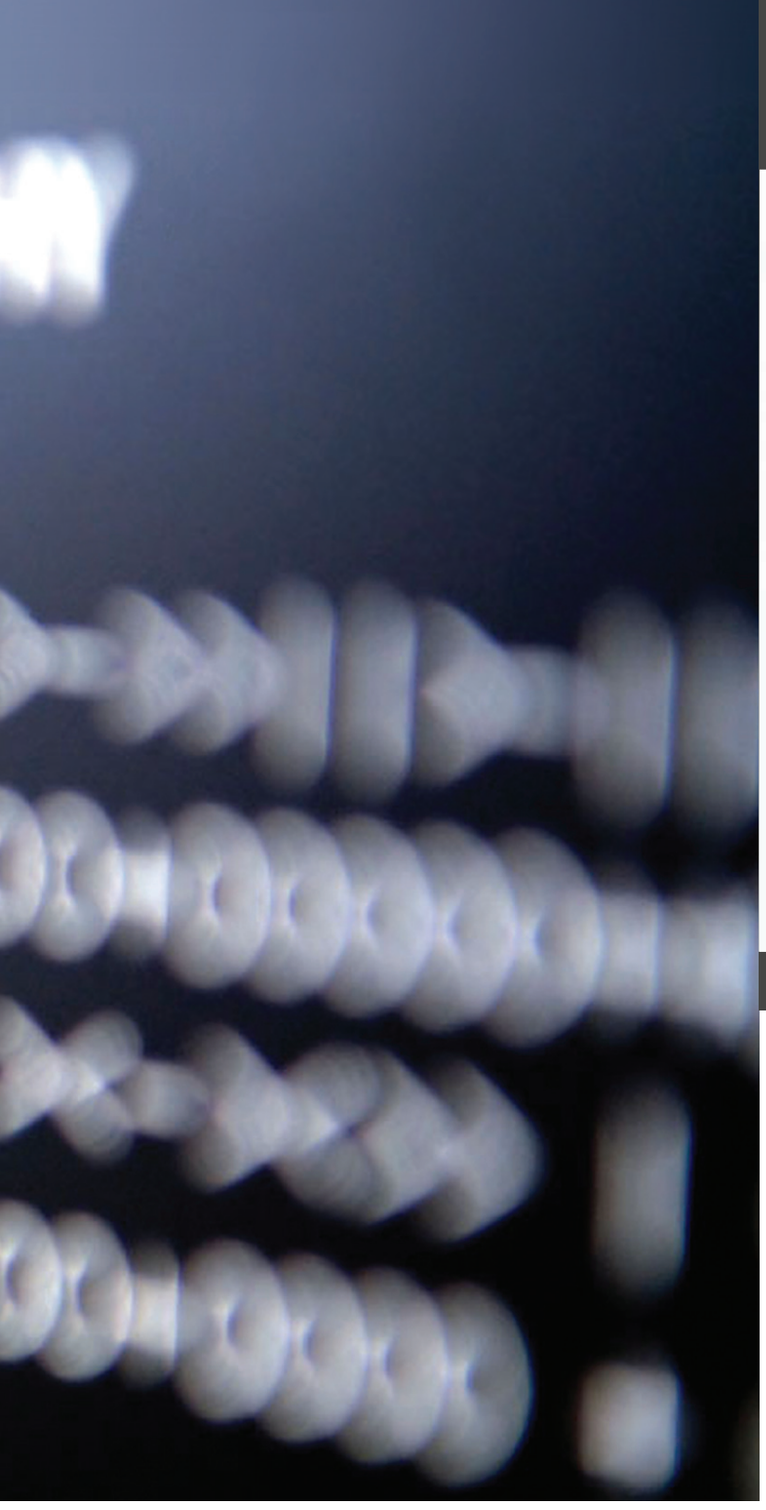
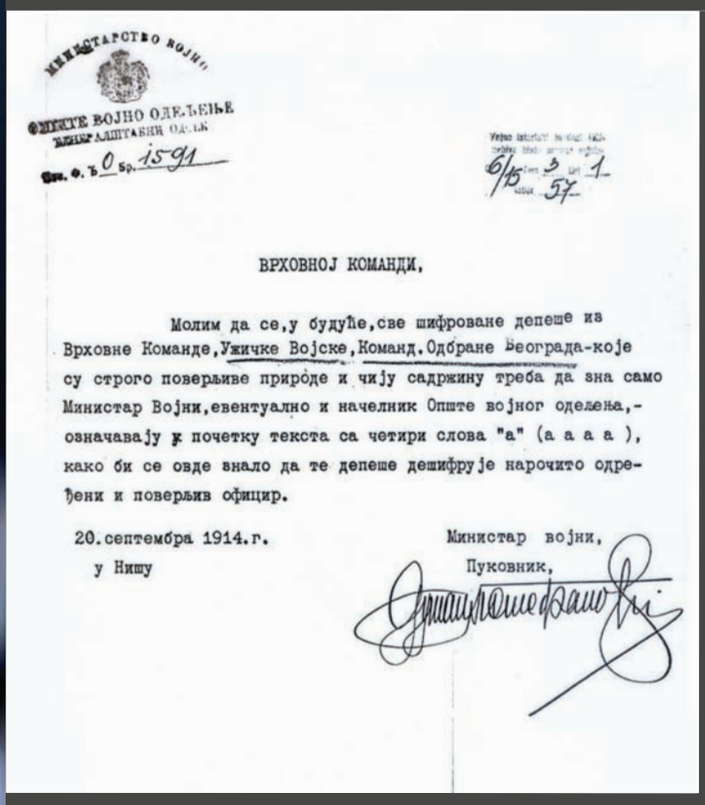
КРИПТОЛОГИЈА

ТАЈНА ПОД КЉУЧЕМ

ПИШЕ САЊА АНЂЕЛКОВИЋ

У настојању да омогуће бржу и лакшу размену информација, људи су непрекидно усавршавали облике споразумевања. Међутим, први сукоби народа условили су и потребу за прикривањем садржаја информација и чувања њихове тајности. Због тога развијају поступке који приликом размене информација прикривају садржај поруке и непријатељу онемогућавају тумачење.





МИНИСТАРСТВО ВОЈНИ
ОПШТЕ ВОЈНО ОДЕЉЕЊЕ
ЕНКРИПТАЦИОНИ ОДЕЉАК
Бр. ф. Ъ 0 Бр. 1591

6/15 9 57 1

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 у 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,

Учинити информацију неразумљивом ономе коме није намењена, али и проналажење метода за откривање њеног садржаја, предмет је криптологије – науке која изучава и анализира метод за заштиту тајности података. Према речима криптолога Центра за примењену математику и електронику Управе за телекомуникације и информатику Генералштаба Војске Србије Искре Пеневе, она обухвата криптографију и криптоанализу. Криптографија је дисциплина која се бави проучавањем и дефинисањем метода за заштиту порука, без обзира на врсту информационог садржаја, и подразумева развијање система за прикривање порука.

– Циљ криптографије јесте да обезбеди теоријске основе и механизме за имплементацију тајности, интегритета, аутентичности и непорецивости. Криптоанализа се односи на разоткривање скривених информација ради њиховог разумевања, односно, изучава методе за откривање информационог садржаја криптографски заштићених порука без претходног познавања криптографског кључа који се користи при трансформацији порука. Покушај криптоанализе назива се нападом, а успешна криптоанализа се зове разбијање или пробијање шифре – каже Пенева.

ОД ПАПИРА И ОЛОВКЕ

До пре неколико деценија методи шифровања података (енкрипције) сводили су се на употребу папира и оловке. Почетком 20. века, открићем комплексних механичких и електромеханичких машина као што је *Енигма*, обезбеђени су софистицираније и ефикасније методи. Развој криптографије одвијао се истовремено с развојем криптоанализе. Све до седамдесетих година, како наводи криптолог Центра Данило Смуђа, криптографија је била строго чувана на нивоу влада. Два догађаја довела су је у јавни домен – креирање јавног енкрипционог стандарда (DES) и криптографије с јавним кључем.

– У средњем веку криптографија стагнира све до почетка 16. века, до ренесансе криптографије, када се јављају први покушаји усавршавања шифри. Дело „Расправа о шифри" италијанског научника Леона Албертија, 15. век, први пут студиозно и статистички анализира језик и поставља математички темељ криптологије – објашњава Смуђа и додаје да се криптографија нагло развија и добија на значају.

– Опат Тритемиус у Немачкој, у 15. веку, штампа прву књигу о криптографији „Полиграфија", а постхумно се

издаје и његова „Стеганографија". Он саставља специфичан кодекс „Аве Марија", којим се слова поруке замењују црквеним речима на 306 различитих начина. Шифровањем овим кодексом свака порука претварала се у молитву или текст религиозног садржаја – каже Смуђа.

Како наводи криптолог, француски дипломата и криптограф Блејз де Вижнер творац је Вижнерове шифре у 16. веку. У историји криптографије та шифра је најдуже кори-

Потпуковник Драган Тривић

КЛАСИЧНА КРИПТОГРАФИЈА

Прве криптографске трагове представљају необични хијероглифски натписи на египатским гробницама, настали пре више од 4.500 година. Сматра се да су они били неразумљиви само у жељи да истакну моћ религијског текста, а такав принцип уношења мистерије и конфузије важи и данас за тајне поруке. Наш криптолог Пенева каже да из доба старог века нема много писаних трагова криптографије. Тамо где је забележена и сачувана, дала је основу за даљу надградњу.

– У почетку су шифровани само делови порука, имена или одређена слова, затим су слова премештана или замењивана на једноставне начине, у текст су убацивани неважећи, збуњујући знаци или коришћени уговорени кодекси. Шифра је сматрана довољно сигурном само јер је непозната противнику, што је било погрешно – наводи Пенева.

Први познати систем за шифровање је „скитала" из 4. века пре нове ере, а користила ју је спартанска војска. Штап одређене дужине и дебљине спирално је обмотаван кожном траком по којој је хоризонтално, дуж штапа, писана порука. Када се трака одмота, слова на њој остају испремештана, а може да их прочита у правилном редоследу само онај ко поседује штап исте дужине и дебљине.

Уз скиталу, објашњава криптолог Смуђа, данас су призната још два класична криптографска система – атбаш и Цезарова шифра. Споменути класични шифарски системи су основа на којој су се развили савремени симетрични шифарски системи.

– Хебрејска атбаш шифра замењивала је слова сређеног алфабета одговарајућим симетричним словима из истог низа. Реч је о шифри замењивања и припада другом класичном криптографском систему. Основни пример за било какав увод у криптографију јесте Цезарова шифра, коју је користио римски цар Јулије Цезар у преписка са својим пристаницама. Идеја шифре замене је да се свако слово из алфабета замени словом добијеним померањем алфабета за три позиције – наводи Смуђа.

шћена, чак четири века. Реализује се уз помоћ таблице и применом одређених математичких релација.

НАСТАНАК „ЦРНИХ КАБИНЕТА"

Криптолог Пенева објашњава да се у 18. веку, у већини европских земаља, отварају посебне тајне канцеларије у којима раде тимови криптолога и лингвиста, познатији као „црни кабинети", који би контролисали пошту, отварали је, проверавали и декриптовали. Међутим, телеграфија је обесмислила рад таквих кабинета, што је довело до њиховог укидања. Створени су услови за рад декриптерских служби, а проналазак радија омогућио је прислушкивање и прикупљање криптоматеријала, чиме је директно подстакнут развој модерне криптоанализе.

– Помак у науци догодио се када је 1881. године холандски научник Аугусте Керкхоф објавио најсажетију и једну од најзначајнијих књига о криптографији „Војну криптографију", у којој поставља основне принципе, актуелне и данас, за добар криптосистем. Декриптовање немачког Цимермановог телеграма потпуно је променило ток Првог светског рата, а то искуство навело је већину земаља да улажу много више у снажније и организованије криптослужбе, па чак и да се удружују пред заједничком опасношћу – каже Пенева.

Начелник Центра за примењену математику и електронику потпуковник Драган Тривић наводи да су се до Другог светског рата увелико користиле електромеханичке машине за шифровање, али оне нису биле практичне за употребу. У том периоду, с развојем модерне српске државе и српске војске, појављује се и криптозаштита односно шифра, која је даље непрекидно пратила развој технологије, каже потпуковник Тривић, показујући неколико сачуваних аката и депеша с краја 19. века, из балканских ратова и Првог светског рата, односно примера коришћења шифре.

У КЉУЧУ ЈЕ КЉУЧ

У савременој криптографији користе се идеје класичне криптографије, али је акценат на имплементацији сложених алгоритама за шифровање уз коришћење додатног параметра – кључа. У савременој криптографији систем криптографски заштићене комуникације подразумева постојање два или више учесника у комуникацији, криптографски заштићене поруке која се преноси комуникационим каналом, шифарска трансформација која омогућава заштиту информационог садржаја поруке тако да се њен садржај учини неразумљивим за неовлашћене кориснике и постојање криптоаналитичара, који, на основу шифрата који им је доступан, настоје да открију информациони садржај заштићене поруке.

Како наводи криптолог Центра мајор Бориша Јовановић, криптографски алгоритми најчешће су јавно доступни, док се сигурност одређеног криптографског система базира на тајности примењеног кључа.

– Начело да криптоаналитичар познаје криптографски алгоритам и да тајност криптографски заштићене комуникације лежи искључиво у тајности криптографског кључа назива се „Керкофов принцип", по фламанском војном криптографу који га је први формулисао 1883. године. Принцип се данас сматра једним од основних у савременој криптографији. Када се криптографски алгоритам учини јавно доступним, на овај начин, постаје предмет експертских анализа различитих стручњака из академских кругова

ЕНИГМА

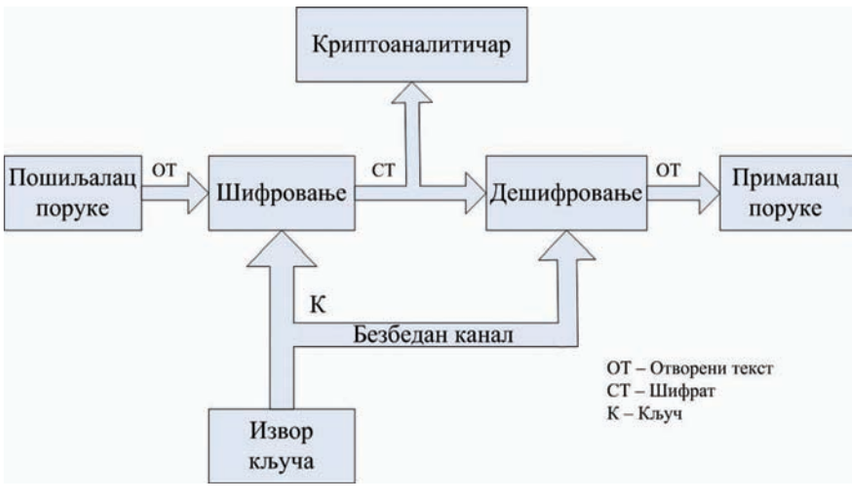
Немачки проналазач Артур Шербијус конструисао је 1920. године електромеханичку роторску машину познатију као *Енигма*. Била је заснована на комплексној електромеханичкој полиалфабетској шифри, како би заштитила осетљиву комуникацију. Разликовала се од осталих машина тог времена јер су помацима ротора управљали зупчаници, чиме се постизало да помаци праве неправилан редослед. Немачка војска користила је *Енигму* од почетка 20. века до краја Другог светског рата, а разбијање *Енигма* шифре био је важан фактор који је допринео победи Алијансе у Другом светском рату. Ова тематика и данас заокупља пажњу јавности, те је недавно снимљен филм „Игра кодова" у коме је приказана прича о разбијању *Енигме*.

За потребе криптослужбе конструисан је и први рачунар ENIAC, 1943. године. Криптоаналитичко одељење службе везе војске САД почело је 1937. године да користи Хотлеритове табулаторе, у интензивним покушајима разбијања јапанских кодова. Јапански пандан *Енигме* називао се PURPLE. Предност примене ових машина над ручном обрадом била је више него очигледна, наглашава - криптолог мајор Јовановић.

– Значај добро организоване криптослужбе САД у потпуности је схваћен тек после напада на Перл Харбур, који се озбиљнијом анализом успешно декриптованих криптограма, можда, могао и предвидети. Од тада се за послове криптослужбе издвајају знатна средства и ангажују најбољи стручњаци. До краја рата ова служба израста у џиновску институцију која располаже са 407 рачунара и армијом људи. Неколико година после завршетка рата, амерички научник Клод Шенон заснива нову математичку грану, теорију информација, у оквиру које дефинише апсолутно сигуран шифарски систем и неопходне услове за његово остваривање – каже мајор.

и може бити верификована његова отпорност на нападе из домена криптоанализе – истиче мајор Јовановић.

Данас се криптографија веома озбиљно схвата и придаје јој се велика пажња у академским круговима. На светским универзитетима изучава се као посебан предмет, а у оквиру еминентних светских институција реализује се велики број истраживачких пројеката, како би се унапредила постојећа и пронашла нова сазнања. Ако се посматра даљи развој савремене криптографије може се рећи да ће се она кретати у правцу квантне криптографије, каже мајор Јовановић, која користи достигнућа квантне механике, како би омогућила безбедну комуникацију учесника. Значајно и јединствено својство квантне криптографије јесте способност учесника у комуникацији да уоче прислушкивање злонамерних учесника, који покушавају да открију информације о криптографском кључу.



КРИПТОЗАШТИТА У СИСТЕМУ ОДБРАНЕ

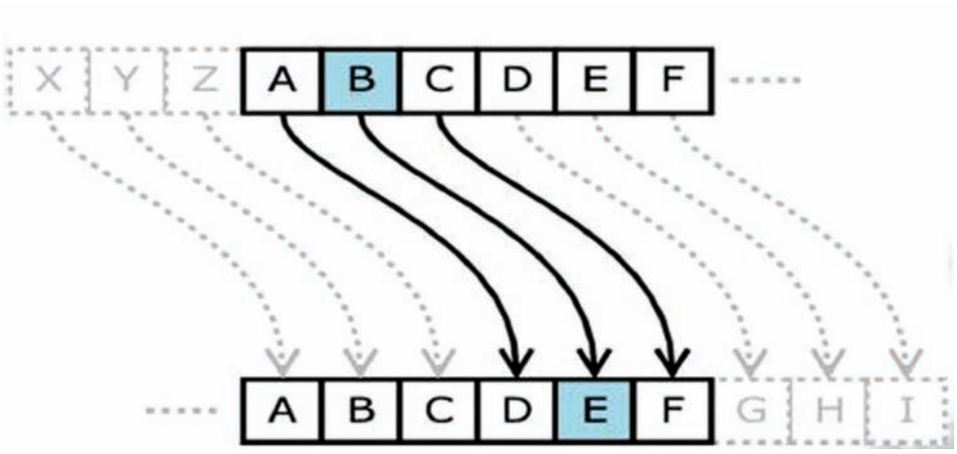
Један од садржаја телекомуникационо-информатичког обезбеђења у Министарству одбране и Војсци Србије јесте криптозаштита којом се у потпуности обезбеђују тајност, интегритет, аутентичност и непорецивост. Према речима потпуковника Тривића, на све тајне информације које се преносе у Министарству и Војсци неопходно је да

КАТАНАЦ СА ШИФРОМ

Пошто очување тајности лежи у кључу, његова дужина је од првенствене важности. Како бисмо дочарали значај дужине кључа, посматрајмо најобичнији катанац са шифром. Отвориће те га тек онда ако поједине цифре сложите у праву комбинацију децималних бројева која отвара катанац. Кључ, у овом случају комбинација бројева, дужине две децималне цифре значи да постоји 100 могућих комбинација. Кључ дужине три цифре повећава број комбинација на 1.000, а онај са шест децималних цифара на милион. Дакле, што је кључ дужи то је потребан већи уложени труд криптоаналитичара за његово разбијање.

се примењују одговарајуће мере криптозаштите.

– У телекомуникационо-информационом систему употребљавају се различите врсте комуникација – радио, радиорелејне, кабловске, као и различите врсте уређаја и система телекомуникација и криптозаштите. Међутим, уз уређаје и системе на првом месту је кадар различитих специјалности који мора бити у потпуности оспособљен да би одговорио тренутним захтевима, као и способан за непрекидно праћење, развој и овладавање новим технологијама. У нашем министарству и војсци криптозаштита је заступљена на свим нивоима и постоје различите команде, јединице и установе које се баве пословима из ове области – планирање и организовање криптозаштите, криптообрада информација, истраживање и развој, школовање и усавршавање кадра криптозаштите, одржавање техничких уређаја и система криптозаштите – наводи потпуковник Тривић.



КОМЕРЦИЈАЛНА КРИПТОГРАФИЈА

Најпознатији и најчешће коришћени симетрични криптографски алгоритми су DES и AES који представљају шифре конструисане као криптографски стандарди америчке владе. Иако су јавно доступни, постали су доминантни и популарни за коришћење у комерцијалне сврхе, почевши од апликација за АТМ енкрипцију до електронске поште. Криптологија обезбеђује информациону сигурност за интернет, мобилну телефонију, картице за плаћање банкарских трансакција, бежични интернет, видео-пренос, идентификационе картице, али и кућне кориснике – апликације које користе шифровање фајлова, диска и безбедност електронске поште.

ОБУКА НА ИНТЕРНЕТУ

На интернету се могу пронаћи различити форуми о војним уређајима, као и о уређајима везе и криптозаштите. То су, како каже потпуковник Тривић, уређаји старије генерације, углавном из седамдесетих и осамдесетих година прошлог века, употребљавани у бившој ЈНА.

– Уређаји приказани на форумима технолошки су превазиђени, с дужинама кључева које у савременим условима не би обезбедиле потребну сигурност. Такође, на интернету се могу пронаћи и информације о различитим курсевима из области заштите и безбедности информација, различите дужине трајања и садржаја. Курсеви пружају одређена знања, али како би се успешно бавили пословима криптозаштите у војсци, неопходно је поседовати посебна стручно-специјалистичка знања – појашњава потпуковник Тривић.

Он тврди да смо сведоци непрекидног и све већег развоја телекомуникационих и информационих технологија, и да се све више послова и активности обавља посредством електронских комуникација. Самим тим повећавају се опасности које прете из сајбер-простора и постављају све већи захтеви у погледу заштите информација.

– Да би телекомуникационо-информациони систем испунио захтеве који се постављају, неопходна су савремена криптолошка решења која морају бити развијена сопственим снагама уз сложене теоријске и практичне услове и изазове. Само сопствена решења у овој области обезбеђују потребну сигурност. Један од услова приликом набавке страних уређаја јесте да је могућ развој и уградња сопствених криптолошких решења. Поседовање сопствених верификованих криптолошких решења од изузетног је значаја и за државни суверенитет – каже потпуковник и објашњава да је неопходно да постоји јединствен и организован научноистраживачки рад у области криптологије, да постоје способности за развој, верификацију и имплементацију сопствених криптографских алгоритама, за генерисање и производњу различитих криптографских параметара и криптографског материјала, као и за израду сертификата за криптографске системе засноване на инфраструктури јавних кључева.

Научноистраживачки рад у области криптологије, као и праћење светских достигнућа, у Војсци Србије постоји скоро пола века. Дан Центра за примењену математику и електронику обележава се 5. маја, када је 1967. године формиран 120. криптоцентар који осамдесетих година постаје Институт за примењену математику и електронику, а од 2006. године установа данашњег назива.■

Снимио Марко РУПЕНА