Mihailo Petrović ALAS

Life Work Times

Serbian Academy of Sciences and Arts

MIHAILO PETROVIĆ ALAS 150th birth anniversary

MIHAILO PETROVIĆ ALAS
150th
birth anniversary

SERBIAN ACADEMY OF SCIENCES AND ARTS

MIHAILO PETROVIĆ ALAS: LIFE, WORK, TIMES
ON THE OCCASION OF THE 150th ANNIVERSARY OF HIS BIRTH

Publisher
Serbian Academy of Sciences and Arts
Knez Mihailova 35, Belgrade

Acting publisher
Academician Vladimir S. Kostić

Editor-in-chief
Academician Marko Anđelković

Editors of publication
Academician Stevan Pilipović
Academician Gradimir V. Milovanović
Professor Dr Žarko Mijajlović

Cover design
Dragana Lacmanović-Lekić

Prepress
Dosije Studio, Belgrade

Selection of artworks
Maja Novaković

English translation
Tatjana Ćosović, Natalija Stepanović
Tanja Ružin Ivanović, Žarko Radovanov, Dora Seleši

Proofreading and editing
Jelena Mitrić

Printing
Planeta print, Belgrade

Print run: 500 copies

ISBN 978-86-7025-818-1

The publication was financially supported by the Ministry of Education, Science and Technological Development of the Republic of Serbia and Telekom Srbija.

MIHAILO PETROVIĆ ALAS
LIFE, WORK, TIMES

ON THE OCCASION OF THE 150th ANNIVERSARY OF HIS BIRTH

SERBIAN ACADEMY OF SCIENCES AND ARTS

Exclusive editions, such as this monograph, call for the engagement, enthusiasm and cooperation of a number of individuals and institutions. We would like to use this opportunity and extend our gratitude to everyone who has taken part or in any way contributed to, or supported the creation and publication of this monograph.

First of all, we would like to express our gratitude to the authors of papers for their effort taken to provide expert and high level insights into some main points of Mihailo Petrović Alas' life and work, at the same time preserving an important aspect of being easy to read and appealing to a broader readership. In addition, we would like to thank to Ms. Snežana Krstić-Bukarica and Ms. Nevena Đurđević from SASA Publishing Section for performing a thorough proofread of the papers, thus making the writing even more articulate.

The monograph features a number of photographs and the copies of documents that have been obtained owing to the kindness of the SASA Archive, SASA Library, SASA Mathematical Institute, Archive of Serbia, Mr. Viktor Lazić from the "Adligat" Society, Mr. Jovan Hans Ivanović and his "Mihailo Petrović Alas" Foundation, "Mihailo Petrović Alas" Primary School, "Svetozar Marković" University Library, Belgrade City Museum, Zavod za udžbenike (Institute for Textbook Publishing) in Belgrade, Virtual Library of Faculty of Mathematics in Belgrade and Digital Legacy of Mihailo Petrović Alas.

The publication of the monograph was financially supported by JP Srbijagas, the Ministry of Education, Science and Technological Development, primarily through scientific projects in which the majority of the authors of the papers takes part, and Telekom Srbija. We would like to express our deep gratitude for their support.

Finally, we would like to express our gratitude to Mr. Mirko Milićević from the publishing house "Dosije Studio" for excellent prepress preparation of the monograph.

S. Pilipović, G. Milovanović, Ž. Mijajlović

CONTENTS

EDITOR'S FOREWORD

As soon as one first encounters the work of Mihailo Petrović, it becomes evident that he was a person that according to its numerous traits was a polymath. Above all, the academician Petrović was a gifted mathematician and a renowned professor at the University of Belgrade, but also a fisherman, writer, philosopher, musician, world traveler and a travel writer. He earned a degree in mathematics at the Belgrade Grand School and a licentiate degree in mathematics, physics and chemistry at the Sorbonne. At the age of 26, only a year after he had completed his studies, he defended his PhD degree in mathematics at the same university, as a student of the famous French mathematicians Henri Poincaré, Charles Hermite and Charles Émile Picard. In the same year (1894) he was elected to the position of professor at the Grand School to which he brought the spirit of the French mathematical school. It was at that point that his long and prolific journey through science began, whereas, owing to him, Belgrade achieved parity with other major European centers in mathematical sciences. He became an initiator and a leader of the Serbian mathematics and strongly contributed to the spirit of the modern European science in Serbia.

Petrović's expertize spanned several mathematical areas in which he achieved scientific results of world-class relevance: differential equations, numerical analysis, theory of functions of a complex variable and geometry of polynomials. He was also interested in natural sciences, chemistry, physics and biology, and he published scientific papers in these fields, too. In his scientific endeavor he managed to meet the most rigorous standards of the most developed European countries. In a brilliant rise, in a few years' time, up to the early 20th century, he wrote around thirty papers that he published in the leading European mathematical journals. It was due to this fact that he was elected a member of the Serbian Royal Academy as early as at the age of 30, and soon after he became a member of a number of foreign academies and prominent expert societies. He won the greatest respect of the global mathematical community: he was among few mathematicians (13) who delivered at least five plenary lectures or lectures as a visiting lecturer at the International Congress of Mathematicians (ICM). He delivered five such lectures (1908, 1912, 1924, 1928 and 1932). One such invitation has been considered by the mathematical community as an equivalent of an induction to a hall of fame. In addition, it has been considered that Petrović was a founder of new scientific disciplines, namely mathematical phenomenology and spectral theory. He invented several analogue computing machines, possessed technical patents and was the main cryptographer of the Serbian and Yugoslav Army.

Up to the Second World War he was the mentor of all doctoral thesis in mathematics defended at the University of Belgrade. Aforementioned is related to one of professor Petrović's greatest and most important achievements – he was a founder of the Serbian mathematical school that has produced a great number of renowned and successful mathematicians not only in Serbia but also around the world.

In 2018, the Serbian Academy of Sciences and Arts and mathematicians in Serbia celebrate the 150th anniversary of the birth of Mihailo Petrović Alas. Throughout this year, the Academy has organized a large exhibition dedicated to Petrović, alongside a solemn gathering and a conference. This monograph commemorates this important jubilee of the Serbian mathematics. Given the fact that a lot of articles on Petrović have already been written, and that his collected works were published at the end of the last century, the editors and authors of the papers in this monograph were faced with a daunting task of finding some new details from professor Petrović's life and career. Even more so given that his body of work is immense, spanning different scientific areas and encompassing topics that at first glance one finds difficult to combine. As Dragan Trifunović, Petrović's biographer and a man who most thoroughly studied his life and work, noted on one occasion that almost an institute was necessary that would encompass professor's entire body of work. Therefore, we set a relatively modest goal to ourselves to shed light upon some main points of Petrović's life and work, times and circumstances he lived in, as well as to elaborate on the present developments in relation to the Serbian mathematical school, through a selection of papers. The authors of the papers steered clear of technical details and excessive use of mathematical language. Hence, the monograph is intended for a broader readership, in particular to those readers who are interested in the history of Serbian science and its evolvement at the turn of the 20th century, but also to those who want to gain a deeper insight into the life of a brilliant mathematician and a polymath, and, we can quite freely say, an unusual personality.

Ž. Mijajlović, S. Pilipović, G. Milovanović

MIHAILO PETROVIĆ ALAS: LIFE AND WORK

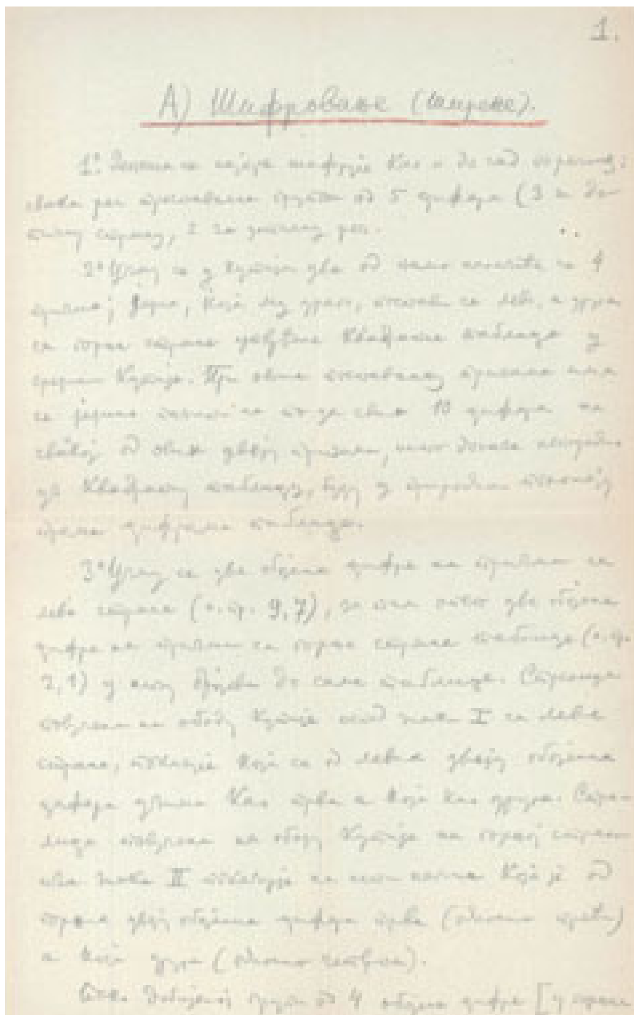
MIHAILO PETROVIĆ ALAS AND THE STATE CRYPTOGRAPHY OF THE INTERWAR PERIOD

Miodrag J. MIHALJEVIĆ
Mathematical Institute of SASA

History acknowledges, and owing to the increasing significance of the field in which he left his mark, history is to place an ever-greater emphasis on the work of Mihailo Petrović Alas in the domain of state cryptography in the period between the two world wars. The results of Petrović's work in the field of cryptography have not stayed on public records, which is not surprising given that research findings in cryptography were in the interwar years classified as military and state secrets. The available documents taken from the Serbian Armed Forces General Staff and the Ministry of the Army and Navy, dating from the period prior to World War II, show that, from the perspective of the general horizon of knowledge at the time, Mihailo Petrović made significant breakthroughs in the design and analysis of coding systems, as well as in the training of staff that operated in the area of cryptography for the purposes of the state.

Petrović's accomplishments in the field of cryptography and coding have been documented in the 15 volumes of the Cipher Bureau of the Intelligence Unit of the Armed Forces General Staff of the Kingdom of Yugoslavia, under the title *Kriptografija – škola za obuku na šifri (Cryptography: Code School),* and in 24 volumes under the title *Sistem (za šifrovanje) (Coding System)*. Based on those documents, the work of Petrović and the ensuing results can be found in the following areas: (a) the methods for encryption; (b) the methods for "breaking" the codes, and (c) educational materials related to the techniques for enciphering and deciphering the encrypted messages.

The basic aim of this chapter is to present the illustrative elements of the source documents accompanied by appropriate commentary. It should especially be noted that an evaluation of cryptographic security of the presented coding systems from modern perspective does not represent the subject of this chapter, because history has shown that nearly all coding systems in operational use prior to World War II are now completely insecure. This fact represents an outcome of the accumulation of knowledge about the techniques that can be used for deciphering the coding systems, as well as of the now available state-of-the-art technological resources.


1.

A) Шифровање (шифре).

Mihailo Petrović's manuscript on encryption (“Adligat” Society)

CODING IN THE PRESENT DAY AND IN THE INTERWAR PERIOD

Our present-day reality represents leading a "parallel life" in real and digital space, which we use for communication and which contains information of vital importance for our daily life. In the digital space there are no boundaries that separate us one from another and, in order to ensure security and privacy, cipher techniques have been used on a massive scale. The widespread use of ciphers is one of the features that differentiate the present-day coding from that of the time when Mihailo Petrović was concerned with it. Modern cipher techniques are "a product of cryptology", a mathematics-based scientific discipline: in his time, cryptology had not yet existed as a distinct scientific discipline – the emergence of cryptology as a scientific discipline is tied to reference [1]. Since the mid-twentieth century, cryptology has been established and intensively developed as a foundation for ensuring security and privacy in the digital space, in which the encryption techniques represent one of the key elements. It now includes a set of other elements that are generally classified either within the domain of cryptography or within cryptanalysis. Plainly speaking, cryptography deals with techniques for protection, while cryptanalysis is concerned with techniques for the evaluation of the security of protection or with techniques for "breaking" the cryptographic protection.

A century ago, coding was not developed within a separate scientific discipline, but either as "a specific craft" or, as in Petrović's case, as "coding designed by a mathematician".

Cryptography, which once, including his time, was associated only with encryption, has been developed for over two millennia as a skill that enables the protection of secrecy of information, and it is now one of the fundamental approaches for ensuring the security and privacy in the digital space. Over the centuries, a great number of methods have been developed for providing cryptographic protection or coding. Up until the 1950's, coding was based on a combination of skillfulness and mathematical methods.

The present-day cryptology is based on the pool of knowledge compared to which the one that served as the basis for the design and analytical methods of coding in the 1930's had been modest to say the least, and thus could not provide the basis for the design characterized by a long-lasting and high-level security. Of this Petrović was well aware: in the introduction to cryptography contained in the volumes in reference [3], he points to the fact that all encryption techniques used in World War I appeared to be insecure, and that it is believed to be necessary to frequently modify the methods of encryption in operational use. This can be exemplified by the following original text from the notebook *Cryptography: Basic Concepts* [reference 3]:

However, few are those who managed to keep the secret of their code intact for long.

It is firmly established that, during the last World War, no method, mode or system of secret correspondence could have been used over a longer period of time.

ALGORITHMS FOR ENCRYPTION

The documents that were at our disposal indicate that the Ministry of the Army and Navy of the Kingdom of Yugoslavia used at least 24 systems for encryption labeled as “System” followed by one of the ensuing numbers: 1, 1a, 2, 2a, 3, 3a, 4, 4a, 5, 6, 6a, 7, 7a, 8, 9, 10, 10a, 11, 12, 13, 14, 15, 16, 17, 18.

The application of the said systems had the following basic requirements: (a) a trained cryptographer, (b) written instructions for work, and (c) only in some cases, certain mechanical devices. The result was to be written on paper and further communicated in the prescribed way, most frequently by telegraph or courier.

If it was included in the system, the basic device used for enciphering was the so-called cipher slide (French *reglette*) – the cited information concerning the slide is presented in the following three figures.

> The cipher slide in question is in its simplest form such that it contains **two fixed well-ordered or jumbled-up letters of the alphabet on a piece of wooden bar**, one on top of another, or only at the top or at the bottom, and in the middle a little movable ruler sliding along the bar, with another set of normal or jumbled-up alphabet. The alphabet lists have to be duplicated on the fixed bar, as well as on the movable ruler.
>
> The alphabet lists have to be duplicated on the fixed bar, as well as on the movable ruler.

Figure 1: Basic information on the module, Notebook 12, reference [3]

Figure 2: Image of the module, Notebook 12, reference [3]

Volume 12, reference [3] presents the mode of usage of the cipher slide:

> **M E T H O D**
>
> **OF ENCRYPTING AND DECRYPTING BY USING SPECIAL DEVICES**
>
> A) **Usage of the cipher slide:**
>
> In this volume we are going to introduce a special method of encryption – called a Saint-Cyr method, which in essence is nothing else than a mechanical application of Vigenère’s method in the specified manner.
>
> Moreover, this method also involves complex substitution

From Notebook 12, reference [3]

Starting from the then known methods for compromising (breaking) the methods of encryption, and in order to obtain a higher level of security, the document in Volume 10, reference [3] presents the technique of "double transposition". An essential explanation of the double transposition is given in the following figure.

> Овде ћемо изнети још теже случајеве, јер је у питању не само шифровање јасног текста већ и прешифравање т. ј. једанпут добијена шифра има се још једанпут шифровати.
>
> Овакви системи шифровања могу се назвати још и **шифровање системом дуплог замењивања по таблици**, који може бити са истим или новим кључем.
>
> Другим речима, ако један јасан текст шифрујемо по једном кључу, ми добијену шифру прешифравамо, било тим истим – првобитним кључем или другим новим кључем. Разуме се да је овај други начин много тежи и компликованији.

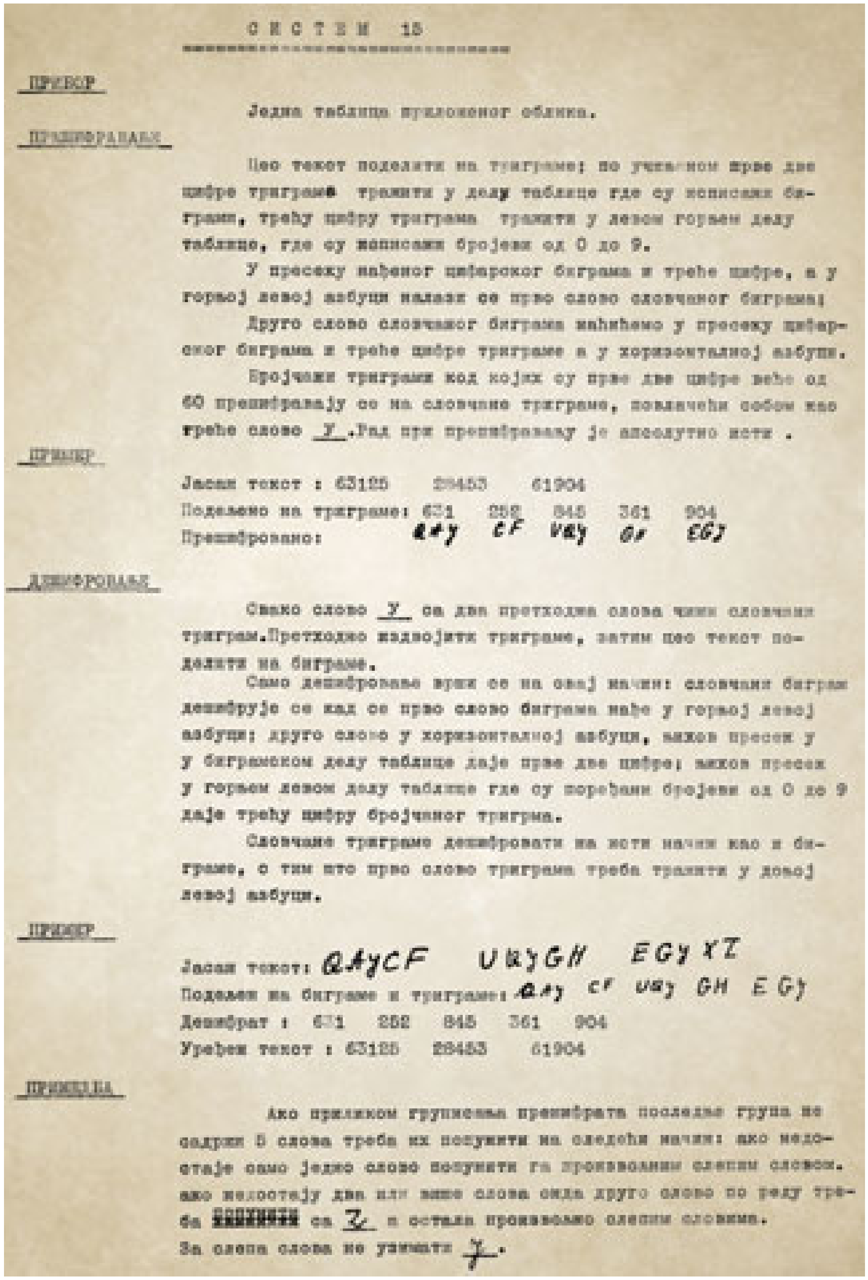
Figure 3: Encryption in accordance with Notebook 10, reference [3]

System 15, reference [2] presents double transposition realized according to the following paradigm:

- by using the chosen cipher algorithm make the first cipher text based on the plain text;
- encrypt the cipher text one more time, in general, using another cipher algorithm.

It is noted that the said approach of improving cryptographic security by iterative encryption represents the basic principle of building the modern block cipher procedures, in which the cipher text is made by repeated encryption using the basic cipher transposition of low-level cryptographic security, thereby providing a high-level cryptographic security after a certain number of iterations.

System 15, in its original form, in compliance with the one given in reference [2], is presented in the following two figures:



СИСТЕМ 15

ПРИБОР

Једна таблица приложеног облика.

ПРЕШИФРОВАЊЕ

Цео текст поделити на триграме; по учињеном прве две цифре триграма тражити у делу таблице где су исписани биграми, трећу цифру триграма тражити у левом горњем делу таблице, где су исписани бројеви од 0 до 9.

У пресеку нађеног цифарског биграма и треће цифре, а у горњој левој азбуци налази се прво слово словчаног биграма;

Друго слово словчаног биграма наћићемо у пресеку цифарског биграма и треће цифре триграме а у хоризонталној азбуци.

Бројчани триграми код којих су прве две цифре веће од 60 прешифрирају се на словчане триграме, повлачећи собом као треће слово У. Рад при прешифровању је апсолутно исти.

ПРИМЕР

Јасан текст : 63125 28453 61904
Подељено на триграме: 631 252 845 361 904
Прешифровано: QAy CF URy G# EGy

ДЕШИФРОВАЊЕ

Свако слово У са два претходна слова чини словчани триграм. Претходно издвојити триграме, затим цео текст поделити на биграме.

Само дешифровање врши се на овај начин: словчани биграм дешифрује се кад се прво слово биграма нађе у горњој левој азбуци; друго слово у хоризонталној азбуци, њихов пресек у у биграмском делу таблице даје прве две цифре; њихов пресек у горњем левом делу таблице где су поређани бројеви од 0 до 9 даје трећу цифру бројчаног триграма.

Словчане триграме дешифровати на исти начин као и биграме, с тим што прво слово триграма треба тражити у доњој левој азбуци.

ПРИМЕР

Јасан текст: QAyCF URyGH EGyXZ
Подељен на биграме и триграме: QAy CF URy GH EGy
Дешифрат : 631 252 845 361 904
Уређен текст : 63125 28453 61904

ПРИМЕДБА

Ако приликом груписања прешифрата последња група не садржи 5 слова треба их попунити на следећи начин: ако недостаје само једно слово попунити га произвољним слепим словом. ако недостају два или више слова онда друго слово по реду треба попунити са Z а остала произвољно слепим словима.
За слепа слова не узимати У.

Figure 4: Encryption system no. 15, reference [2]

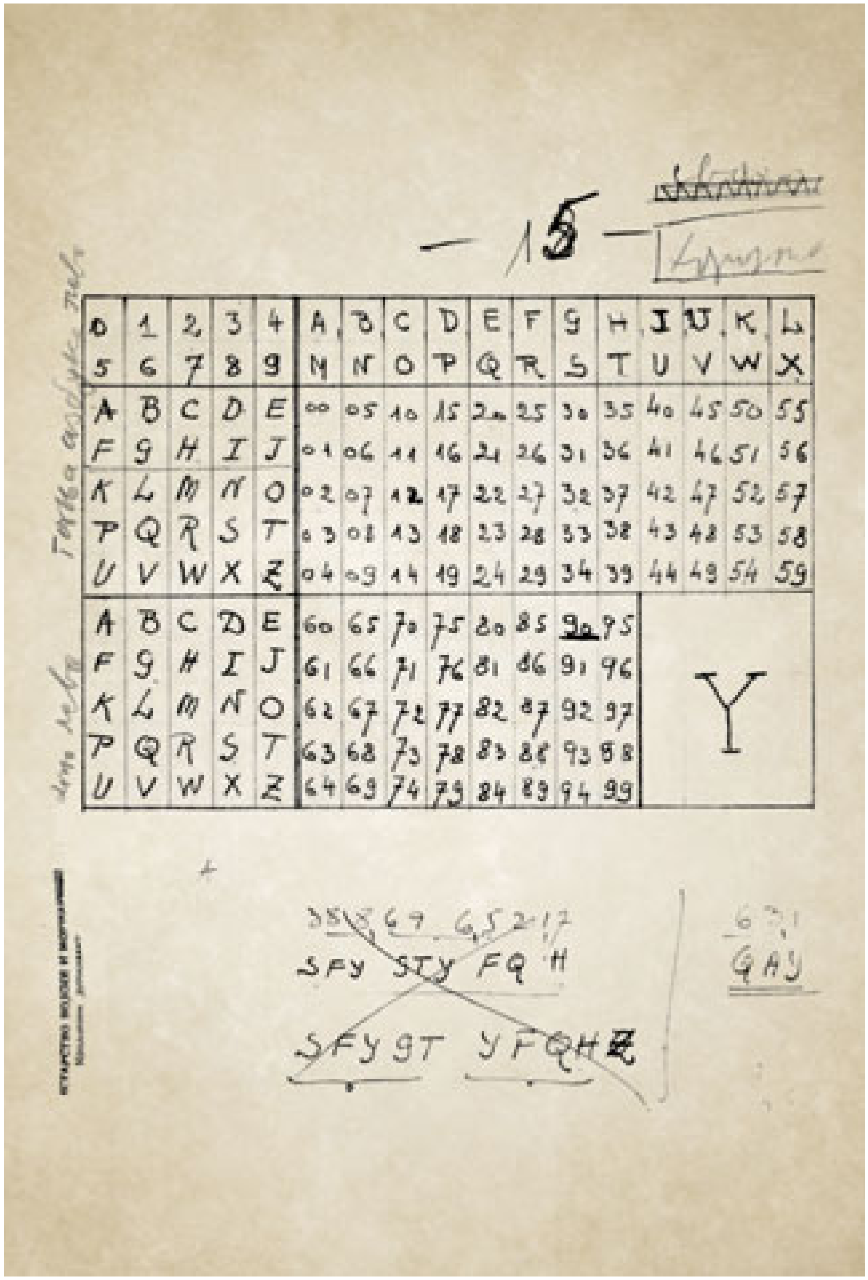


Figure 5: The table used in System no. 15, reference [2]

As the final illustration, the following figure shows coding system 18 in its original form.

С И С Т Е М 18

ПРИБОР

Једна таблица приложеног облика. Таблица је израђена за речник до 60.000 речи, чије стране прелазе преко цифре 600.

ПРЕШИФРАВАЊЕ

Свака прва цифра петоцифреног група са две претходне и две следеће цифре чине триграм.

Само шресифравање врши се на следећи начин: Биграми у сваком триграму, који са првом цифром сваког петоцифреног група, чине триграме траже се у делу таблице у којој су исписани бројчани биграми, слободна цифра сваког триграма налази се у горњем левом делу таблице где су исписани бројеви од 0 до 5.

Прво слово триграмског прешифрата налазимо у пресеку биграма и слободне цифре, а у вертикалној азбуци.

Друго слово наћићемо у хоризонталној азбуци у пресеку биграма и слободне цифре из дотичног цифарског триграма.

ПРИМЕР

Јасан текст: 49382 54831 23492

Прешифрат: Nу JX VV TB TE Uъ

ДЕШИФРОВАЊЕ

Текст поделити на групе од 4 слова. Свакој таквој цифри групи одговара један петоцифрени груп, који добијамо на тај начин што први словчани биграм дешифрујемо на цифрени триграм, а други словчани биграм на бројчани биграм.

Само дешифровање врши се на тај начин што се прво слово нађе у вертикалној азбуци, друго у хоризонталној азбуци, њихови пресеци у делу таблице где су исписани бројчани монограми даје нам прву цифру, а пресеци где су исписани биграми дају нам друге две цифре триграма. Други словчани биграм дешифрује се на исти начин али се у њему узимају само цифре биграма које се нађу у делу таблице где су исписани биграми

ПРИМЕР

Nу JX VY TB TE Uъ

Дешифрат : 49382 54831 23492

Примедба

Последње две цифре које остају заменити их одговарајућим словима из вертикалне и хоризонталне азбуке произвољно

Figure 6: Encryption system no. 18, reference [2], which was used in its improved form in Yugoslavia and for some time after the World War II

ANALYSIS OF THE CRYPTOGRAPHIC SECURITY OF CIPHER ALGORITHMS

The documentation at the Armed Forces General Staff contains information about knowing a set of steps for breaking some, then well-known, coding procedures. The knowledge about those procedures served as the starting point for the design of the coding system resistant to then known attacks.

Volume 10, reference [3] presents an approach to the analysis of the safety of cipher algorithms of "complex transposition with repeated encryption":

> Да нисмо знали кључ, ми би смо га морали наћи, али би посао био много компликованији и скопчан са много више времена, јер би имали да решимо три проблема:
>
> **Први проблем:** Шифру дешифровати системима и начинима објашњеним у свесци бр. 8 и 9. И ако ово изгледа нелогично, ипак се мора приступити прво овом раду па тек онда истраживању кључа и друго. Ако имамо више шифара исте дужине, шифроване овим методом, опет је поступак исти.
>
> **Други проблем:** Добивши јасан текст, треба одредити за свако слово шифре место које оно заузима у јасном тексту, и
>
> **Трећи проблем:** Одредивши место за свако слово шифре, које оно заузима у јасном тексту, пронаћи кључ по коме је извршена замена.
>
> Овај последњи проблем дели се на два друга и то:
>
> – Одредити дужину кључа, и
>
> – Успоставити кључ онакав какав је узет.
>
> Као што видимо, посао је дуг, тежак и скопчан са много стрпљивости, педантности у раду, воље и методичности. При томе се захтева дубока студија и резоновање, јер се без тога не могу имати резултати, – а природни дар и склоност ка криптографији убрзаће темпо рада и смањити грешке, које ће се неминовно појављивати.

Figure 7: Illustration from the document Notebook no. 10, reference [3], about one of the approaches for "breaking" the code

Volume 13, reference [3], contains the following discussion regarding cryptographic security:

— 12 —

б) Када нам није позната ни реглета ни кључ већ само нека јасна реч текста

Када нам није позната ни реглета ни кључ већ само нека јасна реч текста, у том случају је дешифровање тешко и доста компликовано, али ипак приступачно.

Нека имамо шифре по слици бр. 13 — види прилог бр. 1, и нека нам је дато да се у тој шифри налази реч: „D I V I Z I J A".

У том случају наш би поступак на дешифровању ових шифара био следећи:

Претходно ћемо добро простудирати све шифре, па обзиром на распоред и склоп слова било посебних групова, било у заједници са претходећим и следујућим групама, стараћемо се да пронађемо ту дату— познату реч.

Да би се ово лакше могло урадити, потребно је све дате шифре претходно исписати у хоризонталним правцима без обзира на њихове дужине, али тако, да текстови шифара дођу један испод другог односно, да испод првог група прве шифре дођу сви први групови осталих шифара; испод другог група — сви други групови итд., јер се на тај начин добија већа и боља прегледност.

Практично ће то изгледати овако:

Испишу се шифре из слике бр. 13 (види прилог бр. 1), па се тек онда приступа студији свих седам шифара, а једновремено и сваког група понаособ са тежњом да се пронађу истоимени групови у двема или више шифара које би по свом склопу слова одговарале речи: DIVIZIJA.

Студирајући ове шифре примећујемо, да код неких групова у шифрама под бројем 4, 5 и 6 и ако не постоје истоимени групови, ипак постоји такав распоред појединих истоимених слова, која би према карактеристици речи нашег језика могла да означавају реч: „DIVIZIJA".

Тако:

Код шифре под бројем 4 имамо групове:

O M S M P L J . . .

Код шифре под бројем 5 имамо групове:

T M S M P M J

и

L C Z C V C A

Код шифре под бројем 6 имамо ове карактеристичне групове:

E V I V N V

Према броју слова ових групова као и њиховом распореду, а обзиром на конструкцију речи: „D I V I Z I J A", и њена карактеристична три слова I раздвојена са по једним сугласником, могло би се претпоставити, да горња слова ових шифара претстављају реч: „DIVIZIJA.

Групови шифре под бројем 4. и ако имају само два слова M, не треба да нас буне, јер је распоред слова при шифровању био такав, да треће слово „I" — ако би у опште овај груп претстављао реч јасног текста: „D I V I Z I J A" није ни могло бити претстављено словом шифре „M", јер је то треће слово „I" пало у други груп услед чега је и своју шифру променило.

Није згорег да овде напоменемо још и следеће:

Приликом студије шифара сликеб р. 13 — прил огбр. 1, морало нам је пасти у очи још нешто врло маркантно а то је, да код шифара под бр. 4. и 5. наилазимо на ред слова која су потпуно идентична. То су слова седмог, осмог и деветог група то јест, истоимени групови и делови групова:

P P D T N S U K S D . . . .

Figure 8: Illustration of the analysis of encryption safety given in Notebook no. 13, reference [3]

CONTRIBUTIONS TO THE EDUCATION IN CRYPTOGRAPHIC WORK

As noted in section 3, using a coding system required a trained cryptographer and to that end an educational programme was set up for the training in cryptographic work.

Within the programme the focus was not only on introducing the techniques for encryption known at the time, but much attention was also devoted to education in the domain of evaluation of cryptographic security and the methods for compromising it. It is specially noted that in educational documents, reference [3], the volume of text referring to techniques for "attacking" the observed coding system usually far exceeds the volume of text dedicated to the description and usage of the observed coding system.

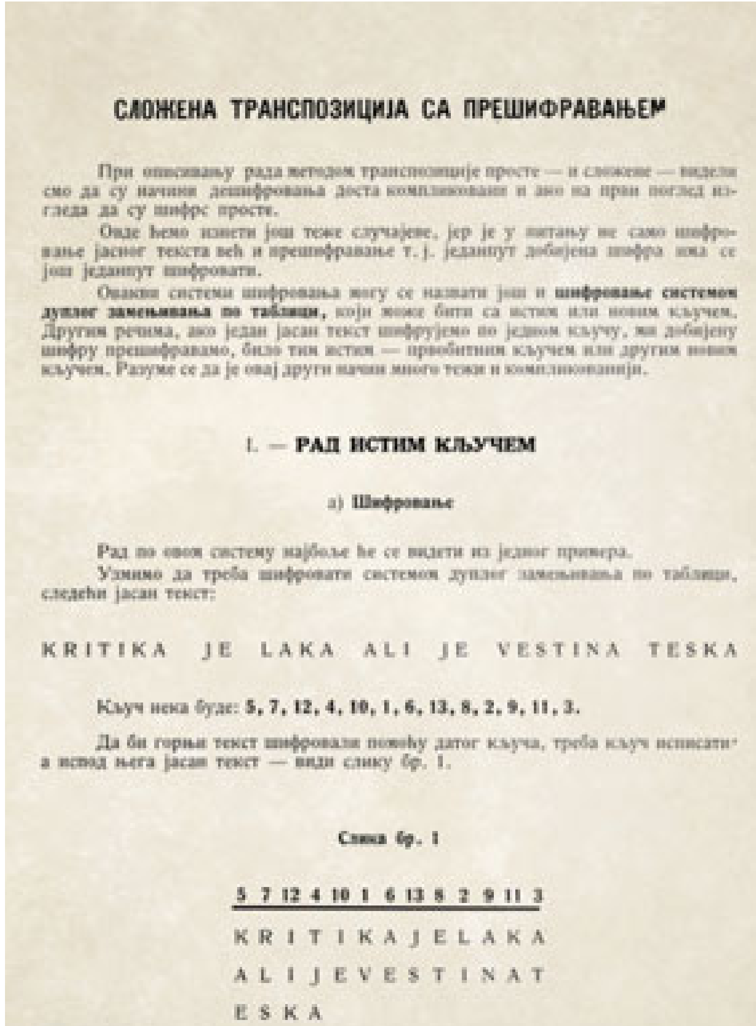
In this section we are going to present some illustrative examples of educational materials for working in the field of cryptography, as well as for techniques for breaking certain codes.

In accordance with all that was previously said, from among the volumes in the series *Cryptography: Code School,* the following is presented as illustrative material:

- Volume: *Basic Concepts*;
- Volume 10: *Complex Transposition with Double Encryption*;
- Volume 14: *An Introduction to the Methods of Encryption Using Key – Dictionary of Secret Correspondence*.

> The invention of secret correspondence is anything but new. Cryptography has its origin from the ancient times, the only difference being that those former methods, systems and modes of usage were completely different from the current ones.
>
> Cryptography, or secret correspondence, is derived from the Greek word *kryptos*, meaning "to hide", and *-graphy*, meaning "to write".
>
> Cryptography or secret correspondence is in its essence, its purpose, and its main objective, a very sensitive and delicate subject.
>
> Sensitive – because the precision of work must be absolutely and fully guaranteed, and delicate, because the very content it conveys is of the most confidential nature, whose disclosure in most cases may have grave and fatal consequences. Greatest care must be taken of the organization, work and secrecy of such correspondence.
>
> Secret correspondence is regularly used by military institutions in times of peace and war alike.
>
> Diplomatic representatives must daily report to their government about the particularly important and confidential matters they found out in the states they are accredited in, which they regularly do by using a secret or code name.

Figure 9: Content illustration of "Cryptography – general terms" notebook, from the School for Encryption Training, reference [3]



СЛОЖЕНА ТРАНСПОЗИЦИЈА СА ПРЕШИФРАВАЊЕМ

При описивању рада методом транспозиције просте — и сложене — видели смо да су начини дешифровања доста компликовани и ако на први поглед изгледа да су шифре просте.

Овде ћемо изнети још теже случајеве, јер је у питању не само шифровање јасног текста већ и прешифровање т. ј. једанпут добијена шифра има се још једанпут шифровати.

Овакви системи шифровања могу се назвати још и **шифровање системом дуплог замењивања по таблици,** који може бити са истим или новим кључем. Другим речима, ако један јасан текст шифрујемо по једном кључу, ми добијену шифру прешифравамо, било тим истим — првобитним кључем или другим новим кључем. Разуме се да је овај други начин много тежи и компликованији.

I. — **РАД ИСТИМ КЉУЧЕМ**

а) **Шифровање**

Рад по овом систему најбоље ће се видети из једног примера.

Узмимо да треба шифровати системом дуплог замењивања по таблици, следећи јасан текст:

K R I T I K A J E L A K A A L I J E V E S T I N A T E S K A

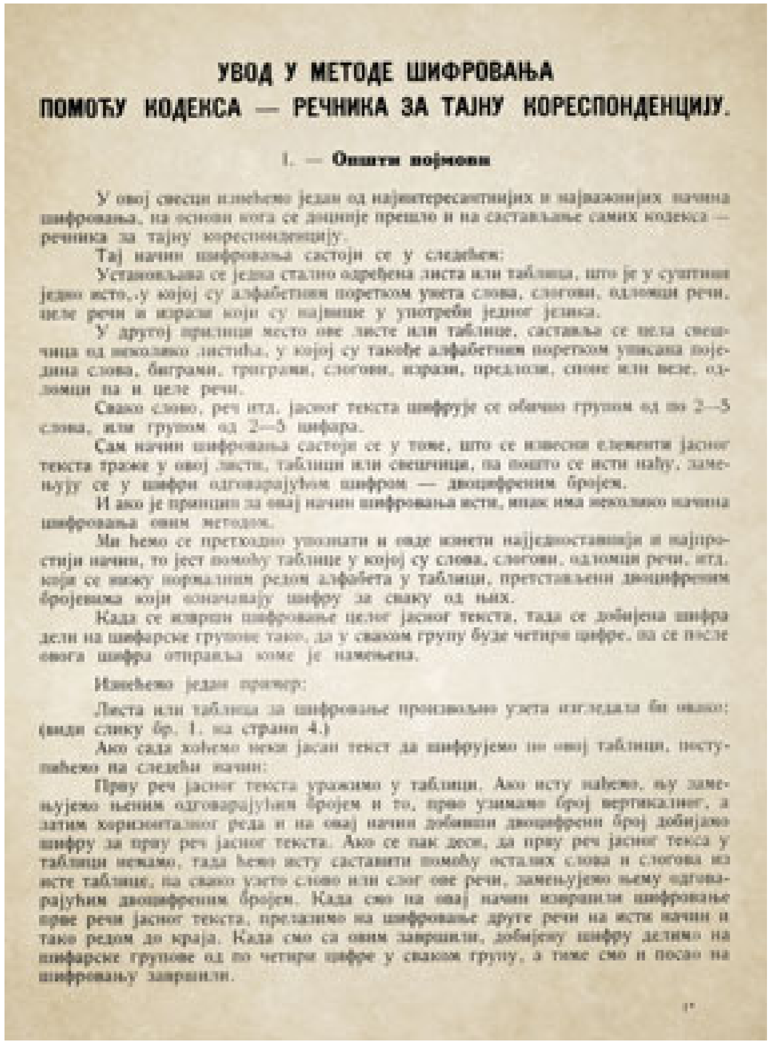
Кључ нека буде: **5, 7, 12, 4, 10, 1, 6, 13, 8, 2, 9, 11, 3.**

Да би горњи текст шифровали помоћу датог кључа, треба кључ исписати а испод њега јасан текст — види слику бр. 1.

Слика бр. 1

5	7	12	4	10	1	6	13	8	2	9	11	3
K	R	I	T	I	K	A	J	E	L	A	K	A
A	L	I	J	E	V	E	S	T	I	N	A	T
E	S	K	A									

Figure 10: Content illustration of Notebook no. 10, from School for Encryption Training, reference [3]



УВОД У МЕТОДЕ ШИФРОВАЊА
ПОМОЋУ КОДЕКСА — РЕЧНИКА ЗА ТАЈНУ КОРЕСПОНДЕНЦИЈУ.

1. — Општи појмови

У овој свесци изнећемо један од најинтересантнијих и најважнијих начина шифровања, на основи кога се доцније прешло и на састављање самих кодекса — речника за тајну кореспонденцију.

Тај начин шифровања састоји се у следећем:

Установљава се једна стално одређена листа или таблица, што је у суштини једно исто, у којој су алфабетним поретком унета слова, слогови, одломци речи, целе речи и изрази који су највише у употреби једног језика.

У другој прилици место ове листе или таблице, саставља се цела свешчица од неколико листића, у којој су такође алфабетним поретком уписана појединачна слова, биграми, триграми, слогови, изрази, предлози, спојне или везе, одломци па и целе речи.

Свако слово, реч итд. јасног текста шифрује се обично групом од по 2—5 слова, или групом од 2—5 шифара.

Сам начин шифровања састоји се у томе, што се извесни елементи јасног текста траже у овој листи, таблици или свешчици, па пошто се исти нађу, замењују се у шифри одговарајућом шифром — двоцифреним бројем.

И ако је принцип за овај начин шифровања исти, ипак има неколико начина шифровања овим методом.

Ми ћемо се претходно упознати и овде изнети најједноставнији и најпростији начин, то јест помоћу таблице у којој су слова, слогови, одломци речи, итд. који се нижу нормалним редом алфабета у таблици, претстављени двоцифреним бројевима који означавају шифру за сваку од њих.

Када се изврши шифровање целог јасног текста, тада се добијена шифра дели на шифарске групе тако, да у свакој групу буде четири цифре, па се после овога шифра отпраћа коме је намењена.

Изнећемо један пример:

Листа или таблица за шифровање произвољно узета изгледала би овако: (види слику бр. 1. на страни 4.)

Ако сада хоћемо неки јасан текст да шифрујемо по овој таблици, поступићемо на следећи начин:

Прву реч јасног текста упражимо у таблици. Ако исту нађемо, њу замењујемо њеним одговарајућим бројем и то, прво узимамо број вертикалног, а затим хоризонталног реда и на овај начин добивши двоцифрени број добијамо шифру за прву реч јасног текста. Ако се пак деси, да прву реч јасног текса у таблици немамо, тада ћемо исту саставити помоћу осталих слова и слогова из исте таблице, па свако узето слово или слог ове речи, замењујемо њему одговарајућим двоцифреним бројем. Када смо на овај начин извршили шифровање прве речи јасног текста, прелазимо на шифровање друге речи на исти начин и тако редом до краја. Када смо са овим завршили, добијену шифру делимо на шифарске групове од по четири цифре у свакој групу, а тиме смо и посао на шифровању завршили.

1*

Figure 11: Content illustration of Notebook no. 14, from School for Encryption Training, reference [3]

REFERENCES

[1] Shannon, C.E. "Communication Theory of Secrecy Systems", *Bell System Technical Journal*, 1949, 28, 656–715.

[2] Sistem (za šifrovanje). Sveske 1, 1a, 2, 2a, 3, 3a, 4, 4a, 5, 6, 6a, 7, 7a, 8, 9, 10, 10a, 11, 12, 13, 14, 15, 16, 17, 18, Ministarstvo vojske i mornarice Kraljevine Jugoslavije, (ca. 1930–1940).

[3] Kriptografija – škola za obuku na šifri, sveske 1–15, Otsek za šifru, Obaveštajno odeljenje, Đeneralštab Kraljevine Jugoslavije, (ca. 1930–1940).