

Уређај криптозаштите *енигма*

# УРЕЂАЈ ЗА ШИФРОВАЊЕ КАО ВЕЛИКА ЗАГОНЕТКА

У Спомен-соби Бригаде везе, која се налази у посебно опремљеној просторији њене команде, и данас се чува једна од најинтригантнијих машина за шифровање радио-телеграфских порука, чије је разумевање, односно правилно тумачење принципа њеног рада значајно утицало на ток и исход Другог светског рата

Пише: поручник Иван ЋУРЂЕВИЋ

Фото: Архива Бригаде везе



Немачки уређај криптозаштите, прецизније средство намењено за примену специфичних криптографских метода, мера и поступака ради трансформисања података у неразумљив облик, тачније шифру, као да своје постојање брани оном познатом латинском изреком да је „име знак”, будући да реч „енигма” у преводу с грчког језика значи – загонетка. Уређај везе конструисао је Артур Шербијус још 1923. године у оквиру своје фирме „Chiffriermaschinen AG Berlin” („Машина за шифровање АГ Берлин”) да би на тржишту комерцијалне природе конкурисао сличним апаратима супарничких фирми као системима за шифровање у цивилне сврхе. Тада је још увек, и прак-

тично све до избијања Другог светског рата, циљ енигме лежао у шифровању телеграфски преношених пословних порука. Наликујући класичној писаћој машини, са тастатуром чија су слова била повезана са сијалицама (тачније, излазним словним знацима), енигма је радила на бази струјног кола, помоћу којег су приказана излазна слова формирала шифровани текст.

Енигма је, дакле, функционисала на принципима спојених ротора и разводне плоче, тако што се текст уносио преко тастатуре од 26 слова, с излазним реченичним производом који се могао прочитати преко сијалица којих је, исто тако, било 26. Управо су ротори, у склопу главног механизма као језгра машине, преносили тај текст, заснован на супституцији знакова, односно померању слова и њиховом пресликавању, до којег се долазило преко уређене таблице, сачињене од стручног лица. Стога је успех ове машине зависио и од могућности да се једно одређено слово,



## СПОМЕН-СОБА БРИГАДЕ ВЕЗЕ

Спомен-соба Бригаде везе је посебна просторија у згради Команде Бригаде везе у Касарни „Бањица“, у којој се налази стална изложбена поставка и у којој су постављени документи, фотографије, уређаји, опрема и други експонати, који сведоче о техничком развоју и слободарским традицијама јединице, њених припадника и народа, којом се изражава припадност Војсци Србије. У њој се тематско документарним материјалом илуструју догађаји из историје развоја ове јединице, излажу се експонати и материјали из ослободилачких ратова Србије, НОР-а, ратних дејстава на просторима бивше Југославије као и предмети и признања које је јединица добила.



после ротирања и излаза у сијалици, појави у што више другачијих облика, односно знакова, како би се избегло једнозначно пресликавање. Тако се и другој страни, оној која је радила на неутралисању дејства енигме, у великој мери отежавало њено дешифровање.

Иако су пре рата полски математичари са Марјаном Рејевским на челу у више наврата успевали да дешифрују машину, искоришћавајући чињеницу да су Немци због сигурности шифре на почетку поруке тзв. кључ поруке (групе од три слова) слали два пута, процес дешифровања је већ од

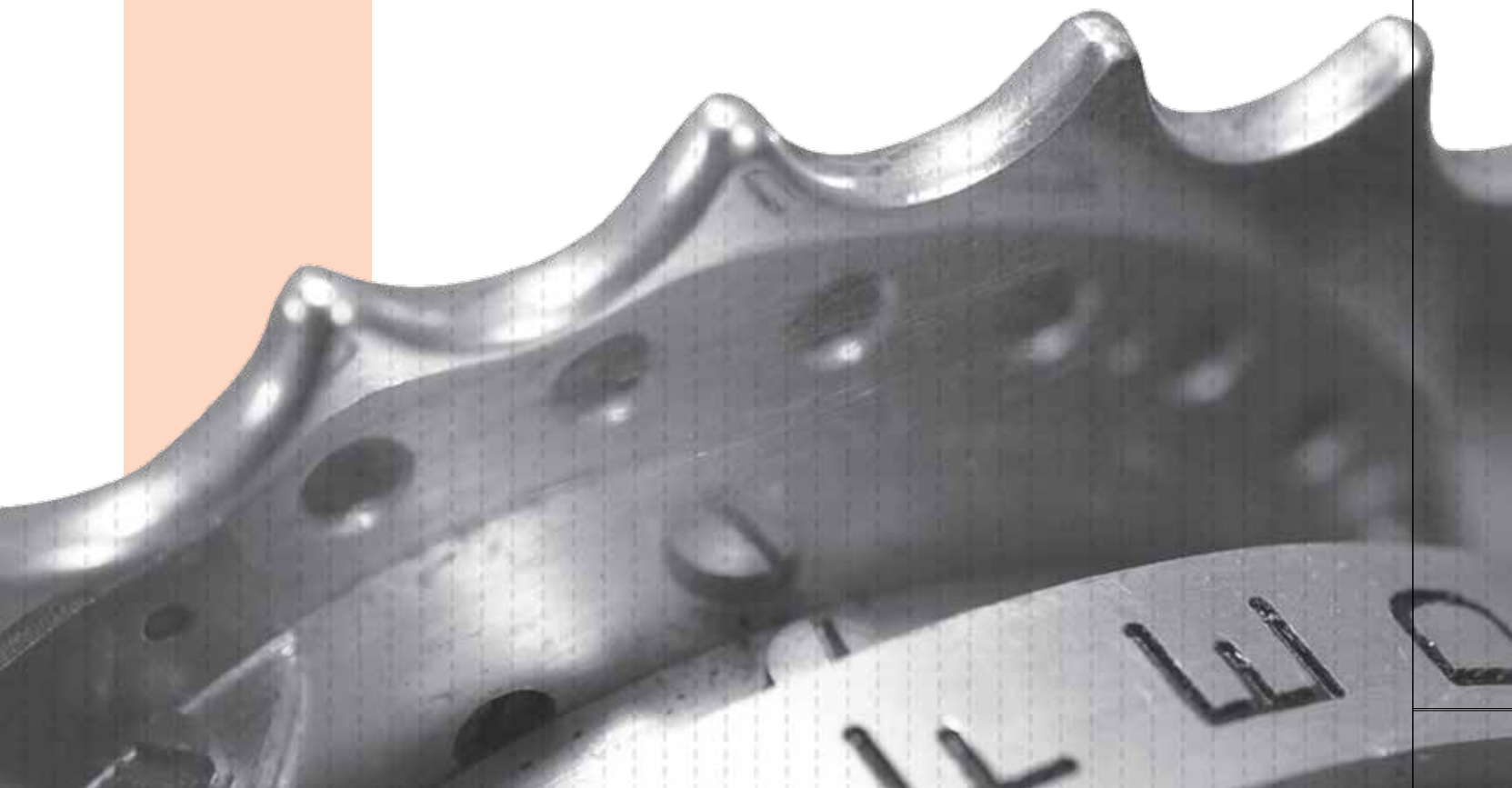
1939. године био знатно отежан, будући да је немачка страна пооштрила параметре енигме, користећи уместо дотадашња три ваљка пет и подижући пресликавање словних отисака на нови и виши ниво. Чинило се да је с таквим моделом употребе готово немогуће пробити шифру, јер се нису више мењала само четири словна пара већ ни мање ни више него десет.

Савезничкој коалицији дуго је требало да уђе у суштину овакве математичке енкрипције података, и поред тога што је пољска обавештајна служба уступила Енглеској и Француској нацрте енигме и њених слабих тачака, поделивши и искуство декодирања од стране научника око Рејевског. У сваком случају британска војска ће ове податке искористити да у једној вили у Блечли парку формира оно што ће временом постати главни центар савезничког разоткривања шифри током Другог светског рата, односно Владино школу кодова и шифри, која ће дуго времена бити и место за врхунске стручњаке, попут Алана Тјуринга и Била Тата.

Фокус стручњака у Блечли парку био је на конструисању што боље „бомбе“, односно електромеханичког рачунара за дешифровање података слатих енигмом, коју је до неке мере развио још Рејевски, да би је до детаља усавршио и сам Тјуринг, отац

модерног рачунарства. Комбинујући комплексну механику с алгоритмима енигме и знањем података одређених немачких шифарника, он је заснивао свој рад на имитацији начина функционисања оригиналног уређаја. Окружен са нешто више од 7.000 запослених којима је руководио попут каквог војног команданта, Тјуринг је успео да добије „невидљиви“ обавештајни рат који је Велика Британија водила са Трећим рајхом, успевајући из дана у дан да дешифрује дневни кључ, чак за свега неколико сати рада, иако је тај кључ немачка команда мењала сваке поноћи.

Прва „бомба“ која је склоплена 18. марта 1940. године названа је „Победа“, и била је тек један од првих корака ка овом својеврсном „информатичком успеху“, који је, према мишљењу одређених стручњака, рат скратио за добрих две године. Значај рада Владине школе кодова и шифри у више прилика истицао је и (после)ратни премијер Велике Британије Винстон Черчил, говорећи да је управо тим технолошким пробојем рат и добијен, а нарочито искрцавањем на Нормандију у лето 1944. године, које је успело, између осталог, и јер су савезници, систематичним обавештајним радом и достављањем лажне информације о искрцавању, Немце заварали, пославши их на другу локацију.





Капетан прве класе  
Катарина Манојловић

### ПРИМЕРАК ЕНИГМЕ У ВОЈСЦИ СРБИЈЕ

У нашој земљи после Другог светског рата остало је сачувано неколико енигми, које су у установе које их и дан-данас поседују дошле или као ратни плен или су пронађене на неочекиваној локацији. Овај други начин доласка до енигме, по свему судећи, био је пресудан за Бригаду везе, како истиче наша саговорница, капетан прве класе Катарина Манојловић, начелник Групе за заштиту информација у Команди ове јединице.

– На територији Републике Србије тренутно се, по информацијама које имамо, налазе две енигме. Прва се налази у Војном музеју на Калемегдану, изложена у оквиру њихове сталне поставке, док је друга енигма у поседу наше команде, коју чувамо у Спомен-соби, у централном делу наше богате колекције – каже наша саговорница, додајући да је овај чувени уређај

за кодирање својевремено пронађен у једном магацину, током његовог уређивања. Како уз уређај није пронађена никаква пратећа техничка документација, она је као експонат изложена само уз кратки опис – „Енигма М4, сер. бр. 7969 из 1944. године”.

О другом сачуваном примерку енигме, у власништву Војног музеја, тек се мало више зна. Наиме, тадашњи заменик директора Војног музеја, према писању дневног листа „Политика” од јула 2008. године, рекао је да иако не постоји пратећа документација, на основу усменог предања неких старијих генерација војне службе безбедности може се претпоставити да је енигма серијског броја 1227 припадала некој од јединица немачке армијске групе „Југ” (немачкој копненој војсци), која се крајем 1944. године преко Србије повлачила из Грчке, те да је заплена током борби на нашим просторима.





## ТЕМЕЉИ ЗА РАЗВОЈ СЛУЖБЕ ТЕЛЕКОМУНИКАЦИЈА

Бригада везе, као једна од формацијских целина Управе за телекомуникације и информатику (Ј-6) Генералштаба Војске Србије, формирана је 30. октобра 2006, када су у њен састав ушле јединице 398. бригаде везе и 235. центра стационарних веза. Основна мисија ове јединице јесте одржавање непрекидности телекомуникационо-информатичког обезбеђења Министарства одбране и Војске Србије, као и целокупни надзор и управљање стационарном компонентом телекомуникационо-информационог система. За свој дан ова јединица одредила је 20. септембар 1916. године, када је на предлог министра војног, престолонаследник Александар Карађорђевић одобрио Уредбу о војном телеграфу, којом су постављени темељи за развој службе телекомуникација у нашој војсци.

Међутим, генерал-мајор у пензији Светко Ковач наводи у својој књизи „Енигма и рат у Југославији” из 2017. године да се на простору бивше Социјалистичке Федеративне Републике Југославије (СФРЈ) налазило пет енигми, и то четири у Србији и једна у Словенији. Али, он исто тако пише да нема докумената који потврђују начин на који су ове енигме дошле у посед Југословенске народне армије.

Према неким подацима, већи број енигми заробљен је од Команде Групе армија Е и армијских корпусних команди након њиховог заробљавања и потписивања безусловне предаје. Савезничка војска заробила је 9. маја 1945. године Штаб

Групе армија Е, чији је командант генерал Александер Лер потписао безусловну капитулацију. До 15. маја заробљене су и разоружане 7. СС дивизија „Принц Еуген” и 373. легионарска дивизија, а затим 22. и 181. немачка дивизија и делови 369. дивизије. Тада је заплена велика количина наоружања и војне опреме и у Загребу је 19. маја 1945. формирана Главна трофејна база у којој су прикупљана заробљена техничка средства и опрема. Када је у септембру 1945. та база расформирана, средства везе распоређена су у Команду веза Министарства народне одбране, где су се вероватно нашле и све те заробљене енигме. Судбине неких од тих уређаја остале су, у складу са својим именом, енигма. ▀

