КРИПТОАНАЛИЗА
ИЗМЕЂУ МИТА И СТВАРНОСТИ

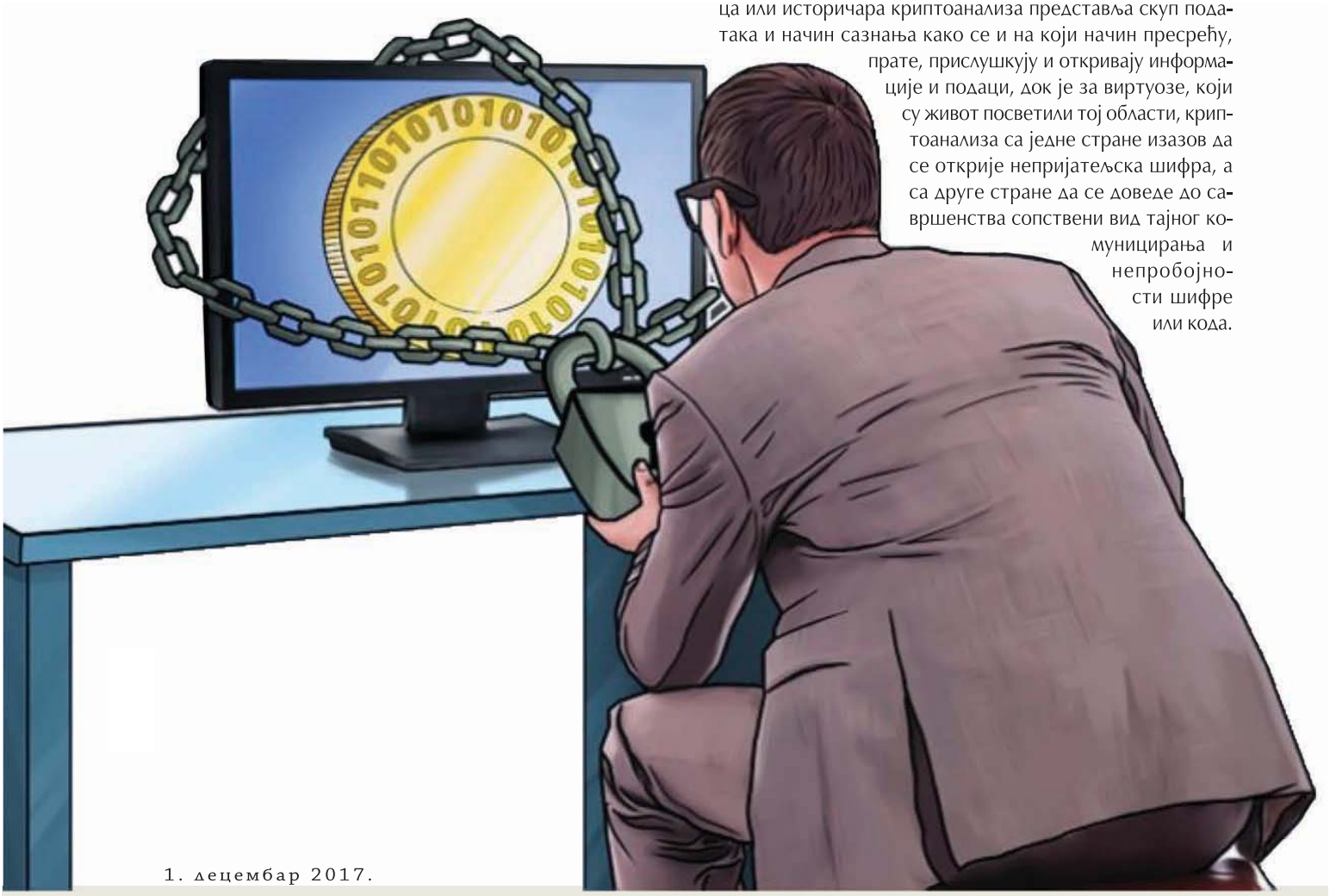
Пише Милорад МАРКАГИЋ

Не може се очекивати да ће свет једног дана бити без тајни. Заправо, из дана у дан све их више, а тако расте и потреба за новим методама шифровања. Са друге стране, обавештајне службе, у тежњама да дођу до скривених података, користе бројне методе прислушкивања и разбијања шифара. Тако се тајна нашла и налази у зачараном кругу између криптозаштите и криптоанализе.

Криптоанализа има велику моћ, убитачнија је од многих оружја. Она изазива или спречава ратове, војсковођама помаже да добију битке, дипломатији да има предност над супарником. Њоме се решавају историјске и текуће загонетке. Декриптовање, односно откривање шифри, и данас је један од најважнијих начина сазнавања тајних информација у модерном свету. Оно даје мноштво прецизних информација и много утиче на политику држава и влада. Ипак, све тајне службе немају довољно квалификованог кадра за декриптовање, те се зато свакодневно труде да пронађу и оспособе особље за ту делатност.

Премда постоје и званична признања и неке јавне публикације о бројности и раду криптоаналитичких служби, ипак је за разумевање њиховог деловања и утицаја на ток неких историјских догађаја потребно мало дубље познавање историјских облика сакривања информација и начина њиховог откривања. Од криптоанализе користи могу имати и државе, али и компаније и појединци, јер је велики део комуникација и пословања из класичног, пренет у свет виртуелног и електронике.

Правци развоја криптоанализе од прастарих времена, односно од прве појаве тајног комуницирања међу људима, па све до данас, пратили су ток цивилизацијског развитка и техничко-технолошки напредак. За обичног читаоца или историчара криптоанализа представља скуп података и начин сазнања како се и на који начин пресрећу, прате, прислушкују и откривају информације и подаци, док је за виртуозе, који су живот посветили тој области, криптоанализа са једне стране изазов да се открије непријатељска шифра, а са друге стране да се доведе до савршенства сопствени вид тајног комуницирања и непробојности шифре или кода.



Криптолози аматери, критоаналитичари/декриптери професионалци и сви други заинтересовани за ту област не могу да нађу информације о начинима деловања и нападима на шифре у званичним публикацијама, научним часописима или их чути у средствима јавног информисања. То пре свега зато што ниједна држава, влада или озбиљнија компанија ни по коју цену не објављује јавно ни своје методе заштите, нити пак методе праћења противне стране, већ се то у свету подводи под најстроже чуване државне и пословне тајне.

Не желећи да читаоца оставимо у заблуди, да кажемо одмах да постоје савршене методе сакривања порука, тако да у неким сегментима, без обзира на технолошки развој и све расположиве капацитете, декриптовање не даје никакве резултате.

Историјски гледано, праћењем архивске грађе, али и књижевне литературе, уочава се да је свака шифра или начин сакривања информација имала своје добре и лоше стране, као и употребну вредност у одређеном периоду. Ни шифранти, ни криптоаналитичари/дешифранти не дале своје интелектуалне моћи. Чак ни међусобно.

И то није све.

Због покушаја да се тајном прогласи и оно што то није, често се упадне у сопствену замку, па се грешке и отицање информација дешавају ненамерно, што умногоме повећава могућности пробоја шифре.

И даље у архивама и библиотечкој грађи постоји мноштво неистражених рукописа, поготово оних који су заробљени, па нису декриптовани, и због сплета околности остављени у запећку. Било да се радило о одлуци да је вредност информације, а самим тим и тајност прошла, било да се дошло до закључка да не постоји начин пробоја, или пак због смрти или дезертерства декриптера, познати су примери да велики број тајних пресретнутих порука никада није „отворен".

Могућност коришћења примарних извора сведена је на минимум, сазнања обавештајних служби су веома мало и ретко доступна, јавних публикација на научној основи нема, те се улога криптоанализе у дипломатији или рату мора повезивати и са низом других објективних околности и чињеница које су доприносиле развоју криптоанализе. Такав приступ доприноси да ову тематику ни раније, ни данас у савременом свету не смемо издвојити из области шпијунаже и аутентичне области јавне дипломатије или политике државе. Идентификовати криптоанализу само њом самом представљало би затварање у круг из кога нема излаза.

Основни појмови

Отворени текстови, односно поруке класификују се по значају, врсти, степену тајности и хитности. Као резултат тога произилази и коришћење различитих техника за шифровање јасне поруке, која се претвара у нејасан текст. Када се користи пермутација на отвореном тексту, као метода сакривања/шифровања поруке, знакови тада поремете своју нормалну структуру и секвенцу, па остају у шифрату, али са другим местом, односно другачијим распоредом у речи.

За декриптовање, односно криптоанализу таквих текстова користи се метода статистичких карактеристика језика – фреквенција слова. Тако се на узорку текста, када се препозна језик на коме је писан, простим бројањем понављања слова у шифрату, шифарским заменама по статистици опредељују слова по фреквенцији у „нормалном" писању. Када се заврши бројање, пронађу фреквенције слова и доделе онима у шифрату, те се упореде са отвореним значењима, сасвим је довољно да се на узорку текста изврши поновна замена, те се на тај начин долази до отвореног значења.

За ову методу криптоанализе потребан је шифровани текст довољне дужине, јер се на кратком тексту не морају нужно одразити све карактеристике учесталости јављања слова у речи и реченици.

Приликом замене знакови отвореног текста замењују се другим, унапред дефинисаним и договореним знаковима. Код тог вида скривања поруке, као шифарске замене могу се користити друга слова, бројеви или знакови интерпункције. Овај систем заснован је на идеји еквивалентних знакова који се користе за претварање обичног у шифровани текст.

Понекад се у неким методама нуди неколико замена за исти знак. То је опција такозваних хомофонских замена, али се и том приликом у шифрат могу убацити и неке замене које не значе апсолутно ништа, односно убацивање лажних знакова у шифрат.

Декриптовање се овде такође своди на проналажење могућих места слова у речи или реченици и распознавању лажних знакова.

Код шифара замене треба направити јасну разлику између кодова и шифри.

Кодови се састоје од више хиљада речи, фраза, слова и слогова и начина на који се замењују елементи отвореног текста. У ствари, код представља огромну шифру замене, у којој су основне јединице отвореног текста речи и фразе, а самим тим и структура шифрата је другачија.

Шифре као основну јединицу користе знак или неколико знакова.

У пракси је дуго, од 14. па све до половине 19. века, доминирао вид шифровања порука који је користио комбинације шифре и кода. Такозвани номенклатори имали су посебан вид употребе, који је укључивао хомофонске замене и погодне кодове са списковима имена, речи и слогова.

Свака шифра користи неки кључ који одређује редослед знакова у шифрату, редослед мешања знакова у замени, односно почетно стања машина које су у то време коришћене за шифровање. Основу почетних стања представљала је нека фраза или број. Назив је и данас остао исти: кључна реч, кључна фраза или кључни број.

Обављање одговарајуће трансформације отвореног текста у шифрату и данас се зове шифровање или кодирање отвореног текста, а резултат се зове шифрат или код-текст.

Завршна обрађена тајна порука је у ствари криптограм.

Термин „шифрат" скреће пажњу на резултат шифровања, док термин „криптограм" наглашава чињеницу да је у питању пренос неразумљиве поруке за трећу страну. Особе које легално имају кључ за шифровање (кодовање) дешифровањем (декодирањем) обављају инверзну трансформацију шифрата, односно код текста да би добиле отворени текст. Овај процес разликује се од криптоанализе, која има за циљ да открије отворени текст (или, другим речима, дешифровање) криптограма, од лица која немају на располагању било који улазни елеменат шифросистема, односно лица која представљају трећу страну, а то је најчешће противник или непријатељ.

Успешна криптоанализа шифре или кода често се назива „отварање", „пробијање" или „провала". Напокон, криптологија и јесте наука која обухвата израду шифре (криптографију) и криптоанализу.

Све је почело доста давно

Пре скоро четири хиљаде година у древном Египту, на обалама Нила, искусан сликар нацртао је неке познате ликове како би испричао причу о животу свог господара. Тако је и не знајући постао оснивач документоване историје криптографије. Те слике нису криптографија у облику у којем је познат савременом свету. За класификацију својих натписа непознати уметник није користио неки нарочити вид енкрипције. Његов натпис, исклесан око 1900. године пре нове ере у гробници једног племића, само у неким деловима састоји се од необичних хијероглифских симбола, уместо познатих ликова. Већина њих налази се у последњих двадесет стубова, у наведеном споменику.

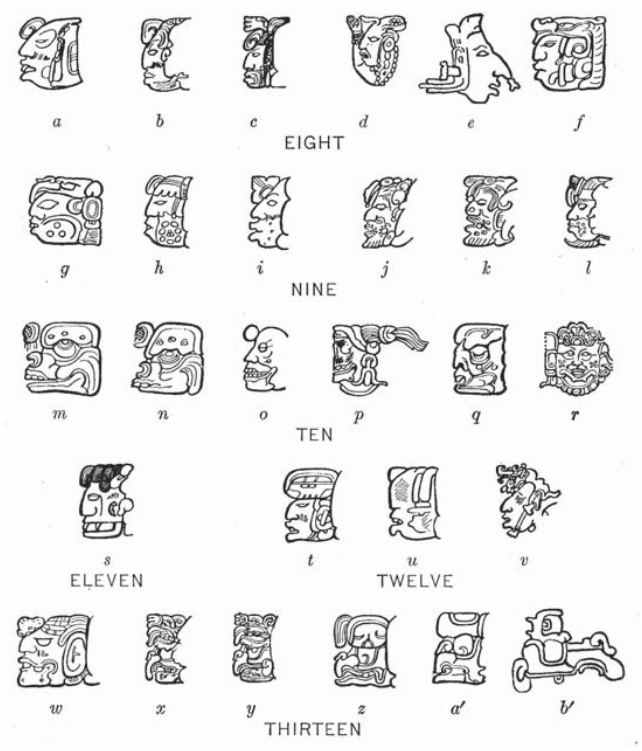
Непознати сликар (или писар или клесач) трудио се да текст буде лако читљив и дао му потребан значај, као што се то ради у свечаној прилици, у којој пише „године хиљаду осам стотина и педесет осме", уместо једноставно 1858. Тако, иако није имао намеру да примени криптографију, он је несумњиво искористио један од битних елемената шифровања – намерну конверзију писаних симбола. Ово је најстарији познати текст који је прошао кроз такве промене.

Као врхунац древне египатске цивилизације јавља се усавршавање списа у гробницама мртвих, тако да конверзије текста постају све софистицираније.

Током времена писци клесари почели су да замењају конвенционалне хијероглифе другачијим облицима, иако су у суштини имали иста значења. Хијероглифи доживљавају трансформацију употребом нових знакова, тако да се изговор у суштини своди на то да је прво слово појма у ствари једино што треба прочитати, тако да ако је на слици копље, треба прочитати само слово „к". Дешавало се да два знака, иако различита, означавају исто слово. Ради убацивања мало мистерије поједини појмови клесани су у камену по принципу ребуса.

С временом су се из хијероглифа развили звуковни појмови па је створено савременије писмо, а хијероглифи су остали само у историји и египатског народа. Такве трансформације видљиве су у многим натписима на гробницама и саркофазима, те се упоредном анализом долази до закључка да има доста сличности у текстовима, што доказује да у то време није много тога требало да буде сакривено, већ је више учињено ради остављања утиска на „читаоце", како у уметничкој структури, декорацији, тако и мистици дељених појмова.

Староегипћани су доста пажње и вере посвећивали животу после смрти, тако да је и жеља за писањем и читањем епитафа постајала већа, а самим тим и намера писаца текстова да на неки начин привуче пажњу читаоца. Из тог разлога неки текстови су и намерно писани у увијеној или скривеној форми. Тако је део криптографских знакова не-



Египатски (горе) и мајански хијероглифи (доле)

намерно завршио у посмртним посветама. Иако је првобитна жеља била да се привуче пажња читалаца, убацивањем неразумљивих знакова, пермутацијама текста и вишеструким заменама за исте речи или појмове изазван је супротан ефекат, па је интерес за њима опадао.

Иако је то писање на гробницама и саркофазима имало за циљ да оствари краткотрајну тајност поруке, део текстова ни данас није у потпуности преведен, односно растумачен. Дакле, иако ненамерна, криптографија хијероглифима представља почетак изучавања основних атрибута криптографије и криптоанализе – тајност и сакривање.

Рађање криптологије, појавних облика тајног комуницирања одвијало се независно у многим цивилизацијама и заједно са њиховим крајем доживљавало и сопствени, док је у неким облицима криптологија ипак надживљавала нестанак цивилизација и држава и преносила се на будућност.

Поједине цивилизације сачувале су писане трагове у литератури, тако да су наредне генерације криптоаналитичара имале некакву полазну основу. Ипак, напредак није био нимало лак, јер није као у другим областима науке постојало акумулирано знање нити је било размене искустава и информација, што је умногоме и данас случај.

Интересантна је чињеница да је у древној индијској цивилизацији још у 3. веку пре нове ере написана расправа о криптографији и криптоанализи, где се дипломатама и агентима сугерише да за комуникацију користе шифровани вид писања и говора, а да слушајући разговоре у земљама у којима су ангажовани покушају да пронађу скривене појмове у свакодневној комуникацији. То је уједно и први писани траг о употреби криптоанализе за државне потребе и уопште први писани траг о криптоанализи у светским размерама.

Мада се не дају конкретне смернице за коришћење криптосистема и криптоанализе, већ само оквирне назнаке, а процедуре се одвијају у тајности, део је након неколико векова изашао у јавност. Радило се о томе да се употребом симбола, свакодневне и верске природе замени право значење речи, а декриптовање се вршило инверзном операцијом.

Период стагнације

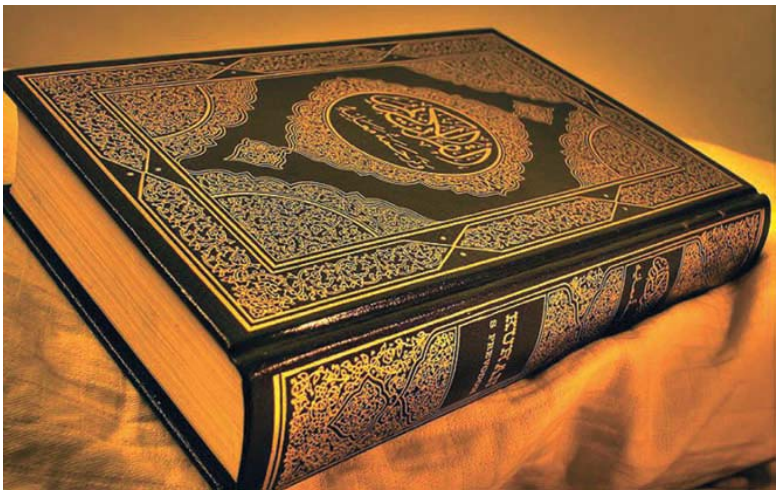
До почетка ренесансе у Европи криптографија прилично стагнира. За покушаје да се и верске књиге, а највише *Библија* прикажу као један вид шифре, као и тумачење разних догађаја из прошлости који су тамо скривено описани, не постоји никаква научна оправданост. Јер како би најумнији људи онога времена пренебрегли чињенице као што је распад Вавилонског царства и слично, не упозоривши своје владаре на то? Данашња тумачења неких појава у појединим државама или догађајима светских размера само су плод маште, шарлатанство и трка за публицитетом и материјалном коришћу.

Криптологија у оба појавна облика, и као скуп шифара и као начин њиховог пробијања, у периоду мрачњаштва, а нарочито након раскола у хришћанској цркви, била је погођена и једном, веома развијеном, болешћу тога доба, а то је забрана бављења науком, па и вештинама попут криптоаланизе, због веровања да спадају у црну магију, а људи који се баве овом делатношћу сматрани су следбеницима Сатане.

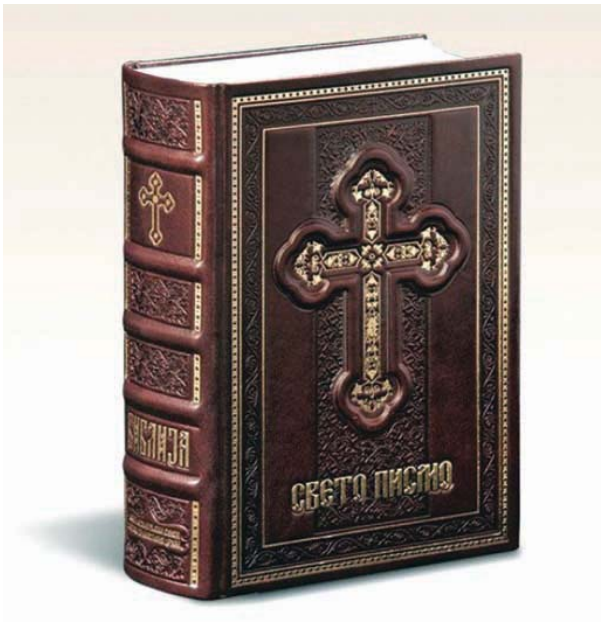
Примењивани шифросистем у Европи био је тада углавном на нивоу просте шифре замене, где су се слова премештала, мењала редослед или су нека добијала бројчану замену, затим се користило писање наопаким редом и слично. Део шифраната користио је и речи страних и старих језика.

Од почетка развоја криптографије коју данас познајемо, основна намена јој је била да сакрије садржај важних делова писаних докумената, а некада и целих докумената.

Треба имати у виду да су у стара времена поруке биле веома кратке. У једном од рукописа о магији из 3. века спомиње се употреба шифре, ради сакривања тајних рецепата, а такође се поуздано зна и да су научници у области астрономије, хемије, медицине и још неких наука своја от-



Покушаји да се верске књиге, а највише „Библија", користе као један вид шифре



крића намерно шифровали, било да их сакрију од непожељних посматрача, или најчешће плашећи се реакција и осврте цркве.

И данас је тешко доћи до ватиканске библиотеке и ископати неке рукописе, а музеји у многим земљама љубоморно чувају писану грађу као експонате и не дозвољавају да се дође до неких података, како оних шифрованих различитим методама, тако и отворених, до којих се дошло разбијањем шифри – криптоанализом.

Поред намерног шифровања писаних текстова у том периоду, приметне су појаве да се и делови фраза, речи или реченице компонују тако да настају нове речи и изрази које су познате само особама које међусобно комуницирају.

Суштина је да се одгонетну тајне коју ти појмови носе, па се разбијање тих „шифара" сводило на методе замене редоследа слова, речи или „превођења" у изворно-појавни облик. Тако је велики део „откривених" порука у ствари имао потпуно другачије значење и тумачен је онако како су творци криптоанализе хтели, без обзира на то шта је порука заправо значила.

Забрана бављења криптографијом и криптаонализом допринела је томе да се велики део открића, пре свега у сфери астрономије, медицине, хемије и још неких наука, намерно шифрованих одређеним симболима, обележавају и данас на исти начин.

У то време криптоанализа је у широкој популацији, без обзира на ниво образовања или положај у друштву, сврставана у ред прорицања, јер се продирање у нешто сакривено и нејасно сматрало немогућим и несхватљивим. Ипак, након 14. века, када се уводе софистицираније методе шифровања, када се производе прве просте машине за шифровање, криптографија писаних текстова добија на већем значају, а паралелно са њом и криптоанализа.

Поред разбијања шифри или кодова велика пажња посвећивала се и коришћењу и откривању писања тајним мастилима. Тако се, осим ретких примера у древним цивилизацијама, за почетак озбиљније криптоанализе узима време од почетка 15. века.

Криптоанализа у арапској култури

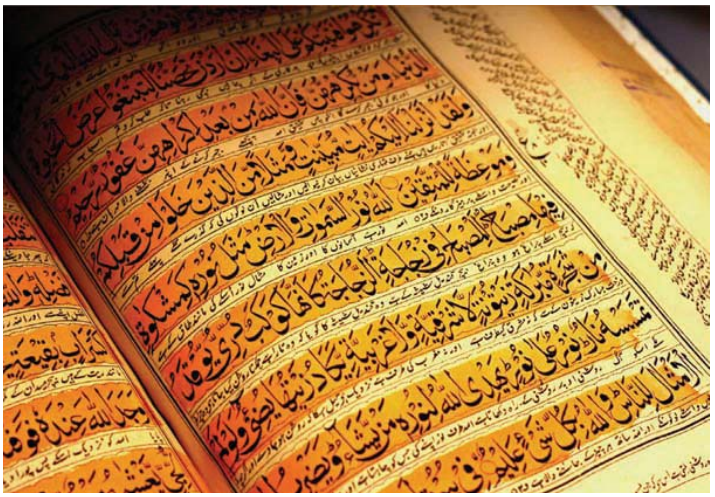
Арапска цивилизација, једна од најнапреднијих у средњем веку, имала је огромне заслуге у многим областима науке, као што су математика, филозофија, медицина, наука о језику, као и у делу који се тиче криптоанализе. Такође, дошли су до многих открића која се тичу вербалних слагалица, загонетки и игре речи, али и откривања тако конципираних текстова, те стога први детаљно описани поступци за криптоанализу припадају баш тој култури и цивилизацији.

Као део граматике изучавана је криптографија. Нажалост, због погрешног или намерно изврнутог текста *Курана*, убрзо је дошло до забране ширења цивилизацијских и научних тековина арапске културе на шире просторе.

Иако криптоанализа код Арапа датира још из 855. године, о чему постоји и књига са описаним методама и поступцима, најпознатија је модификована верзија криптографије која је била састављена од хебрејских слова и која је искоришћена за откривање преписке алжирског регента. Искуства из ове области детаљно су описана у енциклопедији од 14 томова, где се два поглавља односе на криптографију и криптоанализу. Једно поглавље односи се на видове тајног комуницирања – шифре, а друго на невидљива мастила и криптоанализу.

Први пут у историји шифре тада се наводи и метод транспозиције, односно система и замене система шифровања. Ту се први пут спомиње и листа кодова који се користе за вишеструку замену. Део који се односи на криптоанализу у потпуности је засенио први део који се односи на заштиту сопствених порука.

Интензивна и детаљна проучавања верских књига, али и истраживања у школама граматике довела су да се изучава фонетика сопственог језика, али и слова или речи позајмљених из других језика. Такав развој лексикографије неминовно је пратио и развој криптоанализе. На пример, када је састављан први речник арапске културе велика пажња, проистекла из сазнања из области криптологије, посвећена је појавама учесталости слова у речи. Тако је, раме уз раме са развојем науке о језику и писму, и криптоанализа ширила своје поље деловања.



Криптоанализа код Арапа датира још из 855. године

Један од највећих теоретичара криптоанализе Калкасханди описује главну криптоаналитичку методу тог времена: сазнати језик на коме је порука писана, и ако га не разумеш или говориш. Након тога треба сазнати да ли је порука шифрована за политичке, војне или верске потребе, јер је учесталост употребе речи и слова у њима потпуно другачија за различите области.

Наставак криптоанализе своди се, пре свега, на бројање слова, и статистичко утврђивање који се знак колико пута јавља, те формирање таблице фреквенције слова.

Следећи корак био би да се у шифрованом тексту, по статистици, уместо шифарских замена стављају претпостављена слова датог језика. Уколико има поклапања наставља се са заменом, а уколико нема онда се претпоставка мења и узима наредна фреквенција слова. Након неко-

лико покушаја и доласком до једне трећине отворених замена, даљи поступак шифарских замена веома је олакшан. Када се уклопи и последњи еквивалент дође се до садржаја отворене информације.

У то време јавља се и метод биграма и триграма, односно законитости везивања слова у отвореном тексту, а које прате њихове шифарске замене. Интересантан је и податак да су још у оно време изучаване појаве дужине, односно структуре речи, те се за сваки криптограм, уз претпоставку његове намене, тумачила и дужина речи односно број слова у њима.

Много пажње изазвала је и идеја описана у декриптовању једне поруке, за коју се претпоставило да је шифрована употребом поезије, односно једне песме, где су читаве речи мењане речима из поезије, а након тога спајане у целину без размака и знакова интерпункције.

Историја ћути о мери у којој су Арапи користили своје бриљантне криптоаналитичке способности. Иако су криптографија и криптоанализа имале огроман утицај на развој ислама, сва сазнања стављена су у запећак. Тако се штуро и скромно спомиње догађај када је марокански султан Ахмед Ал-Мансоур послао свог изасланика на енглески двор код краљице Елизабете Прве да склопе савез против Шпаније. Изасланик је из Енглеске свом владару послао криптовани телеграм, али није узео у обзир, или није знао, достигнућа Арапа у области криптоанализе. Његово писмо пресрели су и врло брзо одгонетнули скривену поруку у њему, чиме су дошли до значајних и веома корисних информација.

Успон Запада

Западноевропска цивилизација средњег века почела је да користи криптографију као наставак старовековних шифросистема. Може се рећи да се тада није много одмакло од претходних неколико векова, односно да је криптологија у то време још имала статус науке у повоју. Употреба шифре све до средине прошлог миленијума је ретка и нестабилна, како у државним, тако у црквеним круговима. Иако институција са највећим утицајем, црква не одмиче далеко у коришћењу шифре, већ као и друге догме, основне ставове држи као једину свету ствар у криптологији. Истраживачи су успели да уђу у траг криптографском документу који се сматра најстаријим сачуваним на Западу. Данас се чува у ватиканској архиви и представља шифрована имена Египћана и Израелаца. И у венецијанској архиви сачуван је један документ који представља неки вид шифре, где су самогласници замењени тачкама или ознаком крста. Криптоанализа тих порука састојала се у томе да се за више самогласника који су мењани само са два симбола нађе отворено значење и место у речи.

Шифра скитале

Антипапа Климент Трећи, који је у другој половини 14. века пребегао у Авињон и почео да ради на раздору Католичке цркве, јер је себе сматрао наследником папског престола, а до њега није стигао, имао је око себе моћну машинерију следбеника, а међу њима и шифранте. Наредио је да се оформи књига нових кодова за комуникацију са осталим следбеницима широм градова-држава. Његова метода комбинације шифри и кодова, први познати номенклатор и хибридни систем шифровања, остаће у употреби на Западу, са неким модификацијама, пуна четири века.

Појава хомофонских шифри почетком 15. века умногоме је поништила знања криптоаналитичара, те су се технике пробијања морале мењати. Иако је продор ислама на тло Европе веома допринео да „стара дама" искористи, пре свега, знања из математике и других природних наука, нажалост, арапска дела о криптографији и криптоанализи нису преведена ни на један европски језик.

Криптографија и криптоанализа се у Европи, нарочито у западној, масовно почињу примењивати са наглим развојем дипломатије, иако је неких појавних облика било и раније. Познати и као „пријатељски шпијуни", већина дипломата слала је депеше у матичну земљу, користећи легална или нелегална средства за сазнања о земљи домаћину. Имајући у виду да је у њима било доста ствари које је требало сакрити, те да се огроман број преписки онога времена пресретао и „копирао", а затим поново враћао у легалне токове, јавила се потреба за шифровањем и дешифровањем порука. То је условило и формирање посебних служби које су декриптовале пресретнуте поруке покушавајући да дођу до пуне отворене информације. Скоро сви дворови тадашње западне Европе имали су посебно организоване службе криптоанализе, састављене од врсних стручњака из обла-

Краљица Елизабета I

сти математике и ли нгвистике. Први познати декриптер био је шеф кабинета Млетачке републике Ђовани Соро, о коме постоји више писаних трагова.

Познат је догађај када је Соро, слагавши папу Климента XIV да не може декриптовати поруке, створио илузију о непробојности ватиканске шифре, те су плодови његове обмане убирани веома дуго. Њему је канцеларија била на двору владара Млетачке републике и извесно време вођен је документ о његовим успесима и успесима његова два помоћника у криптоанализи текстова написаним на италијанском, шпанском, француском и још неким језицима, али је нажалост „изгубљен".

Иако је црква у почетку сатанизовала декриптере, од 16. века своју кореспонденцију и шпијунирање туђих и она у потпуности базира на криптографији и криптоанализи.

На двору енглеског краља, као и владара Француске, Данске и још многих земаља у то време формирају се одељења, кабинети који су намењени искључиво праћењу, откривању и декриптовању преписки страних дипломата.

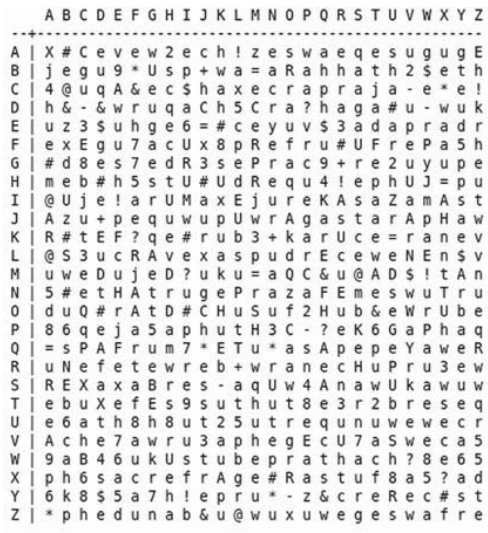
Записан на једном пергаменту и данас је доступан милански текст о криптоанализи шифара, који показује тринаест основних правила за рад на разбијању кодова и шифри.

Вртоглави развој науке и технике допринео је да се и поље шифри шири и преузима сва позната достигнућа, тако да се отварање и дешифровање телеграма које је некада трајало данима и недељама, скратило на неколико часова.

Развој и успеси криптоанализе неминовно су условили и успехе на изналажењу нових и сигурнијих шифросистема. Искористивши као основу Цезарову шифру, француски дипломата Блез де Вижнер створио је такав шифарски систем који је скоро три века био у употреби и до данас остао „непроваљен". Сви покушаји криптоанализе тог система падали су у воду, јер је кључ као основа шифровања толико јак, таблица шифри променљива, а постулати шифровања познати су само двема странама учесницама у кореспонденцији.

Све до 19. века у скоро свим западним земљама појединачно се успостављају криптоаналитичке службе које су се бавиле троструком делатношћу. Први задатак им је био пресретање и отварање поште, преписивање порука и враћање у првобитно стање, те слање примаоцу. Друга ствар је била и тежишна, а односила се на тумачење шифара, њихово разбијање и долазак до отворених информација. Трећи део њиховог посла, иако не директно везан за криптологију, био је стварање тајних мастила и/или проналажење реагенаса за читање скривених порука писаних неким тајним (невидљивим) мастилом.

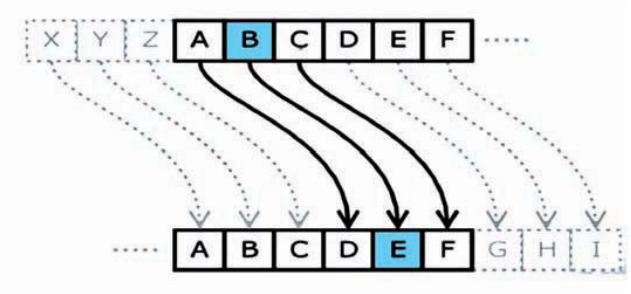
Технички развој средстава телекомуникација, почевши од проналаска Морзеовог кода и телеграфа, изискивао је константно праћење новог вида комуникација и покушаја разбијања нових кодова.



	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	X	#	C	e	v	e	w	2	e	c	h	!	z	e	s	w	a	e	q	e	s	u	g	u	g	E
B	j	e	g	u	9	*	U	s	p	+	w	a	=	a	R	a	h	h	a	t	h	2	$	e	t	h
C	4	@	u	q	A	&	e	c	$	h	a	x	e	c	r	a	p	r	a	j	a	-	e	*	e	!
D	h	&	-	&	w	r	u	q	a	C	h	5	C	r	a	?	h	a	g	a	#	u	-	w	u	k
E	u	z	3	$	u	h	g	e	6	=	#	c	e	y	u	v	$	3	a	d	a	p	r	a	d	r
F	e	x	E	g	u	7	a	c	U	x	8	p	R	e	f	r	u	#	U	F	r	e	P	a	5	h
G	#	d	8	e	s	7	e	d	R	3	s	e	P	r	a	c	9	+	r	e	2	u	y	u	p	e
H	m	e	b	#	h	5	s	t	U	#	U	d	R	e	q	u	4	!	e	p	h	U	J	=	p	u
I	@	U	j	e	!	a	r	U	M	a	x	E	j	u	r	e	K	A	s	a	Z	a	m	A	s	t
J	A	z	u	+	p	e	q	u	w	u	p	U	w	r	A	g	a	s	t	a	r	A	p	H	a	w
K	R	#	t	E	F	?	q	e	#	r	u	b	3	+	k	a	r	U	c	e	=	r	a	n	e	v
L	@	S	3	u	c	R	A	v	e	x	a	s	p	u	d	r	E	c	e	w	e	N	E	n	$	v
M	u	w	e	D	u	j	e	D	?	u	k	u	=	a	Q	C	&	u	@	A	D	$	!	t	A	n
N	5	#	e	t	H	A	t	r	u	g	e	P	r	a	z	a	F	E	m	e	s	w	u	T	r	u
O	d	u	Q	#	r	A	t	D	#	C	H	u	S	u	f	2	H	u	b	&	e	W	r	U	b	e
P	8	6	q	e	j	a	5	a	p	h	u	t	H	3	C	-	?	e	K	6	G	a	P	h	a	q
Q	=	s	P	A	F	r	u	m	7	*	E	T	u	*	a	s	A	p	e	p	e	Y	a	w	e	R
R	u	N	e	f	e	t	e	w	r	e	b	+	w	r	a	n	e	c	H	u	P	r	u	3	e	w
S	R	E	X	a	x	a	B	r	e	s	-	a	q	U	w	4	A	n	a	w	U	k	a	w	u	w
T	e	b	u	X	e	f	E	s	9	s	u	t	h	u	t	8	e	3	r	2	b	r	e	s	e	q
U	e	6	a	t	h	8	h	8	u	t	2	5	u	t	r	e	q	u	n	u	w	e	w	e	c	r
V	A	c	h	e	7	a	w	r	u	3	a	p	h	e	g	E	c	U	7	a	S	w	e	c	a	5
W	9	a	B	4	6	u	k	U	s	t	u	b	e	p	r	a	t	h	a	c	h	?	8	e	6	5
X	p	h	6	s	a	c	r	e	f	r	A	g	e	#	R	a	s	t	u	f	8	a	5	?	a	d
Y	6	k	8	$	5	a	7	h	!	e	p	r	u	*	-	z	&	c	r	e	R	e	c	#	s	t
Z	*	p	h	e	d	u	n	a	b	&	u	@	w	u	x	u	w	e	g	e	s	w	a	f	r	e

Вижнер (лево) и његова шифра

Релативно лак за употребу Морзеов код постаје доступан великом броју људи, те се након врло кратког времена почело са шифровањем кодираних порука. Изузетан напредак у криптоанализи постизали су енглески и фран-



Цезарова шифра

A	.-	.|	K	-.-	|.|	U	..-	..|	5	.....	.....
B	-...	|...	L	.-..	.|..	V	...-	...|	6	-....	|....
C	-.-.	|.|.	M	--	||	W	.--	.||	7	--...	||...
D	-..	|..	N	-.	|.	X	-..-	|..|	8	---..	|||..
E	.	.	O	---	|||	Y	-.--	|.||	9	----.	||||.
F	..-.	..|.	P	.--.	.||.	Z	--..	||..	0	-----	|||||
G	--.	||.	Q	--.-	||.|	1	.----	.|||	.	.-.-.-	.|.|.|
H	....	....	R	.-.	.|.	2	..---	..|||	,	--..--	||..||
I	..	..	S	...	...	3	...--	...||	?	..--..	..||..
J	.---	.|||	T	-	|	4	....-	....|			

Морзеова азбука

цуски стручњаци, што је доводило до тога да су владе тих земаља, очаране успесима криптоналитичара, велику пажњу посвећивале развоју својих шифросистема.

Ера *црних кабинета*

Некако истовремено у више западних земаља, а касније и у САД, формирају се „црни кабинети", који су по структури, намени, а игром случаја и имену, били веома слични. Разликовала их је само бројност особља и начин субординације, али у суштини, сви су били везани за сам врх власти одређене државе, било при двору или у министарствима рата и спољних послова.

Најпознатији црни кабинети, бар према ономе што је историјски познато, били су аустријски, француски, енглески и амерички. Занимљиво је да је још у току грађанског рата у Америци, при штабу генерала Вашингтона, постојала добро организована декриптерска служба, чији је шеф био потчињен лично Вашингтону. У току борбених дејстава било је мноштво примера пресретања криптограма, који никада нису отворени, јер су се шифранти досетили да већ шифровану поруку поново шифрују и то другим кључем, што је знатно отежало њихово декриптовање. Након сазнања да је остварено двоструко шифровање, декриптери би одустајали од исцрпљивања снага и концентрисали се на оне криптограме који су могли да отворе.

Керховс, виртуоз и геније на пољу криптологије, поред утемељења основних принципа криптографије, даје и смернице како да поступају дешифранти, односно како се врши криптоанализа туђих порука, било да су употребили код, кључ или номенклатор – комбинација та два.

Формално распуштање „црних кабинета" свакако не значи и њихов крај, јер се службе оријентишу на пробијање шифара под другом „капом", другачијим именом, али са истом наменом.

О значају америчког црног кабинета, његовим достигнућима и утицају на ток Првог светског рата исписане су многе студије и књиге. Чувена „афера Драјфус" је такође за основу имала пробијање шифара од француских стручњака, а након тога су о том случају испредане многе легенде. Документовани су преписи телеграма који наводе на то да је он заиста био шпијун.

Први кораци књижевне криптоанализе повезани су са причом америчког писца Едгара Алана Поа „Златна буба". Та прича и данас остаје ненадмашено уметничко дело на тему дешифровања.

Развој бежичних (радио) комуникација, односно могућност преноса гласовних порука, допринео је да се информације брже и тачније преносе, што је нарочито утицало на пољу ратних дејстава. Почетак криптозаштите, а самим тим и криптоанализе гласовних порука сводио се на употребу простих таблица и кодова, најчешће кодних речника, који су се задржали у масовној употреби све до друге половине 20. века.

Пренос порука радио-путем изискивао је увођење и новог дела обавештајних служби – прислушкивача, који су у били директној вези са дешифрантима – декриптерима и који су пресретнуте поруке достављали на криптоанализу.

Више се нису морала отварати писма да би се дошло до поруке.

Појава полупроводничке технологије, транзистора и микрочипова у телекомуникацијама и информатици дала је нове могућности за заштиту информација и пред криптоаналитичаре поставила нове изазове.

Криптологија у Русији

Иако појава криптографије у Русији датира из старијих времена, употреба криптографије за заштиту кореспонденција почела је тек за време владавине Петра Првог. Док је криптографија била у масовној употреби, криптоанализа се уводи тек у 18. веку, преузимањем тековина „црних кабинета" са запада. Посао чланова тих кабинета био је отварање поште, преписивање, поновно неприметно затварање и враћање писама у легалне токове, а након тога би следила криптоанализа у коју су били укључени математичари, лингвисти и фалсификатори онога времена.

Велики број криптоаналитичара у Русији били су заправо странци који су уцењивани или добро плаћани и имали разне привилегије.

Запад је био прилично уљуљкан, нарочито Немачка и Француска, који нису веровали да Русија поседује службе из области криптографије и криптоанализе. Међутим, у првој половини 19. века нека успутна случајна сазнања допринела су да се добрано замисле и промене кодове и ши-

фре које су користили у кореспонденцији са својим изасланствима у Русији.

Еклатантан пример успеха руских криптоаналитичара је и њихов допринос победи над Наполеоновом војском, јер су његови генерали били слабо посвећени коришћењу шифара, а и оне које су користили, веома су лако откривање.

У доба грађанских превирања у Русији суверени су масовно користили „црне кабинете" за добијање информација о деловањима побуњеника. Они су били формирани у поштама скоро свих већих градова онога времена, Москви, Петрограду, Кијеву, Харкову, Риги, Виљнусу и још неким.

Петар Први

Све до велике Октобарске револуције криптоанализа је била под изолованим надзором суверена и увид у рад криптоаналитичара имао је веома мали круг људи.

Након револуције нова власт је масовно наставила да експлоатише рад црних кабинета, користивши исте људе и исте или сличне методе рада, који су се задржали све до краја Другог светског рата. Међутим, баш чињеница да је у руској криптоаналитичкој служби било много странаца у неколико наврата допринела је да њихове шифре буду пробијене. Познати су примери преписки између руских обавештајаца и шпанских револуционара, које је на длану западним обавештајцима дао један руски дезертер, затим бекство једног запосленог у Јапан, као и дезертерство капетана, шефа одсека у служби, који се пред почетак Другог светског рата предао Енглезима.

То је натерало власти СССР-а да из темеља промене принципе шифровања порука и да запослене бирају из сопствених редова.

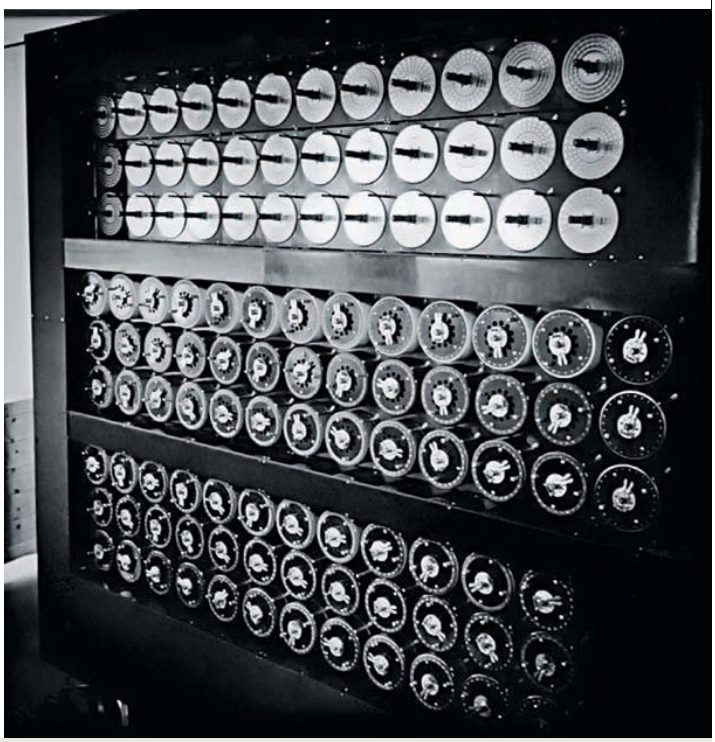
Совјетски Савез успешно је отварао кодове и шифре других земаља, чак и у иностранству, на основу незаконитих активности две агенције – тајне политичке полиције и војне обавештајне службе. Задатак тајне полиције био је да се спроведе надзор над сопственим народом, а обавештајне службе да осигура спољашњу и унутрашњу безбедност земље. Захваљујући сазнањима својих криптоаналитичких служби, СССР, а данас и Русија, створили су неколико апсолутно тајних шифарских система, који су у модификованим верзијама у употреби и данас.

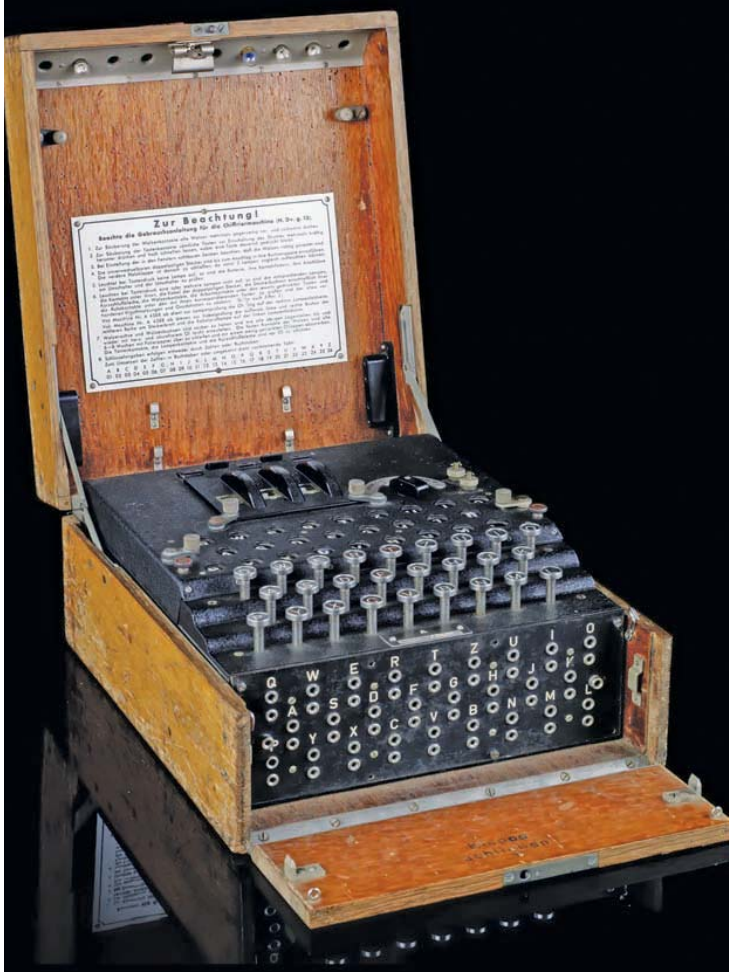
Декриптерске машине

Осим раније споменутих метода декриптовања, које су се махом базирале на мануелном раду, односно коришћењу папира и оловке, проналаском машина за пренос електричних импулса, у жичним и радио-комуникацијама, јавила се потреба за стварањем машина које ће отворене текстове, пре слања на линију ка учесницима, да кодирају или криптују. Тиме се смањивао капацитет, уз истовремено повећање брзина преноса и заштите интегритета поруке. Најчешће се код ових разматрања узима у обзир декриптовање Морзеових знакова и телепринтерских импулса, односно међународног кода број 2. То је код који генерише телепринтер, састављен од струјних и беструјних импулса, а продукт је бушена (перфорирана) петоканална трака.

Шифровало се по принципу замене знака слова, бројева или интерпункције, другим знацима, по унапред договореном алгоритму и применом неког кључа. Пошто је алгоритам био тако подешен да се није радила само проста, једнозначна замена, већ се често у шифрате намерно убацивао низ непотребних знакова или су бројеви и интер-

Тјунингова бомба





Машина „енигма”

пункцијски знаци мењани словима, па затим шифровани, декриптовање је било сведено на активност пре свега превођења двоструких шифарских замена у једноструке, а затим се изводио напад на алгоритам и кључ.

Мноштво телепринтера и кодека (модема) за криптоанализу, иако слични онима за обичну отворену комуникацију које су користиле разне службе, након истека рока употребе је уништавано, заједно са пратећом производњачком и техничком документацијом, па су остале само поједине белешке, веома мало скица и цртежа, а музејски експонати могу се избројати на прсте једне руке. У много већој тајности су држани и држе се уређаји, као и методи декриптовања, од самих апарата и упутстава за употребу шифросистема.

Познате су и често спомињане Тјунингове бомбе, које су изводиле брутални напад на шифроване поруке, пре свега Немаца. Покушаји декриптовања порука шифрованих „енигмом” остали су без успеха, све док Пољаци нису заробили један примерак машине и предали је западним савезницима, криптоаналитичарима.

Појавом шифродиска, затим применом два, а потом и три диска за шифровање, који су имали више хиљада почетних комбинација, декриптери су доведени у неугодну ситуацију да уз помоћ математичких једначина дођу до почетних стања. Ако се узме у обзир да сваки диск има по 26 слова, пермутација само по једног на једном диску и тако све до трећег често је доводила до лутања у математичким израчунавањима, као када се тражи одређено зрно песка у пустињи или длака у јајету.

Зато су ускоро произведени дискови енкодери који су замењивали ручну претрагу криптограма и знатно скраћивали време анализе.

Савремена криптоанализа

Описивање и објашњење до сада познатих метода декриптовања је веома тежак и озбиљан професионални изазов. Закони који важе у изради шифросистема, у инверзном облику важе и за њихово разбијање. У анализи шифара увек се полази од тога којим су методом и поступком оне употребљене, да ли се штити текст, говор, слика или податак, па се на основу тога опредељује за методе које треба применити за декриптовање. Свака шифра има своје карактеристике, па самим тим не постоји општа метода криптоанализе/декриптовања. Да би се савладале методе декриптовања потребно је претходно проучити статистику језика који се користи. Први и најважнији део јесте одређивање порекла криптограма, затим којим језиком, којом шифром, односно шифросистемом је порука криптована, те да ли су шифре моноалфабетске или полиалфабетске. Свакако да се применом рачунарске технологије време анализе смањује јер се напоран део, који се тиче структуре језика, препушта машини.

Веома важан елеменат у пробијању шифре јесте и сазнање о кључу за шифровање. Уколико је кључ, ма које дужине, коначан, утврди се његово растојање у шифрату, затим његова логичка структура, па се траже евентуална преклапања у криптограму. Међутим, ако је кључ непонављајући и бесконачан, све познате методе пробијања падају у воду и до отворене информације се не може доћи. Савремени шифросистеми користе као кључ за шифровање случајни или псеудослучајни низ. Први се релативно лако, уз примену познатих метода и савремене технике, могу декриптовати, док други остају вечно у тајности.

Како људски ум никада не мирује, посао обавештајних служби постаје све обимнији, разноврснији и сложенији. Непрекидно праћење иновација на свим пољима, у комуникацији и размени података не би било могуће, па чак не би имало ни сврху, јер су све важине информације заштићене, уколико се не прибегне методама њиховог декриптовања. Коришћење рачунара у криптоанализи није обелодањено, односно нема података о успешности тога рада, али уложена средства и огроман број запослених на том послу сигурно имају разлога. Проблеми везани за заштиту рачунарских података постају све израженији порастом њихове употребе. Незамислива је сфера људског деловања без примене рачунара у интерној или међузависној корелацији. У датотекама

рачунара, али и у комуникацијским мрежама и рачунарским системима налази се велики број поверљивих података.

Блистава достигнућа људског ума довела су и до уплитања злонамерних људи у ову област. То су хакери, независни појединци или стручњаци у служби државе. Не залазећи у оправданост криптоанализе за државне потребе, напоменимо да је њихова делатност усмерена на све поре друштва.

Споменимо овде тек неке методе савремене криптоанализе рачунарских шифара и алгоритама. Једна од њих заснива се на својству логичке операције „или", односно замени икс бита другим. Ако замислимо да нам је X један бит оригиналне поруке, а Y бит кључа, тада њихова замена, односно „икс ор ипсилон" доводи до стварања новог бита који се користи у комуникацији.

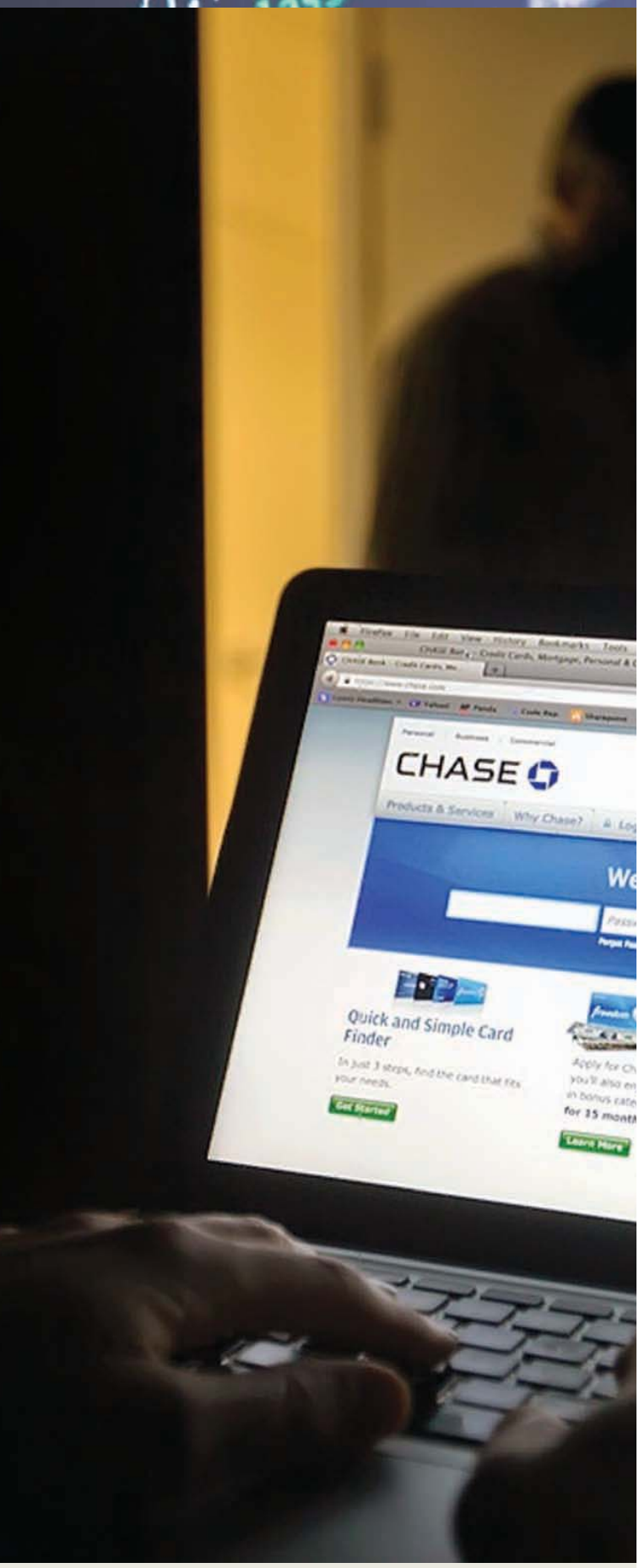
Претпоставимо да имамо шифрован текст довољне дужине. Преклопимо га њим самим. Очигледно, ако га тако упоређујемо функција ће увек давати као резултат 1. Тачније, додајмо један карактер на почетку криптограма. Израчунавајући функцију за текст шифрован самим собом, померањем за једно место удесно, добија се вредност око 0.038. Затим померамо за још једно место удесно и то понављамо све док се не добије вредност за 0.05-0.07. То значи да смо се померили за толико места колика је дужина кључа. Другим речима нашли смо периоду шифровања.

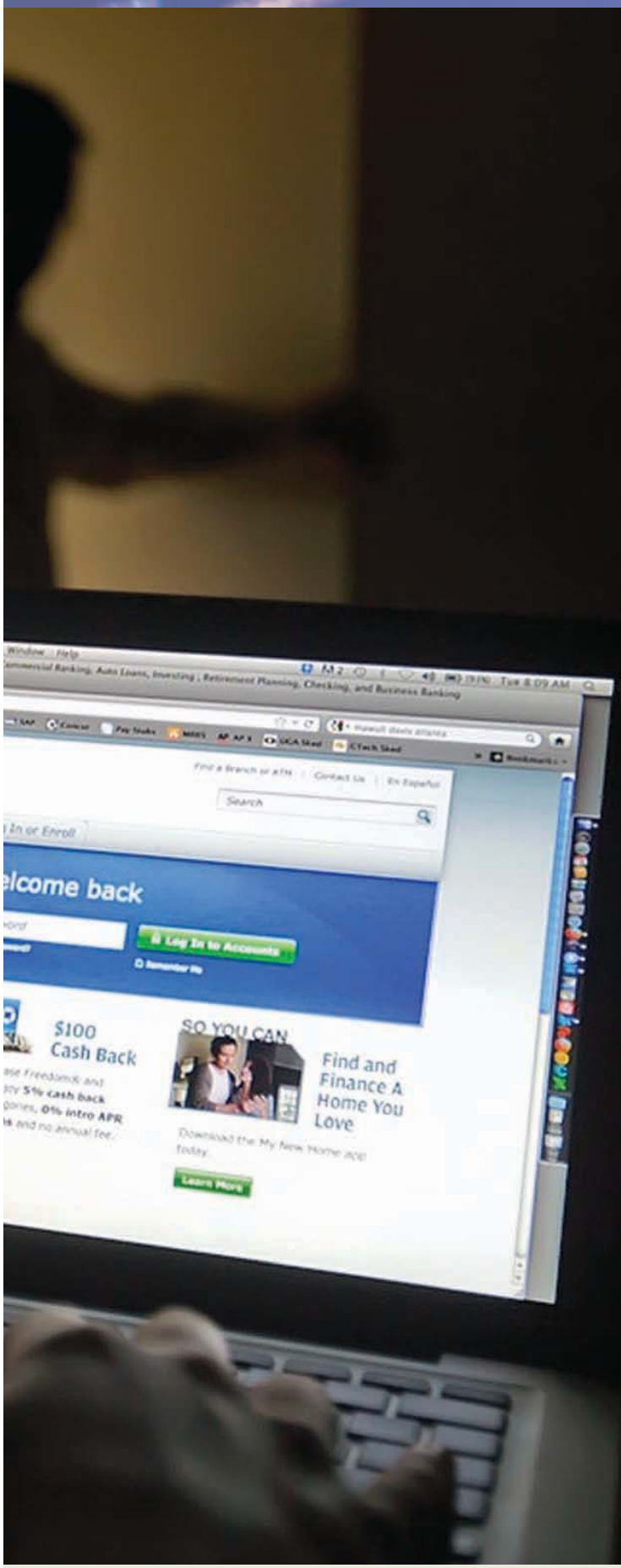
Остатак посла на разбијању шифре је прилично једноставан ако имамо довољно дуг и уобичајен текст (компликованији случајеви су такође „проваљиви", али захтевају лексику за налажење речи). Лако можемо да провалимо текст где је сваки карактер замењен неким другим, тако што знамо учесталост појављивања карактера у тексту. У енглеском језику најчешће је слово *e*, затим *u*, док је у нашем језику слово *a* најфреквентније. Када имамо неколико познатих онда нагађамо остатак.

Рецимо да смо пронашли да је кључ дужине три (он ће наравно бити доста дужи). Замислимо три текста тако да први садржи карактере са индексом 1, 4, 7,..., други карактере 2, 5, 8,..., док трећи садржи карактере са индексима 3, 6, 9,... шифрата. Сада се враћамо на једноставан проблем замене слова. Треба да погодимо само један карактер у нашим замишљеним текстовима и сви остали се могу израчунати преко њега. Најчешћи знак у замишљеном тексту би у оригиналу требало да буде бланко знак. Урадимо операцију икс или ипсилон (енглески хор) тог знака са (20x) и добићемо први карактер кључа. Поновимо исти поступак за други и трећи замишљени текст и сазнаћемо комплетан кључ који је коришћен у криптовању оригиналног текста.

На тај начин нисмо само разбили текст, већ смо нашли и кључ. Већина корисника користи исти кључ поново. Самим тим открили су нам њихов кључ и оставили могућност да разоткривамо њихове поруке.

Криптоанализа је научна дисциплина супротна од криптографије. Бави се разбијањем шифри, декодирањем, заобилажењем система аутентификације, уопште проваљивањем криптографских протокола. Зато проучава поступке откривања отвореног текста без познавања кључа, поступке откривања кључа, уз познавање отворених и/или





криптованих текстова, или уз познавање неких информација о отвореним и/или криптованим текстовима. Различите технике криптоанализе називају се нападима.

Напади на сигурност могу се раздвојити у пасивне и активне нападе. Пасивним нападом само се прислушкује послана порука, па га је много теже детектовати. Активни напад укључује мењање поруке, маскирање, поновно слање и ДоС нападе.

Врсте напада

■ Напад познатим шифрираним текстом је најтежи. Криптоаналитичар познаје само алгоритам криптовања и криптоване текстове.

■ Напад познатим отвореним текстом подразумева да криптоаналитичар познаје одговарајући отворени текст или његов део. Криптоаналитичар зна алгоритам и један или више отворених и криптованих текстова, али не зна кључ.

■ Напад одабраним отвореним текстом када криптоаналитичар бира отворени текст и криптује га. Овај напад омогућује проналажење слабости у алгоритму. Криптоаналитичар зна алгоритам, криптовани текст и један или неколико одабраних парова отворених и криптованих текстова, али не зна кључ.

■ Напад одабраним криптованим текстом када криптоаналитичар бира криптовани текст и на неки начин га декриптује и тако добија отворени текст. Такође може одабрати неки отворени текст по својој жељи. Криптоаналитичар зна алгоритам, криптовани текст и један до неколико наводних криптованих текстова са отвореним текстовима, али не зна кључ.

■ Адаптиван напад одабраним отвореним текстом: криптоаналитичар користи напад одабраним отвореним текстом. Резултати напада користе се за бирање неког другог отвореног текста. Овим начином могуће је унапредити напад. Овај напад познат је под називом „диференцијална криптоанализа". Криптоаналитичару је познат алгоритам, криптовани текст, одабрани отворени текст са криптованим текстом, те одабрани криптовани текст са отвореним текстом.

■ Напад коришћењем сродних кључева: у овом нападу претпоставља се знање о односу између кључева у два различита криптовања. Напад може открити слабости у поступку генерисања поткључева.

■ Делимично знање о кључу: нападач поседује делимично знање о тајном кључу (нпр. због „рупе" у поступку генерисања поткључева). У добрим криптосистемима делимично знање о кључу не би требало да олакша проналажење остатка кључа. Ако није тако, лакше је извести исцрпно претраживање.

Успех криптоанализе може се класификовати према количини и квалитету откривених тајних информација:

1. потпуно пробијање кода – нападач открива кључ;

2. глобална дедукција – када нападач открива функцијски еквивалент алгоритма за криптовање и декриптовање, али не налази кључ;

3. локална дедукција – нападач открива додатне отворене текстове (или криптоване текстове), од раније непознате;

4. информацијска дедукција – нападач добија нове информације о отвореним текстовима (или криптованим текстовима), непознатих од пре;

5. алгоритам који омогућује разликовање – нападач може разликовати криптовани текст од случајне пермутације.

Претраживање целог простора решења је врста напада када нападач покушава да декриптује криптограм пробајући све врсте кључева. Спор и најједноставнији напад који није могуће спречити и на који се не може утицати. Успешност овог напада мери се временом потребним за претраживањем целог простора. Уколико нападач нема неке почетне претпоставке шансе да се сазна прави кључ су минималне.

Претраживање пола простора решења примењиво је код великог броја криптосистема, а нарочито за пробијање ДЕС-а.

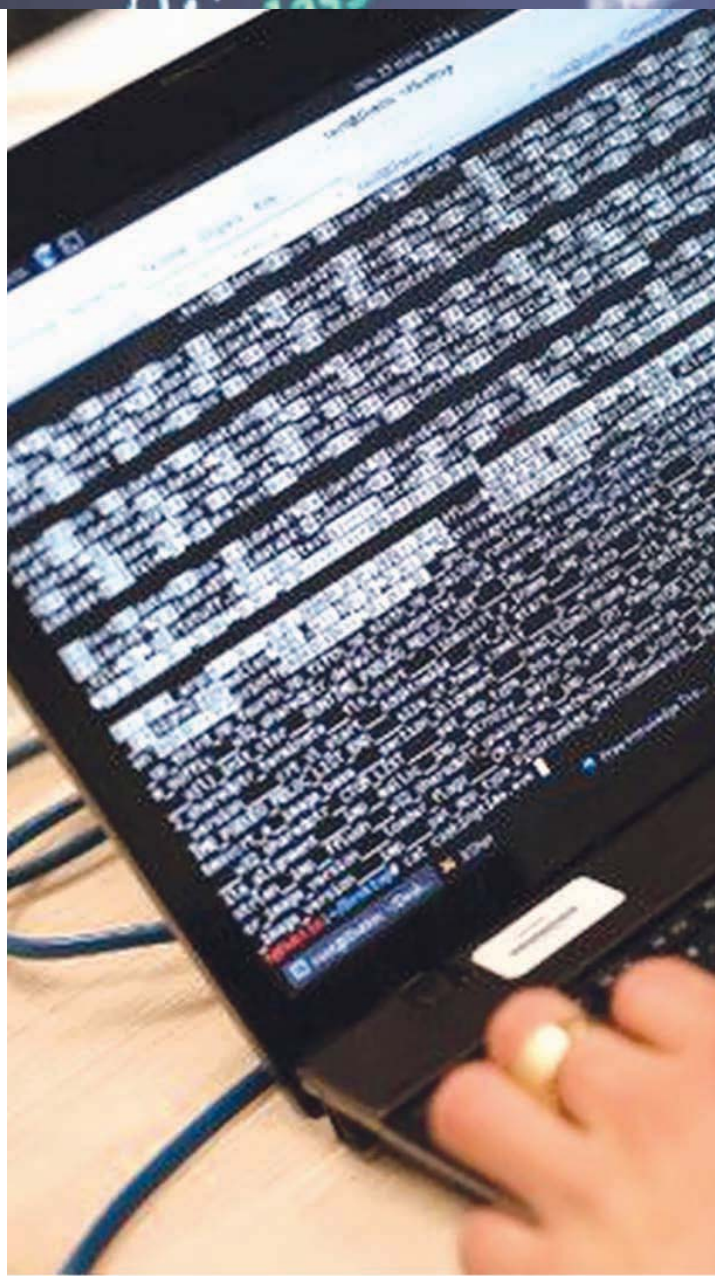
Методе су сличне као и код претраживања целог простора, али се убацивањем једног бита кључа (претпостављеног) штеди 50 одсто времена.

Диференцијална криптоанализа је техника којом се анализира учинак разлике између два иста текста и два резултирајућа криптограма. На тај начин може се одредити простор једног или више кључева.

Линеарна криптоанализа примењива је на симетричне алгоритме када се у покушају напада једнозначно одреди паритет отвореног текста и криптограма, или се претпостављена дужина кључа ефективно смањи за један бит. У пракси је доказано да се пуни ДЕС са 8 односно 12 рунди помераја може пробити коришћењем 247 криптограма за 40 секунди до 50 сати.

Разбијање шифросистема јавним кључем

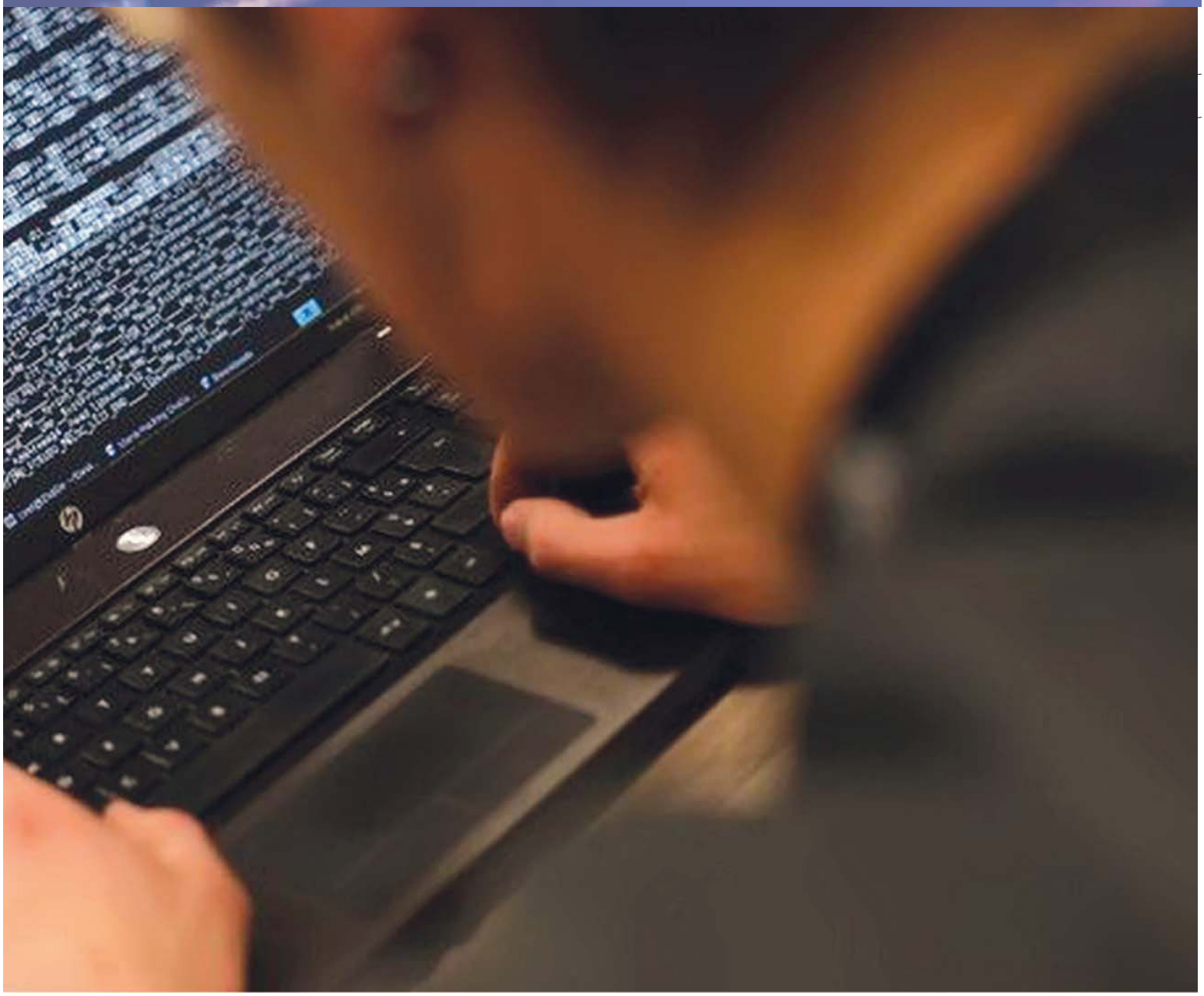
Систем шифровања јавним кључем (асиметрични шифарски систем) такав је да у њему сваки учесник у комуникацији користи два кључа. Један кључ је јавни и може се слободно дистрибуирати, док је други тајни и доступан је само његовом власнику. Иако су различити, кључеви су међусобно повезани одређеним трансформацијама. Познавање једног кључа и алгоритма трансформације не омогућава добијање другог кључа. Најбитније је да се тајни кључ у целом поступку комуникације нигде не шаље јер не постоји потреба да било ко сем његовог власника буде упознат с њим. Основа израде кључева јесте у ствари факторизација великих простих бројева. Последњих година границе алгоритама целобројне факторизације су се веома проширили, проузроковане делом Муровим законом, делом алгоритамским побољшањима. Данас је рутински раставити стоцифрени број, док је лако изводљиво и растављање стопетоцифреног броја (512 бита).



Не постоји ниједан детерминистички или случајан алгоритам, који ради у полиномијалном времену, за налажење чиниоца датог сложеног броја. Ова чињеница је од велике важности јер РСА алгоритам не би био сигуран имплементирањем таквог алгоритма.

Муров закон

Муров закон предвиђа да се густина циклуса удвостручује сваких 18 месеци или више. Наравно, ово није теорема и мора кад-тад пасти, али с годинама се показао исправним. Све док се Муров закон примењује и резултира подударношћу са моћнијим паралелним рачунарима, ми очекујемо да добијемо чврста побољшања за факторизацију, без икаквих



алгоритамских побољшања. Историјски гледано, побољшања у последњих тридесетак година проузрокована су Муровим законом и развојем нових алгоритама.

Доказивањем да је могуће применити целобројну факторизација и наћи чиниоце значи да је могуће разбити РСА у полиномијалном времену. Ако велики број може брзо да се растави на производ два велика проста броја, остатак посла на разбијању РСА криптосистема је јасан.

Можда ту има више прилаза, али то овде није важно. Описани проблем факторизације је у ствари нерешив са тренутним постигнућима у рачунарској технологији, а о другим методама излишно је и говорити. Потврда су управо пар простих бројева. Ако се испостави да је један број исто што и он сам помножен са један, онда се може засигурно урадити факторизација у полиномијалном времену и остатак посла је такође „брз", тако да је крајње време извршавања полиномијално.

Криптографска велесила – САД

Светске суперсиле у великој мери своју моћ дугују изузетно разгранатој комуникацијској мрежи која се користе за пренос информација. Те мреже пружају криптоаналитичарима неслућене могућности да дођу до материјала да разбију кодове и наставе својеврсно такмичење. Управо због тога САД предузимају све неопходне мере како би заштитиле своје комуникацијске канале у земљи и ван ње.

Истовремено, масовно пресрећу и дешифрују порука противничких па и пријатељских држава.

Значај тог проблема утицао је на стварање највеће криптоаналитичке организације у историји човечанства – Агенције за националну безбедност (НСА). Као непосредни повод за оснивање НСА узима се напад на Перл Харбур. Након истраживања околности под којима је Јапан извео виртуозни напад, Амерички конгрес препоручио је влади САД да створи централизовану криптоаналитичку обавештајну агенцију, иако је криптоаналитичка служба постојала и раније, нарочито при морнарици, војсци и Министарству спољних послова. Тако је 4. новембра 1952. председник Труман издао директиву на основу које се формира НСА.

Директива је првобитно степенована као строго поверљива. Током наредних неколико година није било дозвољено јавно помињање НСА у било ком документу или саопштењу. Тек 1957. године, у „Водичу америчких владиних агенција", први пут је споменут кратак опис Агенције, али веома штуро и недоречено. Након неколико година тај опис је мало промењен и допуњен у форми три параграфа.

У прва два сажето је дата информација о настанку агенције, те да је настала директивом председника и да се налази под контролом Министарства одбране. У трећем, најважнија реченица гласи: „НСА пружа високо специјализоване техничке и координацијске функције које се односе на националну безбедност."

Упркос неодређености овог описа, видљиво је да је функција „технички" та да НСА пресреће све, а нарочито шифроване поруке, и врши криптоанализу порука било пријатељске или непријатељске државе. „Координација" је функција која укључује обезбеђивање комуникације, односно организацијски део, контроле и консолидације напора свих заинтересованих агенција (Министарства одбране, Стејт департмента, ЦИА, ФБИ и других) на развоју, производњи и раду средстава за криптозаштиту.

Председничка директива по којој је НСА настала и даље се сматра тајном информацијом. Вео тајне, којом је Агенција обавијена од свог рођења, важи и данас. НСА је тако сакривенија, тиша, тајнија и суморнија организација од ЦИА. Званичници из ЦИА с времена на време дају макар двосмислене изјаве за штампу, док припадници, па ни званичници НСА то нису никада урадили. Тако НСА остаје веома тајанствена и мистериозна организација и међу америчким тајним службама. У првим годинама након настанка била је лоцирана у различитим објектима расутим широм Вашингтона, да би се након неког времена изградио посебан објекат, који после извесног времена, како се Агенција ширила, постаје такође тесан за све њене припаднике.

Агенција је вртоглаво ширила своја поља деловања и самим тим и повећавала број запослених, а кадар се бирао по најстрожим селекцијама. И након запошљавања криптоаналитичари су под будним оком претпостављених, непрестано се контролишу рад и понашање, спроводи се темељна и студиозна дообука, преобука и савлађивање новина у технолошком развоју целог света. Иде се тако далеко да ни чланови најуже породице не смеју знати право радно место запослених.

Међутим, и поред свих мера предострожности, доказало се да је НСА умешана у многе скандале и пропусте у историји Сједињених Америчких Држава. У скорије време јавности су познати догађаји око цурења информација из Агенције, а најпознатији је свакако пребег једног запосленог у трећу земљу.

Запослени у НСА разврстани су по одељењима, зависно од задатака које обављају, од којих су неки: прикупљање криптограма, анализа, упоређивање и одбацивање дупликата или неитересантних, упаривање криптограма, односно груписање у подгрупе оних који су рађени софтвером оперативних система рачунара и оних који су рађени неким одређеним шифарским системом.

Стручњаци НСА у криптоанализи користе велики број софистицираних рачунара као засебних уређаја, али и веома често умрежавају више рачунара. На тај начин рачунари обављају криптоанализу користећи само слободан простор меморије, док се за исцрпније претраге користе потпуни капацитети меморија, која се ослобађа свих процеса.

Ипак, ни у данашње доба рачунар не може заменити људски рад. Шетњом кроз историју криптоанализе, од прапочетака и примитивних замена простих чинилаца, најчешће алфабета, па до моћних рачунара и бинарног преноса и обраде информација, запазили смо да је суштина остала иста. Циљ је пронаћи метод рада на шифровању, алгоритам и кључ. Коначан исход је наравно отворена информација и то углавном писаног текста, мада је и други вид преноса шифрованих информација интересантан, али је веома мало заступљен. Било заљубљеник, ентузијаста-аматер или професионалац, ефикасном криптоанализом успешно се може бавити веома мали број људи. ■