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 И КРИПТОГРАФИЈА

МИОДРАГ ЖИВКОВИЋ*

А п с т р а к т. – Приказана је улога Михаила Петровића у шифрантској служби на основу расположивих докумената о школи криптографије, односно описа шифарских система коришћених у Краљевини Југославији.

Кључне речи: криптографија, шифровање, дешифровање, декриптирање

1. Увод

Криптографија је наука која се бави начинима очувања тајности података, а Петровић је у томе постигао велике резултате. О његовом бављењу криптографијом нема много писаних трагова, што се може разумети, с обзиром на тајновитост којом је криптографија окружена. Драган Трифуновић у књизи [1] каже:

„Још почетком 20. века Михаило Петровић, као математичар, који је познавао дискретну математику и комбинаторику, бавио се шифровањем, односно криптографијом за дипломатску и војну пошту. За Крфску декларацију, састанак вођа Краљевине Србије, Краљевине Црне Горе, Хрватске, Славоније, Војводине из Аустроугарске, Никола Пашић је захтевао од Михаила Петровића да направи шифре преко којих ће те делегације, док рат још траје, да се обавештавају, а да непријатељ не дозна садржај писма-поруке. Тако је почело. Између два рада Михаило Петровић је у Генералштабу, у Обавештајном одељењу, држао часове из шифровања и водио ову службу.

Михаило Петровић је мобилисан у 73. години као потпуковник и ти официри су имали збег у Сарајеву."

Понекад и обичним смртницима буде омогућено да стекну увид у свет посвећених људи који се баве криптографијом. Занимљива слика о томе може

* Математички факултет, Универзитет у Београду, и-мејл: ezivkovm@matf.bg.ac.rs

се наћи у филму[2] The Falcon and the Snowman Џона Шлезинџера. Бојса, главног јунака човек из обезбеђења доводи до врата са електронском шифром[3]. Он има шифру, а човек из обезбеђења – не. Унутра наилази на сараднике посвећене у тајну. Чињеница да у те просторије имају приступ само они утиче на природан начин на њихово понашање: у тешкој каси за тајне документе чувају алкохол; машину за сецкање докумената користе као миксер да смуђкају коктел. Наравно, правила која важе за људе у оваквом окружењу пре свега подразумевају строгу обавезу чувања тајне. Михаило Петровић Алас као главни криптограф имао је врхунску одговорност за шифрантску службу.

1.1. Основни појмови

Уобичајени модел шифроване комуникације има три учесника: пошиљаоца A, примаоца B и „прислушкивача" C. Пре него што A пошаље поруку (*јасни текст*) M намењену примаоцу B, он је *шифрује*, примењујући на њу шифарску трансформацију F_K са *кључем* K, и тако израчунава *шифрат* $F_K(M)$. Израчунати шифрат он шаље примаоцу B посредством јавног (несигурног) канала. Када B прими шифрат, он га *дешифрује* применом инверзне трансформације F_K^{-1}: $M = F_K^{-1}(C)$. Трећи учесник C прислушкује канал везе, и тако долази до шифрата C. На основу тога он покушава да реконструише поруку M. Уобичајена претпоставка је да поступак (алгоритам) шифровања – трансформацију F знају сви, A, B и C, али да кључ K знају само A и B. Дакле, C хоће да прочита (*декриптира*) поруку, иако не зна кључ K. Његова основна идеја је да испроба све могуће кључеве. Због тога сви шифарски системи који претендују на то да буду сигурни, имају астрономски велики број могућих кључева. Декриптирање проверавањем свих могућих кључева је понекад могуће, и за такве потребе C обично има на располагању изузетно моћне рачунаре.

Од давнина криптографију примењују посебно војска, дипломатија. У данашње време су области примене јако раширене, између осталог и за *интернет ствари* (Internet of Things).

1.2. Примери шифри из најновије историје

Са шифрама се мора пажљиво руковати. Између осталог, то је разлог зашто се о (правим) шифрама мало зна. Неки од примера који показују да постоје изузеци од овог правила су шифре о којима се из разних разлога понешто сазнало, као што су

- Енигма и друге немачке и јапанске шифре из Другог светског рата,
- наши уређаји за шифровање коришћени у рату у Босни,

[2] https://en.wikipedia.org/wiki/The_Falcon_and_the_Snowman

[3] https://www.youtube.com/watch?v=YzzeMDJ4lvk, погледати део који почиње од 4:20

- шифарски системи Краљевине Југославије које је смислио Михаило Петровић Алас.

Занимљиво је да се подаци о нашим крипто уређајима могу наћи у холандском музеју криптографије.[4] Уређај за шифровање говора КзУ-63 играо је значајну улогу у „југословенским ратовима" (1991–2001) у току којих је коришћен за заштиту неких важних радио комуникација. Скраћеница КзУ настала је од Крипто-заштитни уређај. За разлику од претходног, несигурног скремблера КзУ-61, уређај КзУ-63 обезбеђивао је сигурно шифровање дигитализованог говорног сигнала[5].

Уређај КзУ-42 служи за ручно шифровање или дешифровање порука у локалу, после чега би те поруке биле преношене куриром, Морзеовом азбуком, телепринтером или гласом помоћу радио уређаја или телефона. Коришћен је у ЈНА[6].

Хрватска војска користила је амерички уређај, скремблер KY-189 [7], као и швајцарски уређај HC-5205 CRYPTOMATIC Electronic Message Unit за преношење порука са уграђеним шифровањем (развијен у Crypto AG у Цугу око 1988. године).[8]

О овим нашим уређајима може се наћи и у записницима Хашког трибунала, посебно у сведочењу Нења Благојевића задуженог за везе у Војсци Републике Српске (1992–1997).[9]

2. Шифарска служба у Краљевини Југославији – школа криптографије

Серија докумената [2] служила је за обуку шифраната, односно разбијача шифри. Приказаћемо укратко неке делове прве две од ових свезака.

2.1. Криптографија – општи појмови

Ова свеска нуди увод у криптографију. Уводе се основни појмови, на начин карактеристичан за оно време. Илустроваћемо то са неколико карактеристичних пасуса.

[4] http://www.cryptomuseum.com

[5] http://www.cryptomuseum.com/crypto/yugo/kzu63/img/302088/026/full.jpg

[6] http://www.cryptomuseum.com/crypto/yugo/kzu42/img/302210/028/small.jpg

[7] http://www.cryptomuseum.com/crypto/usa/ky189/img/ky189_controls.png

[8] http://www.cryptomuseum.com/crypto/hagelin/hc5205/img/302206/009/small.jpg

[9] International Criminal Tribunal for the Former Yugoslavia. Case IT-05-88-T. Prosecutor versus Vujadin Popovic et al. 17 June 2008 (Transcript). http://www.icty.org/x/cases/popovic/trans/en/080617IT.htm

Суштина тајне преписке види се из самога њеног назива. Другим речима, ако две особе хоће и желе да једно другом нешто јаве, саопште или поруче, а да то остане тајна за сваког другог, они ће међусобно морати утврдити и начин којим ће се послужити, те да то остане апсолутна тајна за остале.

Жеља, а врло често и прека потреба трећег лица да у туђу тајну по сваку цену продре, натераће га да употреби сва могућа и немогућа средства, док у овом на било који начин не успе, о чему ће бити говора доцније.

У случају да тајна преписка дође у руке ненадлежног лица, зашто се он истом не може користити? У чему се састоји та тајна? У уговореном кључу између две стране, и све дотле, док се не дође до кључа, тајну преписку је врло тешко, али не и немогуће одгонетати.

У наставку се излажу важни појмови и њихове дефиниције:

- **Криптографија**, наука о тајном писању
- **Криптограф** – човек који се практично бави овом науком; такви се људи зову још: шифрери и дешифрери. Њихов се рад назива: шифровање и дешифровање.
- **Криптограм-шифра,** је резултат крајњега рада шифрера. Другим речима – **шифра-криптограм** је скривеност правог – јасног текста извесним уговореним знацима, који за непозвана лица чине – тајну.

Важан део упутства чине правила „руковања са тајним средствима". Набројане су мере опреза, између осталог

- пре самог шифровања треба настојати да се непозвана лица одстране па и онда, кад је реч о пријатељској особи или члану породице;
- код дешифровања се морају предузети исте мере сигурности као и код шифровања.

2.2. Шифра просте замене и њено декриптирање

У Свесци бр. 1 описан је основни начин шифровања, *проста замена* састоји се од „замене слова или бројева нечим другим". Код просте замене, на пример, користи се фиксирана табела у којој се у првом реду налазе сва слова алфабета („нормалан алфабет"), а у другом реду сва слова алфабета, али измењеним редоследом („алфабет замене"). Једноставан пример такве табеле је следећи:

А	Б	В	Г	Д	Ђ	Е	Ж	З	И	нормалан алфабет
Њ	О	П	Р	С	Т	Ћ	У	Ф	Х	алфабет замене
Ј	К	Л	Љ	М	Н	Њ	О	П	Р	нормалан алфабет
Ц	Ч	Џ	Ш	А	Б	В	Г	Д	Ђ	алфабет замене
С	Т	Ћ	У	Ф	Х	Ц	Ч	Џ	Ш	нормалан алфабет
Е	Ж	З	И	Ј	К	Л	Љ	М	Н	алфабет замене

Пример 11. *Шифровањем поруке*
„вечерас полазим дочекај ме”
добија се шифрат
„пћљћђње дгуљфха сглћчњц аћ”.

Наведена табела није карактеристична за општи случај, јер је у њој алфабет замене добијен цикличком пермутацијом нормалног алфабета. У општем случају примењује се произвољна пермутација нормалног алфабета. За декриптирање („дешифровање” је израз који се у свескама користи и када се зна, и када се не зна кључ) користи се хистограм фреквенција слова, односно чињеница да су просечне учестаности појављивања појединих слова у тексту на сваком, па и нашем језику приближно пропорционалне дужини текста. Те учестаности дакле карактеришу наш језик. У тексту од 10000 слова укупно око 8500 слова је неко од слова из следеће табеле, у којој су приказане и учестаности појављивања тих слова.

А	1159	Н	517	У	393	К	343
О	980	Т	480	Д	381	П	311
И	881	С	476	М	363	Л	273
Е	862	Р	470	В	357	Ј	268

У наставку се детаљно наводе остале особине нашег језика – слова која претходе или следују неком другом слову, посебно за самогласнике и сугласнике; учестаности парова слова (биграма), итд.

Термин *тежиште сваке шифре* односи се на важне речи које се могу очекивати у отвореном тексту. Ове речи олакшавају декриптирање.

Ако се у времену рата ухвати нека војна шифра, природно је, да у њој треба тражити елемент, који је у непосредној вези са ратом. Ти елементи су чисто војничке и ратне природе и треба их тражити у речима војне терминологије као: непријатељ, корпус, армија, дивизија, артиљерија, пешадија, пук, батаљон, напад, муниција, комора, попуна итд.

Или пак, ако се тиче неке мирнодопске дипломатске шифре, природно је, да се у њој неће тражити горњи елементи, већ неки сасвим други као: влада, министар, нота, криза, протест, председник, већина, опозиција, или имена важнијих политичких личности, земаља, актуелни догађаји итд., а што се све може закључити из дневне штампе појединих земаља.

За рад на декриптирању шифрата користи се термин *криптографска студија*. Организација рада приликом криптографске студије према упутству састоји се од три фазе:

- прве фазе: бројања слова, биграма; уочавање понављања у шифрату; из таблице биграма се може са много вероватноће рећи које слово шифре представља самогласник, а које сугласник ...
- друге фазе: тумачења резултата из прве фазе;
- треће фазе: изналажења (по смислу) слова, слогова, речи и одломака речи које се нису могле установити у другој фази.

Ова упутства за декриптирање пропраћена су конкретним задацима – вежбањима.

Остале свеске из ове серије односе се на анализу других, компликованијих система шифровања.

3. Шифарски системи Краљевине Југославије

Занимљиво је да су сачувани описи шифарских система коришћени у Краљевини Југославији. Системи 1а, 1б, 2а, 2б, 3а, 4а, 5, 6а, 6б, 7а, 7б, 8, 9, 10а, 10б, 11, 12, 13, 14, 15, 16, 17, 18 описани су у посебним штампаним документима [3].

3.1. Шифарски систем 1а

Прибор за шифровање чине три реглете (траке) са исписаним низом слова. Плава (означена са Ш) и црвена (означена са Д) су са испретураном азбуком, а средња, бела је са нормалном азбуком. Траке су непомичне и исписане заједно једна испод друге у облику таблице. Изнад плаве реглете налазе се редом исписани бројеви од 1 до 30 који дају редни број слова нормалне азбуке. Таквих таблица има 30 и свака је нумерисана једним словом азбуке.

Другим речима, користи се 30 таблица са простом заменом, при чему се уз сваку пермутацију Ш (плаву) азбуке заједно са њом налази и њена инверзна пермутација Д (црвена). Као пример наводе се три таблице, означене словима П, Ф и О.

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	П
к	м	у	а	з	ж	н	х	ћ	у	ч	ј	и	ф	е	Ш
а	б	в	г	д	ђ	е	ж	з	и	ј	к	л	љ	м	
г	ч	њ	п	с	ш	м	ђ	д	л	к	а	у	р	б	Д

16	17	18	18	20	21	22	23	24	25	26	27	28	29	30	П
с	в	р	г	љ	д	ш	њ	л	т	п	џ	б	о	ђ	Ш
н	њ	о	п	р	с	т	ћ	у	ф	х	ц	ч	џ	ш	
е	ћ	џ	х	о	н	ф	з	в	љ	ж	и	ј	у	т	Д

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	Ф
з	о	р	љ	ш	к	с	н	ж	ф	и	м	т	д	у	Ш
а	б	в	г	д	ђ	е	ж	з	и	ј	к	л	љ	м	
у	џ	с	р	љ	о	ф	з	а	ј	ч	ђ	ч	г	к	Д

16	17	18	18	20	21	22	23	24	25	26	27	28	29	30	Ф
х	л	ђ	џ	г	в	п	ц	а	с	ћ	ч	ј	б	њ	Ш
н	њ	о	п	р	с	т	ћ	у	ф	х	ц	ч	џ	ш	
ж	ш	б	т	в	с	л	х	м	и	н	ћ	ц	п	д	Д

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	О
л	њ	ћ	в	у	џ	ћ	ф	о	м	б	с	ђ	ш	т	Ш
а	б	в	г	д	ђ	е	ж	з	и	ј	к	л	љ	м	
ц	ј	г	џ	т	л	а	н	њ	ф	г	ш	х	р	и	Д

16	17	18	18	20	21	22	23	24	25	26	27	28	29	30	О
ж	з	р	ц	љ	н	д	ч	х	и	л	а	ј	г	к	Ш
н	њ	о	п	р	с	т	ћ	у	ф	х	ц	ч	џ	ш	
с	б	з	в	о	к	м	е	д	ж	у	п	ћ	ђ	л	Д

Поступак шифровања почиње тиме што шифрер испред јасног текста ставља произвољно ДВА слова, на пример пи. Прво слово је редни број таблице која

се користи, а друго својим редним бројем казује број слова групе која ће се шифровати по тој таблици. Пошто је ових десет слова шифровао, ставља поново два произвољна слова, на пример фе и наредну групу од 7 слова (јер је 7 редни број слова е) шифрује по табели ф итд.

При завршетку јасног текста, кад остане неколико слова, на пример 12, онда као друго слово узети 12-то слово, тј. слово к.

Само шифровање појединих група врши се тако што се слово јасног текста тражи на средњој, белој реглети и замењује наизменично одговарајућим словом прво са плаве реглете, друго са црвене, треће са плаве итд.

Пример 12. *Јасан текст НЕПРИЈАТЕЉ ЈЕ У ПОВЛАЧЕЊУ може се шифровати на следећи начин.*

Нумера таблице	*Број слова групе*	
п	*и*	*н е п р и ј а т е љ* *с м г о ц к к ф н р*
ф	*е*	*ј е у п о в л* *и ф а т ћ с т*
о	*д*	*а ч е њ у* *с ћ ћ б х*

Добијени шифрован текст је писмгоцккфнрфеифатћстодсћћбх.

Поступак дешифровања је сличан. Слова шифре траже се на белој реглети и наизменично замењују одговарајућим словима прво са црвене реглете, друго са плаве, треће са црвене итд.

Запажа се да сам шифрер бира које ће таблице да користи. У упутству се каже да се њему може дати неки подскуп таблица. Од њега се очекује да неправилно мења број слова у групама.

За Систем 1а са латиницом користе се 22 таблице нумерисане словима од a до z.

Занимљив детаљ је да је на маргини текста уз пример отиснут печат са натписом

МИНИСТАРСТВО ВОЈСКЕ И МОРНАРИЦЕ
Краљевине Југославије

3.2. Шифарски систем 1б

Систем 1б користи сличан систем таблица са три реглете: плавом и црвеном са испретураном азбуком и белом са нормалном азбуком.

Нарочитим кључем у бинарној азбуци од два знака, плавог и црвеног, одређује се редослед којим ће се употребљавати плава, односно црвена реглета. Тај кључ се доставља на један од четири начина и остаје исти за целу депешу.

I начин У посебним таблицама написани су један испод другог 30 кључева који су нумерисани редом словима азбуке. Кључ се доставља тако што се слово које га одређује стави као индикатор испред шифрованог текста.

II начин За достављање кључева може се узети текст једне уговорене књиге која има најмање 30 страна. Прво слово шифрованог текста је индикатор, који својим редним бројем одређује страну књиге. Почев од првог слова означене стране латиничне књиге исписује се бинарни кључ (плаво, црвено, односно ·, −) на тај начин што се испод сваког самогласника стави плаво или ·, а уместо сваког сугласника црвено или − (шифрер сам бира начин означавања).

III начин Испред шифре ставља се индикатор од пет слова. Та слова исписана Морзеовом азбуком дају бинарни низ (·, −, односно плава, црвена црта) који се користи као кључ. На пример, кључу Гирфо одговара низ

− − · (г), · · (и), · − · (р), · · − · (ф), − − − (о).

IV начин Датум и месец на депешама не шифровати, већ га на депеше јасно написати. Датум преведен на Морзеову азбуку даје бинарни низ кључа (плаво, црвено, односно ·, −). На пример, датум 3. март 1940. одређује кључ

· · · − − (3), − − (м), · − (а), · − · (р), − (т).

Поступак шифровања почиње подвлачењем јасног текста црвеним или плавим цртама, односно са · или −. Ако се кључ исцрпи, понавља се истим редом до краја текста. Свако слово јасног текста тражи се на средњој белој реглети таблице означене са Ш и замењује се (шифрује) одговарајућим словом црвене, односно плаве реглете према томе којом је бојом слово подвучено. Испред шифрованог текста ставља се индикатор кључа, чији број слова зависи од изабраног начина достављања кључа.

Пример 13. *Порука „Непријатељ је у повлачењу" се шифрује кључем б на први начин. Елементи бинарног кључа су у табели означени словом ц (црвена боја) или п (плава боја).*

	Н	*е*	*п*	*р*	*и*	*ј*	*а*	*т*	*е*	*љ*	*ј*	*е*	*у*	*п*	*о*	*в*	*л*	*а*	*ч*	*е*	*њ*	*у*
б	*ц*	*п*	*п*	*ц*	*п*	*ц*	*п*	*п*	*ц*	*п*	*п*	*ц*	*ц*	*п*	*ц*	*ц*	*п*	*п*	*ц*	*ц*	*ц*	*п*
	п	*љ*	*н*	*ж*	*п*	*б*	*з*	*е*	*т*	*е*	*б*	*т*	*б*	*н*	*д*	*ј*	*т*	*з*	*р*	*т*	*в*	*к*

Пошто се дода индикатор б, добија се шифровани текст (подељен у групе по пет слова)

бпљнж пбзет ебтбн ђтзр твк

3.3. Шифарски системи 6а

Не користи се никакав посебан прибор. Датум даје кључ. Датум се не шифрује, већ се на депеши јасно испише. Дан и месец датума се испишу Морзеовом азбуком и тако добијеним низом Морзеових знакова исподвлаче се слова јасног текста, и то: тачком два, а цртом три слова. Кад се кључ исцрпи, он се понавља до краја депеше.

У току шифровања слова означена тачком шифрују се тако да се прво слово замени претходним, а друго наредним словом нормалне азбуке. Слова означена цртом шифровати овако: прво слово заменити претходним, друго не шифровати, а треће заменити наредним словом нормалне азбуке. Ако се текст завршава са једним словом подвученим цртом, оно се замењује претходним словом; ако се текст завршава са два слова подвучена цртом, прво се замењује претходним, а друго наредним словом.

Пример 14. *Потребно је шифровати јасан текст*

23 март 1940

Непријатељске трупе се повлаче

Кључ се формира на основу датума из јасног текста:

2	*3*	*м*	*а*	*р*	*т*
·· – – –	··· – –	– –	· –	· – ·	–

Поступак шифровања приказује следећа табела:

Н	*е*	*п*	*р*	*и*	*ј*	*а*	*т*	*е*	*љ*	*с*	*к*	*е*
·	·	–	–	–								

м	*ж*	*о*	*с*	*з*	*ј*	*б*	*с*	*е*	*м*	*р*	*к*	*ж*

т	*р*	*у*	*п*	*е*	*с*	*е*	*п*	*о*	*в*	*л*	*а*	*ч*	*е*
·	·	·	–	–	–								

с	*и*	*ћ*	*р*	*у*	*т*	*у*	*п*	*п*	*б*	*л*	*б*	*ц*	*ж*

Према томе, шифрат поруке је

23 март 1940

мжосз јбсем ркжсси ћрутџ ппблб цжс

Запажа се да овај поступак није сигуран, јер се кључ – датум исписује на депеши. Неко ко неовлашћено дође до депеше може да је без проблема прочита ако зна за примењени систем, јер се кључ за дешифровање може реконструисати на основу поруке која му је у рукама.

4. Закључак

Михаило Петровић имао је значајну улогу у шифарској служби у Краљевини Југославији. Шифарски системи које је креирао су занимљиви имајући на уму време у ком су настали. Неке варијанте усаглашавања кључа између пошиљаоца и примаоца шифроване поруке су били проблематични.

Захвалница. *Захваљујем се професору Жарку Мијајловићу за помоћ приликом набавке [2, 3].*

Рад је подржан од стране Министарства образовања, науке и технолошког развоја, пројекат 174021.

Библиографија

[1] Универзитет у Београду, Универзитетска библиотека „Светозар Марковић" у Београду. *Легенде Београдског универзитета. Михаило Петровић Алас, Аница Савић-Ребац, Александар Ђ. Костић, Александар Дероко*, Зборник предавања одржаних у Универзитетској библиотеци у периоду 2002–2004, Београд, 2005.

[2] Краљевина Југославија, Главни Ђенералштаб, Обавештајно одељење, Одсек за шифру. *Криптографија. Школа за обуку на шифри*, српскохрватски језик. Адлигат, Музеј српске књижевности. Дигитализовано у Математичком институту.

[3] Краљевина Југославија, Главни Ђенералштаб, Обавештајно одељење, Одсек за шифру. *Шифарски системи 1а, 1б, 2а, 2б, 3а, 4а, 5, 6а, 6б, 7а, 7б, 8, 9, 10а, 10б, 11, 12, 13, 14, 15, 16, 17, 18.* Адлигат, Музеј српске књижевности. Дигитализовано у Математичком институту.

Miodrag Živković

MIHAILO PETROVIĆ AND CRYPTOGRAPHY

S u m m a r y

The role of Mihailo Petrović in cryptographic service of Kingdom of Yugoslavia is presented, based on documents about school of cryptography and on descriptions of cryptographic systems.