ОДБРАНА
СПЕЦИЈАЛНИ ПРИЛОГ 173

КРИПТОГРАФИЈА КРОЗ ВЕКОВЕ

Тајно комуницирање

Пише Милорад МАРКАГИЋ

Скривање информација, порука и кореспонденције од нежељених прималаца од давнина је предуслов успешног одлучивања. А кад је то потребније него у годинама пред рат и током рата. Стога су највећи успеси шифрера, али и њихових противника, декриптера, везани за рат и командовање. Њихов рад је најчешће одлучујуће допринос неочекиваним и испрва необјашњивим победама над непријатељем који је мислио да су му комуникације ефикасно заштићене.

Развојем људског рода од праисторијске заједнице до данас, потреба за комуникацијом и преносом информација пратила је све токове историјских догађаја. Од почетних примитивних знакова у пећинама и кретања људи ради обављања свакодневних активности, јавила се потреба да се, осим директних комуникација, на неки начин поруке и информације пренесу или оставе неким видом писаног – цртаног трага да се касније могу прочитати. Наравно да су методе и поступци пратили ток развоја људске популације и научних достигнућа.

Приметно је да осим прастарих записа у облику цртежа, касније долази до преноса информација употребом алфабета одређене заједнице. Такође, врло су популарни и свима познати методи преноса порука фењерима, барјацима, димним сигналима, бубњевима, црквеним звонима...

Све већа количина информација, као и потреба да због различитих разлога не буду доступне трећим лицима, допринели су осмишљавању различитих начина сакривања или обраде порука, тако да оне буду доступне само одређеном броју особа. У људској природи је и да се нешто што се сматра тајним, прикривеним или недоступним, на сваки начин, па и без директне користи, ипак покуша сазнати или протумачити.

Тако је настала наука о тајном комуницирању, која и данас, иако временски и етимолошки превазиђена, носи име криптографија.

У основи ове науке, која се бави тајним писањем, налазе се грчке речи криптос – тајна и графеин – писање. То је област која се бави обрадом и чувањем информација и података који могу бити читљиви само особи којој су намењене. Иако је само име очувало генезу порекла, данашња криптографија се у правом смислу те речи не односи само на заштиту писаног текста, већ се прожима и кроз све поре поступања са подацима, како на локалном нивоу, тако и у комуникацијама међу појединцима и институцијама. Криптографију прати и криптоанализа, која има супротне циљеве, односно налази начине откривања података, информација и метода криптовања.

Криптографија за подлогу има математику, чије методе користи за развој алгоритама – процеса сакривања порука.

За већину обичних људи криптографија је представљала и представља мистерију. Постоје историјски подаци да се у средњем веку бављење овом материјом везивало за црну магију, односно сматрало се начином комуницирања са демонима и злим силама, те су криптографи сматрани следбеницима сотоне.

Два века пре нове ере стари Египћани су развили начин комуницирања писањем посебних знакова – хијероглифа. То је, у ствари, низ слика и знакова који представљају неке појаве или објекте. Најчешће су коришћени за исписивање по гробницама владара, али се могу наћи и делови који су израђени на обичним плочама или пак у пећинама из оног времена.

Данас се сматра да су хијероглифи коришћени за описивање значајнијих догађаја из живота важних личности. Иако по својој намени нису били замишљени да сакривају значење текста, њихов садржај био је познат веома малом броју појединаца. Ознаке појмова, радњи или предмета допуњаване су цртицама, тачкицама или другим фонетским знаковима, како би се употпунила слика о тематици о којој је реч. Иако се то писмо одавно не користи, сматра се једним од почетака криптографије, а покушаји откривања значења симбола, почецима криптоанализе.

Пошто је коптски језик сличан староегипатском, за разумевање хијероглифа користе се језичко-компаративне студије, чиме се покушава доћи до потпуног значења натписа који су пронађени.

Понесени цивилизацијским достигнућима, неким доступним информацијама и писаним траговима, научници, али и занесењаци разних профила посвећују значајан део времена изучавању овог писма, а велики део легенди и белетристичких радова заснован је управо на чињеницама постојања хијероглифа.

Слично као у старом Египту, у старој Месопотамији коришћени су посебни знакови, такозвано клинасто писмо. Оно се користило за размену порука и првобитно заиста није имало за циљ сакривање порука које се преносе или чувају.

Хебрејска шифра заснивала се на принципу просте замене слова абецеде. Ове су шифре познате под именима атбаш, албам и атбах шифра.

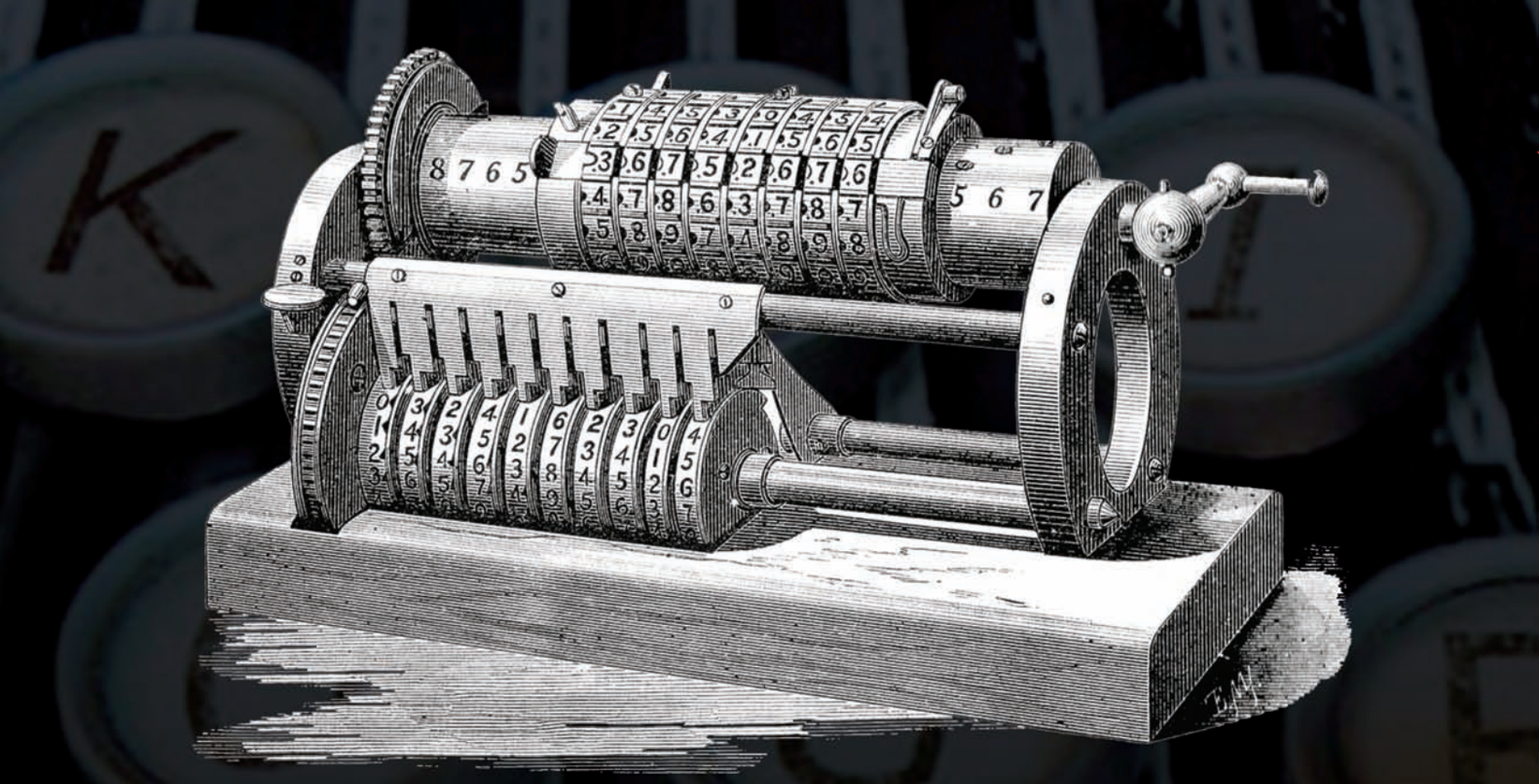
Заједничко им је то да су све користиле реципрочан метод замене слова алфабета, било да се ради о замени првог последњим слогом, а другог претпоследњим и тако редом, или је почетак замене био негде у средини алфабета. Овај вид заштите, уз неке измене, користио се и много векова касније, иако је измишљен још у 6. и 5. веку пре нове ере.

Скоро у свим криптографским школама и данас се изучавају методе криптовања засноване на таблици, комплетној или некомплетној, или на тзв. решетки. Заједничко им је стварање шифре која за основу има квадрат или правоугаоник, у које се упишу слова или знакови и онда се, по договореном кључу, обавља шифровање и дешифровање. Кључ може бити једноструки, двоструки, може прво да се чита хоризонтални, па вертикални део, или обрнуто.

За имплементацију начина криптовања, када не постоје техничка средства за заштиту поруке, већина криптографских служби у свету има развијен шифарски систем или криптосастав базиран на методи папир и оловка. Иако у данашње време могу деловати смешно, па некима и примитивно, ови системи у озбиљним институцијама и државама и те како имају место и улогу и користе се у ванредним ситуацијама, када откажу техничка и електронска средства.

Прва призната шифра

Прва позната и призната шифра, коришћена у сврху тајне кореспонденције јесте спартанска скитала. То је начин шифровања који је подразумевао да се око дрвеног штапа намота папирус и на њему испише текст који би, након одмотавања папируса, остајао нелогичан.



Дешифровање је могао да уради само онај који има штап исте дужине и дебљине.

Треба напоменути да је у основи тајности ове шифре био управо штап који није ношен заједно са папирусом на коме је исписан текст. Ово се може сматрати и првим начином коришћења симетричне шифре.

Јулије Цезар створио је супституцију на абецеди са кружним помаком за одређени број места улево. Иако сада изгледа веома примитивно, у доба када је веома мали број људи био писмен, супституција је и те како служила својој намени.

Цезаров принцип шифровања, додуше модификован, касније су користили многи за заштиту порука, а као основу за своју шифру тај метод искористио је и Вижнер.

Полибије (203–118. пре нове ере), старогрчки историчар, сматра се да је први у криптографију увео метод који смањује број заменских знакова у шифрованом тексту.

Такозвана Полибијусова шифра заснована је на методи шифровања порука уз помоћ „Полибијевог квадрата", у којем се слова распоређују слева надесно и одгоре надоле, у систему од 5×5, који су изнад и са леве стране означени са по пет бројева. На основу бројних шифара и укрштања колоне и реда добијају се појединачна слова шифроване поруке. Његов квадрат за шифарске замене појединих слова изгледао би овако.

	1	2	3	4	5
1	а	б	в	г	д
2	е	з	и	ј	к
3	л	м	н	о	п
4	р	с	т	у	ф
5	х	ц	ч	џ	ш

Зачеци анализе фреквенција

Први писани траг о почетку анализа фреквенције слова за потребе криптоанализе јављају се још у 14. веку, код арапског аутора Ибд ал-Дураима, али постоје тврдње да је та метода коришћена и у Италији, мада нема писаних трагова о томе.

Метода, додуше модификована и осавремењена, допуњена новим правилима, користи се и данас у криптоанализи. Суштина је да се у криптограму пребројавају шифарске замене и на основу статистике језика којим је криптограм рађен дође до закључка које би слово, или знак отвореног текста, било замењено словом или знаком у криптограму. Сваки језик, односно алфабет, има коначан број стања – знакова које се користе у обради текста. Осим појединачне фреквенције слова, битна је и анализа везивања слова у биграме и триграме, као и њихова присутност на одсечку – делу текста или целом тексту.

У средњем веку

У средњем веку долази до значајног развоја криптографије, тако да шифровани вид преписке међу аташеима на дворовима постаје основни начин комуницирања и заштите порука. Методе заштите користе све развијеније државе онога доба. Многи су примери када је шифра омогућила да се нека радња обави без знања друге стране, а истовремено постоје и примери који доказују да је бравурозним деловањем криптографа тајна преписка ипак откривана.

У Венецији се 1452. године формира посебна државна институција са једином наменом да се бави криптографијом. Стално запослена три човека свакодневно су креирала шифре за своју владу. Порастом потреба и повећањем комуникација долази до ширења установе, не само кад је реч о бројном стању, већ и улагању у развој техничких средстава за шифровање.

Леон Батиста Алберти креира 1466. године полиалфабетску супституцију, која омогућава да један знак отвореног текста буде замењен са више различитих знакова у шифрату. То је урадио тако што је направио два бакарна диска који стају један у други и на оба су исписана слова алфабета. Шифровање се одвијало тако што се по унапред дефинисаним принципима слово унутрашњег диска доводило у склад са првим, или било којим другим уговореним словом алфабета, што је представљало почетак шифрата. Након шифровања неколико речи поступак би се понављао тако да се унутрашњи диск доведе на неко друго место према спољашњем диску.

Овај метод пружао је бољи вид заштите од шифара просте замене, али је изискивао много времена и имао јеману да је ипак за шифровање коришћен само један кључ кога је било релативно лако разбити. Тај недостатак довео је до идеје да се створи више кључева за шифровање, с тим да се у шифрату јасно морало нагласити где почиње нови кључ.

Немачки опат Тритам написао је 1518. године шест књига са именом *Полиграфија*. У једној од њих објавио је таблицу која алфабет у сваком реду помера за по једно место, те се за шифровање користи цела таблица тако што се прва реч шифрује у првом реду и тако до краја таблице, а затим се метод понавља.

Ђовани Батиста Беласо проширује технику на тај начин што уводи кључну реч коју пише испред отвореног текста, па слово кључа стоји изнад слова отвореног текста, тако да се положај слова кључне речи испише целом дужином текста, чиме се шифрује. На тај начин слово кључне речи одређује број реда из таблице.

Ипак праву револуцију у криптографију уводи Блез де Вижнер, који у својим радовима описује више различитих полиалфабетских шифара. У основи Вижнерове шифре јесте Тритамова таблица, али са другим начином функционисања. Могуће је било да отворени текст буде шифрован самим собом или да се криптовани текст користи као кључ.

У суштини, може се рећи да је Вижнерова шифра истовремено скуп Цезарових шифара спојен са Тритамовом таблицом и допуњена кључем.

Овај метод шифровања био је веома дуго у употреби, а његова основа је и интегрални основ алгоритма ДЕС, који се и данас користи.

Правилним поступањем са овом шифром, честом заменом кључева за криптовање/декриптовање, информације се могу сматрати апсолутно заштићеним, односно шифра је непробојна.

У борби против Хугенота, 1628. године, француској војсци прилично је помогао А. Росињол, који је успео да декриптује једну заробљену поруку. Након тога стално је био ангажован на пословима декриптовања за своју владу. Он је криптоанализу, односно декриптовање, свео на коришћење две листе. У једној су били садржани елементи отвореног текста по алфабетском реду, а криптовани садржаји били су без поретка, а у другој листи криптовани елементи поређани су по редоследу, а отворени текст био је без редоследа, једноставно набацан. Упоређивањем шифрата и отвореног текста, изналажењем кључних речи или најфреквентнијих слова долазио је до отворених порука.

Поруке онога времена, ако се не рачунају куртоазна писма и јавне преписке, биле су релативно кратке по обиму и типске по садржајима, те је тиме било олакшано доћи до отвореног текста.

После смрти А. Росињола, у Француској су основани такозвани црни кабинети, у којима се известан број људи бавио искључиво декриптовањем непријатељских шифара. До краја 16. века црни кабинети усталили су се у Европи. Један од најпознатијих био је у Бечу са бароном И. де Кохом на челу. Он се пре свега бавио читањем поште која је стизала амбасадорима, и то тако што су писма отварана, копирана, поново затварана и враћана у пошту, као да нису ни дирана.

Ј. Валис (1616–1703), енглески математичар који има заслуге за развој , између 1643. и 1689. године био је главни криптограф за парламент а касније и за краљевски двор. Он је заслужан за увођење симбола –, а офор-

мио је и енглески Црни кабинет 1701. године. Тај кабинет има веома дугу и плодоносну историју рада.

У колонијама европских земаља криптографија није била званично у употреби, већ су се њоме бавили само ентузијасти и свештенство.

Важна је чињеница да се рад криптографа и криптоаналитичара одређене државе никада нису „сударали" нити да су људи који се баве тим пословима имали икакве везе једни са другима, нити сазнања о раду друге службе.

Невидљива мастила

Још као генерал, Џорџ Вашингтон имао је своја два шифрера који су га извештавали о покрету непријатељских трупа око Њујорка, комуницирајући само међусобно и преносећи поруке надређеном, а као додатну меру сигурности користили су невидљиво мастило. Један од видова тајног комуницирања, везаних и за заштиту информација, јесте свакако и невидљиви вид тајног писања, односно употреба невидљивих мастила, која се јављају још у старом Риму, мада се претпоставља да је тај начин писања коришћен и у другим старим цивилизацијама, употребом средстава која не остављају јасан траг на пергаменту, папирусу или папиру.

Познато је да су Британци још крајем 18. века пресретали преписку између америчког председника и његових емисара по Европи. Велики део тих писама био је написан управо невидљивим мастилима.

За тајна мастила користе се разноврсне органске или неорганске материје: течност лука, лимуна, људски секрети, соли кобалта, прах неких од метала. Наоко безазлени текст писан обичним мастилом, садржавао је између редова сакривену поруку, видљиву тек дејством неког реагенса, светлости, топлоте или хемијских материја.

Постоји мноштво историјских, али и публицистичких и белетристичких записа о коришћењу тајних мастила, како на највишим нивоима, у дворовима и владама, тако и у комуникацији међу тајним службама. Било да је реч о сакривању поруке између редова, или испод поштанске маркице, на самој коверти, или се слао „празан" папир, криптоаналитичари су свакако велики значај поклањали откривању тих садржаја.

На енглеском двору у периоду од скоро једног века то је био доминантни начин сакривања порука и кореспонденције. Шкотска краљица Марија Прва, позната и као Мери Стјуарт, једна од учесница у завери да се убиством краљице Елизабете Прве докопа енглеског трона, за дописивање са завереницима користила је преписку тајним мастилом. Након што су писма отворена и из обичног текста није се ништа наслућивало, енглески обавештајци су после неколико покушаја успели да дођу до тајног садржаја преписке, те су сви завереници, међу којима и она, ухапшени и осуђени на смрт.

Књиге шифри, кодови и кодни речници

Књиге шифри састојале су се од речи отвореног текста, тако да је реч шифрована бројевима странице, реда и речи. Реч је о симетричној шифри, где су сви учесници морали поседовати исту књигу шифара. Ове књиге су се посебно конструисале све до појаве речника неког језика, када примат преузимају књиге кодова.

Развој писмености доводио је до потребе да се речи и изрази неког језика сублимирају, сакупе на једном месту и постану стандарди у писаној комуникацији међу људима. Тако настају речници, који веома брзо почињу да се користе у криптографији. Речнику се додељивало кодирано (тајно) име, а странице су нумерисане другачије од штампарских ознака. Некада су се страницама додељивали број и име, или су означаване комбинацијама слова или слова и бројева.

Шифровање је било засновано на принципу замене речи или израза из речника бројном или алфанумеричком ознаком положаја исте у речнику, те је шифрат био скуп бројева или слова и бројева спојених у један низ. Дешифровало се тако што је прималац имао потпуно исту књигу – речник, идентично означен.

Метод заштите био је релативно слаб, па се речник користио за заштиту порука мањег степена тајности и краће трајности.

Шифарске машине

Први шифарник са точком измислио је Томас Џеферсон 1795. године. Уређај сличних карактеристика користио се у морнарици САД до скоро. Тај шифарник је у ствари скуп точкића, на којима се налази насумично исписан алфабет, на сваком различито. Шифровало би се тако што би се отворена порука поставила у одређеном распореду, фиксирали се точкићи, а онда би се други

ред слова користио као шифрат. Дешифровање се радило истим али инверзним методом. Точкови се окрећу док се не добије смислени текст. Овакав вид шифровања употребљив је само за једно шифровање и тада је порука безбедна, јер би понављањем шифровања са истим фиксираним точковима отвореног текста довело до лаке криптоанализе. Ипак шифровање порука заменом места – распореда точкова омогућавало је да се за сваки нови шифрат користи нови кључ, те су поруке остајале трајно заштићене.

На развој криптографије велики утицај имао је телеграф. Бежични пренос порука, или пренос кодираних порука кабловским комуникацијама у бинарном облику, а нарочито *Морзеов код*, као лако средство комуникације, а непознато широј јавности, у почетку је истински допринео бржем преносу информација.

Сам Морзеов код конципиран је тако да је структура знакова, слова, бројева или знакова интерпункције усаглашена са фреквенцијом њиховог појављивања у енглеском језику. Тако су најфреквентнија слова најкраћа по дужини и садрже један или два знака, тачке или цртице, док остали имају од три па навише саставних елемената.

Узрок овог феномена описан је тек након Другог светског рата у теорији чији је творац Клод Шенон – *Теорији информација*. Основа ове студије јесу математички закони који уређују систем за пренос података. Првобитно намењен у решавању проблема телефоније и телеграфије, убрзо је постао примењив на све уређаје, па и рачунаре. Идеје ове теорије прихватила је криптографија, криптоанализа, али и многе друге науке као што су психологија, лингвистика, молекуларна генетика, историја, статистика и неурофизиологија.

Радећи на истраживањима у областима комуникације и математичке теорије шифара током низа година, свој рад уобличио је у делима Математичка теорија комуникација и Теорија комуникације у тајним системима.

Процес описан у овим делима заснован је на анализи употребе језика, односно слова у речима и реченицама, те је криптоанализа почела да примењује знања о правилима фонетике, граматике, идиома, речи и фонетске функције склоности, које заједно дају језичку редундансу. Методе које користе људи у свакодневном животу, криптоаналитичари користе за проналажење деформација отвореног текста. Иако много компликованији и наизглед збуњујући, и криптограм садржи скривени образац, који није изолован од отвореног текста.

Почетак криптоанализе заснива се на чињеници да свуда постоји вишак елемената, да је криптограм произашао из најједноставнијег облика комуницирања, те се анализом фреквенција у писму за конкретан језик долази до финала, тј. превођења криптограма у јасан текст.

Дубоко разумевање јављања слова, њихов распоред и место у речи доводе до закључака о каквој се поруци ради. Ако се узме у обзир да је Вижнерова шифра коришћена за криптовање, а пренос вршен телеграфским кодом, онда је јасно да је велики део порука био брзо пренет, а истовремено и заштићен.

Плејферова шифра

Чарлс Ватсон и Леон Плејфер створили су 1854. године такозвану *Плејферову шифру*. Историјски је то прва позната биграмска шифра јер је за криптовање коришћен пар слова, тако да је продукт зависио од распореда слова у матрици.

Суштина јесте да се отворени текст подели у блокове од по два слова, при чему се посебно води рачуна да се ниједан блок не састоји од два иста слова и да отворени текст у себи мора имати парни број знакова. У случају да се низ, блок или цео текст састоји од непарног броја знакова, произвољно се по договору убаци унапред договорено слово.

Томографска шифра с краја 19. века ради на принципу да се сваком слову или знаку отвореног текста додељује двобројчана замена из таблице формиране од бројева уписаних у два реда. Након тога, бројеви у доњем реду множени су са 9. Из тако уређеног пара одређивала се шифарска замена за сваки знак отвореног текста.

За дектриптовање – дешифровање користила се инверзна операција.

Изазов Касиског

Француски научник Ф. В. Касиски нашао је 1863. године решење за разбијање свих периодично понављајућих полиалфабетских шифара. Основа те криптоанализе била је проналажење поновљеног низа знакова у криптованом тексту, како би се открила дужина кључа. Након сазнања о дужини кључа, на тим целинама примењивала се лингвистичка статистика. Тако је и пред криптографе постављен задатак изналажења новог метода шифровања.

Исто као и у животу, тако се и у борби између криптографије и криптоанализе као непромењиви и ненадокнадиви фактор увек јавља и време. Док криптографи теже да пренесу што већу количну информација, све већом брзином и у тајности, криптоаналитичари се суочавају са проблемом правовременог доласка до информације и њеним декриптовањем у реалном или корисном времену. Неки ће декриптовани садржаји остати само историјска чињеница, јер су изгубили употребну вредност одмах након примопредаје и поступању по инструкцијама у њима.

На рад криптоаналитичара такође утичу и други фактори као што су брзина преноса поруке, време потребно за декриптирање, оправданост декриптирања, односно избора и приоритета ако је више криптограма, као и употребна вредност информације. О тачности декриптованог сувишно је говорити јер је то аксиом.

Професија криптоаналитичара, осим у науку, може се слободно сврстати и у област уметности, јер свака особа која се бави овом делатношћу мора имати изузетне и посебне склоности и бриљантан ум. Помоћу спеку-

лативне и математичке визије света долази до конкретних и опипљивих доживљаја и чињеница. Како се популарно говорило, криптоаналитичар није заинтересован за садржај кодираног телеграма. Његов рад није ситна радозналост и жеља да прочита неку поруку, већ жеља да се победи шифра. Криптоаналитичар не вири кроз кључаоницу. Он разбија врата.

Шифре су вид заштите – оклоп, а криптоанализа разбијање тог оклопа. Шифра је исконска потреба за самоодржањем, везана за закон живљења, а криптоанализа је утицај на живот других.

Ако се циљеви криптографије сматрају искључиво одбрамбеним и заштитничким, а криптоанализе агресивним и застрашујућим, намеће се питање где ли се може пронаћи морално објашњење бављења њоме. Наравно да може, јер је криптографија често излазила и излази из својих оквира заштите и често је усмерена на напад на друге елементе, те се криптоанализа може сматрати методом самоодбране.

У књизи *Војна криптографија*, 1883. године, Керкоф износи шест основних принципа криптографије:

1. Криптовани текст мора бити практично непробојан. Криптограм треба да остане неотворен (неоткривен) чак и када се не користи апсолутно тајни шифарски систем.

2. Шифарски систем мора бити практичан за корисника. Имајући у виду чињеницу да нису сви корисници криптозаштите у пољу деловања ове науке, треба се тако конципирати да са мало утрошеног времена корисник може да овлада системом.

3. Кључ за шифровање и дешифровање треба бити лак за памћење и лако променљив.

4. Криптовани текст мора бити прилагођен средствима преноса телекомуникације.

5. Криптоуређај треба да буде покретан.

6. Криптоуређај треба да буде једноставан за употребу.

Ови принципи криптографије, прилагођени условима савремених средстава комуникације, начину и методу обраде и преноса података, важе и данас.

Почетком 20. века, а нарочито у току Првог и Другог светског рата долази до наглог развоја криптографије и криптоанализе. Производе се и у употребу уводе електромеханички уређаји за шифровање, чиме је поступак криптообраде знатно убрзан. Сви ти уређаји били су засновани на истим принципима на којима се шифровање обављало помоћу папира и оловке.

Тајна Собе 40

Почетком Првог светског рата, у раним јутарњим часовима 5. августа 1914, када је скоро цела Европа већ била захваћена ратним дејствима, један случајни разговор између шефа британске поморске обавештајне службе контраадмирала Х. Оливера и А. Јуинга о томе да иако пресрећу огроман број немачких кодираних порука, никако не могу наћи начин да их декриптују, умногоме је променио ток историје криптоанализе. У међувремену, проучавање кодова неколико немачких комерцијалних компа-

нија био је узалудан посао, као и анализа кода отетог с једног трговачког брода у Аустралији, јер нису имали додирних тачака са новим кодирањем у ратној морнарици.

Пошто пионири британске криптоанализе нису имали неког посебног предзнања нити било каквог формалног образовања на том пољу, није било чудно што у почетку рата нису имали значајнији успех и што је њихов рад био у стагнацији. У току поподнева Јуинг је већ имао у рукама изворне, пре свега морнаричке телеграме и замолио је да му се повери задатак да покуша да их отвори.

Као образован, тих, повучен научник, са знатним похвалама и наградама у биографији за оданост заједници 1914. године, Јуинг са својих 59 година, иако у поодмаклом добу, одлучује да успостави криптоаналитички биро, који ће, како ће се касније испоставити, имати велики утицај на ток светске историје.

Темељно је почео да проучава све криптографске материјале који су се могли наћи у библиотеци британског музеја, као и кодове Централне поште, где су се налазиле све копије комерцијалних књига кодова. У своју активност укључио је и четири професора са различитих факултета, личне пријатеље, који су између осталог и познавали немачки језик. Почели су са проучавањем низа слова и бројева како би дошли до идеје како да се почне рад на пробијању кодова.

Немачка порука од 4. августа прва је међу пресретнутим порукама која је мучила декриптере, а односила се на склапање уговора о савезу између Немачке и Турске од 3. августа, а којом се наводи да ратни бродови крену ка Медитерану, односно према Турској. Закаснело откривање довело је до тога да британска поморске снаге нису могле на време да адекватно реагују, па је један разарач, пробивши се кроз Дарданеле, бомбардовао руске луке на Црном мору, чиме је Турској омогућен улазак у рат без опасности од изоловане Русије, бар за неки период, у поморским операцијама.

У то време, Јуинг пише својој породици у Шкотској: „Ја сам усред специјалне операције која превазилази моје уобичајене активности."

Јуинг је радио данонoћно, без одмора, и своју специјалну операцију у септембру и октобру полако уводи у контуре праве криптоанализе, чиме Британија почиње да предњачи у односу на остале државе.

Из Черчилових мемоара, који описује догађај када је у Балтичком мору из потопљеног брода извучено тело младог немачког официра који је код себе имао део шифарника, видљиво је да су криптоаналитичке службе савезника сарађивале и надопуњавале своја знања. Пошто су руски криптоаналитичари уз његову помоћ могли да декриптују део порука, сматрали су да Британци, као водећа криптоаналитичка сила, треба да добију ове шифарнике. Специјални брод послат је у Петроград да преузме књиге кодова.

Иако су у рукама сада имали кодове, Британци у почетку нису могли да их искористе, све док на сцену није ступио интендантски официр Ч. Ротер, иначе стручњак за Немачку, који је утврдио да се једном кодирана порука, по једноставном алгоритму, поново кодира другом кодном књигом.

Сјајни почеци британске криптоанализе базирали су се на том открићу. Показало се да је ако се имају обе кодне књиге, веома просто урадити инверзну операцију претварања криптограма у полушифрат, а након тога у смислени текст.

Имајући у виду да се као и у свакодневном говору, тако и у криптограму, поједини знакови, речи или слова јављају ређе или чешће, пронађен је структурални систем. Наиме, пронађен је начин да се фрагменти текста појављују на више различитих локација, те да се, иако у различитим кодним књигама, смисао криптованог текста не мења пуно. Такође су открили да немачки код користи и методу којом се сугласници мењају самогласницима. На тај начин су, познајући особине кода, лако уклањане потешкоће поновног кодирања поруке.

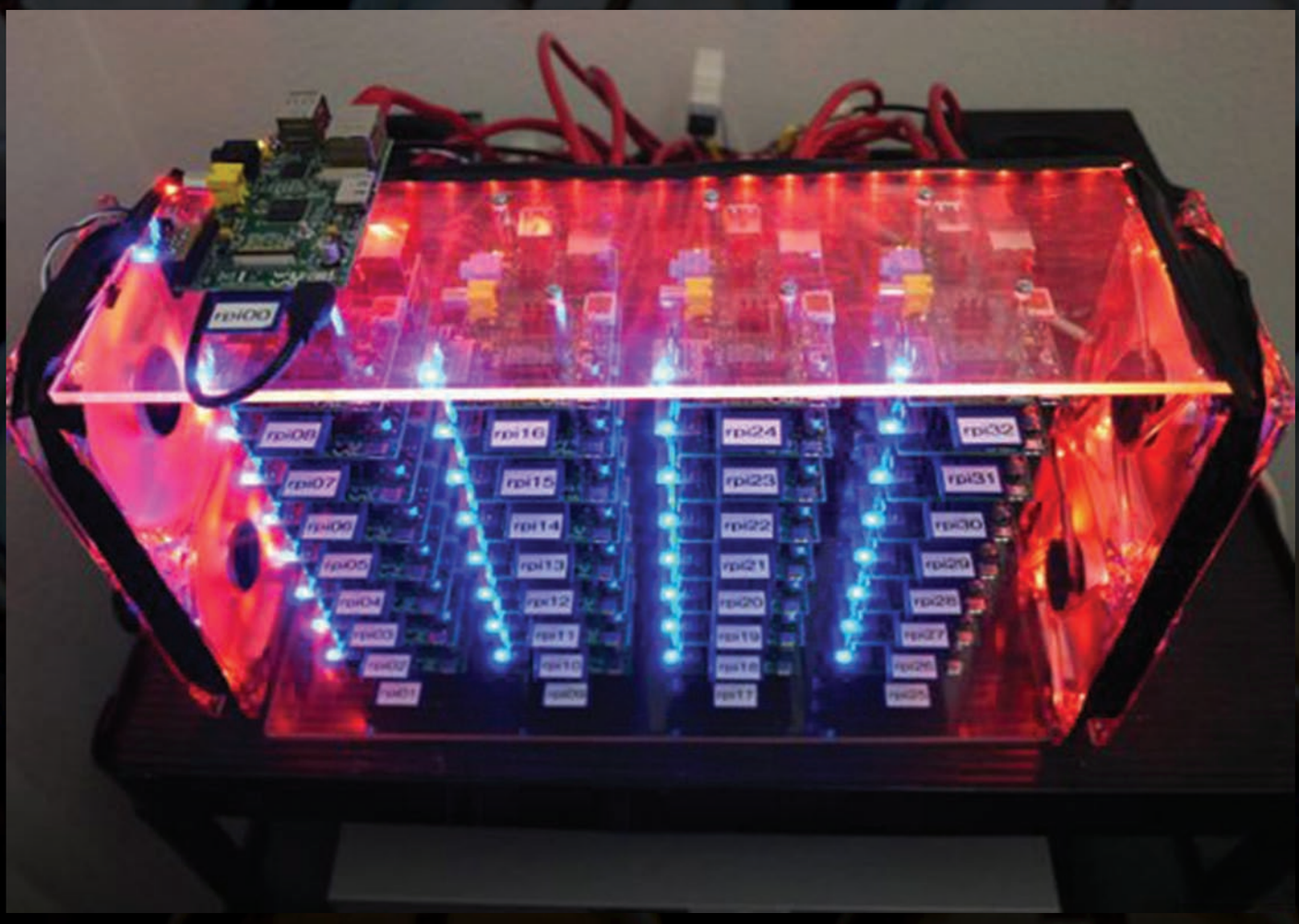
Иако ово делује као лак посао, ипак је декриптерима требало по три недеље да у потпуности пробију поруку, а имајући у виду да је велики део њих био део текуће стандардне преписке и да није садржавао много тајних података, било је тешко у самом почетку одвојити битне од небитних криптограма.

Постепено се број запослених криптоаналитичара повећавао, те је одлучено да се сви концентришу на једном месту. Октобра 1914. године група је смештена у једну просторију старог адмиралитета, која је носила број 40. Позиција собе одговарала је намени јер је била скрајнута од најпрометнијих делова, а истовремено релативно близу одељења за операције, које је примало све пресретнуте радио-поруке непријатеља. Формални назив групе био је 25. одсек обавештајног одељења, али је назив Соба 40 био конспиративнији, те га је цело одељење са поносом користило, па и онда када је пресељено у други и већи простор, због повећаног обима посла.

Крајем децембра заплењен је један сандук са немачког разарача потопљеног у бици у Хелголандском заливу, и тада је откривено да се међу бројним књигама на немачком језику налази и једна кодна књига, која је недостајала у руском открићу. Криптоаналитичари Собе 40 одмах су почели да је проучавају и дошли су до закључка да се наведени кодови користе за преписку између Берлина и аташеа у иностранству.

Повећањем броја порука, повећавао се и број запослених. Људство за ове послове бирало се на типичан и непосредан начин, без знања јавности, у кругу пријатеља и проверених познаника. Из мемоара појединих чланова видљиво је да су без много бирократских препрека чиновници разних специјалности довођени у одељење за криптоанализу, а формално имали статусе чувара, преводилаца, статистичара и слично. Попуна кадром за потребе криптоанализе имала је апсолутни приоритет. Наравно да су се, осим струке и знања, приликом избора кадра у обзир узимале и карактерне особине.

Растом радио-саобраћаја, који Немци нису могли избећи, расте и број размењених и откривених порука, тако да Британци ни не скривају активности на њи-



ховом праћењу, а тиме маскирају важнији сегмент прислушкивања – криптоанализу.

Адмиралитету се, поред криптоанализе података из исте собе, сервирају и подаци о значајнијем кретању и локацијама пловила непријатеља, а које су критоаналитичари систематично пратили, пратећи позивне знаке станица. Осим назива, односно тајног назива станице на пловилу, праћене су и карактеристике саобраћаја.

Овим начином постизан је двоструки ефекат. Осим сазнавања поруке, уз откривање положаја, прецизно се

одређивало кретање и бојне намере непријатеља, те је Черчил наредио да се сви важнији подаци достављају командантима јединица британске војске.

Захваљујући резултатима криптоанализе Британци су све чешће били у прилици да пресрећу и уништавају немачке подморнице, које су им до тада наносиле много зла.

После доказаног успеха Јуингу се даје потпуна и неограничена слобода деловања. Он је то искористио да повећа број прислушних станица као и број запослених на пословима пријема, криптоанализе и анализе информација.

Наслућујући да их Британци прате и прислушкују, Немци су, издајући неколико лажних наређења, покушавали британску флоту да намаме у замку. Промењени су и знакови за идентификацију станица. Тадашњи покушаји британске команде да последичне пропусте пребаце на криптоаналитичаре из Собе 40, осујећени су доказима да су грешке чинили запослени на бродовима. Иако су резултати дешифраната били веома драгоцени, често је ароганција командне структуре доводила до лоших исхода поморских битака на штету Британаца.

Увођењем немачких подморница у масовнију употребу, расте и интересовање криптоаналитичара за њихову комуникацију, тако да једном приликом оформљују и посебан тим ронилаца, који је претражио олупине потопљене подморнице. У соби кокпита пронађена је књига шифара у једној металној кутији. Тако се након тог открића један активиста из криптоаналитичарске службе специјализовао и до краја рата тражио искључиво кодове на уништеним пловилима. Он сам у забелешкама тврди да му је након неког времена постала рутина у проналажењу, јер су се кодови налазили скоро увек на типичним местима. Један атипични код пронађен у подморници умногоме је надопунио сазнања у Соби 40 и допринео бољем критоаналитичком раду.

Процењује се да су запослени у Соби 40 од 1914. до 1918. године пресрели и дешифровали око 15.000 немачких телеграма. Њихов рад није прекидан чак ни у време бомбардовања. Радило се у свим условима, непрекидно 24 сата.

Задивљујућа је чињеница, која се у јавности појавила тек након пола века, да је организација одељења за криптоанализу била конципирана тако да запослени у појединим деловима нису имали никакве међусобне односе, нису се ни познавали, а сваки контакт током и ван радног времена био је строго забрањен. Координација послова, пријем порука односно криптограма, класификација, криптоанализа, куцање и прекуцавање у одређеном броју примерака, достава корисницима и архивирање, били су кружно организовани, тако да је било скоро немогуће пратити који одељак који посао у које време ради, нити је, сем малог броја људи, знао ко му је сарадник у суседној канцеларији.

Једна од великих промена у овој организацији десила се када је Јуинг поднео оставку и прешао на место ректора Универзитета у Единбургу.

Након завршетка рата ова структура остала је да ради у склопу обавештајне службе. Због карактеристичних односа са цивилним друштвом, сви запослени добијали су чинове, а запослен је и известан број особа женског пола, пре свега за административне послове.

Ипак, као и сви сегменти друштва, и посао криптоаналитичара и обавештајаца није имун на сплетке и интриге, тако да су родоначелници криптоанализе и творци Собе 40 бесправно и аморално гурнути у ћошак историје.

Тајна Собе 40, као и све информације о црним кабинетима, спада у врх најстроже чуваних тајни и сваки податак који доспе у јавност је или историјско-архивског карактера или плод деловања обавештајних служби. У сваком случају, послови којима се наведена лица баве доступни су и познати веома уском кругу људи. Шездесетих година прошлог века масовнијом употребом рачунара полако се развијају и симетрични алгоритми, што можемо сматрати зачецима савремене криптографије. Убрзо након симетричних развијају се и асиметрични (алгоритми јавног кључа), који осим шифровања порука, омогућавају и њихово дигитално потписивање.

На помолу је и развој квантне криптографије, која се сматра будућношћу криптографије.

Развој криптоанализе

Иако кроз историју развој шифровања неминовно прати и развој криптоанализе, највећи искорак у овој сфери дешава се почетком 20. века, када скоро све државе формирају посебне службе које се баве разбијањем шифара. Британски црни кабинет, иначе веома познат и изучаван и у науци и у свакодневним расправама када је о шифрама реч, био је и остао водећа институција за криптоанализу. Највећи успех имао је у разбијању немачких морнаричких шифара. Немци су за шифре, односно кључеве користили стандардизоване речи, те је њихова преписка праћена и долазило се до отворених информација.

Америчка криптоаналитичка организација МИ-8 деловала је од почетка 19. века, мада се за њено оснивање узима 1929. година. О тој организацији написана је и књига Амерички црни кабинет, која је веома популарна и данас.

Појава радија 1895. године доприноси промени приступа криптографији и криптоанализи. Све до почетка Првог светског рата Французи су имали велики број прислушних станица којима су пратили немачки радиосаобраћај и веома лако декриптовали двоструку транспозициону шифру.

Руска искуства

Иако се појава криптографије у Русији везује за рани средњи век, сматра се да је њена употреба за заштити-

```
oot@localhost:~/Desktop/CloudFail# python cloudfail.py --target seo.com --tor
 ____ ____ ____ ____ ____ ____ ____ ____ ____ ____
||C |||l |||o |||u |||d |||F |||a |||i |||l |||0 ||
||__|||__|||__|||__|||__|||__|||__|||__|||__|||__||
|/__\|/__\|/__\|/__\|/__\|/__\|/__\|/__\|/__\|/__\|
  v1.0                                  by m0rtem

16:37:54] Initializing CloudFail - the date/time is: 12/06/2016 16:37:54
16:38:00] TOR connection established!
16:38:00] New IP: 5.135.158.101
16:38:00] Fetching initial information from: seo.com...
16:38:00] Server IP: 104.28.2.64
16:38:00] Testing if seo.com is on the Cloudflare network...
16:38:00] seo.com is part of the Cloudflare network!
16:38:00] Testing for misconfigured DNS using dnsdumpster...
16:38:03] [FOUND:HOST] toolsapi.seo.com  107.170.121.228 AS62567 Digital Ocean, Inc. U
16:38:03] [FOUND:HOST] cm.seo.com Apache/2.4.7 (Ubuntu) 198.199.116.160 AS14061 Digital
16:38:03] [FOUND:HOST] crm.seo.com nginx/1.4.6 (Ubuntu) 192.241.202.147 AS14061 Digital
16:38:03] [FOUND:HOST] deathstar.seo.com Apache/2.4.6 (CentOS) PHP/5.4.16 104.236.144.
16:38:03] [FOUND:HOST] deathdev.seo.com  209.90.66.178 AS5048 FIBERNET Corp. United St
16:38:03] [FOUND:HOST] host.seo.com nginx 173.255.232.177 AS8001 Net Access Corporatio
16:38:03] [FOUND:MX] 64.233.190.26 AS15169 Google Inc. 30 alt2.aspmx.l.google.com.
16:38:03] [FOUND:MX] 74.125.141.26 AS15169 Google Inc. 20 alt1.aspmx.l.google.com.
16:38:03] [FOUND:MX] 74.125.141.26 AS15169 Google Inc. 40 aspmx2.googlemail.com.
16:38:03] [FOUND:MX] 64.233.176.26 AS15169 Google Inc. 10 aspmx.l.google.com.
16:38:03] [FOUND:MX] 64.233.190.26 AS15169 Google Inc. 50 aspmx3.googlemail.com.
16:38:03] Scanning crimeflare database...
16:38:05] [FOUND:IP] 173.255.232.177
16:38:05] [FOUND:IP] 198.74.56.156
16:38:05] [FOUND:IP] 209.90.89.217
16:38:05] Scanning 2898 subdomains, please wait...
16:38:34] [FOUND:SUBDOMAIN] FOUND: blog.seo.com IP: 173.255.232.177 HTTP: 200
16:38:38] [FOUND:SUBDOMAIN] FOUND: blogs.seo.com IP: 173.255.232.177 HTTP: 200
16:39:04] [FOUND:SUBDOMAIN] FOUND: client.seo.com IP: 173.255.232.177 HTTP: 200
```

ту информација почела у време владавине Петра Првог. У 19. веку Русија је већ имала своје црне кабинете, махом смештене у поштама, где је постојао одређен број људи који су се бавили неприметним отварањем коверти, преписима, превођењем и криптоанализом по потреби.

Црни кабинет деловао је у Русији и у време владавине царице Елизабете. Познато је да је француски амбасадор знао да Руси прегледају његову преписку, али пошто је кореспонденција била кодирана, тврдио је да се осећа безбедно и да Руси не могу открити његове шифре. Тако се десило да су његове декриптоване изјаве како је царица „склона хировима" и „прилично неозбиљна и разуздана жена", на крају допринеле да Елизабета, која је иначе гајила велике симпатије према Француској, откаже гостопримство и врати амбасадора назад.

У музеју у Москви може се пронаћи и писмо министра спољних послова Русије с почетка 19. века, када је амбасадору дао инструкције да имају шифру за споразумевање са дипломатијом, те уколико постоји сумња да се откривају преписке, кодира једну обичну поруку и види да ли ће је Немци декриптовати, како би се предузеле адекватне мере заштите.

Велики допринос победи Руса над Наполеоном дали су управо криптоаналитичари који су Француске слабе кодове откривали скоро у реалном времену, што у својим мемоарима спомиње и цар Александар Први.

Јачањем покрета за борбу против царске апсолутистичке власти расте и број црних кабинета којима је тај-

на полиција пратила преписку осумњичених. Црни кабинети били су лоцирани у поштама у Петрограду, Москви, Варшави, Одеси, Кијеву, Харкову, Риги, Виљнусу, Томску и Тифлису, а по потреби су се формирали и на другим локацијама. Занимљиво је да су радници запослени у тим кабинетима углавном били странци са руским држављанством.

Неколико битака и операција, за које се сматрало да их Немачка и Аустроугарска држе у строгој тајности, откривени су и планови су пропадали, а да нису успели да пронађу узрок отицања тајни. Руси нису на сва звона оглашавали да декриптују поруке.

Дезорагнизацијом руске војске 1917. године опада дисциплина у шифровању порука, а самим тим и интересовање за декриптовањем непријатељских информација.

У зачетку бољшевичке револуције и првим годинама успоставе социјалистичке власти, у СССР-у се махом користило искуство из царске Русије, све до 1921. године, када су Немци и Американци открили многе тајне нове власти. Тада долази до огромног успона руске криптографске службе и паралелно са њом и криптоаналитичког дела. Тада и Американци признају да, иако су имали више од 3.000 руских телеграма, не знају много, јер за њихово декриптовање, и то само појединих, треба између шест месеци и једне године.

Иако се у почетку за дешифровање порука махом прибегавало крађи шифара, кодова и кључева од страних амбасада и конзулата и то полулегалним начинима, дејством агентуре, или шпијуна, совјетска „практична криптоанализа" касније ће постати узор свим службама у свету.

Најпознатија криптомашина енигма појављује се 1919, а у званичну употребу у немачкој војсци улази након неколико модификација 1926. године. То је електромеханички уређај који је имао 26 дирки, 26 сијалица тињалица, роторе и електромеханичке плоче, а напајао се батеријом.

Притиском на одређену дирку, кроз мрежу контаката ротора затварано је струјно коло и палила се тињалица која означава криптовано слово. На роторима је било по 26 дискова, увезаних без логичног редоследа. На трећем ротору се као продукт појављивао излазни криптовани текст. Сваким новим притиском на дирку мењао се положај ротора и пут затварања струјног кола, тако да се није дешавало да се два пута исти знак шифрује на исти начин. Ротори су се окретали циклично и сваки наредни зависио је од положаја претходног.

Покушаји декриптовања текстова шифрованих енигмом нису дали плода све док није заробљен један примерак те машине, што је омогућило да се немачке поруке током рата масовно прате и лако декритују.

Американци су за шифровање користили машину СИГАБА, познату и под именом ECM, једини уређај који током Другог светског рата није био пробијен. Радио је на сличним принципима као и енигма, са разликом да се 10 од постојећих 15 ротора могло премештати са једног положаја у машини на други, док су код енигме ти ротори били фиксирани. Такође се притиском на одређено дугме могло стартовати од било ког ротора, а не увек од првог како је било код енигме. Сви покушаји немачких и јапанских криптоаналитичара да пробију тај уређај остали су безуспешни.

Немачки сименс T52 био је уређај за он-лајн шифровање, чиме се знатно штедело на времену у обради и предаји порука..

Познато је још низ електромеханичких уређаја који су коришћени за шифровање порука, а развој рачунара допринео је и развоју криптовања и криптоанализе.

Јапанци су својим машинама за шифровање давали имена по бојама, тако да су познате корал, жад, пурпле и сличне. Радиле су на сличним принципима, али нису имале роторе већ телефонске склопке.

Турингова бомба једна је од најпознатијих машина за декриптовање из средине прошлог века, а развијена је током Другог светског рата.

Прва позната машина за безбедно комуницирање у телефонском саобраћају, која је користила импулсно-кодну модулацију и компресију преносног опсега, развијена у Беловој лабораторији био је Sigsaly. Оваква два апарата налазила су се у Пентагону и Лондону. Били су великих габарита и тежили 55 тона.

Савремени криптоалгоритми, базирани на рачунарској технологији, користе мноштво принципа шифровања и дешифровања, употребе кључева и додатних апликација.

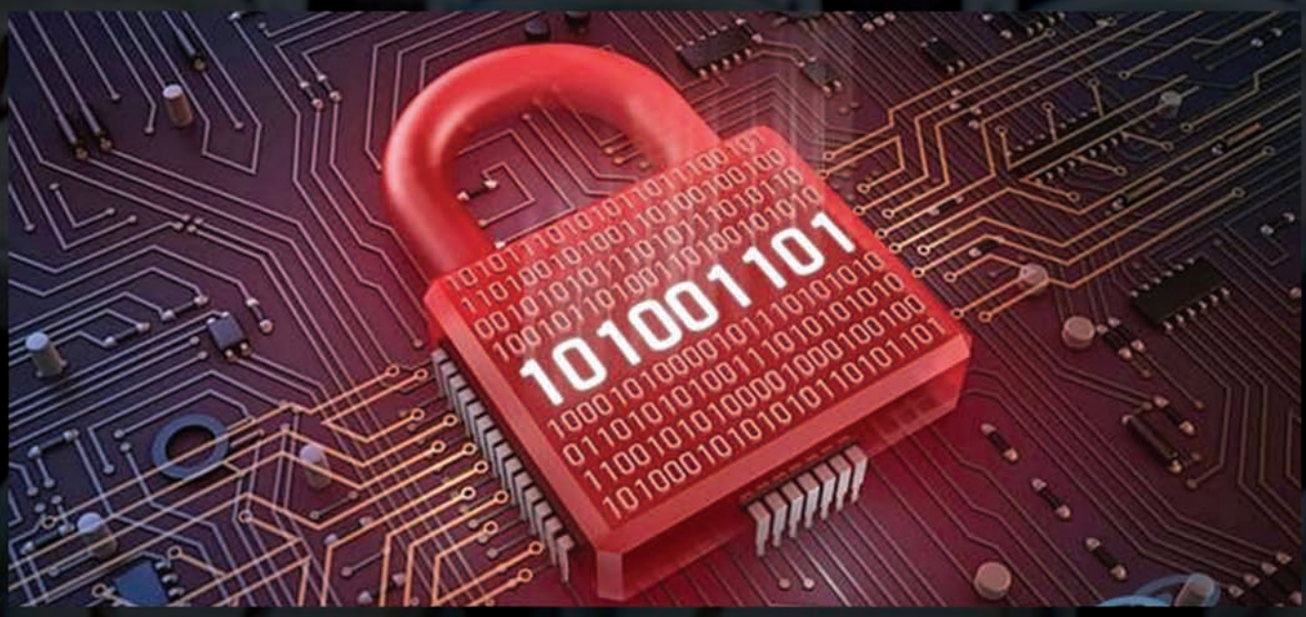
Било да је реч о симетричним, асиметричним или хибридним криптосистемима, за свој рад користе стандардизоване методе, а тајна остаје само у реализацији и употреби шифарских кључева. Савремени приступ криптографији, са јавним кључем, заснован на принципу јавног кључа за шифровање и тајног кључа за дешифровање, у основи има факторизацију целих простих бројева.

Иако се поуздано зна да у свету постоји неколико алгоритама који служе за решавање факторизације, нигде се не може наћи ни наговештај метода рада. Стога, иако се то не открива, сигурно је да постоје.

Можемо слободно тврдити да у овом тренутку једини поуздан начин шифровања јесте метода једнократног кључа, који постиже апсолутну тајност без обзира на време и ресурсе нападача–декриптера–криптоаналитичара.

Једно од прелазних решења за размену приватног било пара или дела кључа, у зависности који се криптосистем користи, јесте и квантна дистрибуција кључа, која је основа даљег развоја треће генерације криптосистема, односно квантне криптографије. Свакако да се будућност криптографије налази у квантној физици. Квантни рачунари постоје, производе се на неколико локација у свету, а где се тренутно користе, то остаје у сфери маште или нагађања.

За оне који се први пут сусрећу са овом темом, пре него што објаснимо принципе функционисања квантних рачунара и могућност њихове примене, реци-



мо да у теорији, квантни процесор са 1к кјубита има број стања реда величине броју ламбда, односно хипотетичком броју свих атома у универзуму!

Класичан и квантни рачунар

Апстракно говорећи, класичан електронски рачунар посматран из информатичког угла карактеришу битови. Зна се да бит има два стања. Нулу или јединицу, које физички репрезентује транзистор који се налази у закочењу (стању нула) или засићењу (стању јединица). Калкулацију на битовима омогућио је диверзитет дигиталне електронике, који данас имамо у свету информационих технологија.

Ако класични рачунар репрезентују битови (нуле и јединице), кванте репрезентују кјубити. Кјубит осим нуле и јединице има и једно додатно стање. Наиме, кјубит може да се у исто време налази у оба стања.

Занимљиво је да су се алгоритми за кванту калкулацију као теоријски модели појавили много пре квантних рачунара, скоро пола века раније, налазећи основу у квантој физици, без реалне везе са информационим (информатичким) светом.

Оно што на први поглед перципира већина људи који се не баве квантном механиком је претпоставка да је димензија једног транзистора, или у овом случају кјубита, сведена на квант, односно атом. Међутим, не ради се квантним системима по структури, него по функцији, а функције или процеси који су карактеристички искључиво за кванте системе су:

– дискретност енергије – одавно је утврђено да електрон који кружи око атома има тачно одређену, дискретну вредност енергије; када се ексцитује – када га погоди фотон, он пређе на нови, виши енергетски ниво са новом дискретном вредношћу; парадокс се огледа у томе да извесно, додуше веома кратко време, постоји на оба нивоа;

– суперпозиција – појава да путања електрона није предвидива, односно он се са одређеном вероватноћом налази на више места; иако представља честицу, понаша се као талас, те овај феномен омогућава паралелизам у обради података;

– квантна сплетеност – реално можда најбизарнији феномен, омогућава неку врсту телепортације; наиме, ако су две честице квантно сплетене, и једној се промене параметри, рецимо спин, и на другој се спин тренутно мења; у основи овог феномена је стабилност материје, а недавно је и Нобелова награда у физици додељена за ову област и експеримент у коме су две квантно сплетене честице удаљене неколико километара;

– тунеловање – пре више од 120 година, у Радефордовим експериментима утврдило се да електрони, иако немају довољно енергије, могу савладавати потенцијалну баријеру, као да лопта спонтано искаче из бунара; ни данас се не зна услед чега се ово дешава, одакле електрон позајмљује енергију, просто констатује се и већ више деценија примењује у класичној електроници као што је тунел диода.

Примена квантне теорије у информатици

Област примене квантне теорије у информатици и криптографији потпуно је мистична. Како математички проблем апроксимирати квантним процесима у оквиру квантног алгоритма, како тај алгоритам транспоновати на квантни процесор и како очитати решење након квантне калкулације.

Имајући у виду да је објектно оријентисано програмирање било и јесте проблем, ово је још већи ниво и већа непознаница. Свакако да ће ово бити следећи изазов за нове генерације софтверских инжењера.

Квантна криптографија користи квантну механику како би омогућила безбедна комуникација. То је, у ствари, начин да две стране у комуникацији креирају заједнички насумични бит стринг који је познат само њима, а може се користити као кључ за шифровање и дешифровање.

Јединствено својство квантне криптографије је могућност учесника у комуникацији да примете присуство непожељног учесника. То је, у ствари, принцип по коме се процес мерења квантног система нарушава ако у канал уђе трећа страна. Прислушкујући кључ она га мора мерити и тиме изазива неправилности које се уочавају у каналу.

Користећи квантне особине, а преносећи информацију у квантном стању може се имплементирати систем комуникације који је у стању да препозна прислушкивање. Ако је тај ниво прислушкивања испод одређене границе вредности, може се генерисати кључ који ће бити безбедан, а у противном није могуће остварити безбедан кључ и комуникација се прекида.

Безбедност квантне криптографије ослања се на основе квантне механике у поређењу са традиционалном криптографијом јавног кључа, која се ослања на рачунску тежину појединих математичких функција, и не може да пружи индикације о прислушкивању или гаранције за сигурност кључа.

Квантна криптографија за сада се користи за креирање и дистрибуцију кључа, али не и за пренос поруке. Предност је да се овакав кључ може користити у било ком алгоритму за шифровање и дешифровање поруке која се преноси преко било ког телекомуникационог канала.

Квантна комуникација подразумева кодирање информација у квантна стања, насупрот низа битова који се користе у стандардној комуникацији. Обично се фотони користе за та квантна стања. Квантна криптографија користи поједина својства квантних стања да би осигурала безбедност. Више је различитих приступа дистрибуцији квантног кључа и покушај да се он објасни спада пре у сферу науке него да се пласира широј публици.

Квантна стања више одвојених објеката могу постати повезана тако да се могу описати као комбиновано квантно стање, а не као индивидуални објекти. То значи да спровођење мерења на једном објекту утиче и на други објекат. Ако се испреплетени пар објеката пошаље комуникацијским каналом, покушај пресретања било које честице проузрокује промену комплетног састава, што доводи до открића треће стране, односно нападача у комуникационом каналу. Постоји више породица протокола, али најзаступљенији је онај са дискретним варијаблама. Остали протоколи углавном су оријентисани ка савладавању практичних ограничења у експериментима.

Поравнање информација у квантној размени кључа, у ствари, представља начин исправљања грешака који се спроводи између кључева пошиљаоца и примаоца, у покушају осигуравања идентичности оба кључа. Цео поступак спроводи се јавним каналом, па је битно да се информације о послатим кључевима сведе на минимум.

Појачање приватности је, у ствари, метод за смањење и уклањање делимичних информација које прислушкивач има о кључу. То се најчешће постиже или сажимањем кључева или њиховим дељењем на више блокова.

Примена ових метода још је у теоријским разматрањима и спроводи се у лабораторијским условима или експериментално на већим даљинама, коришћењем оптичког система преноса.

До сада се успело да се сигурно пренесу информације на даљинама од око 150 километара. Многе светски познате компаније које се баве софтверским инжењерингом улажу знатна средства у развој квантне криптографије, а комерцијални квантни криптографски системи испробани су у неколико земаља.

У перспективи се осим садашњих комерцијалних квантних криптографских система, сигурно може очекивати да се квантна размена кључева угради у постојећу инфраструктуру информационо-комуникационих система. Свакако да је размена кључева овом методом много јефтинија, сигурнија, лакша и бржа од класичних и питање је дана када ће она у потпуности заменити класичне методе размене.

Вероватно је да цена опреме и недовољна оспособљеност људства спречавају масовнију употребу, али ће поузданост и даљи развој засигурно убрзати ове две области, те ће се у скорој будућности квантна криптографија, у склопу постојећих система преноса, заузети место које јој се намеће и искористити све предности које има. ■


KRIPTOGRAFIJA