ОДБРАНА
СПЕЦИЈАЛНИ ПРИЛОГ 168

50 ГОДИНА ЦЕНТРА ЗА ПРИМЕЊЕНУ МАТЕМАТИКУ И ЕЛЕКТРОНИКУ

ИГРА СЛОВА И БРОЈЕВА

Пише пуковник Драган ТРИВИЋ

Вековима се криптографи боре да заштите тајност порука, док криптоаналитичари настоје да их разоткрију. Некад су у предности били једни, а некад други. Често се сматрало да је пронађена шифра „нерешива", али с временом је скоро свака разбијена, од првобитне шифре просте замене па до електромеханичке машине попут *енигме*. За данашње шифре сматра се да су потребне милијарде година да се разбију. Тако се мислило и у прошлости, па је време од милиона година сведено на свега неколико минута. Да ли ће се то исто десити или се већ десило и са данашњим шифрама?

Настојећи да омогуће бржу и лакшу размену информација људи су непрекидно усавршавали различите облике споразумевања. Први сукоби условили су потребу да се сазнају намере противника, али и да се прикрију садржаји информација ради очувања тајности сопствених намера. Почели су да се развијају поступци који су имали за циљ да у размени информација непозванима онемогуће приступ и евентуалну употребу. Заштита информација појавила се као производ жеље да своје поруке и намере на неки начин прикријемо и да их разуме само онај коме су намењене.

Војсковође великих битака често су познавале намере својих противника, што је доприносило њиховим успесима. Размена информација увек је била изложена могућностима прислушкивања и њиховог откривања, а када су информације падале у погрешне руке, последице су биле кобне. Опасност да противник дође до драгоцене информације утицала је на развој криптографије – технике којом се порука претвара у облик разумљив само ономе коме је намењена. Циљ криптографије није да сакрије постојање саме поруке, већ њено значење. Да би порука постала неразумљива, она се трансформише у неразумљив облик, према протоколу који познају само пошиљалац и прималац. Прималац инверзном трансформацијом претвара неразумљиву поруку у почетни, разумљив облик.

Због потребе да се сачува тајност информација настају криптографске службе, намењене за изналажење решења, смишљање и проналажење нових, што бољих шифри. Истовремено су противнички криптоаналитичари непрекидно покушавали да разбију шифре и дођу до тајних информација. Управо је ова непрекидна „борба" између криптографа и криптоаналитичара утицала на развој криптологије, науке која обједињава криптографију и криптоанализу.

Одређена шифра увек је изложена нападима криптоаналитичара. Када се дође до нових сазнања и механизама за њено разбијање, престаје да буде од било какве користи. Тада је потребно предузети мере да се шифра надогради и побољша, или да се осмисли и развије потпуно нова, отпорнија. Та нова шифра одмах постаје мета напада криптоаналитичара.

Непрестано надметање између оних који осмишљавају и развијају нове шифре и оних који покушавају да их разбију пресудно је утицало на развој великог броја научних достигнућа. Криптографи настоје да осмисле шифре које ће сачувати тајност информација, док криптоаналитичари непрекидно изналазе методе за њихово разбијање. Да би се ова „борба" могла уопште водити, потребно је велико знање из различитих научних области које су се развијале кроз векове – математика, лингвистика, електроника, информатика...

Од половине прошлог века све више доминира чињеница да информација има све већу вредност. Данас се мирно може рећи да онај ко влада информацијама, влада и простором и временом. Како информација постаје све драгоценија, тако и њена заштита има све важнију улогу, а криптографија је управо та која штити једно од најважнијих својстава информације – тајност. Потреба за заштитом тајности информације непрекидно расте.

Криптологија, као наука о тајности информација, углавном је и сама тајна. Рад криптолога често је такав да се не износи у јавност и дуго после престанка употребе одређене шифре. Сазнања до којих се долази дуго се јавно не објављују.

Почеци криптографије

Историја криптографије, од најстаријих записа до данас, прати њен развој од нивоа вештине и умећа до мултидисциплинарне науке. Разноврсне идеје и оригинална решења сведоче о ширини људске маште, духа, ума и генијалности појединаца.

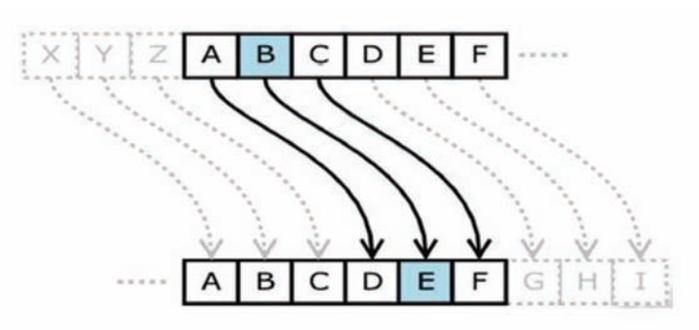
Зачеци криптографије уочавају се још у необичним хијероглифским записима на египатским гробницама. Хијероглифи су, како се сматра, били неразумљиви да би истакли моћ религијског текста.

Коришћење тајних писама помињао је још Херодот (484. п.н.е. – око 425. п.н.е.), „отац историје". Он је у свом делу „Историја", описујући сукобе између Грчке и Персије, који су се дешавали почетком 5. века п.н.е., описао како је послата порука, која је упозорила Спартанце на планирани напад Персијанаца. Тајно писмо послато је тако што је узета таблица за писање састављена од две плочице, са таблице је скинут восак и на дрвету плочице исписана порука о плановима Персијанаца, а затим је таблица поново преливена воском. Када су Грци прочитали поруку, организовали су одбрану и Персијанци нису постигли ефекат изненађења. У овом случају порука није трансформисана у неразумљив текст, већ је прикривано да она уопште и постоји. Постизање тајности на тај начин да се прикрије да порука уопште постоји назива се стеганографија. Пример стеганографије је, рецимо, невидљиво мастило.

У 5. веку п.н.е. забележено је и коришћење спартанске *скитале*, која представља један од првих примера класичне шифре премештања. То је био дрвени штап око којег је обмотавана трака, најчешће од коже. Пошиљалац поруке исписивао је поруку дуж штапа, а затим је трака одмотавана и на тај начин је изгледала као низ бесмислених знакова. На тај начин порука је била шифрована. Да би се прочитала, прималац је обмотавао траку око штапа истог пречника. Курир који је преносио траку везивао ју је уместо каиша, чиме је прикривано да порука уопште и постоји. Из тог времена позната је и хебрејска *атбаш* шифра.

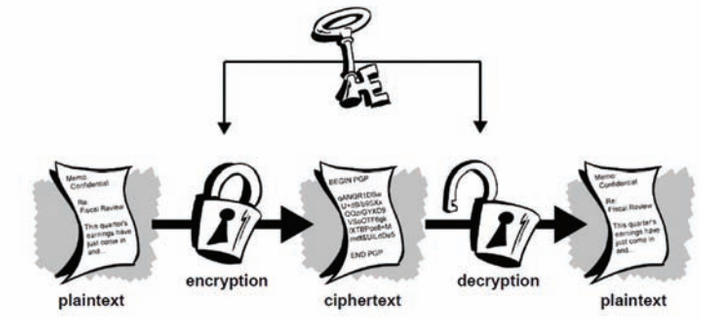
Прву шифру замењивања бележи Јулије Цезар. Цезар је једноставно свако слово поруке заменио словом које се у

абецеди налази три места даље. У криптографији се користе термини *почетни алфабет* (или *алфабет отвореног текста*) – алфабет којим је писана оригинална порука, и *шифровани алфабет* (или *алфабет кључа*) – састављен од слова којима су замењена слова из почетног алфабета.



Цезарова шифра

Цезар је померао слова за три места, а очигледно је да је њихово померање могуће у броју у зависности од броја слова у алфабету (на пример српски језик састоји се из 30 слова, па их је могуће на 30 различитих начина померити).



Шифровање и дешифровање

Свака шифра може се представити алгоритмом и кључем. Алгоритам представља криптографски метод, а кључ даје детаље одређеног поступка шифровања. У Цезаровој шифри алгоритам је *замена сваког слова,* а кључ је *број за колико места је померен алфабет*. Слово отвореног текста увек се замењивало једним истим словом кључа и ова шифра назива се *шифром просте замене*.

Безбедна шифра мора да обезбеди што већи број различитих шифарских кључева. Цезарова шифра је за један знак могла имати 25 различитих шифарских замена, колико је износио алфабет. Међутим, када би се слово из почетног алфабета могло заменити са било којим словом из шифрованог алфабета, тај број се повећава на 400.000.000.000.000.000.000.000.000 различитих кључева.

Настанак криптоанализе

Због своје једноставности и (у то време) поузданости, *шифра просте замене* била је заступљена током целог првог миленијума нове ере. Истовремено, био је развијен и систем безбедне комуникације, тако да се сматрало да нема потреба за даљим усавршавањем шифре, те да је због огромног броја могућих кључева практично нерешива. Међутим, криптоаналитичари и у том времену долазе до решења: уместо милијарди година потребних за разбијање шифре, до отвореног текста долазе за само неколико минута. Такву велику промену омогућио је развој лингвистике и статистике.

Метод за разбијање шифре просте замене, која је вековима употребљавана, успели су да пронађу арапски криптоаналитичари, у моменту када је и наука достигла одређени ниво развоја, а посебно лингвистика и математика. Арапски научници у периоду од 8. века проучавају језик, анализирају структуру речи и појединачних слова. Тада су открили да се у језику нека слова појављују чешће од осталих. У српском језику, на пример, најчешће се појављује слово „а" (око 11%), а најређе „ф" (око 0,2%). Откриће да се слова појављују у различитом проценту довело је и до нових сазнања у криптоанализи. Схватило се да је потребно имати криптограм „дугачак отприлике једну страну", пребројати колико се пута које слово у криптограму појављује, све док се сва не послажу, а затим слова из шифрата треба заменити словима из језика. Слово које се најчешће појављује у криптограму заменило би се словом које се најчешће појављује у стварном језику и тако све до слова које се најмање појављује. Очигледно је да је поступак једноставан и да је потребна само одређена дужина текста криптограма, у којем се испољава тзв. фреквенција (број појављивања) слова.

Криптографија у средњем веку

Криптографијом и криптоанализом у средњовековној Европи највише су се бавили монаси, који су проучавали скривена значења у Библији. Тек у 15. веку, за време ренесансе, када је дошло до развоја науке и образовања, криптографија доживљава процват. Тада је већ била развијена дипломатија, потреба за разменом и шифровањем порука била је све израженија, па државе оснивају шифрантска одељења. Знале су се слабости *шифре просте замене* и задатак криптолога био је да пронађу и развију бољу шифру, која ће заштитити поруке од противничких криптоаналитичара. Било је потребно разбити статистичке карактеристике језика, првенствено фреквенцију слова у језику.

Један од примера такве шифре је *двобројчана шифра.* Као што сам назив говори, у тој шифри слова су замењивана двоцифреним бројевима, а у шифрат су поред замена насумично убацивани и други двоцифрени бројеви. На пример, српски језик има 30 слова, двоцифрених бројева постоји 100, а ако рачунамо да је двоцифрени број са почетном цифром „0", онда остаје 70 двоцифрених бројева који се могу насумично уписивати у текст шифрата. Оваква шифра делимично отежава посао криптоаналитичарима, али и код ње је била довољна одређена дужина криптограма да би се једноставно могла разбити.

Покушај повећања поузданости шифре просте замене је и увођење *кодова,* који замењују слова, изразе, целе


A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
A Z Y X W V U T S R Q P O N M L K J I H G F E D C B
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

речи или реченице. На први поглед кодови имају предност у односу на шифре, јер су отпорнији на статистичке анализе. Међутим, имају и практичне недостатке. Било је потребно дефинисати кодне замене за хиљаде речи. Књиге кодова морале би имати и по неколико стотина страница и личиле би на речник. Било је потребно време и велики труд да се те књиге израде, а највећи недостатак је био да падну у руке противника. Тада су последице биле огромне: противник је могао да одгонетне све поруке и морало би се поново отпочети са дуготрајним процесом израде књиге кодова. Након израде књиге следио би процес достављања књиге свима који су укључени у тајну комуникацију. Са друге стране, коришћење шифре, код којих су кључеви далеко краћи и једноставнији за израду, било је практичније. Ако би противник дошао до кључа, било је једноставније и брже израдити нови кључ и лакше га дистрибуирати.

„Нерешива шифра"

Криптографи су имали велики задатак да измисле нову и јачу шифру, коју криптоаналитичари неће моћи разбити. Таква шифра није се појавила све до краја 16. века, а њени корени иду у 15. век, до појаве *Албертијеве шифре,* коју је осмислио фирентински математичар Леон Батиста Алберти, око 1467. године, по којем је и добила име. У овој шифри су се уместо једног, као што је било у Цезаровој шифри, користила два или више шифрованих алфабета (алфабета кључа), на тај начин што су се слова из почетног алфабета наизменично замењивала словима из различитих шифарских алфабета. Што је више шифарских алфабета, квалитет шифре био би бољи и све више би се разбијале карактеристике језика. Албертијево откриће било је једно од најзначајнијих у криптографији у последњем миленијуму, али не и у потпуности заокружено. Његово дело „Расправа о шифри" први пут анализира језик и поставља математичке темеље криптографије.

Албертијеву шифру касније је разрађивало више научника, а коначно ју је уобличио Блез де Вижнер, француски дипломата рођен 1523. године. Вижнерова шифра уместо једног, користи 26 шифрованих алфабета и назива се *шифра сложене замене.*

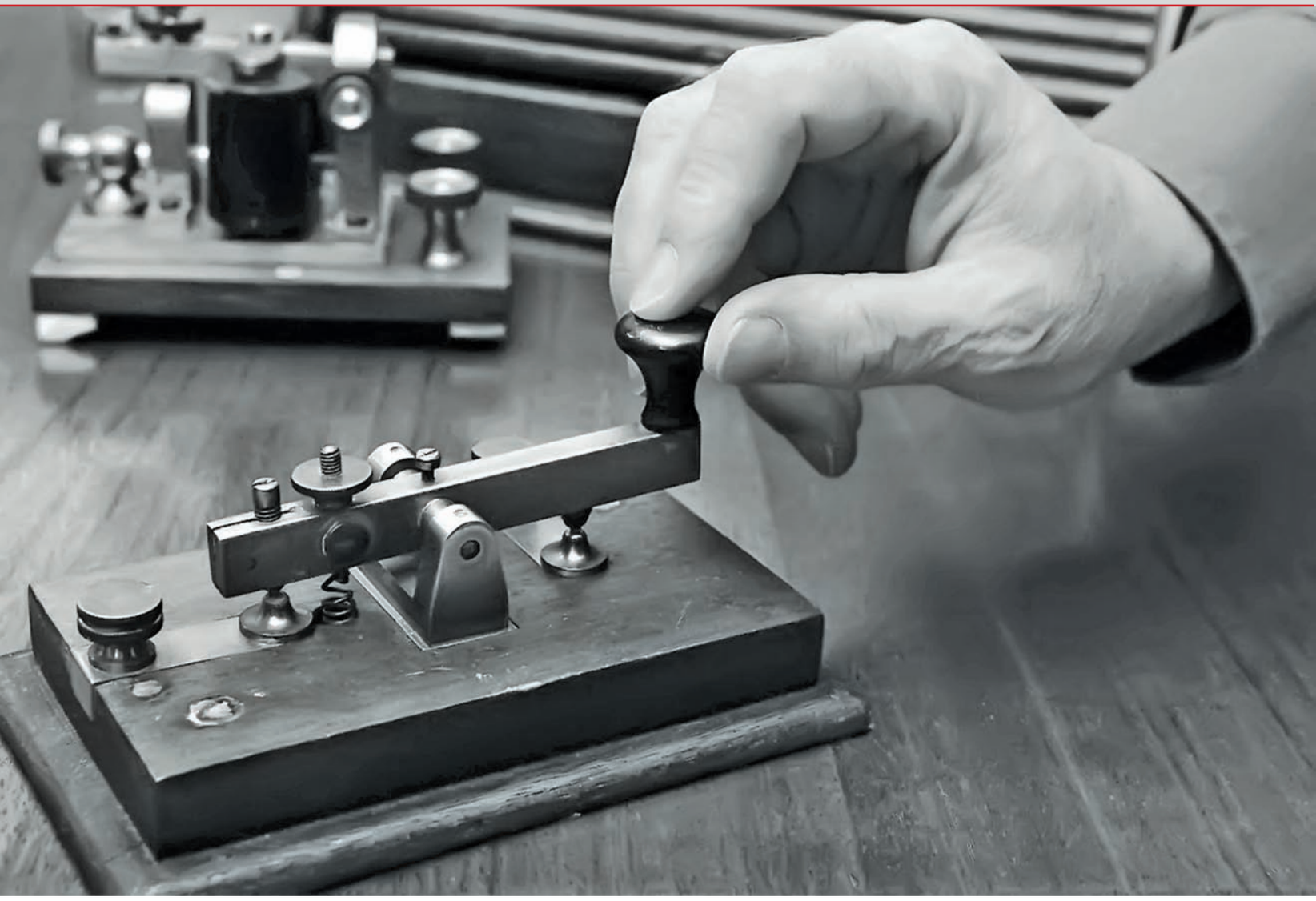
За разлику од шифара просте замене, та шифра уместо једног користи 26 различитих шифрованих алфабета. Из Вижнеровог квадрата уочава се да се свако слово отвореног текста може заменити било којим словом, односно може имати 26 различитих шифарских замена. Ако би се за шифровање користио само један шифровани алфабет, то би у ствари била Цезарова шифра просте замене, који се са лакоћом разбија. Међутим, Вижнерова шифра примењује се тако да се за свако слово из поруке користи различити ред из Вижнерове шифре, односно различити шифровани алфабет. На пример, ако се користи други ред из Вижнеровог квадрата слово „а" замењује се словом „б", а ако се користи последњи ред, слово „а" заменило би се словом „з". Било је битно само утврдити на који начин се прелази из реда у ред, а то се постиже помоћу кључа. У то време кључ је био одређена, такозвана *кључна реч*, која се приликом шифровања понављала.

Вижнерова шифра је таква да је могуће у потпуности разбити статистичке карактеристике језика, што је био огроман напредак у развоју криптографије. Такође може имати и огроман број различитих шифарских кључева, што криптоаналитичару онемогућава да их све испроба. Кључ може бити било која реч, реченица или нешто потпуно измишљено. Међутим, и поред изузетне снаге ове шифре, није била довољно прихваћена, како због неопходних поступака који су се морали применити у њеном коришћењу, тако и због тренутног развоја комуникација, које су наравно у то време биле на нивоу курира. Чак и тамо где је безбедност била од изузетног значаја, избегавала

Вижнерова шифра

Алфабет отвореног текста

Алфабет кључа	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	T	U	V	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	T	U	V	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	T	U	V	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	T	U	V	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	T	U	V	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	R	S	T	U	V	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	R	S	T	U	V	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	R	S	T	U	V	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	R	S	T	U	V	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	R	S	T	U	V	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	R	S	T	U	V	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	R	S	T	U	V	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	R	S	T	U	V	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	R	S	T	U	V	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	R	S	T	U	V	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	R	S	T	U	V	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	R	S	T	U	V	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
R	R	S	T	U	V	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
S	S	T	U	V	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	R
T	T	U	V	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S
U	U	V	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	T
V	V	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	T	U
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	T	U	V



Телеграфија

се њена примена, већ се покушавало пронаћи неко компромисно решење, сложеније од шифре просте замене, а једноставније од Вижнерове шифре.

Телеграф и радио

Компромисна решења било је могуће применити у 17. веку, али већ од 18. века криптоанализа улази у масовну употребу. Све тадашње велике европске силе имале су организоване службе за декриптовање порука и прикупљање обавештења, такозване црне коморе. Пристигла писма, која су на пример била упућена амбасадама, а била су шифрована, прво су завршавала у овим службама. Ту су писма одмах отварана, прављени су дупликати рукописа, поново пакована у оригиналне коверте и за неколико сати враћана у пошту да би била достављена правим примаоцима. Копије писама достављане су криптоаналитичарима, који су ефикасно разбијали све врсте шифара просте замене. Оваква ситуација приморала је криптографе да коначно прихвате сложенију, али далеко сигурнију Вижнерову шифру. Криптоаналитичари су приморали криптографе да са шифара просте, пређу на шифре сложене замене, које боље разбијају статистичке карактеристике језика.

У то време долази и до индустријске револуције, која је од краја 18. до средине 19. века темељно изменила раније политичке, привредне и друштвене системе у већем делу света. Долази до развоја *телеграфа,* који је додатно поставио захтеве за безбеднију криптографску заштиту порука. Проналазак Морзеовог кода, 1838. године, којим се свако слово алфабета представља одређеном комбинацијом тачака и цртица, представља револуцију у систему преноса информација.

Телеграфија и примена Морзеовог кода брзо се шири и постаје све значајнија. Криптографска заштита постаје све већи проблем, јер Морзеова азбука, сама по себи, не представља шифру и порука ни на који начин није скривена. При слању и пријему поруке у њу има увид велики број лица. Морао се пронаћи начин да се порука заштити, а решење је било да се шифрује пре него што се преда оператеру, који је претвара у Морзеов код. Било је потребно поруку пре преноса што више скратити, тако да се на сцену поново враћају кодови, усавршени по обиму и садржају. Помоћу кодова

целе речи, групе речи или реченице могле су се замењивати одговарајућом кратком заменом.

Најбољи начин за криптографску заштиту и даље је била Вижнерова шифра, јер се сматрало да се не може разбити. Постала је позната под називом *chiffre indéchiffrable* – нерешива шифра. У то време криптографи су били у предности у односу на криптоаналитичаре.

Пред криптоаналитичарима се појавио нови задатак – како разбити шифру сложене замене? Код шифара просте замене задатак је наравно био много лакши – препознавала се одређена статистичка карактеристика језика, најчешће фреквенција слова. Код шифара сложене замене то наизглед није било тако, јер се свако слово шифрује на различити начин, у чему лежи снага шифре. Као кључ код Вижнерове шифре може се користити кључна реч, реченица или неки потпуно неразумљив текст. Ако је као кључ коришћена кључна реч, на пример реч КРИПТО, свако слово отвореног текста може се шифровати на шест различитих начина, јер се кључ састоји од шест различитих слова. Ово наизглед делује као добро решење, али у суштини даје могућност разбијања Вижнерове шифре, јер је практично свако шесто слово криптограма шифровано истим кључем, односно криптограм се може разложити на шест шифара просте замене које се веома лако разбијају.

Кад су криптоаналитичари анализом криптограма најзад дошли до тог открића, приметивши да се одређени делови криптограма понављају, предност криптографа почела је да се топи. Разлагањем криптограма, проналазили су кључну реч која је коришћена као кључ за шифровање. Развијене су технике за криптоанализу, а откриће је приписано Фридриху Вилхелму Касиском, пензионисаном официру пруске армије, који 1863. године издаје епохалну књигу „Тајно писмо и уметност декриптовања", у којој објављује до тада нерешив проблем – декриптовање шифре периодичним кључем. Тест је по њему и назван „тест Касиског". Суштина је била у томе да су код примене Вижнерове шифре коришћени кључеви мале дужине, најчешће кључне речи. Приликом шифровања кључ је најчешће био логична реч, мале дужине, која се периодично понављала. Показало се да само кључеви који су велике дужине, који нису логични и који се не понављају пружају потребну сигурност, што у то време у пракси није био случај.

Овим открићем криптоаналитичара Вижнерова шифра више није била безбедна, посебно без далеко квалитетнијих и за израду сложенијих шифарских кључева. Телеграфија се све више развијала и било је потребно уложити огромне напоре и трошкове да би се обезбедили кључеви потребне дужине, који се не би периодично понављали. Пред криптографима се тако поново, пред крај 19. века, појавио нови задатак. Било је потребно пронаћи нови поступак који би сачувао тајност порука. Крајем века долази до још једног великог проналаска: бежичног преноса информација, односно ради-

ја. Домет радија повећао се веома брзо, од почетних неколико километара на прекоокеанске даљине. Тим открићем сигурна криптографска заштита постаје још неопходнија.

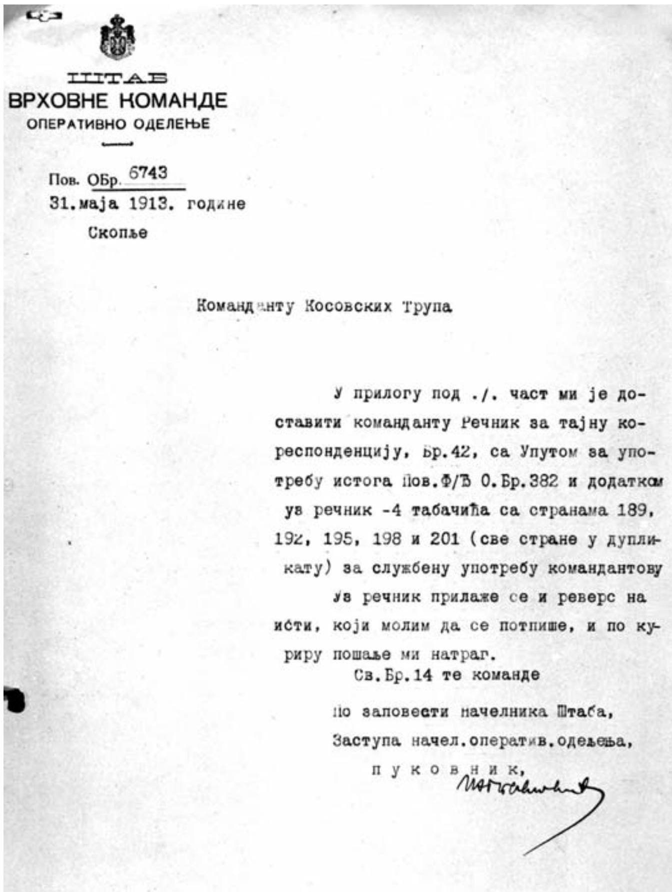
Откриће радија буди велико интересовање и у војним круговима. Његове предности у односу на жицу биле су очигледне: велики домет, могућност комуникације са било које две тачке. Постављање жица често је било непрактично, а понекад и немогуће. Али, радио је имао и једну велику слабост: поруке се лако прислушкују, па је сигурна и поуздана шифра постала истински неопходна.

Врло брзо по проналаску телефона, јављају се и прве идеје о криптографској заштити говора, а ускоро је патентирано и прво решење. Ипак, практична примена нових идеја заживела је тек између два светска рата.

Шифре у Србији

О употреби шифре у Србији у периоду пре балканских ратова и Првог светског рата постоји мало трагова. Осамдесетих година 19. века, за време владавине Милана Обреновића, употребљавају се кодови, односно речник за тајну војну кореспонденцију.

У листу „Ратник”, у броју из септембра 1905. године, објављен је чланак „Војна криптографија или шифровање и дешифровање депеша”, који је написао Никола Ј. Дероко, инжињеријски капетан прве класе. У чланку даје кратак


ШТАБ
ВРХОВНЕ КОМАНДЕ
ОПЕРАТИВНО ОДЕЛЕЊЕ

Пов. ОБр. 6743
31.маја 1913. године
Скопље

Команданту Косовских Трупа

У прилогу под ./. част ми је доставити команданту Речник за тајну кореспонденцију, Бр.42, са Упутом за употребу истога Пов.Ф/Ђ О.Бр.382 и додатком уз речник -4 табачића са странама 189, 192, 195, 198 и 201 (све стране у дупликату) за службену употребу командантову

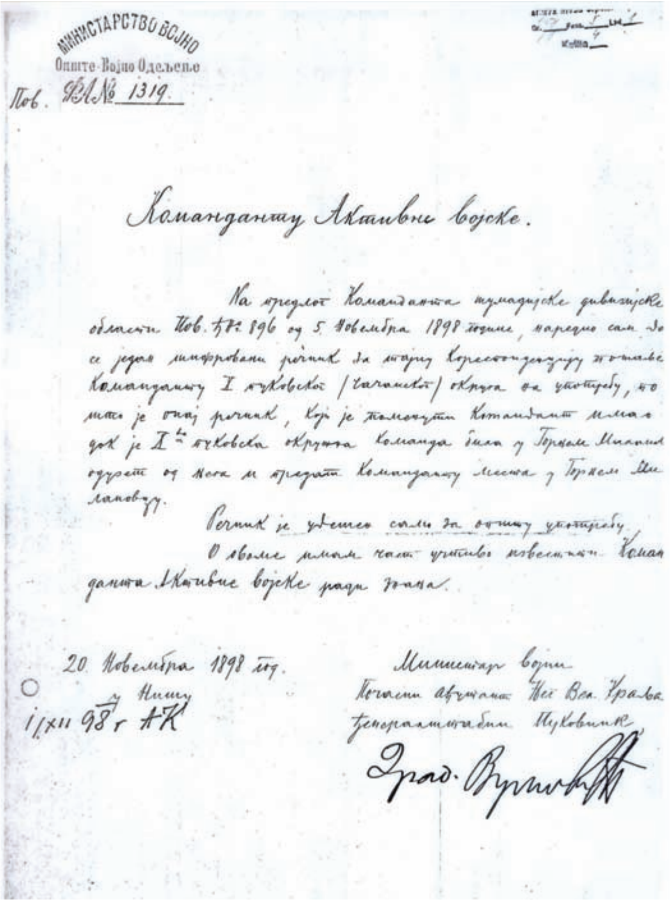
Уз речник прилаже се и реверс на исти, који молим да се потпише, и по куриру пошаље ми натраг.

Св.Бр.14 те команде

По заповести начелника Штаба,
Заступа начел.оператив.одељења,
пуковник,

Акт из 1913. године

Акт из 1898. године


МИНИСТАРСТВО ВОЈНО
Опште-Војно Одељење
Пов. ФАЊ 1319

Команданту Активне војске.

На предлог Команданта шумадијске дивизијске области Пов. [illegible] 896 од 5. Новембра 1898 године, [illegible]

20. Новембра 1898 год.
у Нишу

Министар војни
[illegible]

ТАЈНО ДОГОВАРАЊЕ У СРПСКОЈ ВОЈСЦИ

„Данас, кад је примена телеграфа врло распрострањена и кад је у свим Европским војскама и коњица снабдевена телеграфом, опасност од крађе депеша постала је тако велика, да упорно захтева изналажење средстава за сузбијање те опасности. Као најбоља средства против крађе депеша биће правилно организована служба у чувању телеграфских линија на позорници војних дејстава и шифровање депеша. Кореспонденција у шифрама усвојена је данас готово у свим европским војскама.”

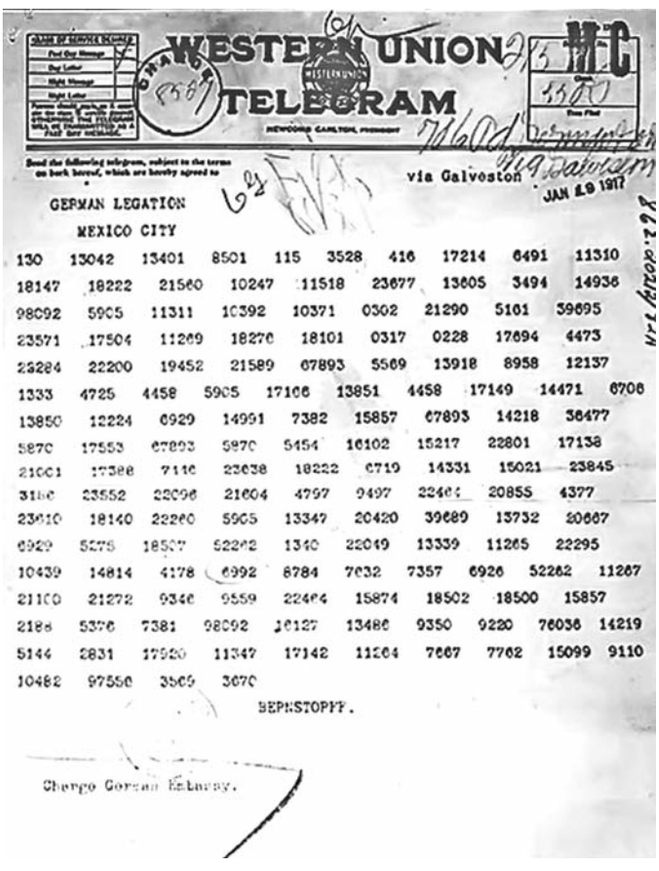
„Најбољи ђенерали мишљења су данас, да је неопходно потребно, да разни команданти једне армије имају известан систем тајног договарања, да би могли слободно кореспондирати не само између себе и с главним командантима, него и са својим потпоручницима. Тако на пример тактичар, којег поменусмо, мисли да треба шифром снабдети у мирно и ратно време ђенерале, шефове пукова, команданте колона и стража...

Ту ствар треба предвидети и уредити пре рата,..., јер кад су једном операције већ почеле, сувише је доцкан мислити на то. Уосталом, чак и за време мира потребно је, и то сваког тренутка, тајна кореспонденција”.

(Из листа „Ратник”, септембар 1905. године)

историјски преглед и значај војне криптографије, савремени значај и стање војне криптографије, погодбе којима треба да одговори војна криптографија, разне методе у криптографији (премештања, замењивања, шифре с двојним и тројним кључем...), описује шифроване речнике. У закључку пише: „Да видимо како то питање стоји код нас. У колико је познато, *ми за сада имамо само криптографски речник (шифру) усвојен за тајну кореспонденцију између појединих надлештава*. У одељку, где смо говорили о шифрованим речницима изложили смо јасно да сам шифровани речник има много својих незгода и да не може да задовољи ратне потребе ... Очигледно је, дакле, да би смо и ми требало да за ратну употребу усвојимо какву практичну криптографску систему. Остаје само да видимо каква би система најбоље одговорила циљу. Рекли смо: што је система сложенија, у толико ће теже бити њено дешифровање без кључа; али уколико је система сложенија, утолико је тежа и неизводљива за употребу. Тај захтев, да система буде што тежа за дешифровање, има места код великих војсака, у којима ће бити и људи специјално спремни за службу дешифровања без кључа и откривања тајних депеша, које су од непријатеља ухваћене. Код малих војсака, као што је наша, или наших вероватних противника, једва ће бити кога, који би се специјалисао за овај посао. Без нарочите спреме или праксе није лако постати дешифрант, јер овај посао сем велике умешности, оштроумља... изискује још и дуговремену праксу. Значи, дакле, да би смо ми требало да усвојимо такву систему, где су у превази лака употреба и проста, те да можемо, кад справу за шифровање изгубимо, или је заборавимо, и сами ову за сразмерно врло кратко време да направимо".

Цимерманов телеграм


WESTERN UNION TELEGRAM

via Galveston

JAN 19 1917

GERMAN LEGATION
MEXICO CITY

130 13042 13401 8501 115 3528 416 17214 6491 11310
18147 18222 21560 10247 11518 23677 13605 3494 14936
98092 5905 11311 10392 10371 0302 21290 5101 39695
23571 17504 11269 18276 18101 0317 0228 17694 4473
23284 22200 19452 21589 67893 5569 13918 8958 12137
1333 4725 4458 5905 17166 13851 4458 17149 14471 6706
13850 12224 6929 14991 7382 15857 67893 14218 36477
5870 17553 67893 5870 5454 16102 15217 22801 17138
21001 17388 9116 23638 18222 6719 14331 15021 23845
3186 23552 22096 21604 4797 9497 22464 20855 4377
23610 18140 22260 5905 13347 20420 39689 13732 20667
6929 5275 18507 52262 1340 22049 13339 11265 22295
10439 14814 4178 6992 8784 7632 7357 6926 52262 11267
21100 21272 9346 9559 22464 15874 18502 18500 15857
2188 5376 7381 98092 16127 13486 9350 9220 76036 14219
5144 2831 17920 11347 17142 11264 7667 7762 15099 9110
10482 97556 3569 3670

BEPNSTORFF.

Chargé German Embassy.

Управо пред балканске ратове и Први светски рат, поред постојећег речника за тајну војну кореспонденцију, долази до увођења других, мање сложених шифара, које нису имале велику криптолошку вредност, али су биле практичне и једноставне за употребу.

Први светски рат

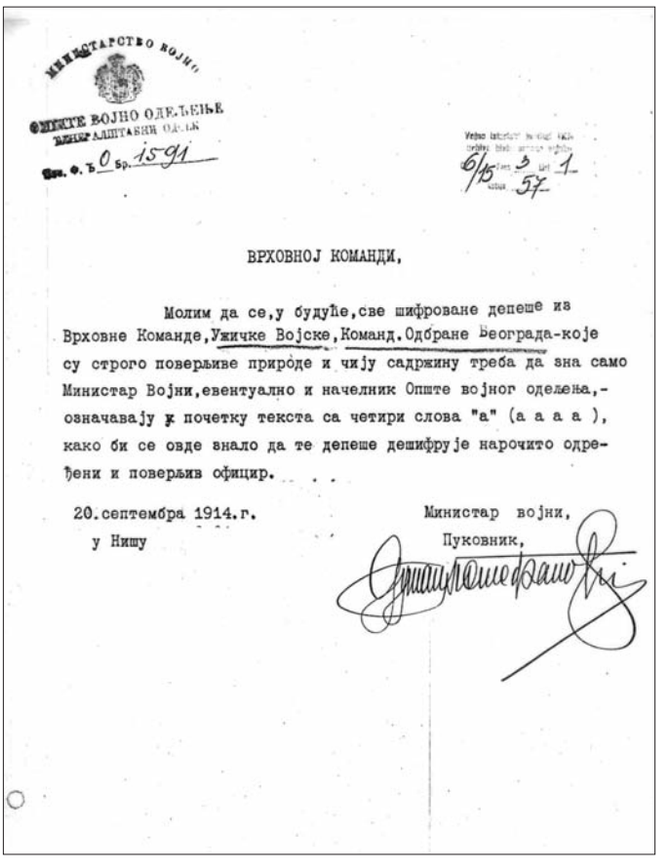
По избијању Првог светског рата у фокус интересовања долазе и добре и лоше особине радија. Било је потребно пронаћи најбољи начин да се искористи једноставност комуникација радио-везом, уз истовремено једноставно, ефикасно и поуздано шифровање. Међутим, у периоду Првог светског рата није дошло до значајнијих криптографских открића. Осмишљено је неколико нових шифара, али су све биле разбијене, јер су најчешће биле комбинације и варијације шифара из 19. века. Оне су у почетку пружале одређену сигурност, али су их криптоаналитичари релативно брзо разбијали. За криптоаналитичаре у Првом светском рату проблем и изазов представљао је сам обим радио-саобраћаја.

Сматра се да су француски криптоаналитичари били најбоље организовани и најефикаснији, јер су имали најјачи и најспособнији тим. Своју криптоанализу заснивали су на открићима Аугуста Керкхофа, који је 1881. године објавио једну од најзначајнијих књига у криптографији „Војна криптографија", у којој поставља основне принципе за добар криптосистем. Ови принципи су и данас актуелни. Основни принцип је да тајност криптографски заштићене комуникације лежи у тајности криптографског кључа, а не и криптографског алгоритма.

Поред Француза, знатан допринос криптоанализи у Првом светском рату дали су и Американци и Британци. Случај декриптовања Цимерманових телеграма, ухваћеног у јануару 1917. године, утицао је и на исход Првог светског рата.

Познато је да су Сједињене Америчке Државе све до априла 1917. године биле неутралне и да је амерички председник Вудро Вилсон одбијао да пошаље америчке трупе у рат. Цимерман, у то време министар спољних послова Немачке, шаље телеграм немачком амбасадору у САД, који га касније прослеђује свом колеги у Мексику. Телеграм је садржао обавештење о намери Немачке да отпочне подводни рат без ограничења. У случају да САД не остану неутралне, Мексику се предлаже савез за поновно освајање делова територије Сједињених Америчких Држава. Од амбасадора Немачке у Мексику тражи се да о томе обавести председника, да се позове и Јапан да нападне САД са запада, чиме би се спречило евентуално учешће САД на европском ратишту. Декриптовање овог телеграма довело је до промене одлуке САД о неутралности и њиховог уласка у рат.

Готово до окончања Првог светског рата криптоаналитичари били су у предности у односу на криптографе. Та предност практично је трајала још од криптоанализе Ви-



ВРХОВНОЈ КОМАНДИ,

Молим да се,у будуће,све шифроване депеше из Врховне Команде,Ужичке Војске,Команд.Одбране Београда-које су строго поверљиве природе и чију садржину треба да зна само Министар Војни,евентуално и начелник Опште војног одељења,- означавају к почетку текста са четири слова "а" (а а а а), како би се овде знало да те депеше дешифрује нарочито одређени и поверљив официр.

20.септембра 1914.г.
у Нишу

Министар војни,
Пуковник,

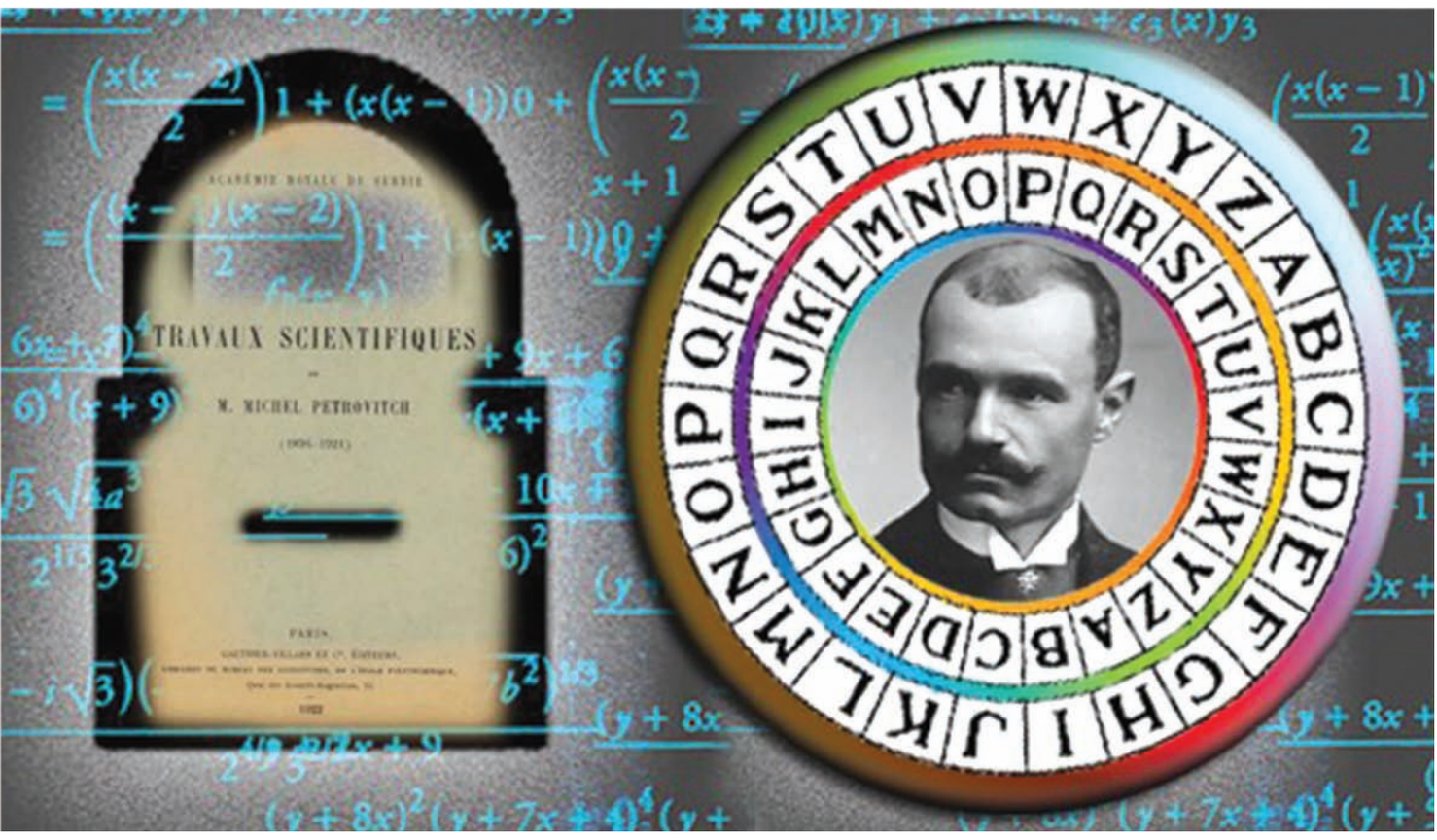
Акт из 1914. године

Михаило Петровић Алас

жнерове шифре. Међутим, пред крај рата долази до новог успеха криптографа, који су открили да Вижнерова шифра може понудити савршену безбедност информација. Дотадашњи проблем с којим су се суочавали криптографи био је у слабости кључа који је коришћен за шифровање. Установили су да се квалитет шифре драстично побољшава ако се кључна реч продужи.

Како се рат приближавао крају, установљен је концепт случајног кључа – кључа који се није састојао од логичних речи већ од низа насумично поређаних слова. Ускоро су израђене свеске са стотинама редова насумично исписаних слова. Кључеви су израђивани у по два примерка, за пошиљаоца и примаоца. Свеске су се састојале из листова који би се уништавали одмах после употребе, да се не би више пута употребио исти кључ за две или више различитих порука. Једини начин за разбијање оваквог криптограма је потрага за свим могућим кључевима, што је било апсолутно немогуће.

Шифре у којима је кључ у потпуности случајан и не понавља се, *апсолутно су сигурне*. Међутим, и поред апсолутне теоријске сигурности, такве шифре су у пракси имале недостатке и слабо су употребљаване. Први проблем био је са количином потребних кључева. Дневно се размењивао велики број порука и биле су потребне свеске и свеске случајних кључева, што је био огроман задатак, који је захтевао много напора и новца. Други проблем био је дистрибуција тако израђених свезака случајних кључева, што је у ратним дејствима изузетно компликовано. У пракси су се свеске са случај-



ним једнократним кључевима користиле тамо где су постојале потребе за апсолутном сигурношћу комуникација.

Војска Краљевине Србије је уочи Првог светског рата располагала одређеном количином радио-телеграфских станица, а део станица набавила је и непосредно по избијању рата. Због бојазни од прислушкивања, те станице употребљаване су само за проверу везе и прислушкивање непријатељског радио-саобраћаја, а никако за предају телеграма и пренос тајних информација. За пренос шифрованих информација коришћене су жичне и курирске везе. Чак је и Аустроугарска на крају рата признала да је успела да декриптује шифроване телеграме свих европских вој-

	1	*4*	*0*	*2*	*3*	*8*	*9*	*6*	*7*	*5*
8	00	01	02	03	04	05	06	07	08	09
4	10	11	12	13	14	15	16	17	18	19
0	20	21	22	23	24	25	26	27	28	29
9	30	31	32	33	34	35	36	37	38	39
2	40	41	42	43	44	45	46	47	48	49
6	50	51	52	53	54	55	56	57	58	59
1	60	61	62	63	64	65	66	67	68	69
3	70	71	72	73	74	75	76	77	78	79
5	80	81	82	83	84	85	86	87	88	89
7	90	91	92	93	94	95	96	97	98	99

Три картона

ски осим српске, јер се у њој тајне информације нису преносиле радио-везом.

Основни начини заштите тајности порука у српској војсци биле су шифре просте замене и премештања, као и употреба кодова, односно речника за тајну војну кореспонденцију. Најпознатији речник за тајну војну кореспонденцију, употребљаван и на Солунском фронту, израђен је 1917. године. У својој садржини и техничкој обради био је један од најбољих таквих речника у то доба. Тај речник користила је и југословенска војска, а остао је у употреби све до 1939, када је престао да се користи. Садржао је око 50.000 слова, слогова, речи и израза. Речник је био подељен у два дела. Први део обухватао је слогове и одломке речи, а други је садржао целе речи и најчешће изразе. Да би се сачувала тајност речника, више пута је извршавана пренумерација страна и израза кода и мењао се сам начин шифровања – формирања комбинација петоцифрених група. У речнику је било одштампано и упутство за шифровање, а уз речник је постојао и засебан додатак „Кључ за шифровање". Претпоставља се да је по том додатку вршено „надшифровање", односно дупло шифровање кодних замена добијених из речника. Групе добијене шифровањем по коду претварале су се у неке друге словне и бројчане групе, чиме се добијало на квалитету шифре.

Знатан допринос развоју шифре у Великом рату, а и касније, све до почетка Другог светског рата, дао је и наш чувени математичар Михаило Петровић Алас. Његова веза са војском, првенствено кроз рад у криптографији, трајала је

РАЗРЕЗ

Речника за тајну војну кореспонденцију, издање Министарства војске и морнарице Стр.Пов.Ђ.ОБ.Бр. 171 од 8 фебруара 1927 године, намењен за употребу у мирно, мобилно и ратно доба.

Редни број	НАЗИВ ЈЕДИНИЦЕ И ЗА КОГА			Колико комада	Примедба
1	Војна кућа Њ. В. Краља — за Првог Ађутанта Њ. В. Краља			5	
2	Министарство војске и морнарице	за Обавештајни отсек Ђенералштабног одељења		4*)	
3	Министарство војске и морнарице	за Команду позадње железничко-пловидбене службе		1***)	
4	Врховна инспекција војне силе — за начелника штаба			1	
5	Главни ђенералштаб - за секцију шифре Обавештајног одељења			4**)	
6	Инспекција земаљске одбране — за начелника штаба			1	
7	Команда	Београда	за ђенералштаб	1	
8	Команда	Краљеве Гарде	за ђенералштаб	1	
9	Команда	Жандармерије — за Команданта		1	

Разрез Речника за тајну војну коресподенцију 1 и 2

— 2 —

Редни број	НАЗИВ ЈЕДИНИЦЕ И ЗА КОГА			Колико комада	Примедба
10	ШТАБ	армиске области	за ђенералштаб	2	
11	ШТАБ	дивизиске области	за ђенералштаб	2	
12	ШТАБ	коњице	за начелника штаба	1**)	
13	ШТАБ	инжињерије	за начелника штаба	1**)	
14	ШТАБ	Боке Которске — за Ђенералштабно одељење		2*)	
15	ШТАБ	Шибеника	за ђенералштаб	2*)	
16	ШТАБ	Утврђивања	за ђенералштаб	1*)	
17	ШТАБ	Граничне трупе — за начелника штаба		2	
18	ВОЈНИ ИЗАСЛАНИК	У Сједињеним америчким државама	ЗА ВОЈНОГ ИЗАСЛАНИКА	1	
19	ВОЈНИ ИЗАСЛАНИК	У Енглеској	ЗА ВОЈНОГ ИЗАСЛАНИКА	1	
20	ВОЈНИ ИЗАСЛАНИК	У Француској	ЗА ВОЈНОГ ИЗАСЛАНИКА	1	
21	ВОЈНИ ИЗАСЛАНИК	У Италији	ЗА ВОЈНОГ ИЗАСЛАНИКА	1	
22	ВОЈНИ ИЗАСЛАНИК	У Немачкој	ЗА ВОЈНОГ ИЗАСЛАНИКА	1	
23	ВОЈНИ ИЗАСЛАНИК	У Мађарској	ЗА ВОЈНОГ ИЗАСЛАНИКА	1	
24	ВОЈНИ ИЗАСЛАНИК	У Румунији	ЗА ВОЈНОГ ИЗАСЛАНИКА	1	
25	ВОЈНИ ИЗАСЛАНИК	У Бугарској	ЗА ВОЈНОГ ИЗАСЛАНИКА	1	
26	ВОЈНИ ИЗАСЛАНИК	У Грчкој	ЗА ВОЈНОГ ИЗАСЛАНИКА	1	
27	ВОЈНИ ИЗАСЛАНИК	У Турској	ЗА ВОЈНОГ ИЗАСЛАНИКА	1	

више од пола века, све до почетка Другог светског рата у Југославији. Михаило Петровић је још 1898. године положио испит за резервног потпоручника, учествовао у Првом балканском, а затим и у Великом рату. У чин мајора произведен је 1921, а у чин потпуковника 1925. године. Као потпуковник дочекао је и Други светски рат.

Михаило Петровић је 1917. године израдио нови систем шифри, који је одмах ушао у употребу. Тај систем, назван Три картона, усавршаван је и после рата и дуго се задржао у раду војске и дипломатије. Њиме је задржана једноставност употребе, уз истовремено повећање сигурности шифре и броја могућих шифарских кључева, што је давало знатну предност у односу на друге шифре које су тада употребљаване у српској војсци.

Између два светска рата

По стварању Југославије (Краљевина СХС) 1918. године, пред новом државом стајали су задаци организације државног апарата и војске, а самим тим и службе за тајну кореспонденцију. Краљевина Срба Хрвата и Словенаца није имала времена за израду нових шифара и кодова, већ је за потребе војске и тајне дипломатске кореспонденције преузет „Речник за тајну војну кореспонденцију српске војске", израђен 1917. године.

По Уредби о Главном ђенералштабу и ђенералштабној струци из 1923. године, Обавештајно одељење делило се на четири секције, а четврта секција бавила се студијама и израдама војних шифара. Новом Уредбом о Главном ђенералштабу из 1927. године секције су преименоване у одсеке, али су практично задржале исте надлежности.

Нови код за тајну кореспонденцију у војсци израђен је 1925. године и дат на употребу. Тај код је по уређењу био бољи од претходног, јер је био „несређен", тј. слова, слогови, речи и изрази су у првом делу речника (шифрант) били поређани апсолутним алфабетским редом, док су шифарске замене, које су се састојале од петоцифрених група, биле исписане поред сваког израза без икаквог реда, потпуно испретуране. Други део речника (дешифрант) садржавао је све петоцифрене шифарске замене сређене апсолутним децималним редом, а крај њих су биле исписане одговарајуће речи – изрази. Оваква подела омогућавала је брже шифровање и дешифровање порука. Међутим, тај код је, због сумње да је компромитован, убрзо стављен ван употребе.

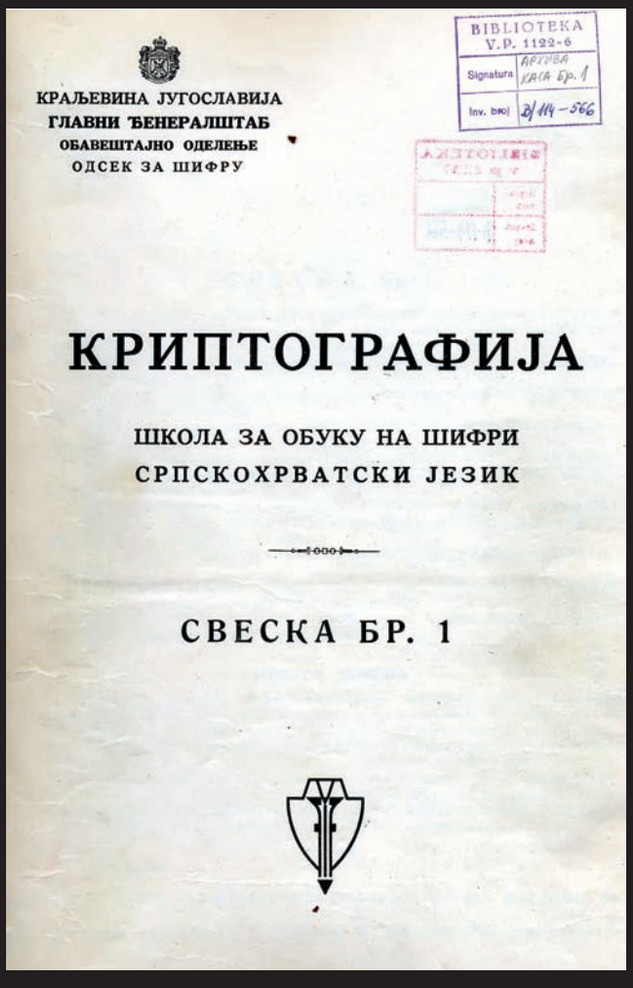
Следећи код издат је 1929. године, за тајну кореспонденцију у војсци и са војним изасланицима у иностранству. Остао је у употреби све до капитулације 1941. године. И по том коду се сваки текст додатно шифровао по одређеном кључу. Постојале су две врсте кључева за шифровање: за саобраћај унутар земље и за саобраћај са војним изасланицима ван земље.

Поједине установе израђивале су и сопствене кодове за своје потребе. Команда жандармерије израдила је код са 30.000, а Команда морнарице са 75.000 слова, слогова, речи и израза.

До 1935. године криптографија је у југословенској војсци била слабо коришћена. Мали број официра ју је познавао и њом се бавио. У војсци су постојала свега два официра, пуковник Живко Стефановић и капетан Златија Мишковић, која су завршила курс криптографије у Француској. Због слабог познавања криптографије и недостатка потребног добро обученог кадра, исте године Одсек за шифру, у саставу Обавештајног одељења Главног ђенералштаба, као највиши орган те службе, организује курс криптографије у трајању од шест месеци. Курс је био организован дописним путем. Сви примљени официри, а било их је 300, поред својих редовних дужности решавали су (декриптовали) задатке из укупно седам свезака које су добијали за време трајања курса. Све свеске су садржавале основне системе шифровања, дешифровања и декриптовања простијих шифара.

Мада је циљ курса био доста амбициозан, да се одабере официри који имају смисао за криптологију, већ кроз месец дана број слушалаца драстично се смањио, па их је остало свега једна трећина. На крају, курс је са успехом завршило само 14 слушалаца, док је још њих 30 уведено у евиденцију за накнадно усавршавање. Завршни курс за пр-

Свеска „Криптографија", насловна и прва страна



вих 14 официра био је организован у Обавештајном одељењу Главног ђенералштаба и трајао је 45 дана. Ту се допуњавало стечено знање и решавали компликованији задаци из криптологије из још, у међувремену израђене, три свеске са задацима. На крају курса слушаоци су били упознати са кодовима који су били на употреби (кодови 1917, 1925. и 1929. године) и приказан им је начин рада са машинама за шифровање, које још нису биле у употреби, али се испитивала њихова сигурност и вредност.

Виши курс успешно је завршило свих 14 слушалаца, од којих су петорица одређена на дужност у Обавештајном одељењу, по један у штабове пет армијских области, по један у команде ваздухопловства, морнарице и граничне трупе, док је један слушалац био распоређен у Команду жандармерије, мада тамо никад није упућен. После тога курсеви из криптографије нису се више одржавали. Касније су израђене још четири свеске, које су достављене свим официрима, којима је био признат претходни курс, да решавају задатке и уче методе шифровања.

Усавршавање официра и криптографске службе правилно се развијало до 1938. године, када је пензионисан пуковник Живко Стефановић, који се залагао за усавршавање официра специјализованих за шифру и који је највише допринео да се криптографија у Војсци уздигне на потребан ниво. Његовим пензионисањем осетно опада интересовање за криптографију. Рад се свео на шифровање и дешифровање и израду нових шифара и упутстава, док је проучавање страних шифара и даље усавршавање официра специјализованих за шифру скоро у потпуности запостављено.

Поред описаних кодова постојали су и други, како у војсци, тако и у цивилним установама. У то време постојала је и радио-телеграфска шифра, којом су руковали сами послужиоци на радио-уређајима. То је била таблица 22×22 поља, а у сваком пољу налазило се слово или израз. Шифровали су по принципу просте замене. Циљ ове шифре био је да се послужиоци увежбавају у примопредаји шифрованих порука, а не за обезбеђење тајности порука.

За потребе мобилизације била је израђена таблица 10×10, у којој су се у квадратима налазила слова, слогови и речи. Носила је назив „таблица А" и чувана је као највећа тајна. Таблице су биле запечаћене и достављене јединицама, уз напомену када се могу употребити. И ово је била шифра простог замењивања, једноставна за декриптовање. Постојало је још око 30 шифри намењених за употребу у току рата. Шифре са упутствима чувале су се у Одсеку за шифру Обавештајног одељења у потребном броју примерака, колико је било предвиђено по ратној формацији јединица. За случај рата нису били предвиђени кодови, због њихове непрактичности, већ углавном шифре сложене замене и шифре премештања.

У погледу декриптовања страних тајних порука, у војсци и држави Краљевине Југославије није било неких нарочитих успеха. Декриптоване су тајне поруке шифроване шифром просте замене и шифром премештања, док су код сложенијих шифара и кодова декриптери остајали немоћни.

У целини, у Краљевини Југославији су између два светска рата употребљаване шифре које су се базирале на папиру и оловци. Све развијеније земље у то време оловку и папир замењују машинама и справама за шифровање, имају далеко развијенију криптографску службу и криптографске бирое, са далеко већим бројем криптолога. Знања добијена од Француза сигурно нису била најсавременија.

	1	2	3	4	5	6	7	8	9	0
1	A	1	AL	AN	AND	AR	ARE	AS	AT	ATE
2	ATI	B	2	BE	C	3	CA	CE	CO	COM
3	D	4	DA	DE	E	5	EA	ED	EN	ENT
4	ER	ERE	ERS	ES	EST	F	6	G	7	H
5	8	HAS	HE	I	9	IN	ING	ION	IS	IT
6	IVE	J	O	K	L	LA	LE	M	ME	N
7	ND	NE	NT	O	OF	ON	OR	OU	P	Q
8	R	RA	RE	RED	RES	RI	RO	S	SE	SH
9	ST	STO	T	TE	TED	TER	TH	THE	THI	THR
0	TI	TO	U	V	VE	W	WE	X	Y	Z

Таблица 10 x 10

Енигма

Због практичних недостатака иначе теоријски савршене шифре, настављена је потрага за практичнијом шифром. Времена за дуго чекање није било, а да би се дошло до практичне и истовремено сигурне шифре, било је потребно оставити папир и оловку и користити новије технологије.

Немачки инжењер Артур Шербијус 1918. године конструише електромеханичку машину за шифровање коју назива *енигма* и коју почиње да производи у фабрици *Шербијус и Ритер,* основану са Ричардом Ритером. Машина се састојала од неколико генијално смишљених компоненти, склопљених у сложену машину, а може се објаснити као скуп

три елемента: тастатуре за уношење поруке, скремблера који шифрују слова почетног текста у одговарајућа слова шифрата и плоче са неколико лампи које служе за приказивање слова шифрованог текста. Притиском на одговарајуће слово на тастатури, слао се електрични импулс кроз централну скремблерску јединицу на другу страну, где се на плочи осветљавало одговарајуће слово шифрата. Најважнији део машине био је скремблер начињен од дискова који се аутоматски ротирају после сваког откуцаног слова. Тиме је свако слово шифровано у различитом положају скремблера. Да би се постигла додатна сложеност, машина се састојала од три скремблера, што је давало 26×26×26, односно 17.576 различитих положаја. Поред тога, у машину је као новина уграђена и плоча са кабловима, између тастатуре и првог скремблера, која је пошиљаоцу давала могућност укрштања слова пре уласка у скремблер. Такође, редослед дискова могао се мењати, што је додатно повећавало број могућих различитих шифар-

Енигма

ских кључева. Комбинацијом оријентације скремблера, редоследа дискова скремблера и укрштања каблова на плочи са кабловима, долазило се до приближно 10.000.000.000.000.000 различитих кључева, што је у време конструкције *енигме* био огроман број.

Машина је била намењена за комерцијалну употребу, а с временом су почеле да је користе и државне институције. Била је скупа, али и поред тога немачка војска закључује да *енигма* представља одлично решење за криптографску заштиту. У току 1925. године започиње њена масовна производња и убрзо улази у војну употребу. Немачка војска се у наредном периоду опремила са готово 10.000 примерака и тако постала водећа сила у области криптографије.

Још једанпут су криптоаналитичари пред собом имали неслућени изазов. Британски и француски криптоаналитичари почињу да пресрећу поруке које нису успевали да декриптују. Сви њихови покушаји да разбију *енигму* били су безуспешни. Међутим, прве успехе у њеном сламању постижу криптоаналитичари једне друге државе – Пољске.

Пољска је непрестано страховала за свој суверенитет, угрожаван како са Истока тако и са Запада. Пољски официри Бироа за шифровање зато одлучују да ангажују математичаре и осмишљавају грандиозан план. Најпре за групу од 20 студената Универзитета у Познању организују обуку из криптологије, да би им, након четири године стажирања, дали јасан задатак – разбијање *енигме*. Ови студенти су течно говорили немачки језик. Тројица научника из ове групе изабрана су да раде за Биро, а најталентованији је био Марјан Рејевски.

На први поглед, то је била немогућа мисија, али то није обесхрабрило пољске криптоаналитичаре. Предузели су данонoћне напоре да би се ушло у срж *енигме* и пронашла слабост. Рејевски своју криптоанализу заснива на принципијелној чињеници да је понављање делова текста или кључа непријатељ безбедности. У примени *енигме* најочигледније понављање било је код кључа за поруку, који је шифрован два пута на почетку сваке поруке.

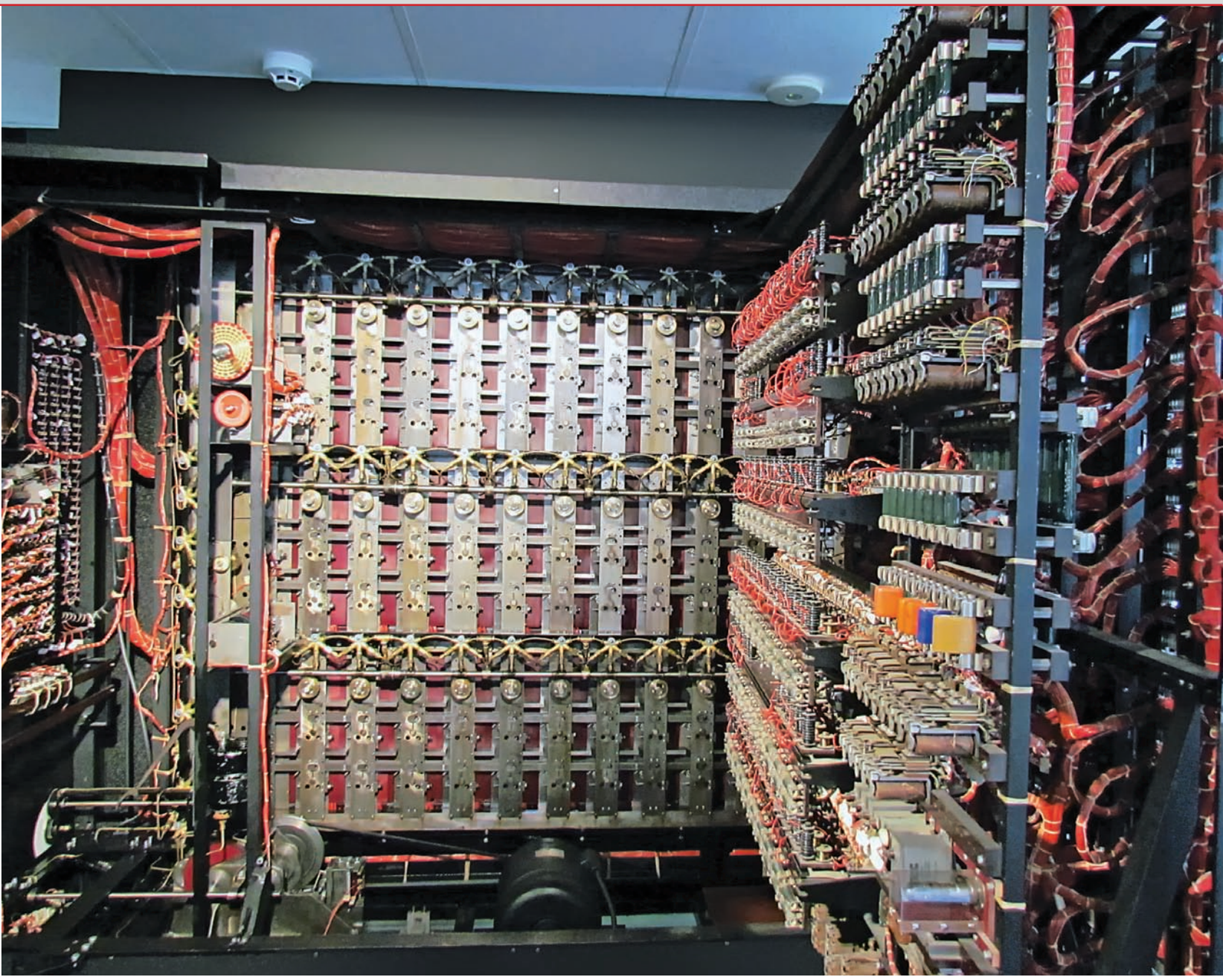
Помоћу уређаја – такозваних бомби, Марјан Рејевски 1932. године успева да разбије код који је, по мишљењу свих, било немогуће разбити. Тај успех постигнут је практично непосредно пре доласка Хитлера на власт у Немачкој. Све до 1938. године, када Немци побољшавају безбедност *енигме*, та машина је, првенствено за пољске криптоаналитичаре, била прочитана књига. Немци ускоро повећавају број скремблера са три на пет, чиме се и број њиховог различитог распореда повећао са шест на шездесет, што је условило да се без улагања додатних средстава више није могао открити дневни кључ, па је декриптовање било немогуће. Тако *енигма* постаје не само изузетно коришћено средство тајне комуникације, већ и једна од основа Хитлерове стратегије – блицкрига.

Пред сам почетак Другог светског рата, 1939. године, Пољаци деле своје знање са француским и британским обавештајним службама. Британци су по добијању резултата пољских криптоаналитичара одмах у Центар за криптологију у Блечли парку довели најбоље младе математичаре са својих универзитета.

Други светски рат

У освит Другог светског рата, у јесен 1939. године, британски научници у Блечли парку брзо овладавају знањима преузетим од Пољака. Било је много више и запослених и средстава. Али било је потребно разбити практично нову машину, десет пута сложенију од оне коју су разбили Пољаци. Процедура се из дана у дан понављала: немачки послужиоци на *енигми* у поноћ су прелазили на нови дневни кључ, када се практично по-


25
24
23
22
21
20
19
18
17
18
17
16
15
14
13
12
11
10



Тјурингова бомба

чињало испочетка и са криптоанализом. Предстојало је откривање новог дневног кључа, а након тога декриптовање пристиглих порука. У свему томе морало се водити рачуна да Немци не открију да је *енигма* разбијена.

Немци су током рата наставили да усавршавају једну од најбољих криптографских машина икада, што је пред криптоаналитичаре увек изнова постављало све сложеније захтеве на откривању нових решења за разбијање *енигме*. Личност која је дала посебан значај у разбијању те машине је свакако Алан Тјуринг, који је открио њене највеће слабости.

Његови резултати омогућили су разбијање *енигме* и у најтежим околностима, које су у основи биле у понављању садржаја. Проучавајући поруке које су декриптоване, Тјуринг је уочио могућност да предвиди садржај поруке која још није декриптована, на основу места и времена одакле је порука послата. Испоставило се да су поједини извештаји, које су Немци достављали, били у потпуности унифицирани. Касније, 1940. године, Тјуринг осмишљава и успева да конструише машине за криптоанализу, такозване Тјурингове бомбе, које су подсећале на бомбе Рејевског. Мада прва бомба није дала очекиване резултате, у наредних годину и по дана појавило се још њих петнаест. На крају се успело да бомба открије дневни кључ за сат времена, након чега би све поруке тог дана биле разбијене. Да би се то постигло, нису биле довољне само бомбе, већ је било потребно и много рада на њиховој правилној поставци.

Везисти из племена Навахо

Колики је био значај разбијања *енигме* убрзо су схватили и на највишим државним и војним нивоима, тако да је и Винстон Черчил, у септембру 1941. године, посетио криптоаналитичаре. Након те посете криптоаналитичари добијају „одрешене руке". Број бомби се до краја 1942. године повећава на 49, а убрзано се повећава и број криптоаналитичара.

И даље је било веома важно да Немци не посумњају у то да је *енигма* разбијена, јер би засигурно предузели мере да је надограде. Због тога су предузимане одговарајуће мере предострожности. Као пример може се навести веома дискретно понашање Британаца у вези са сазнањем о кретању немачких подморница. Иако су Британци декриптовањем немачких порука на време откривали и прецизно знали положаје њихових бродова и подморница, нису их све нападали, јер су подозревали да би то упозорило Немце да им је шифра проваљена.

Сматра се да је британско разбијање *енигме* утицало на трајање Другог светског рата, односно да су криптоаналитичари убрзали крај Хитлерове Немачке. Успеси криптоаналитичара из Блечли парка остала су дуго тајна, све до седамдесетих година 20. века.

Један од чувених примера криптографије у Другом светском рату је и коришћење језика Навахо Индијанаца, језика који је за све ван племена био неразумљив. Амерички инжењер Филип Џонстон долази на идеју да би језик Навахо, или неког другог индијанског племена, могао бити одлична шифра у рату са Јапанцима. Размишљао је да послужиоци на радио-уређајима у сваком батаљону на Пацифику буду Индијанци, чиме би комуникације у потпуности биле безбедне. Било је потребно пронаћи племе у којем су Индијанци знали енглески језик и били довољно писмени. Избор је пао на Навахо племе, које је било и најбројније. Неколико месеци после бомбардовања Перл Харбора, прва група Навахо Индијанаца започиње оспособљавање. Пошиљаоци су преводили поруке са енглеског на навахо језик, а примаоци су их преводили у обрнутом смеру. Амерички криптоаналитичари су први тестирали систем и резултати су били савршени, а Навахо шифрери су ускоро потврдили своју вредност и на бојном пољу.

Постоји податак да су у америчкој војсци била укупно 402 Навахо шифрера. Као и у случају британских криптоаналитичара из Блечли парка, Навахо Индијанцима је након рата било забрањено да говоре о свом раду. Тек 1968. године обелодањени су њихов значај и допринос, да би после тога били и одликовани, а навахо шифра једна је од ретких у целој историји криптографије која за време употребе није проваљена.

НАЈПРОСТИЈЕ ШИФРЕ

„У време које сам ја провео у штабу користили смо следеће шифре: двобројчане, код којих је, зависно од начина коришћења, коришћен алфабет од 30 слова без знакова интерпункције, затим алфабет од 30 слова, слова X, Y, Q i W и знакови интерпункције и алфабет од 26 слова и четири знака интерпункције; једнозначне словчане шифре код којих је примењиван алфабет од 30 слова; двословчана шифра са применом алфабета од 30 слова; разнозначне бројчане шифре и разнозначне бројчане шифре са применом коначног кључа за надшифровање. Наведене шифре коришћене су саме за себе, без примене надшифровања полушифрата. Шифрат је исписиван у групе од по два слова или броја, односно у групе од по два, односно једно слово, ако је примењивана разнозначна шифра. Такав начин исписивања шифрата говорио је већ унапред о врсти примењене шифре, међутим ми то у оно време нисмо уочавали. Шифрат је настао као резултат шифровања разнозначном шифром и кључем за надшифровање (кључем за маскирање). Такав начин исписивања шифрата није омогућавао већ на први поглед распознавање шифре.

При изради шифре најважније је било да свако слово добије своју шифарску замену и да се такве замене у једној шифри не понављају. То је све што смо тада знали из теорије криптографије. Да зло буде веће код шифровања смо примењивали и делимично шифровање, а то значи да су у шифрату неки делови текста, за које смо сматрали да нису конспиративни, остајали отворени. Ово је још више олакшавало непријатељу отварање шифрованих депеша. Шифре су израђиване руком, а исто тако умножаване. Касније смо такве шифре израђивали и умножавали писаћом машином. Редовно је вођена евиденција израђених шифара, и то: у колико је примерака израђена, коме је послата и када је уништена. Шифра је била на употреби 10 до 15 дана након чега је замењена новом. По истеку из употребе шифра је обавезно уништавана спаљивањем".

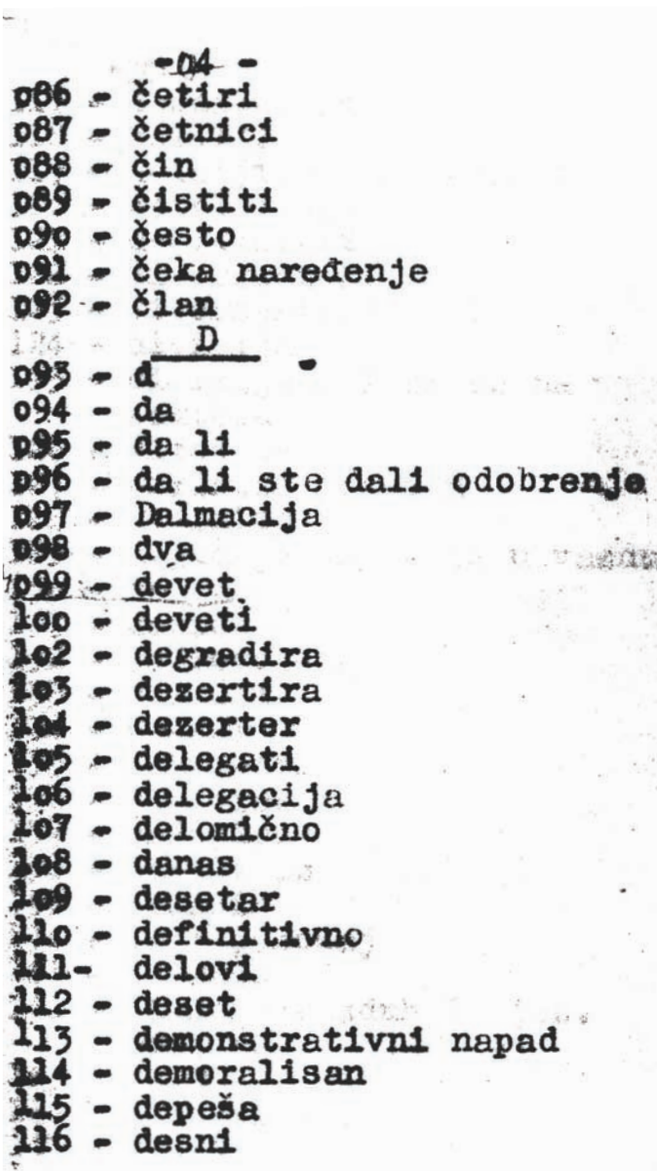
(Сећање шифрера, из књиге „Ратна сећања – везе у НОБ-у 1941–1945")

У НОБ-у

Формирањем првих партизанских јединица указала се потреба за криптографијом. Било је потребно давати упутства, наређења, примати извештаје. Организација руковођења и командовања захтевала је поуздан, брз и заштићен пренос информација.

Шифре које су коришћене у почетку биле су најпростије – шифре простог замењивања, које су израђиване на брзину, када би се појавила потреба за њима. Најчешће су то биле двобројчане шифре (када се свако слово замењује двоцифреним бројем). Шифре просте замене, као што је већ речено, врло су слабе и лако се разбијају. Међутим, због слабог познавања криптографије и недостатка кадра, сматрало се у почетку рата да су сигурне.

У каснијем периоду НОБ, од 1943. године, шифре просте замене употребљавају се тако да се обавља „двоструко шифровање" помоћу још једног кључа, чиме је донекле побољшана сигурност, али не толико да се шифра



-04 -
086 - četiri
087 - četnici
088 - čin
089 - čistiti
090 - često
091 - čeka naređenje
092 - član
D
093 - d
094 - da
095 - da li
096 - da li ste dali odobrenje
097 - Dalmacija
098 - dva
099 - devet
100 - deveti
102 - degradira
103 - dezertira
104 - dezerter
105 - delegati
106 - delegacija
107 - delomično
108 - danas
109 - desetar
110 - definitivno
111- delovi
112 - deset
113 - demonstrativni napad
114 - demoralisan
115 - depeša
116 - desni

„Партизански код"

не може разбити. Касније су употребљаване шифре сложеног замењивања, али су због неквалитетних шифарских кључева такође биле врло слабе. Ове шифре, иако слабог квалитета, биле су применљиве ако су акције биле релативно брзо изведене, тако да непријатељ није имао довољно времена да декриптује поруке.

Употребљаване су и разнозначне шифре, код којих се поједина слова поруке замењују једноцифреним, а поједина двоцифреним бројем, као и шифре премештања. Те шифре биле су нешто боље, али и даље недовољно сигурне да би се обезбедила тајност поруке. Обично су шифре дељене на две врсте: телефонске и радио-шифре. Телефонске шифре биле су обично словчане, слабијег квалитета, с обзиром на то да су употребљаване жичне везе. Радио-шифре биле су нешто бољег квалитета, бројчане, али ипак недовољне да би се обезбедила тајност информација.

Формирањем све већег броја јединица, одреда, група и проширивањем система веза, потреба за криптографијом све више се повећавала. Све већу примену добијале су радио-станице. Употреба шифре сваким даном имала је све

СВАКА ШИФРА ИМА СЛАБОСТИ

„Сваки систем има своје слабости и можемо рећи да се свака шифра, са више или мање напора, може дешифровати, ако је тај који дешифрује стручњак у познавању шифарских система, односно у познавању принципа шифровања. Напоминьемо још и то, да свако може сам саставити свој систем шифровања, ..., разумљиво – у договору с оним с ким се дописује.

Сада од другова који употребљавају шифре, зависи какав систем ће се изабрати, како ће га поједноставити (за пријатеља), односно компликовати (за непријатеља). При том нека имају на уму, да шифре буду што једноставније за запамтити, да се употреби што мање времена за претварање јасног текста у тајни, односно тајног у јасни. Такође треба пазити и то, да их непријатељ не може разумети у случају да шифроване поруке доспу у његове руке".

(Из свеске „Криптографија", 1944. година)

Павле Савић

видније место. Са друге стране, недостајао је стручни кадар. Било је потребно успоставити посебан центар који ће обједињавати и израђивати шифре. При Врховном штабу НОВ и ПОЈ формира се такав центар, а руководилац за шифру и носилац развоја био је наш чувени академик Павле Савић.

Криптографска („шифрантска") служба била је организована од виших према нижим јединицама све до батаљона па и самосталних чета, које су извршавале специјалне задатке. Један од разлога употребе једноставнијих, али и слабијих шифара, био је и у недостатку кадра. Било је потребно пронаћи и обучити кадар. За кадар криптозаштите бирани су најчешће чланови КПЈ, писмени и који су имали било какво додира са шифрама. При већим јединицама одржавани су курсеви, који су трајали по неколико дана, а присуствовало је од три до пет људи. На рад са шифром често су примани и људи без икаквог курса и обучавали су се на самој дужности шифрера. Дешавало се да су у криптографску службу одређивани људи који су раније припадали непријатељским јединицама, најчешће домобранским или усташким, што се тек касније откривало. Било је и појава умножавања кључева и предаје кључева непријатељским снагама.

За везу између виших штабова употребљаване су нешто сигурније шифре, али ипак недовољно сигурне да обезбеде апсолутну сигурност поруке. То су биле шифре сложеног замењивања. На једном табаку папира било је исписано 30 шифарских кључева, у облику испретураног алфабета, а изнад првог алфабета био је исписан низ двоцифрених бројева. Свако слово поруке шифровано је помоћу различитог кључа: прво слово помоћу првог кључа (алфабета), друго слово помоћу другог кључа (алфабета) итд. Овакву шифру употребљавао је и Врховни штаб. Очигледно је да се свако тридесето слово поруке шифровало истим кључем, односно да се ова шифра у ствари састојала од 30 шифара просте замене. С обзиром на то да се шифарски кључ практично није мењао и по неколико месеци, кључ се веома често понављао и омогућио непријатељу декриптовање порука. Практично су све шифре које су се употребљавале користиле кључеве који су се често понављали, што је омогућавало декриптовање порука.

Постоје подаци да је у месту крај Беча био формиран центар обавештајне немачке службе за декриптовање порука. Центар је бројао око 1.000 људи, а био је намењен за балканске земље. Поред тога, свака већа немачка јединица имала је бар једног криптоаналитичара.

Проблем приликом употребе сложенијих и квалитетнијих шифара био је и у њиховој компликованости. Такве шифре су изузетно осетљиве на грешке, тако да су и вео-

ма мале грешке у шифровању или предаји поруке на пријемној страни изазвале велике потешкоће у дешифровању или га чак и онемогућавале. Због тога се дешавало да се иста порука више пута поново шифрује или поново шаље, што је одузимало драгоцено време.

Употребљавани су и мањи кодови. То су биле књижице са око 1.000 слова, речи и израза. Речи су биле поређане апсолутним алфабетским редом, а шифарске замене, које су биле троцифрене, апсолутним децималним редом. Ово су били мали кодови који нису у потпуности задовољавали потребе. Поред тога, кодови су осетљиви на грешке, јер погрешно додавање или недостатак одређене цифре у шифрату отежавао је или онемогућавао дешифровање, па је често било потребно поново или шифровати или поново вршити примопредају поруке.

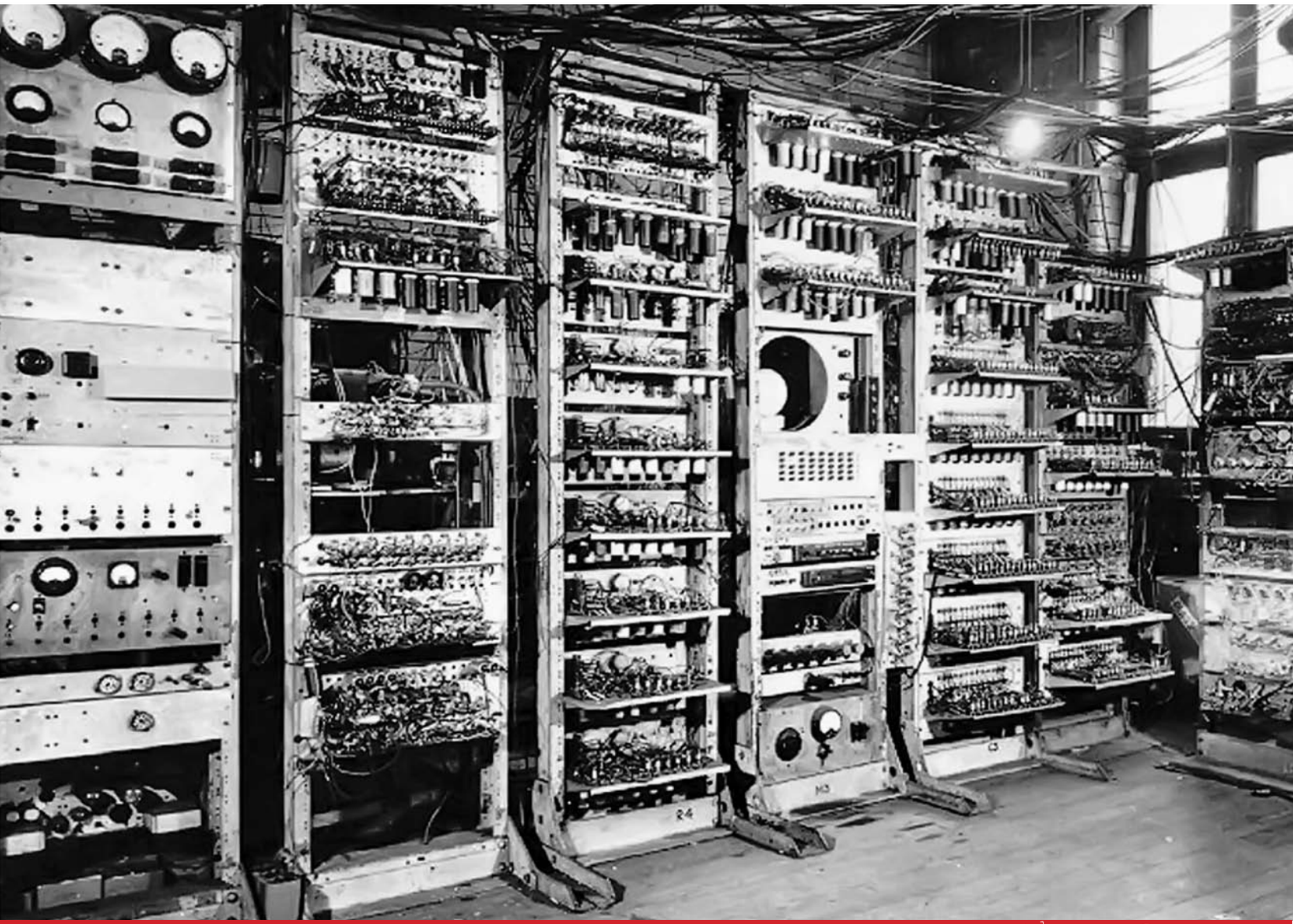
Како се НОВЈ повећавала и развијала, тако су и шифре постајале све боље и сигурније, применом нових метода шифровања, а нарочито после сазнања да Немци успешно декриптују поруке. Међутим, и те нове побољшане шифре нису биле апсолутно сигурне. Формира се и посебна криптографска администрација. Поруке се након шифровања или дешифровања заводе у посебне књиге, текстови се преписују и улажу у одређену књигу.

Крајем 1944. године јавља се и разнозначна шифра, над којом је рађено друго шифровање помоћу дневних кључева, који су се састојали од 10 петоцифрених група. Наредбом врховног команданта НОВ и ПОЈ, од 10. маја 1944, донета је „Привремена инструкција шифарских органа НОВ и ПОЈ". Крајем године уводе се нове шифре, које су биле врло сигурне и нема података да их је непријатељ декриптовао. Употребљавани су квалитетнији кључеви који су се чешће мењали.

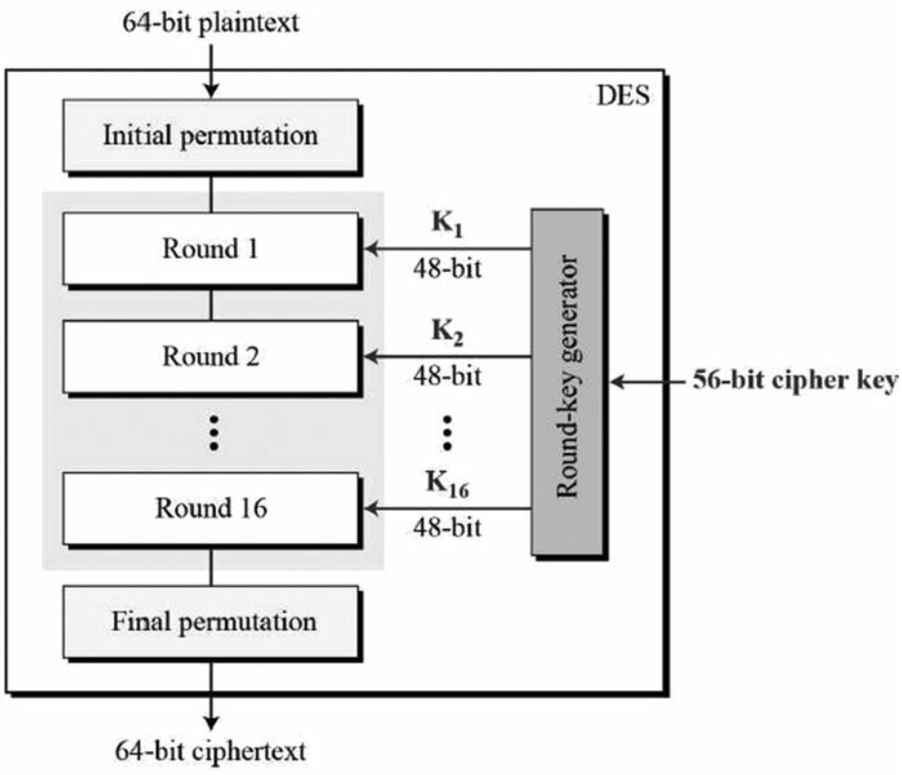
Појава рачунара

Први рачунари појављују се за време Другог светског рата, између 1940. и 1945. године. Први рачунар за потребе криптослужбе, звани ENIAC, појавио се 1943. године, а до краја рата америчка криптослужба располаже са 407 рачунара и огромним бројем људи.

ENIAC - први рачунар за потребе криптослужбе



Пошто су учествовали у стварању првих рачунара, криптоаналитичари настављају да развијају рачунарску технику, ради примене за разбијање шифара. Због брзине рачунара, повећали су могућност проналаска кључа којим је порука шифрована. Али појава рачунара користи и криптографима – почиње употреба рачунара за конструисање све сложенијих шифара. Рачунари постају кључни у даљем надметању криптографа и криптоаналитичара. Значајнији рад „Теорија комуникација система за заштиту тајности" аутора Клода Шенона објављен је 1949. године. Клод Шенон заснива нову математичку грану, теорију информација, и поставља апсолутно сигуран шифарски систем и неопходне услове за његово остваривање.



DES - дуго година званични амерички стандард за шифровање

Шифровање порука помоћу рачунара слично је традиционалним облицима шифровања (замењивање, премештање...), али постоје и значајне разлике. Рачунару се могу задати много сложеније математичке операције које извршава за кратко време. Рачунари не оперишу са словима, већ са бинарним бројевима и цифрама „0" и „1", односно битима. И поред тога, шифровање се обавља на принципима замењивања и премештања. Не премештамо и замењујемо слова и све бројеве, већ само „нуле" и „јединице".

У почетку су рачунари били ретки, скупи и доступни само владиним службама и војсци. Касније се њихова израда све више комерцијализује и они постају доступни ширим слојевима. Моћ рачунара све више се повећавала, а истовремено су постајали све јефтинији. Рачунари су све више улазили у употребу, помоћу њих су обављане разне трансакције и потреба за криптографском заштитом је све више расла. Ово је проузроковало потребу за стандардизацијом у криптографији и увођењем јавно доступног, опште прихваћеног алгоритма.

Један од најчешће коришћених алгоритама назван је *луцифер*, који шифрује поруку тако што се она прво претвара у бинарни низ цифара јединица и нула. Затим се тај бинарни низ дели на делове (блокове) од по 64 цифре и ши-

фровање се реализује са сваким блоком посебно. Цифре се у сваком блоку премештају и замењују кроз веома сложене поступке, а цео процес шифровања спроводи се у 16 рунди. После 16 кругова мешања порука се шаље, а на другој страни се обрнутим поступком дешифрује.

Под утицајем америчке Државне безбедносне агенције NSA, која је хтела да буде сигурна да ће у употреби бити ограничен број кључева, тај алгоритам своди се са 64 бита на 56 бита кључа, што даје могућност броја различитих кључева који се изражава 18-цифреним бројем, али је тај број кључева знатно мањи од броја могућих различитих кључева. Тај алгоритам усваја се 1976. године, добија назив DES (Data Encryption Standard) и дуго је био званични амерички стандард за шифровање.

Касније се појављују и други алгоритми, од којих је најпознатији AES (Advanced Encryption Standard), код којег се порука дели на блокове од 256 бита. Кључ дужине 256 бита даје могућност различитих 2^{256} шифарских кључева. Тај број кључева изражава се декадним бројем са око 77 цифара, што је наравно неупоредиво више у односу на алгоритам DES. Познати су још и алгоритми RC4, TripleDES и IDEA.

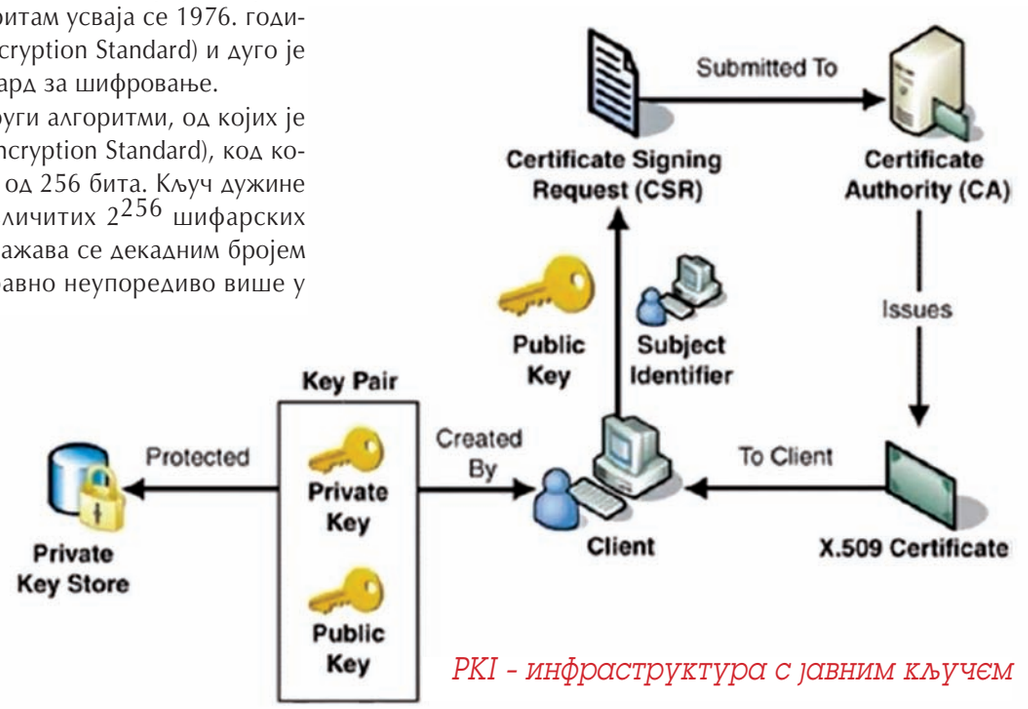
Како се број рачунара повећавао и потребе за криптографском заштитом расле, све више је до изражаја долазио вишевековни проблем – *дистрибуција кључева.*

Криптографија јавног кључа

Проблем дистрибуције кључева мучио је криптографе током историје. Чак и шифре које су теоријски потпуно сигурне, имале су проблем са дистрибуцијом кључева. За дистрибуцију кључева била су потребна велика улагања, како у материјалним, тако и у људским ресурсима. Кључеви су морали физички да се преносе и достављају примаоцима (куририма и сл.).

Средином седамдесетих година група криптографа успела је да осмисли решење за тај проблем, а ово откриће се у криптографији сматра највећим достигнућем још од осмишљавања шифре просте замене.

Један од зачетника решења за безбедну размену кључева био је чувени криптограф Витфилд Дифи, којег је тај проблем посебно интересовао. Схватао је да ће онај ко пронађе решење за дистрибуцију кључева бити проглашен за једног од највећих криптографа у историји. Већ тада је имао визију да ће се број рачунара све више повећавати и да ће ускоро свако домаћинство имати рачунар, који ће бити умрежен у јединствену рачунарску мрежу – интернет. Свако ће једног дана имати потребу да криптографски заштити тајност својих порука, а размена кључева на дотадашњи начин је практично била немогућа. Сазнавши да постоји још један криптограф који се озбиљно бави проблемом дистрибуције кључева, ступа с њим у контакт. Био је то Мартин Хелман, а Дифијево и Хелманово партнерство постаје најпознатије у историји криптографије. Почели су заједно да проучавају проблем дистрибуције кључева, а као резултат њиховог рада настаје Дифи–Хелманов алгоритам за размену кључева, заснован на сложеним математичким функцијама. Доказано је да за дистрибуцију кључева не мора постојати сигуран канал. Остало је да се осмисле ефикаснији начини за дистрибуцију кључева.

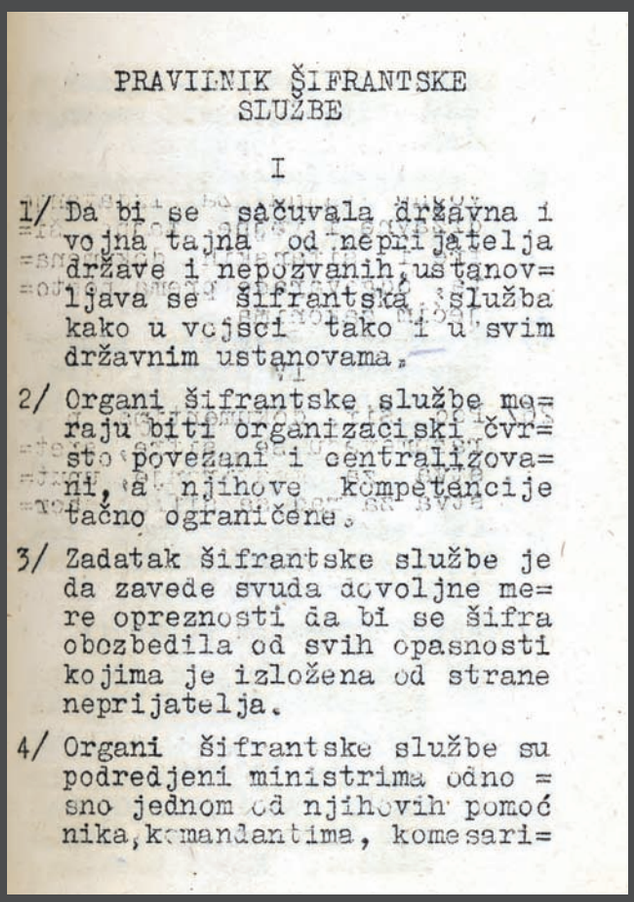


PKI - инфраструктура с јавним кључем

Први пут је осмишљена шифра са *асиметричним кључем.* Све дотадашње шифре биле су *симетричне.* Симетричне шифре користе исти кључ за шифровање и за дешифровање, односно и пошиљалац и прималац морају поседовати у потпуности идентичан кључ.

Асиметрична криптографија

Асиметрична криптографија, или *криптографија јавног кључа,* заснива се на томе да кључ за шифровање и кључ за дешифровање нису идентични. Принцип криптографије јавног кључа заснива се на томе што сваки учесник у комуникацији поседује пар кључева – *јавни и приватни кључ.* Јавни кључ, као што само име говори, може бити доступан било коме и он служи за шифровање. Приватни кључ држи се у тајности и служи само за дешифровање. Свако ко поседује јавни кључ може шифровати поруку, али само онај који поседује приватни кључ, ту исту поруку може дешифровати. Да би два учесника међусобно могла размењивати шифроване поруке, претходно морају размени ти јавне кључеве. Након тога предавалац у свом рачунару проналази јавни кључ примаоца, шифрује и шаље поруку, а прималац својим приватним кључем дешифрује поруку.



PRAVILNIK ŠIFRANTSKE SLUŽBE

I

1/ Da bi se sačuvala državna i vojna tajna od neprijatelja države i nepozvanih, ustanovljava se šifrantska služba kako u vojsci tako i u svim državnim ustanovama.

2/ Organi šifrantske službe moraju biti organizaciski čvrsto povezani i centralizovani, a njihove kompetencije tačno ograničene.

3/ Zadatak šifrantske službe je da zavede svuda dovoljne mere opreznosti da bi se šifra obezbedila od svih opasnosti kojima je izložena od strane neprijatelja.

4/ Organi šifrantske službe su podredjeni ministrima odnosno jednom od njihovih pomoćnika, komandantima, komesari-

Правилник шифрантскє службє из 1945.

Да би се ова идеја остварила у потпуности, било је потребно осмислити одговарајућу математичку једносмерну функцију. Решење проналазе три научника: Рон Ривест, Леонард Адлман и Ади Шамир, а алгоритам добија назив RSA (Rivest, Shamir, Adlman).

Велика предност криптографије јавног кључа је у отклањању проблема дистрибуције кључева. Не постоји опасност да било ко види јавни кључ, јер служи само за шифровање и са њим се порука не може дешифровати. Једино се приватни кључ мора чувати код себе. Али и овде се поставља неколико питања – да ли је јавни кључ који смо примили и са којим треба да шифрујемо нашу поруку заиста од праве особе? Да ли смо сигурни у квалитет шифарских кључева? Одговор на ова питања представља сертификационо тело, поверљива трећа страна, која издаје електронске сертификате (парове јавног и тајног кључа) и која гарантује тајност поруке и идентитет власника сертификата. Формира се такозвана инфраструктура са јавним кључевима, PKI (Public Key Infrastructure).

Данас су у употреби такозвани *хибридни крипто-системи,* који комбинују најбоље особине симетричних и асиметричних криптосистема. Асиметричном криптографијом шифрује се само симетрични кључ, који је краћи од поруке. Шифровани симетрични кључ достави се другој страни и даље се поруке шифрују симетричним кључем.

Криптографски билтєн

Примопрєдаја шифрованих тєлєграма

Криптографска служба ЈНА

Развој криптологије и криптографске службе у Југославији наставља се у континуитету по завршетку Другог светског рата. Већ 1945. године Министарство народне одбране издаје Правилник шифрантске службе.

Носилац послова криптозаштите постаје VII одељење Генералштаба ЈНА, које у свом саставу располаже целинама за криптоанализу и израду шифарских докумената. Педесетих година у саставу одељења формира се и декриптерски одсек. Тих година у њихов састав улазе и врхунски стручњаци из различитих научних области (математика, електроника, телекомуникације...) и почиње озбиљан истраживачки рад из области криптологије. Већ тада настоје да прате доступна научна достигнућа и да изналазе сопствена квалитетна и сигурна решења за криптозаштиту информација, што се постиже све до данас. Преводе се стране књиге и радови и пишу сопствени радови из области криптологије. Изучавају се основни статистички подаци страних језика, као и случајност и случајно изабрани бројеви.

У систем веза уводе се радио-телепринтерске и радио-релејне везе, као и радио-станице веће снаге. Центри везе међусобно се повезују, како у ЈНА, тако и са другим имаоцима. Постепено се прелази са папира и оловке на употребу криптографских машина, шифротелепринтера и касније рачунара. Изналазе се сигурна решења базирана на квалитету шифарских кључева. Долази се и на идеју израде и објављивања криптографског билтена, а нацрт билтена израђен је 1956. године.

Идеја почиње да живи 1964. године, када излази први број „Криптографског билтена". Билтен је садржао разне теме: историја криптографије, справе и машине за шифровање, декриптовање, математика и криптографија и друго. Садржао је и задатке за декриптовање, а имао је и енигматски део.

Шездесетих и седамдесетих година прошлог века научноистраживачки рад све више долази до изражаја. Успешно се изналазе сопствена решења за криптозаштиту. Производе се сопствени криптографски кључеви базирани на потпуној случајности. За потребе криптографске службе раде врсни криптолози, међу којима је најпознатији Александар Трифони.

Посебна пажња посвећује се организацији курсева криптозаштите. Развијају се шифарски системи базирани на чисто случајним и на псеудослучајним низовима кључева.

Уређај КЗУ из осамдесетих година

Награда АВНОЈ-а додељена 1989. године

Врши се криптозаштита писаних и говорних информација у свим врстама веза – радио, радио-релејним и жичним.

Служба везе и криптозаштите у ЈНА обједињава се 1967. године и издваја се декриптерска служба, која се обједињава са радио-извиђачком службом. Савезни секретаријат за народну одбрану постаје најодговорнији за организацију криптозаштите у СФРЈ.

Исте године, 5. маја, започиње и историјат Центра за примењену математику и електронику, када се наредбом државног секретара за народну одбрану СФРЈ у саставу ЈНА формира 120. центар за израду шифара. Формирањем овог центра обједињена је делатности криптозаштите на нивоу државе. Први пут је формирана засебна установа која се бави криптологијом.

Наредбом савезног секретара за народну одбрану из 1976. године у оквиру 120. центра обједињени су послови научноистраживачког рада и развоја средстава криптозаштите.

Интензиван рад респектабилног научноистраживачког кадра и постигнути резултати допринели су да се 120. центар, Одлуком Савета за научни рад у ОС СФРЈ у децембру 1981. године, региструје као научна јединица за општа и примењена истраживања и упише у Регистар научноистраживачких јединица ЈНА.

На основу Наредбе савезног секретара за народну одбрану из 1982. године, 120. центар (криптографски) преформиран је и преименован у Институт за примењену математику и електронику (ИПМЕ).

Као научни институт званично је регистрован 1985. године. Одбор за награду АВНОЈ, новембра 1989. године, доделио је Институту награду АВНОЈ, као посебно друштвено признање за стваралаштво и рад од општег значаја за развитак СФРЈ у области примењене математике и електронике.

Од септембра 2006. године Институт мења име у Центар за примењену математику и електронику и има статус истраживачко-развојне установе. Током педесетогодишњег постојања Центар успешно реализује научноистраживачки рад из области криптологије, развија и имплементира сопствена верификована криптолошка решења.

У континуитету се прате научна и технолошка достигнућа из поља природно-математичких наука у научним областима математичких и рачунарских наука и техничко-тенолошких наука у научној области електротехничког и рачунарског инжињерства (научне дисциплине: електромагнетика, електрична мерења, теорија електричних кола, дигитална обрада сигнала, детекција сигнала, препознавање облика и електромагнетна компатибилност) кроз проучавање стручне литературе, присуство научним и стручним скуповима, усавршавање на специјалистичким курсевима и школовање кадра на докторским студијама. Да би се адекватно одговорило на безбедносне ризике и претње, потребно је имплементирати ефикасне механизме заштите у информационо-комуникационим системима на коришћењу у МО и ВС. Пројектовање решења заштите у великој мери зависи од нивоа сазнања заснованих на постојећим решењима за заштиту, али и од непрекидног научноистраживачког рада ради пројектовања нових решења заштите у складу са растућим безбедносним ризицима и претњама.

У последњих десетак година дошло је до значајне модернизације ТкИ система у МО и ВС, која се одликује преласком са аналогних на дигиталне системе. Са развојем ТкИ система дошло је до увођења великог броја нових сервиса. Све те промене пратио је развој криптозаштите кроз научноистраживачки рад и имплементацију нових криптографских техника, што је резултовало модернизацијом постојећих и дефинисањем нових криптографских система.

Будућност криптографије

Вековима се криптографи боре да заштите тајност порука, док криптоаналитичари настоје да их разоткрију. Некад су у предности били једни, а некад други. Често се сматрало да је пронађена шифра „нерешива", али с временом је скоро свака разбијена, од првобитне шифре просте замене па до електромеханичке машине попут *енигме*. За данашње шифре сматра се да су потребне милијарде година да се разбију. Тако се мислило и у прошлости, па је време од милиона година сведено на свега неколико минута. Да ли ће се то исто десити или се већ десило и са данашњим шифрама?

Све више је покушаја, поред криптоанализе, да се до тајних информација дође и на неки други начин. Један од тих начина је путем компромитујућег електромагнетног зрачења – сваки електронски уређај емитује електромагнетне таласе који се на одређеној удаљености могу „ухватити" и евентуално реконструисати у корисну информацију. Да би се та могућност спречила, потребна су велика улагања у заштиту од таквог нежељеног зрачења. Други начин је путем малициозних напада на рачунаре (рачунарски вируси, тројански коњи...). И поред тих могућности, основни циљ криптоаналитичара је разбијање савремених симетричних и асиметричних шифара (AES, RSA...), а да би се то остварило потребан је технолошки напредак.

И криптоаналитичари и криптографи будућност криптографије виде у развоју квантног рачунара. То би били рачунари који би, уместо на законима класичне физике, функционисали на законима квантне физике. Док криптоаналитичари сматрају да би им овакав рачунар омогућио да разбију постојеће шифре, криптографи у њима виде могућност конструисања такве шифре која би нудила савршену заштиту. Сматра се да би проналаском квантног рачунара и квантне криптографије све данашње шифре постале бескорисне. Поред тога, има мишљења да се квантна криптографија не може ни практично ни теоријски разбити. Ако би се порука шифрована квантном криптографијом разбила, то би значило да квантна теорија није исправна. Да ли ће криптографи коначно победити? ■