text encoding. Simplification is to save words: the encrypted text is divided into the same words as plain text.

4. A real example of an encrypted letter with an unencrypted signature. Here the breakdown of the encrypted text into words differs from the breakdown into open-text words, but the open-text words are not split.

5. Another real example of an encrypted letter. Here the encryption is complicated in comparison with the previous example: when the encrypted text is broken down into words, the words of the open text are split into parts (Fig. 3).

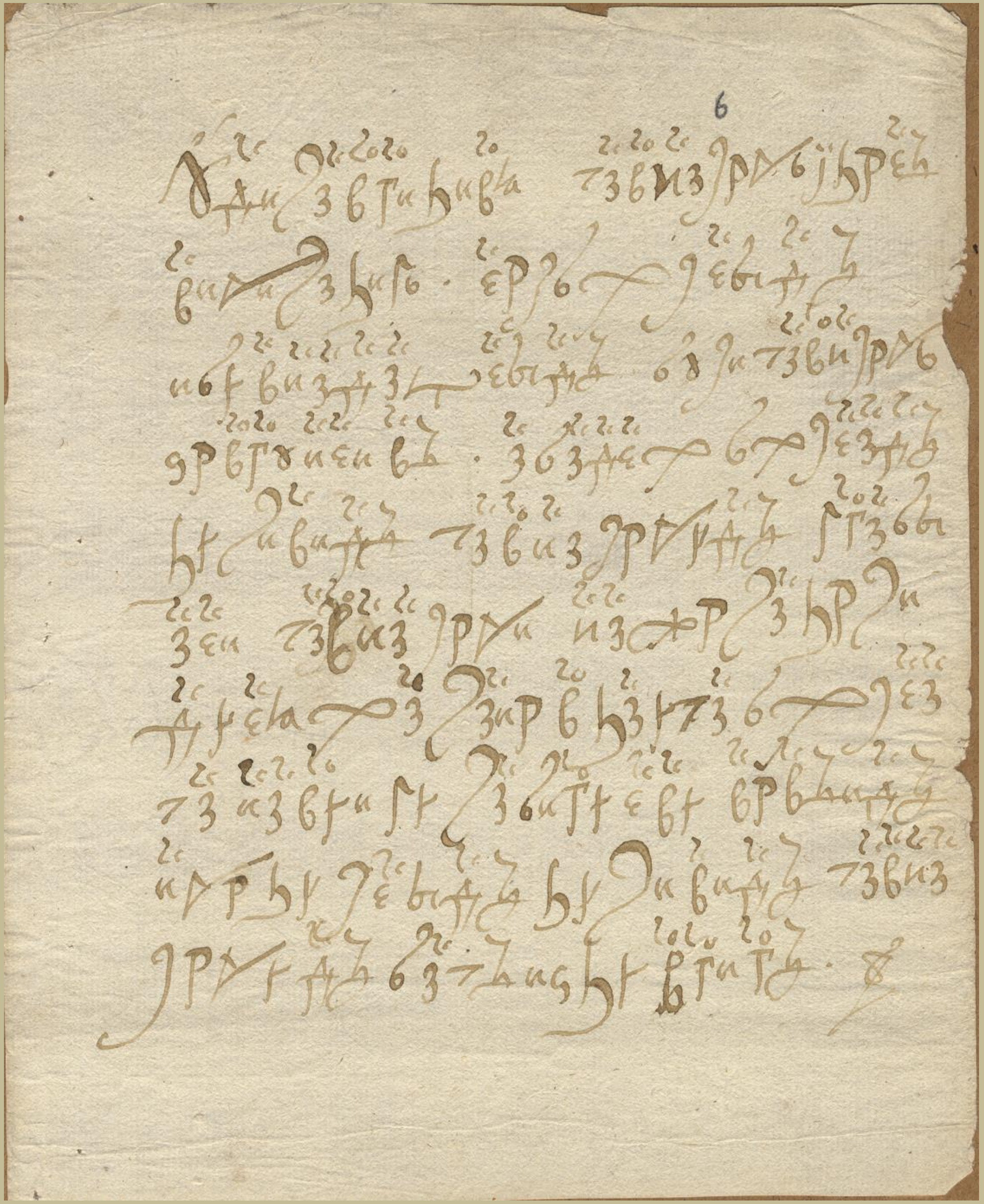


Fig.3. Sample Encrypted Mail

It can be assumed that the manual was drafted with the personal participation of Patriarch Filaret, his text is encrypted with his hand: "Dmitri Franzbekov is beating the master with Ivan Kirilovich (Gryazev)" (Fig. 4).

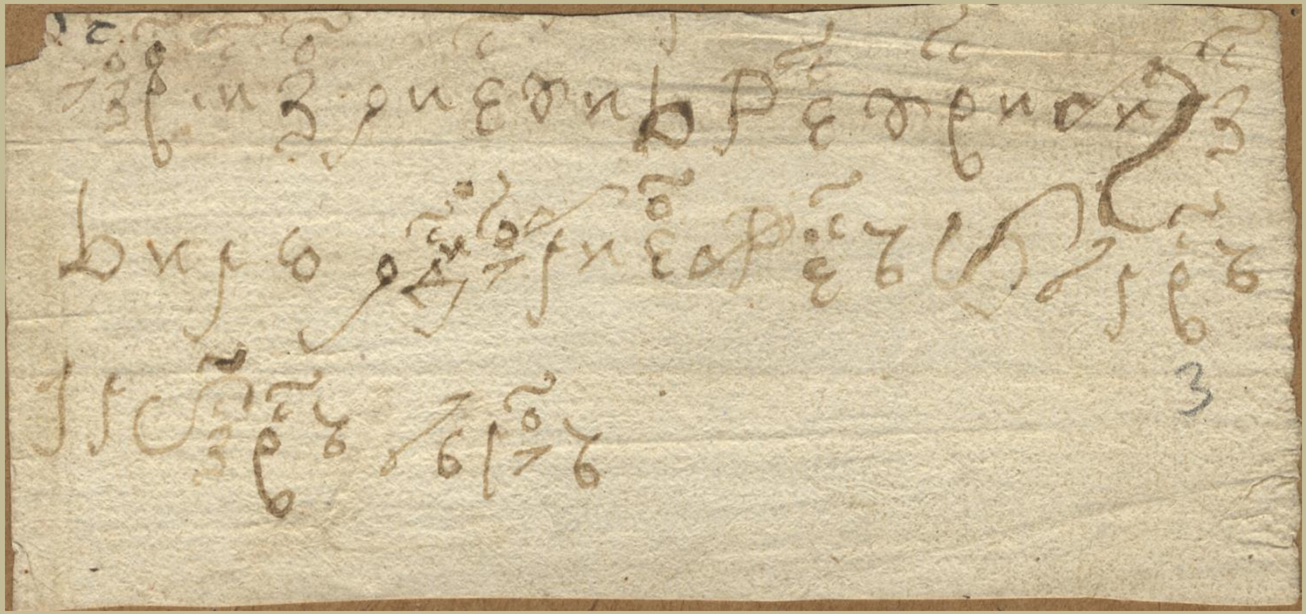


Fig.4. An example of the use of the cryptographic alphabet, the autograph of Patriarch Filaret

This is an example of the use of the cryptographic alphabet, mentioned in the patriarchal order. The manual contains another autograph of Patriarch Filaret - his cryptographic alphabet (Fig. 5).

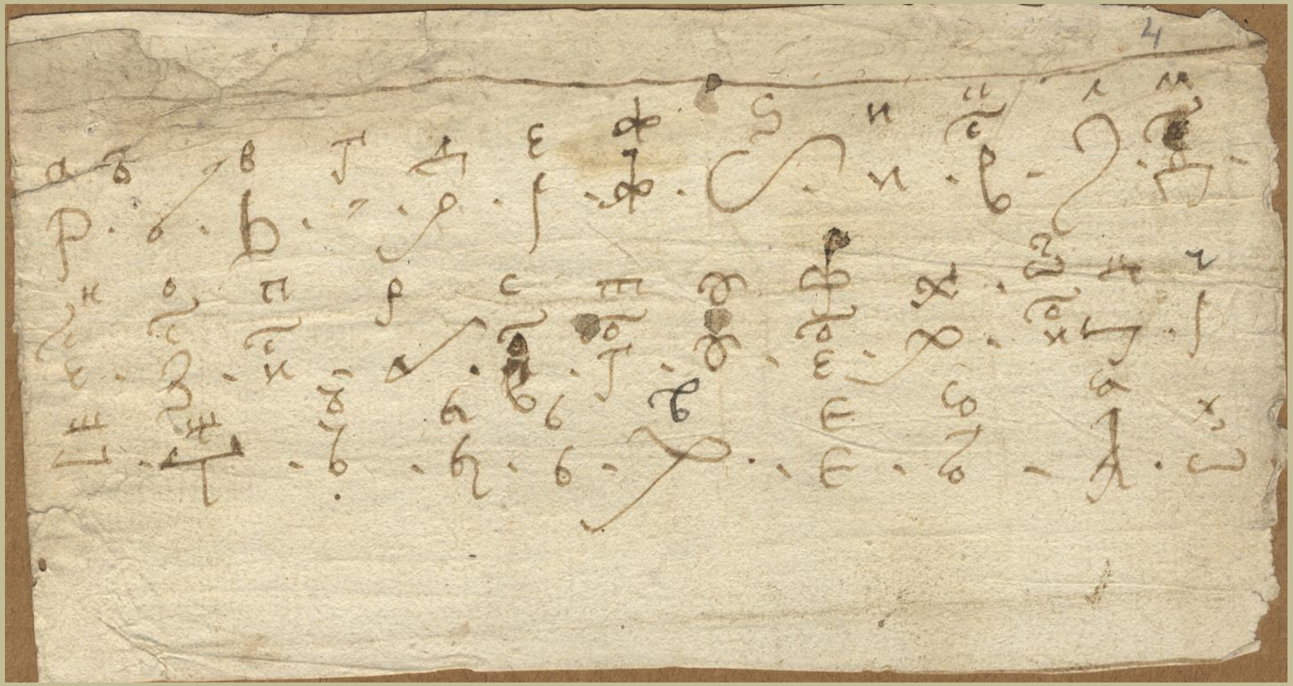


Fig.5. "ABC" of Patriarch Filaret, his autograph

In Figure 5, the reader will easily find 6 lines. In the first, third and fifth lines in order written letters of the Russian alphabet. In the second, fourth and sixth lines under the Russian letters their conditional (coded) notations are signed. To encrypt any Russian text it is enough to replace its letters with their symbols, taken from the patriarchal alphabet. So Patriarch Filaret composed his note (Fig. 4).

The personality of Patriarch Filaret gives special significance to the documents presented. He united in one person the highest secular and spiritual authorities. Thus, we have a directive document with a detailed study of its practical implementation in the manual. We add, and actually implemented in diplomatic work, given the business trip of Franzbekov to Sweden.

Documents related to the trip of Franzbekov, first of all the order, testify to the order of work with the cipher documents already established in the Posolsky order. Dmitry Franzbekov was given detailed instructions on what matters to write to Moscow with a closed letter. Judging by the documents, the term "closed letter" was established in 1634.

Commenting on the documents examined by us, A. Popov made an important conclusion: "The note of the Posolsky Prikaz and the order to Franzbekov can serve as clear evidence that Moscow diplomacy since the first Tsars of the House of Romanovs considered it necessary to use secret records in ambassadorial relations. The reason for this measure can be considered to be that since that time permanent residents of foreign powers have started at the Moscow court. "

Cryptographic supported the communication among agents. Probably, a significant part of the ciphers, created by Moscow cryptographers at that time, was used to classify intelligence information.

So, in 1642 the future famous diplomat Afanasy Lavrentievich Ordin-Nashchokin regularly sent to Moscow intelligence director F. Sheremetev encrypted messages from Moldova. Then relations with Turkey deteriorated because of Azov, the danger of the Turkish-Polish union against the Moscow state increased. And Ordin-Nashchokin from the city of Iasi observed the relations of Turkey, Crimea and Poland. This was done with the knowledge of the Moldovan ruler Vasily Lupu, who took Afanasii

Lavrentievich under a different name to his entourage. In the RGADA, A. Ordin-Nashchokin's reports were preserved: more than 140 pages contain encrypted text.

Archival documents show that Russian statesmen used encryption in the internal business correspondence of the first half of the 17th century.

Development of diplomatic relations and foreign economic relations. During the reign of Alexei Mikhailovich (1645-1676), the field of activity of Moscow diplomats stretched from Madrid to Beijing. The translators of the office worked with more than 20 languages. Among the translators were graduates from European universities, some of them had worked for Western diplomatic services, as a Moldovan, called Nikolai Spafariy.

No major foreign policy action of the Russian state, especially the military one, could not be do without preliminary diplomatic work in European capitals and the press. In Europe, a network of Moscow government agents was created on the base of local merchants. They collected information, organized the necessary publications, recruited thousands of military and civilian specialists to work in Russia, purchased weapons and necessary goods. Their value was estimated at hundreds of thousands of rubles. Communication with agents was maintained through messengers from the Ambassadors Department and the Department of Secret Affairs. Messengers, as a rule, used cryptography to communicate with Moscow.

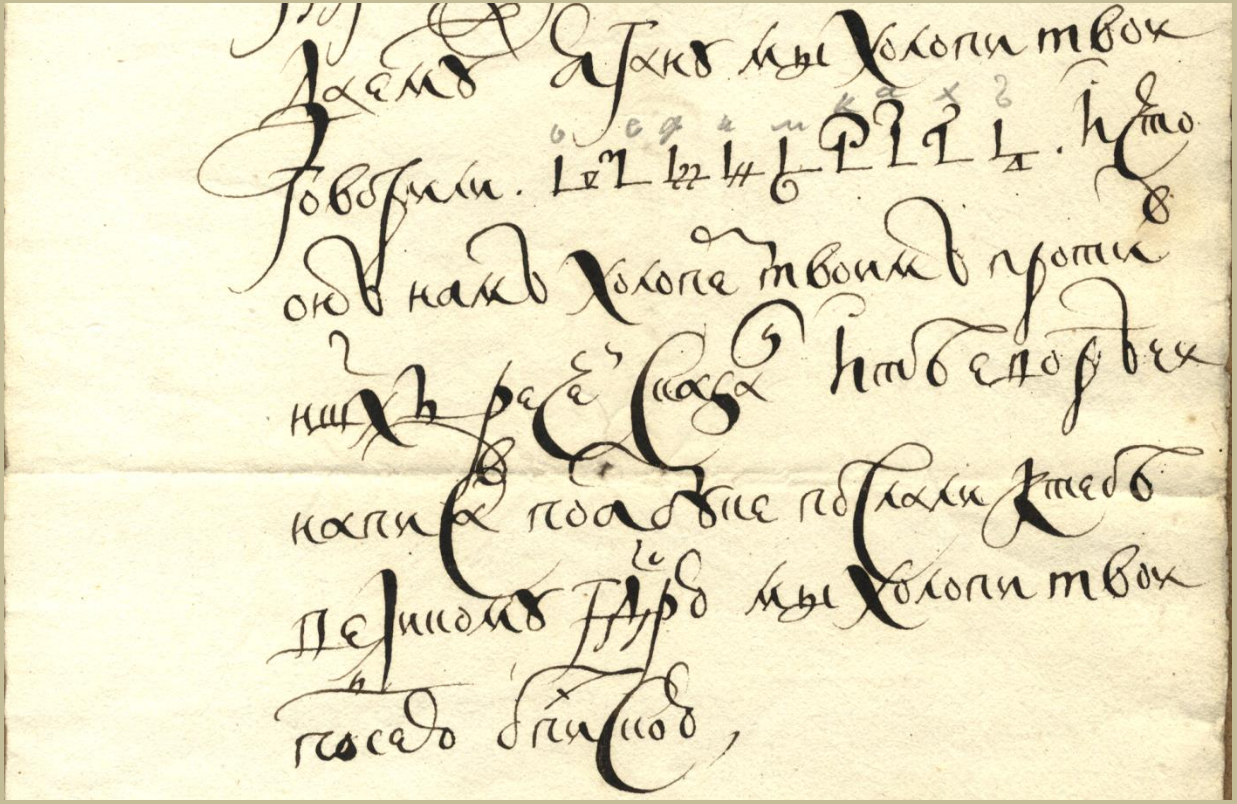
Using cryptography to ensure the confidentiality of large financial transactions. As you know, the second half of the 50's and the first half of the 60's of the XVII century became a period of heavy military tension for the Russian state. The thirteen-year war with the Polish-Lithuanian Commonwealth was supplemented by two more years of sharp confrontation with Sweden. The situation required responsible decisions in the financial and economic sphere as well. It included the adoption of copper coins along with silver and silver money, and then, after the copper riot of 1662, their discontinuance.

The surviving archival documents show that cryptography played a certain role in reducing costs while returning to a silver coin. The problem was the absence of silver. In fact the only source of money silver in Russia at the time was Western European thaler. Such a coin contained about 30 grams of high-purity silver. In Russia, these coins were used mainly as raw materials for minting their own coins.

But for large transactions, in addition to reliable partners, it was also necessary to ensure the secrecy of negotiations and contracts. Several embassies in Western Europe in 1662 had the task was to obtain loans. Meanwhile, it was a question of relatively small transactions, about tens of thousands of thalers. But simultaneously there took place carefully concealed negotiations on a loan of hundreds of thousands of thalers.

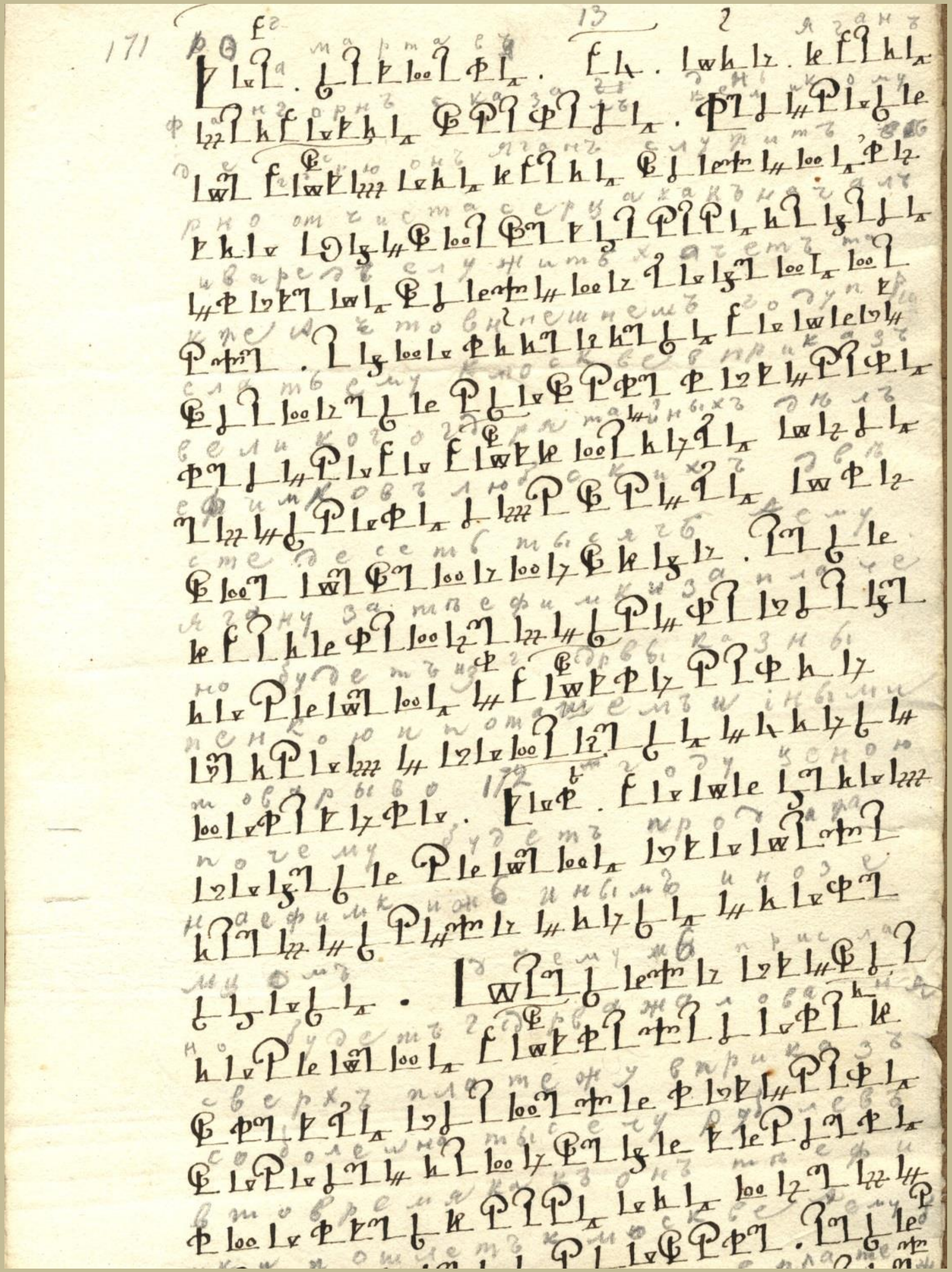
At the time, the embassy of Bogdan Ivanovich Ordin-Nashchokin, where Fedor Kazanets, official of the Department of Secret Affairs, worked, carried out its tasks in Denmark and Holland.

They included an order for financial negotiations with Yagan Fan Gorn, a longtime partner of the Moscow government. On August 17, an encrypted letter was sent from Moscow with a clarified assignment to the diplomats. The original open text of the letter was preserved in the archive of the Department of Secret Affairs: “To Fyodor Kazants. Tell Yagan fan Horn about sending of thalers and with the former one about two hundred ten thousand. And about the payment and the dacha against the former – as he had been ordered verbally”.



Talks between diplomats and Yagan Fan Gorn were held in Lubeck, the largest center of the Hanseatic League. The report on the subject of the talks was immediately sent to Moscow. Figure 6 shows a fragment of the initial part of the report. Only the words "about efimki" (about thalers) are encrypted here.

Fig.6. A fragment of the report with encrypted piece.



The next part of this report is more abstractive and encrypted completely. Its beginning is shown in Fig. 7. The encrypted part of the report contains about 340 words.

Fig.7. The beginning of the encrypted part of the report

Messages of other Russian diplomats in 1663 were much alike with the content of the report of Boris Ordin-Nashchokin and Fyodor Kazantz. We will point out here an encrypted dispatch of t Yuri Nikiforov, official of the Department of Secret Affairs, sent to Moscow on February 7. The end of his letter is shown in Fig. 8. The report contains about 320 words.

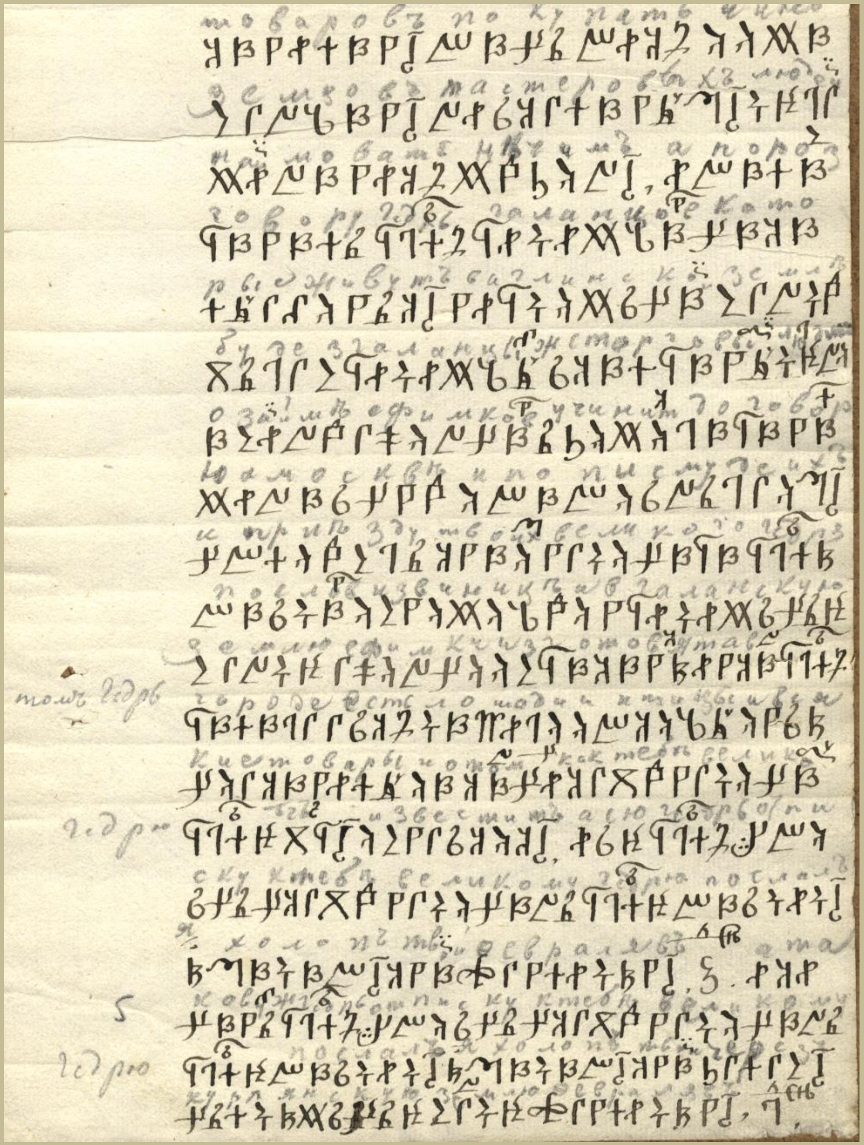


Fig.8. Ending of the letter by Yury Nikiforov

It can be assumed that the ambassadorial reports played a certain role in the decisions of the Moscow government.

Encrypted correspondence of the Department of Secret Affairs. First of all, dozens of boyars holding important posts, as well as the most important departments, had an encrypted connection with the Department of Secret Affairs. In addition to them, there were dozens of people of lower ranks, who carried out important royal assignments. This is confirmed by the remained documents of the order.

Diplomatic cryptography usually came to the ambassador's Department, but the same questions were raised in secret correspondence, which passed through the Department of Secret Affairs, if the Tsar gave them especially important significance. There were many cases when messengers delivered means of secret correspondence to members of negotiating delegations, who enjoyed the special trust of the sovereign for personal communication with him. In correspondence, the Department of Secret Affairs did not substitute other orders. The inviolability of competence in military matters of the Discharge Department, which was actually the General Staff, was emphasized by Alexei Mikhailovich. It could be imagined that the volume of encrypted correspondence of the discharge Department was also significant.

Interest in cryptography was maintained by Alexey Mikhailovich during all his life. In the personal papers, remained in the archive of the Department of secret affairs, encrypted lines are constantly encountered. They can even be seen in the hook records of notes and excerpts from prayers. One such passage is shown on **Fig. 9**

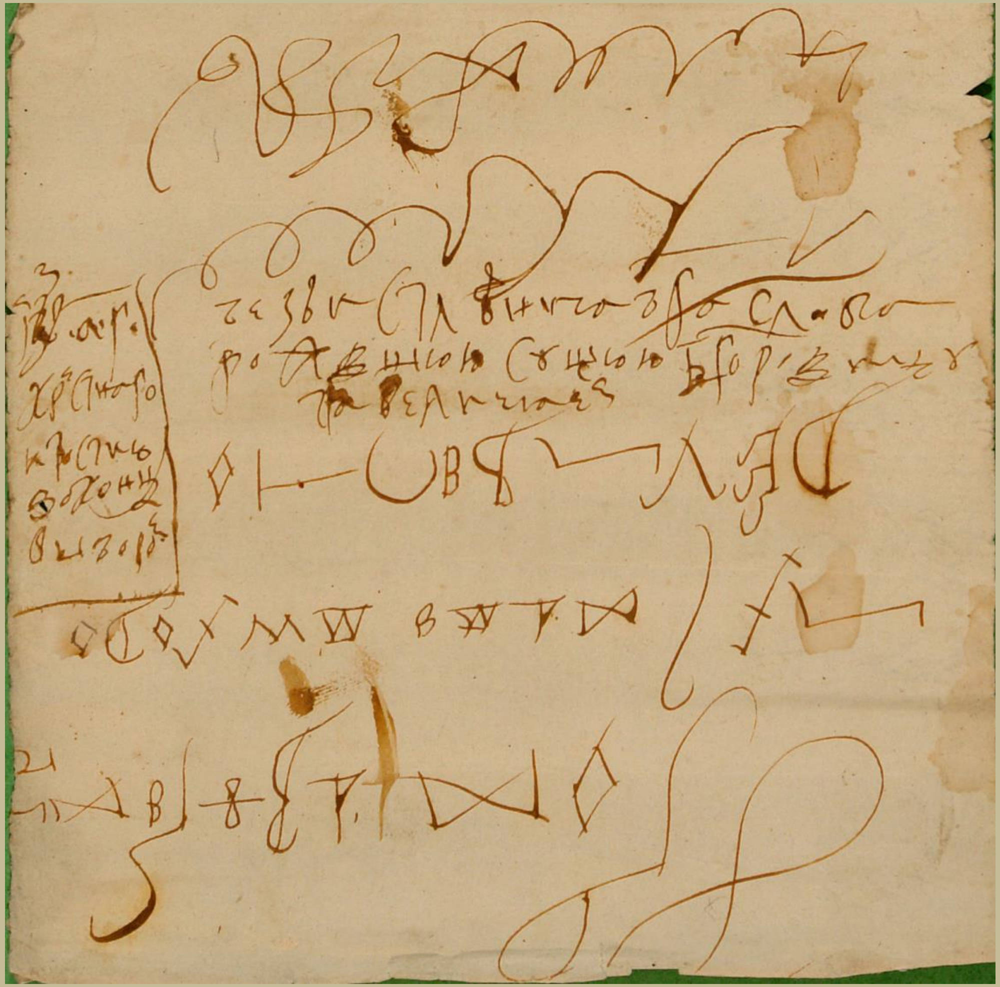


Fig. 9 Ending of the everyday notes of Aleksei Mikhailovich

Cryptographic activity in Russia in 1655-1676. During the reign of Alexei Mikhailovich, there were no orders connected with the activity of the cryptographic service as a formal institution. Although the actual cryptographic activity at the time showed that there was a special cryptographic service. It is possible to give a schematic description of this informal service, relying on information on the encryption records management. One can also specify the leaders and organizers of cryptographic activity, which should be ranked as officers of the cryptographic service.

Structural organization of cryptographic records management. Probably, in 1655-1676 the cryptographic records management system consisted of two main parts and several smaller ones. The main parts are in the Posolsky Department and in the Department of Secret Affairs. The others were part of the government (boyar Duma) and other important departments. At least in Razryadny, the main of military department; In the Local one, that was in charge of locating and contenting the service population throughout the country; In the Petchatny one, the main legal body; In the Strelets' department, who was in charge of the tsar's guard.

E. R. Yuryev, embassy clerk, was probably the coordinator of the work of the two main parts of the cryptographic service, and D. M. Bashmakov, the Duma clerk, also the tsar's secretary, supervised the entire service.

Documents to be encrypted. Diplomatic documentation. Tsar's correspondence, including correspondence with his family members. Correspondence concerning national importance. A part of the current documents of departments, including economic orders.

The nature and scope of the use of cryptography in letters was very different. There were letters entirely encrypted; and those where cryptography made up only 2-3 lines. Sometimes separate words were encrypted.

By the beginning of the 1670s, apparently, a certain standard of using encryption in diplomatic correspondence had been worked out. This can be seen from the letters of Colonel Tyapkin, a tsar’s spokesman in Poland. In his messages, standard turns (e.g. “it was decided” and others) are not encrypted, only important information is classified.

The volume of encrypted correspondence was probably very large. There are reports that have been saved containing 300-400 encrypted words. And an order that had been given to Y. Nikiforov, officer of the Department of secret affairs, about what to talk to A.L. Ordin-Nashchokin, contained about 700 encrypted words.

Cryptographic means. Cryptographic means of the Moscow cryptographers of the second half of the 17th century are ciphers of simple or multiciphered substitution. They used mainly symbolic alphabets.

Under V. V. Golitsyn, head of the Posolsky Department, the volume of correspondence, including encrypted one, with foreign representatives of Russia has grown significantly. Sometimes those were volumes of considerable size. For example, P.V. Voznitsyn's collection of resident letters in

Poland consists of 766 pages, including 95 pages with encrypted text. The diplomat sent his letters to Moscow weekly, from February 1688 to May 1689. The key is the same as that of Tyapkin.

"The original notes in figures with the translations of the former resident Ivan Volkov in Poland" include 668 pages of encrypted text sent to Moscow from April 1689 to December 1691. During this time, the key changed twice. Cipher symbols are basically the same as in Tyapkin's key, but with a new meaning.

The volume of reports of the resident in Poland Boris Mikhailov has a volume of more than 2500 pages, of which 521 pages contain encrypted text. About 300 pages consist entirely of encrypted text. The original key is the same as that of Tyapkin and Voznitsyn. For five years, the key has changed two times. All three ciphers are iconic, simple substitutions.

On the normative documents of the pre-Petrine time. The creation of the cryptographic service was not carried out apart; at the same time the state administration apparatus and other special services - counterintelligence and intelligence services, border guards were formed. Much, done in this regard, is connected with Patriarch Filaret. Of course, one would like to see the relevant legal acts and regulatory documents. This is the habit of people of our time, but it was not always like that. In the opinion of S.O. Schmidt: "In the period before the broadcast state reforms of the early 18th century and the numerous decrees and written decrees of Peter I following them, many innovations for a long time were not officially fixed and, having become established as a convenient custom, only later they acquired the status of a law and received an appropriate justification, and not always, by the way. This observation extends even to the history of the most important institutions".

A striking example, confirming the words of S.O. Schmidt, is the history of the creation of the Posolsky Department. The problem of determining the time for creating an order was solved at the beginning of the 20th century. The source for the date selection was the entry, marked February 10, 1549. It stated: "The embassy is ordered to Ivan Viskovatoy".

On this record, the date of the creation of the Ambassadorial Department was based. Nothing more significant than the above record could not be found. S.A. Belokurov, the author of the proposed date, wrote at the beginning of the 20th century: "Nowhere has there been any act on the establishment of the Posolsky Department, and nor the duty of the embassy officer and the terms of reference of the Posolsky Department".

About the time of the birth of the cryptographic service of Russia. The foregoing can be attributed to the instruction by Patriarch Filaret on August 8, 1633, connected with cryptographic activity. It is to be noted that it also includes an order and a responsible person. At the same time, there were the characteristic features of the normative document of our time in the instruction of Patriarch Filaret, and it looks more important than that of 1549. The order was reinforced by administrative measures, in particular, the preparation of a manual on cryptography, the training of cryptographers, and special registration of cryptographic documents.

Although there is no formal institution responsible then for cryptographic activity, the achieved results indicate a special service existed at the time. It is necessary to specify, first of all, the established encryption and decryption work, which includes both perusal and special clandestine records management. Detailed study of documents regulating the work with ciphers indicates the availability of personnel engaged in such activities, and their qualifications.

Therefore, it seems that August 8, 1633 can be regarded as a reasonable choice of birth of the cryptographic service of Russia.