СРПСКА АКАДЕМИЈА НАУКА И УМЕТНОСТИ

SERBIAN ACADEMY OF SCIENCES AND ARTS

SCIENTIFIC MEETINGS

Book CLXXXII

PRESIDENCY

Book 12

MIHAILO PETROVIĆ ALAS

REGARDING ONE HUNDRED AND FIFTY YEARS SCIENCE BIRTH

Scientific meeting with an international partake,
held at the Serbian Academy of Sciences and Arts
on October 2–3, 2018

BELGRADE 2019

СРПСКА АКАДЕМИЈА НАУКА И УМЕТНОСТИ

НАУЧНИ СКУПОВИ

Књига CLXXXII

ПРЕДСЕДНИШТВО

Књига 12

МИХАИЛО ПЕТРОВИЋ АЛАС

ПОВОДОМ СТО ПЕДЕСЕТ ГОДИНА ОД РОЂЕЊА

Научни скуп са међународним учешћем одржан
у Српској академији наука и уметности,
2–3. октобра 2018.

БЕОГРАД 2019




Уредници
академик Градимир Миловановић
академик Стеван Пилиповић
др Жарко Мијајловић

Издавачи
Српска академија наука и уметности
Београд, Кнеза Михаила 35
Математички факултет Универзитета у Београду
Београд, Студентски трг 16
Математички институт САНУ
Београд, Кнеза Михаила 36
Друштво математичара Србије
Београд, Кнеза Михаила 35/IV

Дизајн корица
Драгана Лацмановић-Лекић

Технички уредници
Александра Делић
Миљан Кнежевић
Никола Стевановић

Лектура и коректура
Весна Шубић

Штампа
Colorgrafx, Београд

Тираж
600 примерака

Подршка Министарства просвете, науке и технолошког развоја

ISBN: 978-86-7025-825-9
ISBN: 978-86-7589-136-9

Садржај

МИХАИЛО ПЕТРОВИЋ АЛАС – НАШ ВОДЕЋИ КРИПТОГРАФ ИЗМЕЂУ ДВА СВЕТСКА РАТА

РАДОМИР С. СТАНКОВИЋ*

МИОДРАГ МИХАЉЕВИЋ**

А п с т р а к т. – Шифровање је данас један од стандардних приступа за остваривање безбедности и приватности у дигиталном простору и постоји велики број експерата који се баве шифровањем како са научно-истраживачког становишта тако и у доменима великог броја различитих примена. У време Михаила Петровића Аласа, бављење шифровањем је било веома редак и веома специфичан посао, а он је истовремено био и главни научник-истраживач и главни државни саветник одговоран за шифре између два светска рата. О овом, за то време и историју, веома битном сегменту рада и достигнућа М. П. Аласа остало је релативно мало записа у форми војних докумената али који неспорно указују на велике заслуге М. П. Аласа за нашу државу у домену криптологије и пре него што је она оформљена као светска научна дисциплина [4]. Овај рад, на основу [1] – [3] и [5] – [6], сумира неке од историјских чињеница о М. П. Аласу као нашем главном криптографу између два светска рата.

У поменутим документима је забележено да су се рад М. П. Аласа и резултати овога рада налазили у: (1) методама за шифровање, (2) методама за „разбијање" шифара и (3) едукацији о техникама шифровања и разоткривању порука које су биле предмет шифровања.

Историја признаје, а због растућег значаја области у којој је оставио траг, историја ће још више истицати рад Михаила Петровића Аласа у домену државне шифре између два светска рата.

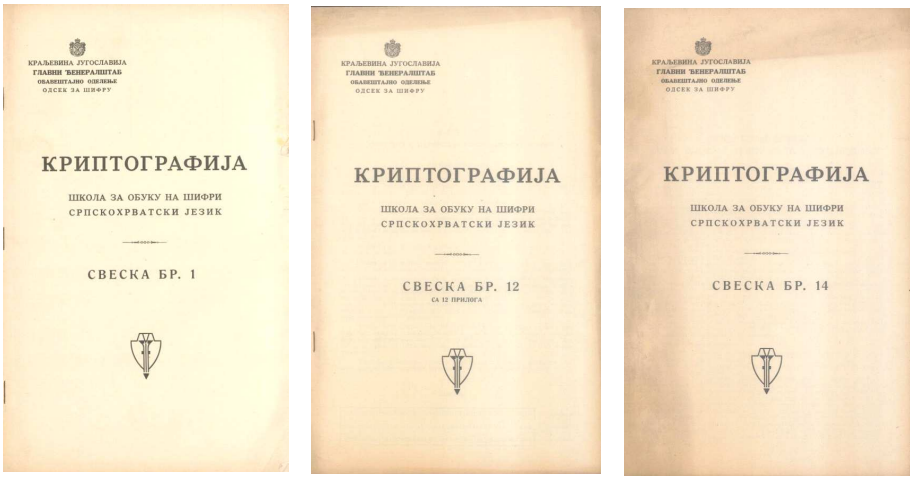
Кључне речи: заштита тајности, шифровање, криптографија

* Математички институт САНУ, и-мејл: radomir.stankovic@gmail.com

** Математички институт САНУ, и-мејл: miodragm@turing.mi.sanu.ac.rs

1. Увод

Непосредно пред Први светски рат у Краљевини Србији, за време рата, затим у Држави Срба, Хрвата и Словенаца, и касније у Краљевини Југославији, свест о потреби и значају шифровања у војној и дипломатској државној преписци била је на врло високом нивоу о чему јасно сведоче бројни документи и приручници за обуку кадрова из ове области. Слика 1 приказује корице неких од свезака посвећених криптографији а намењених обуци људства у Обавештајном одељењу Ђенералштаба Краљевине Југославије.



(*a*) (*b*) (*c*)

Слика 1. Корице докумената о криптографији – шифровању (*a*) Шифровање методом замене и анализа ових шифрата, (*b*) Метод шифровања и дешифровања помоћу нарочитих справа, (*c*) Шифровање помоћу Кодекса – Речника за тајну кореспонденцију

Имајући у виду значај оваквих послова, сасвим је природно да је на томе био ангажован Михаило Петровић као један од најобразованијих и најумнијих грађана тога доба. Радећи у овој области Михаило Петровић је остварио значајна достигнућа у

1. пројектовању и анализи шифарских система,
2. едукацији кадрова коју су оперативно радили у областима шифровања за државне потребе.

У овом раду нећемо се бавити анализом сигурности техника шифрирања коришћених у доба када је Михаило Петровић радио у овој области. Сасвим је разумљиво да су напретком научне мисли као и технолошким достигнућима ове

методе превазиђене. Уосталом, Михаило Петровић је јако добро разумео проблеме и несавршености свих оваквих система о чему сведочи његово тврђење

Поуздано се зна, да за време последњег светског (Првог) рата ни један метод, начин или систем тајне преписке није се могао дуже време употребљавати [1].

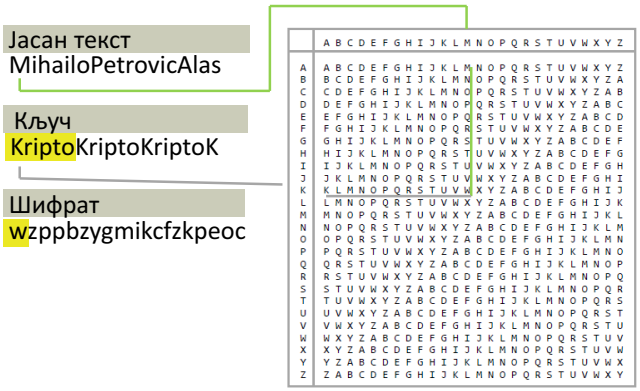
Циљ излагања је да се истакне улога и значај дела Михаила Петровића Аласа у научној дисциплини данас познатој као криптологија, а која у времену од 80 до 100 година уназад није била уобличена као наука какву данас познајемо и чије резултате користимо у свакидашњој пракси. Као илустрацију нивоа знања у Србији у области криптологије у време Михаила Петровића, навешћемо неке од метода коришћених у пракси од стране војних и државних институција у Србији у то време, а представљале су основу за даљу разраду и побољшања од стране Михаила Петровића као и његов рад на припреми приручника за обуку кадрова у одговарајућим службама.

2. Реглета

Једна од поменутих свезака о криптографији садржи опис *Метода шифровања и дешифровања помоћу нарочитих справа*, под чим се подразумева рад са реглетом за извршавање Виженерове методе назване по Blaise De Vigènere-у који је још у 16-том веку разрадио метод најпре оригинално предложен 1550. од стране Ђованија Батисте Беласо (Giovani Battista Bellaso). Метод је био толико поуздан да је тек 1863. Фридрих Касиски (Friedrich Kasiski) објавио општи начин његовог дешифровања.

Реглета је једноставна справа која се састоји од једног покретног и једног или два непокретна дела који сви подсећају на дрвени лењир. На свим деловима исписан је алфабет који се користи за исписивање јасног текста, при чему алфабет може бити исписан у нормалном или пермутованом редоследу ради повећања сложености поступка а тиме и његове поузданости. Померањем покретног дела одређују се слова којима се замењују слова јасног текста како би се добио шифрат. Поузданост шифре се заснива на броју могућих комбинација замене слова. Уколико се користи свих 30 слова, број комбинација је $30 \times 30 = 900$. У шифрирању се најчешће ради без акцентованих слова ч, ћ, ж, љ, њ, ш, џ, у ком случају је број комбинација $22 \times 22 = 484$.

Беласо је користио такозване табеле са 5 алфабета, док је Виженер радио са 10 алфабета. Такође, у оригиналном Беласовом методу шифре су биле засноване на првом слову речи, док је Виженер користио слово унапред усаглашено између страна које комуницирају. У суштини, овде се ради о добро познатој Цезаровој шифри где се свако слово замењује словом које одговара алфабету



Слика 2. Пример шифровања Виженеровом методом

помереном за неку вредност. На пример, низ $(A, B, C, D, E, F, G, H, I, J, K, \dots) \rightarrow (D, E, F, G, H, I, J, K, \cdots)$. *У* том смислу, Виженеров метод је примена више Цезарових шифри за различите помераје. При томе избор алфабета за дато слово зависи од поновљене кључне речи до дужине јасног текста. Слика 2 илуструје овај поступак шифрирања који је био описан у поменутим Свескама намењеним обуци кадрова у Србији због његове једноставности и релативне поузданости.

3. Технике фреквентирања симбола шифрата

Слика 3 је извод из Свеске 1, који потврђује добро познавање начина за разбијање шифре замене применом технике фреквентирања симбола шифрата. Техника се састоји у запажању да ако је у криптограму најфреквентније слово K, а друго по фреквенцији слово D, тада су њихове декрипције слова E и T као најфреквентнија слова латинског језика. Важно је уочити да се у то време у Србији било у току са савременим достигнућима у овом подручју.

4. Метода шифровања помоћу Кодекса

У контексту шифрирања, *Кодекс* је листа или таблица у коју су алфабетским поретком унета слова, речи, одломци речи и изрази који су највише у употреби у неком језику. Елементи из листе или свеске замењују се групом од 2 до 5 слова или цифара.

Слика 4 приказује прву страну свеске у којој се образлаже поступак шифрирања применом Кодекса посматраног као речник за тајну кореспонденцију.

— 7 —

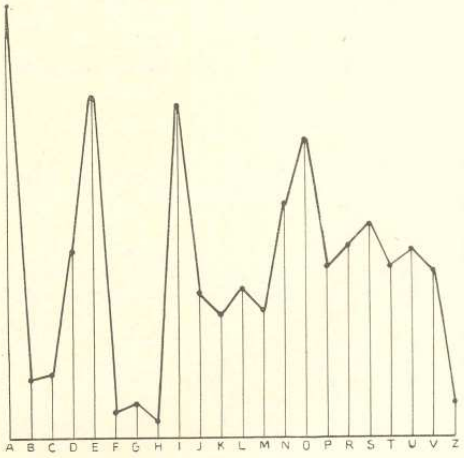
Пажљивим разгледањем овог графикона латиницом, можемо доћи до закључка, да се наша латиница може да сведе од **30** на **22** слова, када изоставимо двојна слова и акцентирана слова као што су: **Ć, Č, Ž, Đ, Lj, Nj, Š, Dž**.

Та слова се практично, специјално у телеграфском општењу и не јављају. Она се изражавају својим основним словом. Због тога ако би и њихову учесталост придали њиховим основним словима, добићемо нову фреквенцију, која у дешифровању неће ни у колико чинити ма какве сметње.

Ако би сад ову нову фреквенцију латиницом изразили графички, добили би графикон упрошћене фреквенције:

III ГРАФИКОН

упрошћен латиницом на 1000 слова



У досадањим излагањима изнели смо закон о фреквенцији и устаљивање графикона фреквенције, који служе дешифреру као помоћно средство при откривању шифара шифрованих начином просте замене. Међутим, дешифрер ће врло често увидети, да сви његови напори на том пољу не дају скоро никаквог резултата, па ће бити у недоумици, у чему је ствар.

У криптографији не постоје непроменљиви закони, управо постоје такви закони, само што они нису увек применљиви услед честог недостатка довољних елемената за дешифровање.

Зато сваки дешифрер приликом дешифровања мора да се у главном ослања на:

1. — Закон фреквенције, закон биграма и фонетичне особине језика на коме се ради, и

2. — На претпоставке, могућности подложене општим принципима логике.

Фреквенција почетних слова речи

Врло фреквентна слова су: **П, С** и **Д.**

Фреквентна: **Н, И, Ј, О, К, Т, У, М, З, В** и **Б.**

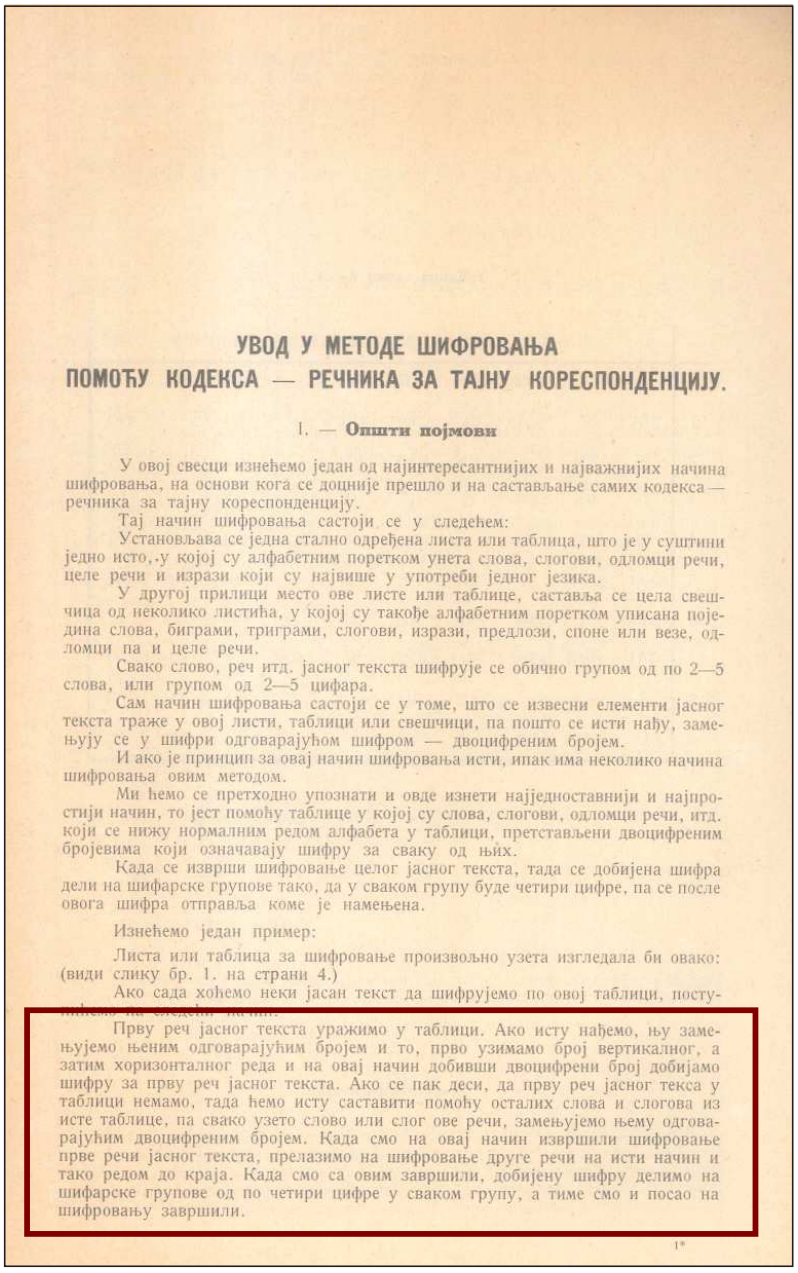
Фреквенција последњих слова речи

Фреквентна: **М, Х, Ј, Г, Н** и **Т.**

Ретка: **К, Д, Р, В, С, Ш** и **Ћ.**

Напомена: овде нису показате фреквенције самогласника, пошто се у нашем језику **90**% **речи завршава на самогласнике,** од којих су најфреквентнији **А** и **Е,** а после њих долазе: **И, У** и **О.**

Слика 3. Илустрација познавања технике фреквентирања



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

I. — 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 појединa слова, биграми, триграми, слогови, изрази, предлози, споне 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 цифара.

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 групове тако, да у сваком групу буде четири цифре, па се после овога шифра отправља 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 уражимо 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 сваком групу, а тиме смо и посао на шифровању завршили.

1*

Слика 4. Илустрација познавања технике шифрирања помоћу Кодекса

Поступак шифрирања Михаило Петровић је објаснио следећим речима

Прву реч јасног текста тражимо 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.

Ако се пак деси, да прву реч јасног текста 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 сваком групу, а тиме смо и посао на шифровању завршили.

5. Нумерички спектри и криптографија

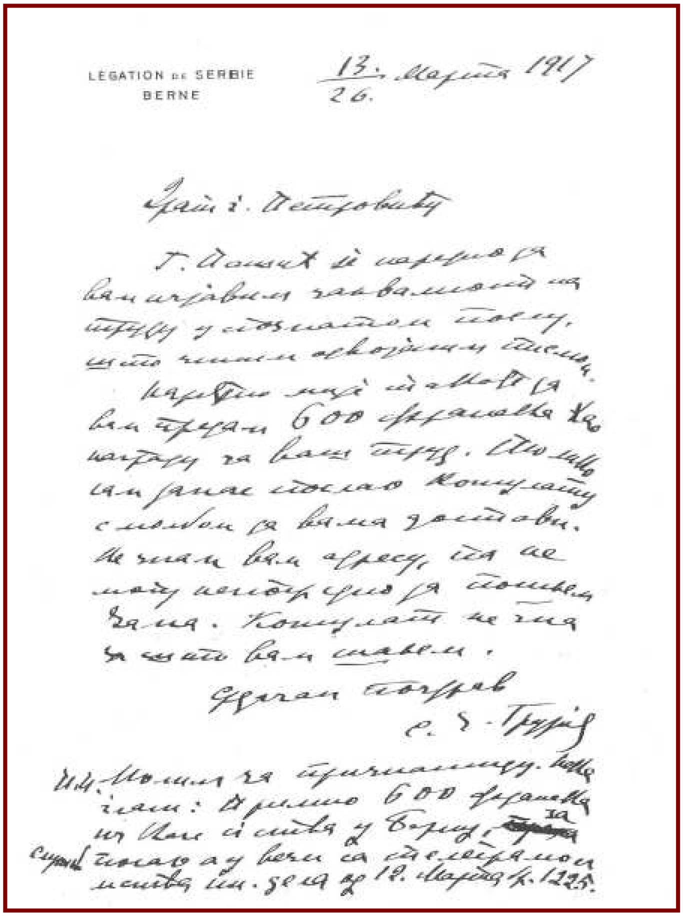
Занимљиво је уочити да је упоредо са практичним радом у криптографији, Михаило Петровић у истом раздобљу радио на дефиницији и развоју теорије нумеричких спектара. О вези између ових готово паралелних делатности најбоље сведоче речи Петровићевог најпотпунијег и најпосвећенијег биографа проф. др Душана Трифуновића [6].

Погрешно је мишљење да су нумерички спектри директна последица аналогија у физичким и хемијским наукама. Шифровање дипломатске поште (*криптографија*), *које изискује налажење одређеног кода између писма једног језика и цифара декадног система, било је пресудно у Петровићевом проналаску.*

Петровић је своје спектре поставио као врсту кода – функционале или оператора између функције и скупа децималних бројева. Петровић је спектре проналазио у времену када је највише радио на криптографији (*1917–1918*) *под директном контролом Николе Пашића, председника владе Краљевине Србије у то време. У доцнијем раду* Бројни спектри појава *Петровић је ове поверљиве чињенице и јавно објавио* [2].

Петровић је 1917. године дефинисао нумеричке спектре и реализовао свој познати систем шифровања и дешифровања *Три картона* који појмове описане речима кодира цифрама декадног система за потребе војске и дипломатије [3]. Предложени метод је био тако успешно решен да је остао у важности све до 1926. године.

Колико је рад Михаила Петровића био од значаја за Србију јасно говори податак да је о томе лично водио рачуна тадашњи председник владе Никола Пашић, који му на томе захваљује посредством др Славка Грујића посланика Краљевине Србије у Швајцарској у писму од 13. марта 1917. године приказаном на слици 5.



LÉGATION DE SERBIE
BERNE

13./26. Марта 1917

Слика 5. Писмо др Славка Грујића у коме се преноси захвалност председника владе Николе Пашића Михаилу Петровићу за рад на шифрама за потребе Краљевине Србије

Михаило Петровић је наставио рад у области криптографије и након Првог светског рата, а у вези са тим задацима октобра 1919. године боравио је у Француској по налогу Министарства исхране и обнове земље и Министарства спољних послова јер је радио на изради новог система шифровања дипломатске поште. Као резултат тог рада, 5. децембра 1919. предаје дорађену верзију система *Три картона* министру спољних послова уз следећу пратећу поруку:

По поруци Министарства част ми је поднети нов систем за шифровање депеша, о коме сам раније имао споразум са помоћником Министра г. др Михаилом Гавриловићем.

Предности овог новог система у односу на дотада коришћени Михаило Петровић је сумирао на следећи начин

1. *што је шифровање по њему боље сакривено, јер се и последња цифра шифрује, а не дописује онаква каква је, као до сада,*

2. *што један прибор за шифровање даје* 720 *разних кључева на место* 196 *као до сада,*

3. *што се у њему промена кључа врши само једном петоцифреном групом, која и извештава дешифрера о тој промени и даје у исто време нов кључ, што се до сада постизало помоћу двеју петоцифрених група,*

4. *што се не захтева никакав апарат, не квари се, заузима веома мали простор и лако се чува и преноси,*

5. *што се после извесног времена могу лако променити свих* 720 *кључева. Промена се састоји само у томе да се на већ постојећих* 10 *картона, не мењајући им централну таблицу, ни нумере на наличју, преко црних шифара прелепе две узане траке од хартије на којима су одштампане две нове пермутације цифара* $0, 1, 2, 3, 4, 5, 6, 7, 8, 9,$ (*таквих пермутација има на хиљаде милијарди*).

Следећи детаљи много говоре о начину размишљања и рада Михаила Петровића, његовом приступу ка послу и ефикасности при томе, што је и разлог и оправдање за њихово навођење.

Узимајући у обзир обуку надлежног особља, Михаило Петровић надаље извештава да се механизам шифровања и дешифровања не разликује много од досадашњег, тако да ће се они који су већ радили по досадашњем систему, лако и са мало пажње прлагодити новом.

У овом поднеску Министарству Михаило Петровић извештава да је прибор израђен у 100 примерака од којих сваки стаје по 4 динара. Даље наводи

Те примерке предајем Министарству заједно са упутством за шифровање и дешифровање. Све је израђено у дефинитивном облику тако да се може одмах разаслати Посланствима и пустити у рад почевши од једног одређеног дана.

У пратећем писму ресорном Министру Михаило Петровић наводи

По поруци Министарства Спољних послова исплатио сам за рачун Министарства за 100 *примерака прибора за шифровање депеша* (*систем Три картона*) *и то за* 1000 *картона, штампање у две боје и нумерисање картона и за* 100 *комада кувертa за прибор, суму од* 400 (*четири стотине*) *динара у сребру.*

Из ових детаља се јасно види да је Михаило Петровић налазио за потребно да комплетан посао уради до коначног производа и преда га спремног за непосредну примену практично од момента предаје. Такође, занимљиво је приметити да је сматрао једноставнијим да у реализацију најпре уложи сопствена средства, а касније тражи надокнаду, избегавајући при томе вероватно сложену комуникацију и процедуру са државном администрацијом што би могло да утиче на ефикасност извршавања посла. Чини се да и овом приликом до пот-

пуног изражаја долази изванредна комбинација његове свестране, научничке, и практичне, рибарске, природе и начина размишљања.

6. Завршни коментари

Према расположивим подацима, о чему с обзиром на предмет разматрања, из разумљивих разлога нема много записа и докумената, Михаило Петровић је за време Првог светског рата, конкретно од 1916. и посебно 1917, и надаље више година по завршетку рата, био водећа личност у Србији на пословима израде метода шифровања и дешифровања државних докумената и војне и дипломатске преписке. Једнако важно, радио је на практичној реализацији одговарајућих система до њихове спремности за непосредну примену, као и на припреми материјала за обуку кадрова одговарајућих државних институција.

Библиографија

[1] *Криптографија – школа за обуку на шифри*, свеске 1–15, Одсек за шифру, Обавештајно одељење, Ђенералштаб Краљевине Југославије, оквирно 1930–1940.

[2] М. П. Петровић, *Бројни спектри појава*, Српска краљевска академија, Глас, књ. CRXXVII, први разред, књ. 58, Београд, 1927, стр. 45–66. Саопштено у Академији природних наука, АПН 20. 12. 1926., резиме на француском.

[3] М. П. Петровић, *Transformateur des chiffres, Genève*, 1917, 50 страна, формат $12,4 \times 18,6$. Издање Посланства Краљевине Србије у Швајцарској.

[4] C. E. Shannon, *Communication Theory of Secrecy Systems.* Белл Систем Течницал Јоурнал, 1949, 28, 656–715.

[5] *Систем* (*за шифру*), свеске 1–24, Одсек за шифру, Обавештајно одељење, Ђенералштаб Краљевине Југославије, оквирно 1930–1940.

[6] Д. В. Трифуновић, *Летопис живота и рада Михаила Петровића*, Српска академија наука и уметности, Одељење природно-математичких наука, Београд, Србија, 1969, примљено 16. 2. 1968. на основу реферата академика Радивоја Кашанина и Војислава В. Мишковића, 631 страна.

Radomir S. Stanković
Miodrag Mihaljević

MIHAILO PETROVIĆ ALAS – OUR LEADING CRYPTOGRAPHER BETWEEN THE TWO WORLD WARS

S u m m a r y

Encryption is today one of standard approaches for achieving security and privacy in the digital space, and a large number of experts works in this area both from a scientific and research perspective and in the domains of a large number of different applications. At the time of Mihail Petrović Alas, dealing with encryption was a rather rare and very specific job, and he was at the same time the main scientist-researcher and chief state advisor responsible for the codes between the two world wars. It is preserved a relatively small number of records mainly in the form of military documents about this very respectable segment of work and achievements of Mihailo Petrović that was very important at that time and is also important and interesting from the historical perspective. These documents undoubtedly indicate great merits of M. P. Alas for our country in the domain of cryptology even before it was established as a world level scientific discipline [4]. This paper summarizes, based on [1] – [3] and [5] – [6], some of the historical facts about the M. P. Alas as our main cryptographer between the two world wars.

In the mentioned documents, it was noted that the work of M. P. Alas and the results of this work can be found in: (1) Methods for encryption, (2) methods for "breaking" the codes and (3) education on encryption techniques as well as deciphering of encrypted messages.

History acknowledges, and due to the growing importance of the area in which M. P. Alas has left his mark, history will even further emphasize the work of Mihailo Petrović Alas in the domain of the development of the Serbian state ciphering methods between the two world wars.