Sveučilište J. J. Strossmayera u Osijeku

Filozofski fakultet Osijek

Preddiplomski studij informatologije

Ivana Dejanović

Kriptografija

Završni rad

Mentor: doc. dr. sc. Boris Badurina

Komentor: dr. sc. Anita Papić

Osijek, 2017.

Sveučilište J. J. Strossmayera u Osijeku

Filozofski fakultet Osijek

Odsjek za informacijske znanosti

Preddiplomski studij informatologije

Ivana Dejanović

Kriptografija

Završni rad

5. Područje društvenih znanosti, 5.04. Informacijske i komunikacijske znanosti, 5.04.11 informacijsko i programsko inženjerstvo

Mentor: doc. dr. sc. Boris Badurina

Komentor: dr. sc. Anita Papić

Osijek, 2017.

Sažetak

Cilj je ovoga rada prikazati tijek razvoja kriptografije, prvotno ukazujući na najranije primijećene kriptografske karakteristike u tekstovima i zapisima drevnih civilizacija, nedugo nakon pojave samoga pisma. Potrebe tvoraca zapisa za osiguravanjem tajnosti pisane riječi i zaštitu privatnosti dovele su do osmišljavanja strategija za zaštitu sadržajne razumljivosti, koje bi otežale prodiranje u sadržajni smisao, ako ne i u potpunosti prodiranje u sadržajnu bit. Navedenim primjerima takva djelovanja će se pobliže objasniti prvi kriptografski pokušaji. Definirat će se sam pojam kriptografije i osnovni princip zaštite sadržajnog značenja, a objašnjeni primjeri će se svrstati u kategorije kriptografskih metoda. Kronološka analiza kriptografije dosegnut će do primjera starih i po nekoliko tisuća godina, još prije nove ere. Također će se objasniti bliskost kriptografije i steganografije te prednosti njihova kombiniranja, a zatim će započeti uspon po novoj eri. Pojava kriptoanalize na Bliskom istoku pogurat će razvoj kriptografije jer će te dvije strane kriptologije otada biti u neprestanom nadmetanju. Renesansni procvat kriptografije u Europi rezultirat će osnivanjem tzv. mračnih ureda s glavnim ciljem razbijanja šifri. Tehnološki razvoj će omogućiti nove kanale komunikacije, između ostaloga, komuniciranje putem telegrafa i radija. Potreba za šifriranjem istih rezultirat će izumom uređaja za šifriranje. Zaključno tome će se, na primjerima Zimmermanova telegrama i Enigma stroja, ukazati na činjenicu da su kriptografija i kriptoanaliza svojim nadmetanjem odredile ishod svjetskih ratova i oblikovale povijest kakva nam je danas poznata.

Ključne riječi: kriptografija, šifriranje, kriptoanaliza, komunikacijski kanal, uređaji za šifriranje

Sadržaj

1. Uvod

Pisana se kultura počela razvijati tisućama godina prije Krista. Stare su civilizacije imale svoje sustave pisanja – klinasto pismo, kinesko pismo, egipatske hijeroglife, feničko pismo i druge. Nerijetko su se pismom pojedine civilizacije znali služiti samo pojedinci unutar nje i to su bili razni pisari u službi svojih vladara čiju su riječ pratili i zapisivali. Malo tko je mogao shvatiti sadržaj tih zapisa što je pisare uzdiglo na cijenjenu poziciju u društvu. Vremenom se razvija pismenost, zapisi prestaju biti nerazumljivi i poznavanjem pisma otkriva se njihov nekada nerazumljiv sadržaj. Po osnovnom modelu pisane komunikacije pošiljatelj šalje poruku primatelju koja do njega putuje komunikacijskim kanalom. No, komunikacijskom kanalu može pristupiti i treća osoba te vidjeti poruku iako joj ona nije namijenjena. Sukladno tome, raste prijetnja da se otkriju važne informacije, jer su tako napisane postale razumljive većini – iako većini nisu bile namijenjene. Uz sverastuću prijetnju razotkrivanja sadržaja zapisa raste i potreba za zadržavanjem njihove tajnosti. To dovodi do osmišljavanja metoda kojima bi poruka na svom putovanju od pošiljatelja do primatelja došla bez da ju itko s treće strane primijeti i preuzme. Osmišljavale su se razne podloge za pisanje, načini prikrivanja pisma, načini pisanja, materijali za pisanje i druge tehnike. Usmjeravalo se na fizičko prikrivanje poruke. Jednom otkriveno postojanje poruke je razotkrilo i cijeli njezin sadržaj. Bilo je jasno da nije dovoljno sakriti fizički zapis, već da se treba orijentirati i na značenje sadržaja zapisa. Prvotne su ideje bile zamijeniti znakove/slova zapisa ili ih ispremještati u zapisu, čime bi sadržaj postao nerazumljiv onome koji ne zna po kojem su pravilu napravljene promjene. Time se osigurala tajnost sadržaja zapisa čak i ako bi taj zapis došao u neželjene ruke. Takve su metode funkcionirale, no s određenim rokom trajanja. Kako su smišljane metode za očuvanjem tajnosti zapisa, tako su neprestano traženi i načini probijanja istih.

2. Princip djelovanja kriptografije

Kriptografija je znanstvena disciplina čiji je naziv izveden iz grčkih riječi kryptos (skriven) i grafo (pisati). Predstavlja tehniku kojom se ne skriva postojanje poruke, već skriva značenje sadržaja poruke. Ukoliko se dogodi da poruka dospije u neželjene ruke, kriptografija osigurava tajnost sadržaja jer 'presretač' gledajući u taj sadržaj ne može vidjeti pravo značenje; tek pošiljatelj poruke i njezin primatelj mogu, jer imaju unaprijed dogovorenu metodu šifriranja i

dešifriranja poruke.[1] Da bi se dvjema stranama omogućila komunikacija putem nesigurnog komunikacijskog kanala (unutar kojeg je prisutna i treća strana koja taj kanal nadzire) potrebno je osigurati tajnost njihove poruke. Princip je sljedeći: pošiljatelj poruke i njezin primatelj unaprijed dogovaraju ključ za šifriranje. Zatim pošiljatelj tim ključem pretvara razumljivi tekst poruke u šifrat (kriptogram, tj. nečitljive podatke) i šalje ga putem komunikacijskog kanala. 'Presretač' može doznati sadržaj šifrata, ali ne može odrediti tekst poruke. Za razliku od njega, primatelj kojemu je poruka poslana zna ključ kojim je šifrirana poruka te može dešifrirati šifrat i učiniti tekst ponovno razumljivim.[2] Takav način šifriranja/dešifriranja uključuje podijeljeni ili tajni ključ i predstavlja simetričan tip kriptografije. Drugi tip je asimetrična kriptografija. Djeluje s javnim ključem koji je slobodno distribuiran te privatnim ključem vlasnika. Poruka se šifrira javnim ključem, a dešifrirati ju može samo pridruženi privatni ključ.[3]

3. Rana potreba za kriptografijom

Kao jedni od začetnika pisane kulture, Egipćani su još oko 3000. godine prije Krista razvili slikovno pismo kojim su naučili prenositi pisanu riječ i stvorili si novi pravac u komunikaciji. Tako su imali dva moguća pravca prenošenja poruka – govornim i pisanim putem. Hijeroglifi su se mogli sagledati kao kriptografski elementi sami po sebi jer ih nitko drugi nije mogao razumjeti osim Egipćana (čak i među njima su na početku to bili samo pisari koji su pisali poruke, po naredbama vladajućih faraona drugim pisarima koji su ih potom iščitavali). Vremenom su u oba pravca počeli nailaziti na poteškoće u zadržavanju tajnosti sadržaja poruka od gladnih presretača koji su taj sadržaj, iako nenamijenjen njima, htjeli razotkriti. Upravo se iz te potrebe zadržavanja tajnosti podataka i očuvanja privatnosti općenito počelo razmatrati o mogućnostima 'šifriranja' sadržaja poruka. Egipćani su počeli pojednostavljivati kompleksnu strukturu hijeroglifa dok nisu razvili pojednostavljena pisma (hijeratsko i demotsko). Unatoč tome, bile su potrebne tisuće godina da se hijeroglifi uspiju odgonetnuti. Tome je na put dodatno stala spoznaja da su pisari u tim pojednostavljenim verzijama znali zamjenjivati slova poruke s

[1] Usp. Mathai, Jacob. History of Computer Cryptography and Secrecy Systems. URL: http://www.dsm.fordham.edu/~mathai/crypto.html (2017-09-17)
[2] Usp. Dujella, Andrej. Klasična kriptografija: osnovni pojmovi. URL: https://web.math.pmf.unizg.hr/~duje/kript/osnovni.html (2017-09-17)
[3] Usp. IBM Knowledge Center. URL: https://www.ibm.com/support/knowledgecenter/hr/ssw_i5_54/rzahu/rzahurzahu0cmcryptogco.htm (2017-09-17)

drugim slovima po njima poznatom pravilu – ključu za zamjenu slova u prvobitno stanje i otkrivanje pravog sadržaja poruke.[4]

4. Počeci kriptografskih metoda

Tek zahvaljujući pronađenoj kamenoj ploči iz Rosette (i tekstu koji je na toj ploči napisan hijeroglifskim, demotskim i grčkim pismom) je 1822. Godine Jean-Francois Champollion uspio dešifrirati značenje hijeroglifa. Njegovo je postignuće dovelo do boljeg shvaćanja egipatske kulture koja se mogla iščitati iz, od tada razumljivih, hijeroglifa. Jednako tako su se mogle shvatiti i preinake u pismu te simboli koji su odudarali od poznatih hijeroglifa.

4.1. Prvi zapisi drevnoga Egipta

Najstariji dokaz 'skrivenog pisanja' zabilježen je na krhotini posude za koju se smatra da datira iz 3300. godine prije Krista, a pronađena je u Harappi te je u sebi imala upisane preinake hijeroglifskih simbola.[5] Također su, oko 1900. godine prije Krista, ispisani hijeroglifi u unutrašnjosti grobnice Khnumhotepa II, u čijim su se redovima na ponekim mjestima uobičajenih hijeroglifa pronašli simboli koji su se razlikovali od poznatog ostatka. Svrha im nije bila sakriti poruku već izmijeniti oblik poruke čime bi se zaštitila prepoznatljivost i uzdigla dostojanstvenost sadržaja. Natpis u grobnici smatra se najstarijim pronađenim primjerom u kojem je izvršena neka vrsta transformacije originalnog teksta.[6]

4.2. Supstitucija i transpozicija

Hebrejski pisari su u 6. stoljeću prije Krista koristili metodu prevrtanja abecede, kojom su zamjenjivali zadnje slovo abecede prvim i obrnuto. Metoda je poznata kao 'atbash'.[7] Želimo li na primjer šifrirati riječ na hrvatskom jeziku, uzmemo li riječ „informacija“, 'atbash' metodom postat će „mhofđižvmljž“ – bez ključa nerazumljiv sadržaj. Takva se zamjena slova u kriptografiji naziva još i supstitucija.

---

[4] Usp. Origin of cryptography. URL: https://www.tutorialspoint.com/cryptography/pdf/origin_of_cryptography.pdf (2017-09-17)
[5] Usp. Sidhpurwala, Huzaifa. Cipher writing of ancient India was called mlecchita vikalpa, pre-alphabetic, pre-syllabic cryptography of Indus Script Corpora, 2014. URL: http://www.academia.edu/12160041/Cipher_writing_of_ancient_India_was_called_mlecchita_vikalpa_pre-alphabetic_pre-syllabic_cryptography_of_Indus_Script_Corpora (2017-09-17)
[6] Usp. Red hat. A brief History of Cryptography, 2016. URL: https://access.redhat.com/blogs/766093/posts/1976023 (2017-09-17)
[7] Cohen, Fred. A Short History of Cryptography, 1995. URL: http://web.itu.edu.tr/~orssi/dersler/cryptography/Chap2-1.pdf (2017-09-17)

Spartanci su u 5. stoljeću prije Krista za šifriranje svojih poruka koristili skital, posebnu napravu u obliku drvenog štapa oko kojeg se namotavala vrpca pergamenta. Na nju se okomito pisala poruka, zatim bi se odmotala te bi ostali izmiješani znakovi čiji bi se smisao prepoznao tek ponovnim namotavanjem vrpce na štap iste debljine.[8] U tom slučaju, točnu debljinu štapa znali su pošiljatelj poruke te njezin primatelj, a bilo tko drugi, tko je htio otkriti sadržaj poruke, morao je prvo saznati točnu debljinu štapa. Takvo se premještanje slova u kriptografiji naziva još i transpozicija.

4.3. Cezarski kod

Jedan od poznatijih primjera jednostavne supstitucije korišten je u 6. desetljeću prije Krista u vrijeme slavnog Julija Cezara. Kako nije vjerovao ni svojim glasnicima, razvio je metodu šifriranja svojih poruka kako bi one, ukoliko se presretnu, bile besmislene presretačima. Svoju bi poruku napisao po pravilu zamjene slova pomakom od 3 mjesta abecede. Tako bi u poruci umjesto slova A napisao D ili, ukoliko bi se dogovorila zamjena po 2 mjesta abecede, umjesto A bi pisalo slovo C i tako dalje. Tek kada bi se napisana slova pomjerila nazad za dogovoren broj mjesta, poruka bi postala smislena.[9] Cezarova jednostavna metoda korištena je stotinama godina nakon, posebice u vojne svrhe. Unatoč svojoj jednostavnosti, metoda je funkcionirala te je poslužila kao temelj za unaprjeđivanje takve metode supstitucije. Povijest je takav primjer ostavila u uskoj povezanosti s Cezarom te je danas poznat, između ostaloga, i kao Cezarova šifra, cezarsko šifriranje i cezarski kod.

5. Kriptografija i steganografija

Drugačiji primjer 'skrivenog pisma' pronađen je u pisanoj kulturi starih Grka. Njihova se zaštita poruke temeljila na prikrivanju cijelokupnog postojanja poruke, a ne samo na prikrivanju značenja sadržaja poruke. Prioritetno su se trudili slati poruke na način da ne probude sumnju u neželjenim pogledima – da im se neka poruka nalazi pred očima.

Idući primjer sličnog djelovanja poznat je iz zapisa povjesničara Herodota koji je pisao o prognanom Grku i njegovoj poruci Grcima o namjeri perzijskog kralja Xerxesa da napadne Grčku. Poruku je napisao na drvenim ploškama koje je zatim prelio voskom kako se tekst ne bi

[8] Usp. Dujella, Andrej. Klasična kriptografija: osnovni pojmovi. URL: https://web.math.pmf.unizg.hr/~duje/kript/osnovni.html (2017-09-17)
[9] Usp. Cruise, Brit. Ancient Cryptography: The Caesar cipher, 2012. URL: https://www.khanacademy.org/computing/computer-science/cryptography/crypt/v/caesar-cipher (2017-09-17)

vidio u susretu s perzijskim čuvarima. Drvene su ploške došle do Grka koji su sastrugali vosak i vidjeli sadržaj poruke te su uspjeli na vrijeme pripremiti obranu i pobjedonosno se vratiti iz bitke.[10] I u ovome su slučaju jedino pošiljatelj poruke i njezin primatelj znali da se iza voska skriva poruka koja će se vidjeti čim se vosak sastruže.

Takvom prikrivenom razmjenom informacija se bavi znanstvena disciplina steganografija. Riječ je izvedena iz grčkih riječi steganos i graphein koje u prijevodu zajedno čine skriveno pisanje. Steganografija nastoji prikriti postojanje poruke putem naizgled bezazlenog medija (primjer s drvenim ploškama prelivenim voskom) ili skupa podataka.[11] Također uključuje pisanje poruke 'nevidljivom tintom' (o kojoj je pisao Plinije Stariji), ali i brijanje glave glasnika i utiskivanja poruke te njeno 'slanje' kada glasniku naraste kosa i prikrije poruku. Takvi primjeri jasno govore koliko je steganografija drevna tehnika te se počeci korištenja takvog pristupa mogu smatrati primitivnima u povezanosti s tajnim sustavima i tajnom komunikacijom.[12] Zaključno tome, steganografijom je poruka u početnom obliku 'nevidljiva' – ona ne postoji, no ukoliko se ta poruka primijeti ugrožen je, tada jasno vidljiv i razumljiv, cijeli sadržaj poruke.

Kako bi se osigurao viši stupanj zaštite podataka, kriptografija i steganografija se mogu ukombinirati.[13] Time se nastoji sakriti značenje sadržaja poruke, a ujedno i postojanje same poruke. Ukoliko se poruka pronađe, sadržaj neće odmah biti ugrožen (kao što je slučaj u korištenju samo steganografije). Zahvaljujući kriptografiji, za razumijevanje sadržaja dodatno je potrebno i dešifriranje.

6. Kriptografija kao umjetnost

Pridavanje važnosti kriptografije očitovalo se i na području Indije, oko četvrtog stoljeća, gdje ju je poznati filozof Vatsyayana, u svojoj prepoznatljivoj Kama Sutri, uvrstio među 64 umjetnosti kojima se treba ovladati. Neke od smatranih umjetnosti su one o kuhanju, odijevanju i pripremi parfema, a na 45. mjestu popisa nalazi se „mlecchita-vikalpa“, odnosno, umjetnost tajnog pisanja. Vatsyayana je zagovarao poznavanje takve umjetnosti kako bi se uspješno prikrile

[10] Usp. Kotas, William August. A Brief History of Cryptography, 2000. URL: http://trace.tennessee.edu/cgi/viewcontent.cgi?article=1398&context=utk_chanhonoproj (2017-09-17)
[11] Usp. Steganografija, 2006. URL: http://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2006-04-154.pdf (2017-09-17)
[12] Usp. Mathai, Jacob. Nav. dj.
[13] Usp. Isto.

pojedinosti ljubavne veze, a kao tehniku je preporučio slučajno uparivanje slova abecede te potom zamjenjivanje svakog slova u poruci sa svojim partnerom.[14]

7. Pojava kriptoanalize na Bliskom istoku

Sukladno razvoju kriptografije razvijala se i kriptoanaliza – znanstvena disciplina koja proučava metode otkrivanja značenja kriptiranih informacija bez potpunog poznavanja informacija za dekriptiranje.[15] Ključnu ulogu u razvitku kriptoanalize imali su Arapi, koji su, već poznati po naprednom razumijevanju polja matematike, otkrili varijacije u učestalosti pojave slova arapske abecede. Tako su, na primjer, primijetili da se slovo 'L' u prosjeku koristi deset puta više od slova 'J'. Učestalost pojavljivanja slova su iskoristili za određivanje šifre korištene za enkripciju poruka na način da su usporedili učestalost pojavljivanja slova unutar šifrirane poruke sa poznatom učestalošću slova arapske abecede te su iz jednakosti pojavljivanja slova otkrili koje pravo slovo predstavlja ono šifrirane abecede.[16] Postupak (danas poznat kao frekvencijska analiza) je u devetom stoljeću prvi dokumentirao arapski filozof i matematičar Al-Kindi[17], razbivši time sigurnost tada postojećih enkripcijskih sustava, kao što je stotinama godina korišteni cezarski kod i slični primjeri supstitucijskog šifriranja. Može se reći da su kriptografija i kriptoanaliza u svome međudjelovanju podupirala jedna drugu na jačanje te si konstantno stvarale izazove za napredak.

7.1. Postignuća arapskih učenjaka do 10. stoljeća

Profesor sigurnosnog inženjeringa na Cambridgeu Ross Anderson je u svom djelu „Security Engineering: A Guide to Building Dependable Distributed Systems“ iznio zanimljivo viđenje kriptografije kao mjesta gdje sigurnosni inženjering susreće matematiku.[18] Upravo u skladu s tim, na Bliskom istoku, arapski su učenjaci razvijali svoje znanje u području matematike i logike te su tim stečenim znanjima nastojali doprinijeti razvitku kriptografije, a posebno razvitku kriptoanalize.

---

[14] Usp. Simon Singh: The Black Chamber. URL: https://www.simonsingh.net/The_Black_Chamber/index.html (2017-09-17)
[15] Usp. Kriptografija, 2009. URL: http://www.cert.hr/sites/default/files/CCERT-PUBDOC-2009-08-275.pdf (2017-09-17)
[16] Usp. Kotas, William August. Nav. dj.
[17] Usp. Simon Singh: Arab Code Breakers. URL: https://simonsingh.net/media/articles/maths-and-science/arab-code-breakers/ (2017-09-17)
[18] Usp. Anderson, Ross. Security Engineering: A Guide to Building Dependable Distributed Systems. URL: https://www.cl.cam.ac.uk/~rja14/Papers/SE-05.pdf (2017-09-17)

U osmom stoljeću je arapski leksikograf i filolog Al-Khalil napisao Knjigu kriptografskih poruka u kojoj je razmotrio metodu vjerojatne riječi.[19] Riješio je bizantsku kriptografsku zagonetku napisanu na grčkom nagađajući da ona započinje tekstom „U ime Boga“. Zahvaljujući toj pretpostavci, koja se ispostavila točnom, uspio je shvatiti ostatak teksta. Zapisivanjem svoje metode u djelu učinio je da se ono kasnije smatra prvim djelom koje sadrži segmente kriptoanalitičke tematike.[20]

Deveto stoljeće, osim što je obilježeno Al-Kindijevom dokumentacijom frekvencijske analize, obilježeno je šifrarnim abecedama koje je Abu Bakr zapisao u korist šifriranja čarobnih recepata.[21]

7.2. Zapisi kriptoanalitičkih metoda od 10. stoljeća

Nešto kasnije, u dvanaestom stoljeću, Ibn Adlan je za tadašnjeg kralja Al-Ashrafa napisao knjigu s detaljno opisanim uputama za kriptoanalizu.[22] Istovremeno Ibn Dunainir piše sveobuhvatne upute za rješavanje kriptograma u kojima predstavlja algebarske šifre; zamjenjuje slova brojevima i mijenja ih aritmetičkim operacijama.[23]

Četrnaesto stoljeće obilježio je arapski kriptolog Ibn Ad-Duraihim u djelu Ključ otkrivanja tajnih spisa.[24] Iznio je svoju metodu dešifriranja poruka frekvencijskom analizom, naglašavajući točan redoslijed analiziranja, koji je započinjao od dvoslovnih riječi, zatim troslovnih i nakon njih nastavljao analizom četveroslovnih i peteroslovnih. Posebnim tablicama naznačio je koja se slova ne mogu pojaviti zajedno u jednoj riječi. Osim detaljne provedbe metode, naglasio je i nužnost postavljanja hipoteza pri postupku dekodiranja.[25] Njegovim stopama nastavio je arapski matematičar Qalqashandi sastavljanjem enciklopedije Subh al-asha u 14 svezaka među kojima se nalazi i poglavlje o kriptografiji. U poglavlju su obrađene metode transpozicije i supstitucije te primjeri kriptoanalize, a po prvi puta je opisana i polialfabetna supstitucija - šifra koja jedno slovo jasnog teksta mijenja sa više slova šifriranog teksta.[26]

---

[19] Usp. Pommerening, Klaus. Cryptology: Some Notes on Early history, 2015. URL: https://www.staff.uni-mainz.de/pommeren/Cryptology/Classic/1_Monoalph/EarlyHist.html (2017-09-17)
[20] Usp. Machinae: Cryptology. URL: http://www.machinae.com/crypto/ (2017-09-17)
[21] Usp. Šaban, Josip. Povijesni pregled računalne sigurnosti. URL: http://sigurnost.zemris.fer.hr/ostalo/2002_saban/index.htm (2017-09-17)
[22] Usp. Pommerening, Klaus. Nav. dj.
[23] Usp. Isto.
[24] Usp. Isto.
[25] Usp. Weber, Ralph. United States Diplomatic Codes and Ciphers: 1775-1938. Routledge, 2010. Str. 7.
[26] Usp. Šaban, Josip. Nav. dj.

Kriptografijom su se bavile mnoge civilizacije, dok se nikakav značaj nije pridavao kriptoanalizi. Tek su se arapski učenjaci počeli njome baviti, pisati o njoj, proučavati ju i razvijati. Stoga se opravdano smatra da je kriptologija, znanost koja se bavi i razvijanjem šifri i razvijanjem metoda za njihovo razbijanje, nastala među Arapima.[27]

8. Kriptografski (ne)razvitak u Europi

Nasuprot aktivnog Bliskog istoka, u Europi je vladalo zatišje do trinaestog stoljeća. Tek onda su samostani počeli poticati proučavanje kriptografije, prvenstveno kako bi uspjeli dešifrirati poruke unutar Biblije.[28] Engleski filozof i alkemičar Roger Bacon pisao je o metodama šifriranja te ih i sam koristio prilikom zapisivanja uputa za pravljenje eksploziva, kako bi smisao uputa bio nejasan u krivim rukama. Tako je na primjer u obliku anagrama zapisao potrebnu količinu drvenog ugljena. Također je smatrao ludima one koji bi tajnu pisali u bilo kojem obliku koji tu tajnu neće prikriti.[29] U to vrijeme se kriptografija počela širiti političkim krugovima, gdje su vladajući sve više koristili šifre kojima bi prikrili povjerljive informacije. Posebna takva upotreba našla je svoje mjesto u Italiji, u arhivima Venecije. U tamošnjim su se zapisima mogli pronaći križići i točkice s funkcijom zamjenjivanja samoglasnika tvoreći tako naizgled raspršene riječi.[30]

U četrnaestom je stoljeću talijanski kriptolog Gabrieli di Lavinde, na zahtjev pape Clementa VII, sastavio priručnik ukombiniranih šifri i kodova sa supstitucijskom abecedom, koja je sadržavala slova bez značenja s namjerom zbunjivanja kriptoanalitičara. Također su bili popisani dvoslovni kodovi koji su zamjenjivali neke nazive i uobičajene pojmove.[31] Iako nije bila najsigurnija metoda, koristila se idućih 450 godina zbog svoje praktičnosti.[32]

9. Renesansni procvat kriptografije u Europi

Najvećim renesansnim pokretačem promjena u kriptografiji može se smatrati Italija. U Veneciji je sredinom 15. stoljeća osnovana državna institucija čija je svrha bila baviti se kriptografskim

[27] Usp. Bushra et al. Cryptoanalysis of Arabic Poetry: Ibn Tabata Treatise. // Scholars Journal of Engineering and Technology 2, 5(2017). URL: http://saspublisher.com/wp-content/uploads/2017/03/SJET5262-69.pdf (2017-09-17)
[28] Usp. Kotas, William August. Nav. dj.
[29] Usp. Machinae: Cryptology. URL: http://www.machinae.com/crypto/ (2017-09-17)
[30] Usp. CivilWarSignals. URL: http://www.civilwarsignals.org/pages/crypto/cryptotl.html (2017-09-17)
[31] Usp. Weber, Ralph. Nav. dj. Str. 8.
[32] Usp. History of Encryption, 2001. URL: https://www.sans.org/reading-room/whitepapers/vpns/history-encryption-730 (2017-09-17)

problemima. Imali su tri 'tajnika' koji su dešifrirali jedne šifre, a druge stvarali za potrebe ministarstva.[33] Uspješna diplomacija zahtijevala je sigurni prijenos informacija što je dovelo do toga da svi veleposlanici imaju na usluzi svog tajnika, a u svakom je narodu osnovan posebni šifrarni ured. Nekad sigurni i neprobojni kodovi postali su krhki i beskorisni pred frekvencijskom analizom koja je pronašla svoj put od Bliskog istoka do Europe te su pristaše jednostavnih supstitucijskih metoda time postali laka meta kriptoanalitičarima.[34] Time je započeo razvoj kriptoanalize u Europi. Vrlo brzo su zemlje uvidjele slabosti jednostavnih monoalfabetskih supstitucijskih šifri i počele težiti naprednijim metodama zaštite od neprijateljskih kriptoanalitičara.[35]

Izumom polialfabetne supstitucije proslavio se talijanski kriptograf Leon Battista Alberti jer se upotrebom takve vrste supstitucije jedan simbol poruke predstavljao skupom šifriranih simbola što je značajno utjecalo na uspješnost dešifriranja frekvencijskom analizom. Ujedno je dizajnirao i dva šifrarnička diska na kojima je bila upisana abeceda. Jedan se disk slagao unutar drugoga te se odabirom slova unutarnjeg diska i poravnavanjem sa slovima valjskog diska pronalazila zamjenska šifra. Nakon nekoliko šifriranih riječi, disk se okretao te se početno slovo unutarnjeg diska tada nalazilo uz novo slovo vanjskog diska. To je uvelike smanjilo učinkovitost frekvencijske analize, a Alberti je nazvan ocem zapadne kriptografije.[36]

U šesnaestom stoljeću njemački fratar Johannes Trithemius piše serijal od šest knjiga pod nazivom Polygraphia. U petoj knjizi serijala uvodi 'tabulu rectu', tablice abeceda u kojima se abeceda svakog reda napravi pomicanjem one prethodne za jedno polje u lijevo. Time je poruka šifrirana iskorištavanjem svih dostupnih šifri prije nego bi se iste morale ponoviti (što se događa nakon izmjene 26 . slova).[37] Metodu je proširio Giovan Batista Belaso odabirom ključne riječi iznad originalnog teksta, gdje svako slovo ključa stoji iznad jednog slova originalnog teksta. ključ se ponovno piše iznad svake riječi, a slovo ključne riječi koje je iznad slova jasnog teksta određuje redak Trithemiusove tablice kojim se šifrira slovo. Na primjer, ukoliko je slovo iz jasnog teksta 'b', a iznad njega slovo ključne riječi 'r', za šifriranje slova 'b' koristit će se redak u Trithmeniusovoj tablici koji počinje sa 'r'.[38]

---

[33] Usp. Cohen, Fred. A Short History of Cryptography, 1995. URL: http://web.itu.edu.tr/~orssi/dersler/cryptography/Chap2-1.pdf (2017-09-17)
[34] Usp. Kotas, William August. Nav. dj.
[35] Usp. Đuraković, Adriana. Klasična kriptografija, 2014. URL: http://www.mathos.unios.hr/~mdjumic/uploads/diplomski/%C4%90UR80.pdf (2017-09-17)
[36] Usp. Cohen, Fred. Nav. dj.
[37] Usp. Isto.
[38] Usp. Šaban, Josip. Nav. dj.

9.1. Vigenereova šifra

Najistaknutije postignuće stoljeća je zasigurno ono francuskog kriptografa Blaisea de Vigenerea. Proučavao je ranije objavljene kriptografske radove (uključujući Trithemiusove abecedne tablice i Belaso-ovo korištenje ključne riječi), pronalazio im slabe točke, tražio rješenja za naprednije kriptiranje i u konačnici je razvio nova sredstva za bolju enkripciju. Nazvane po njemu, Vigenereove šifre koriste sustav 26 različitih šifri abecede za enkripciju poruke. Šifrirane su abecede jednostavni primjeri cezarove šifre od prve do 26-e raspoređene u kvadrat. Svako se slovo poruke enkriptira koristeći različiti red Vigenerova kvadrata koji pri tome služi kao odabrana šifrirana abeceda. Da bi se odabrao red za korištenje, birala se i ključna riječ. Ta bi se riječ zatim zapisivala iznad svakog reda koji je čekao da se enkriptira i tako se ponavljala dok sva slova u redu ne bi imala svoju odgovarajuću slovnu zamjenu u kodiranoj riječi. Na primjer, ukoliko se odabere ključna riječ SMILE, dobit će se idući rezultat: „smi lesmil esmi le sm iles“ koji bi predstavljao poruku „the attack will be at dawn“. Korištenjem dužih ključnih riječi i fraza omogućava se ubacivanje većeg broja abeceda.[39]

Vigenere je na taj način pronašao rješenje protiv frekvencijske analize, koja u ovom slučaju nije mogla odgonetnuti šifrirane poruke, kako nije postojala mogućnost određivanja učestalosti pojedinog slova jer se ono skrivalo iza nekoliko različitih slova. Dodatno tome, za enkripciju se moglo zadati i više ključnih riječi.[40] Može se reći da je unio nov pogled u funkcionalnost šifri, bazirajući se na ključnim riječima koje su djelovale kao enkripcijski ključevi. Tako je za dešifriranje poruke bilo potrebno poznavanje enkripcijskog ključa (koji je bio proizvoljan s neograničenim brojem mogućnosti), te se rasteretio pritisak na očuvanje sigurnosti samog sustava.[41]

Njegovo se otkriće smatralo prvom stabilnom inovativnom metodom od pojave cezarove šifre. Krajem šesnaestom stoljeća je objavio knjigu Traicte de Chiffres u kojoj je zapisao sva tada poznata znanja o kriptografiji. Unatoč tome, bila su potrebna skoro dva stoljeća da se njegova nova šifra prihvati u svijetu kriptografije.[42]

[39] Usp. Kotas, William August. Nav. dj.
[40] Usp. Isto.
[41] Usp. Red hat. A brief History of Cryptography, 2016. URL: https://access.redhat.com/blogs/766093/posts/1976023 (2017-09-17)
[42] Usp. Kotas, William August. Nav. dj.

10. Mračni uredi

Krajem sedamnaestog stoljeća francuska je vlada imala poveći broj zaposlenih u području kriptografije. Zajedno su osnovali tzv. Cabinet Noir (hrv. Mračni ured) s ciljem izrade sigurnosnih šifri i pronalaženja metoda za razbijanje neprijateljskih.[43]

Osamnaesto stoljeće obilježeno je osnivanjem mračnih ureda diljem Europe. Najpoznatiji The Geheime Kabinetz-Kanzlei je osnovan u Beču i provjeravao je svu poštu koja se razmjenjivala sa stranim veleposlanstvima. Nakon provjere, pošta bi se kopirala, ponovno zapečatila i vratila nazad u poštanski ured. Također je dekriptirao i ostale presretnute vojne i političke poruke, a poznato je da su znali analizirati i do sto pisama dnevno.[44] U povijesti je ostao poznat i engleski mračni ured za kojeg je zabilježeno da je dugi niz godina uspješno djelovao u svojim kriptografskim poslovima.[45] Takva kriptoanalitička organizacija zabrinula je tadašnje kriptografe koji su u konačnici morali prihvatiti Vigenereove šifre ne bi li osigurali sigurnost svojih poruka.[46]

Mračni su uredi uspješno odgonetali većinu američkih šifri, no bez dolazećih ratova, postepeno su gubili na važnosti te su do sredine devetnaestog stoljeća ukinuti.[47]

11. Pomagala za šifriranje

Sličan sustav šifriranja Vigenereovim šiframa izradio je Thomas Jefferson na samom kraju osamnaestog stoljeća. Poznati Jeffersonov kotač pokazao se kao još bolja zaštita. Kotač se sastojao od 26 kotačića na kojima je bila slučajno raspoređena abeceda, a oni sami su bili numerirani i u posebnom poretku što je bio temeljni ključ tog enkripcijskog algoritma. Poruka se šifrirala na način da se kotačići namjeste tako što bi u jednoj liniji činili tekst poruke, čime bi šifrirani tekst bio sadržan u bilo kojoj drugoj liniji. Osoba koja dekriptira šifrirani tekst mora imati kotačiće u posebnom poretku šifriranog teksta kako bi se u jednoj od linija opet prikazao pravi tekst. Unatoč kompleksnoj strukturi i sigurno uspješnoj inovaciji, Jefferson nikad nije razvio svoj enkripcijski sustav. Tek je početkom devetnaestog stoljeća američka vojska izradila

[43] Usp. Kriptografija. URL: http://archive.cnx.org/contents/6c69c406-cf73-4520-86ef-6a6db4bd317c@1/kriptografija (2017-09-17)
[44] Usp. Sihegee: Evolution of Cryptography – Are you really protecting your Data?, 2013. URL: https://sihegee.wordpress.com/2013/03/24/evolution-of-cryptography-are-you-really-protecting-your-data/ (2017-09-17)
[45] Usp. Cohen, Fred. Nav. dj.
[46] Usp. Kotas, William August. Nav. dj.
[47] Usp. Cohen, Fred. Nav. dj.

sustav poput njegova kotača, a da nisu ni znali za već postojanje istog. Time je bilo jasno da je Jefferson bio sto godina prije svoga vremena, a američka je vojska takav sustav koristila do sredine dvadesetog stoljeća.[48]

Pukovnik Decius Wadsworth je 1817. razvio sustav dva diska – jedan u drugom. Vanjski je disk sadržavao 26 slova engleske abecede i brojeve od 2 do 8, a unutarnji samo slova abecede. Diskovi su bili namješteni tako da im se brojevi okretaja odnose u omjeru 26:33. Kriptiranje se vršilo na način da se unutarnji disk vrtio sve dok se željezno slovo nije pojavilo na vrhu, a broj okretaja diska potrebnih za pojavu slova je značio kriptirani tekst. Pukovniku izum nikada nije bio priznat. Tek će nekoliko godina kasnije britanski znanstvenik Charles Wheatstone izumiti sličan sustav i za njega dobiti priznanje.[49]

12. Playfair sustav

Prvi sustav koji je koristio parove simbola za enkripciju bio je Playfair sustav. Izmislio ga je Wheatstone sredinom devetnaestog stoljeća, a popularizirao barun Lyon Playfair po kojemu i nosi naziv. Radi se o bigramskoj šifri, u smislu da se šifriraju parovi slova, a rezultat ovisi i o jednom i o drugom slovu. Algoritam se bazira na 5x5 matrici slova, koja se izgrađuje na temelju ključne riječi. Otvoreni se tekst potom mora podijeliti na blokove od po dva slova. Niti jedan se blok ne smije sastojati od dva jednaka slova i duljina teksta mora biti parna. Ukoliko je potrebno, može se umetnuti npr. slovo X da se postigne sve navedeno. Zatim postoje tri slučaja koja mogu nastupiti: u prvom se slova nalaze u istom retku te ih mijenjamo sa slovima koja se nalaze za jedno mjesto udesno (ciklički); u drugom slučaju slova se nalaze u istom stupcu i mijenjamo ih sa slovima koja se nalaze jedno mjesto ispod (ciklički) i treće, gleda se pravokutnik koji određuju ta dva slova te se mijenjaju s preostala dva vrha pravokutnika. Redoslijed je određen na način da prvo dolazi slovo iz istog retka u kojem je prvo slovo polaznog bloka.[50] Prednost ove metode je da se gube u šifratu jednoslovne riječi koje dosta utječu na frekvencije i broj bigrama je puno veći od broja individualnih slova. Time je podosta otežana frekvencijska analiza te se metoda dugo vremena smatrala sigurnom.[51]

---

[48] Usp. McDonald, Nicholas. Past, present, and future methods of cryptography and data encryption. URL: http://www.eng.utah.edu/~nmcdonal/Tutorials/EncryptionResearchReview.pdf (2017-09-17)
[49] Usp. Galinović, Andro. Povijest kriptografije, 2005. URL: http://web.zpr.fer.hr/ergonomija/2005/galinovic/PovijestKriptografije.pdf (2017-09-17)
[50] Usp. Dujella, Andrej. Klasična kriptografija: Playfairova šifra. URL: https://web.math.pmf.unizg.hr/~duje/kript/playfair.html (2017-09-17)
[51] Usp. Isto.

13. Novi putevi komunikacije – novi kriptografski izazovi

Novi izazov kriptografiji postavljen je sredinom devetnaestog stoljeća izumom telegrafa. Za slanje poruke telegrafom, pošiljatelj je morao kopiju svoje poruke dati telegrafskom operateru, što je otvaralo mogućnost podmićivanja operatera za otkrivanje sadržaja poruka. Komunikacijom putem telegrafa najviše su se koristili vrhovni zapovjednici kako bi trenutno slali poruke nižim zapovjednicima na bojištu. Kako bi se zaštitila sigurnost poruke, jedino je rješenje bilo enkriptiranje poruke prije nego se ona da operateru u ruke. Time bi se onemogućilo njegovo shvaćanje poruke tijekom prijenosa putem telegrafskih linija. Pošiljatelji poruka su se oslonili na Vigenereove šifre koje su se dotada još smatrale neprobojnima.[52]

Kako je telegraf utjecao na promjene u kriptografiji sredinom devetnaestog stoljeća, tako je i pojava radija mijenjala kriptografiju krajem stoljeća i postavila nove prepreke. Prijenosi poruka putem radija bili su otvorenog karaktera i fizička sigurnost nije bila moguća. To je omogućilo presretanje neprijateljskih poruka, kao što su npr. Francuzi presretali poruke Nijemcima. Njemački pokušaji zaštite poruka dvostupčanom transpozicijom 'Ubchi' nisu uspjeli, jer su ju francuski kriptoanalitičari lako razbili.[53]

Krajem devetnaestog stoljeća Auguste Kerckhoffs je u svom djelu La Cryptographie Militarie postavio šest osnovnih zahtjeva kriptografije: 1. Šifrirani tekst treba biti neprobojan u praksi; 2. Kriptosustav treba biti prikladan za korisnike; 3. Ključ treba biti lako pamtljiv i promjenjiv; 4. Šifrirani tekst treba biti telegrafski prenosiv; 5. Uređaj za šifriranje treba biti lako prenosiv; 6. Stroj za šifriranje treba biti relativno jednostavan za korištenje.[54]

14. Propusti u kriptosustavima

Slabu točku Vigenereovoj šifri pronašao je Charles Babbage. Tada već poznat kao iznimni kriptoanalitičar, bio je izazvan da pronađe metodu razbijanja šifre. Primijetio je da se dijelovi pisma ponavljaju nakon određenog seta slova. Pretpostavio je da su to možda uobičajene riječi kodirane slijedom šifrirane abecede što se ispostavilo točno te je u tom zaključku pronašao ključ za razbijanje šifre. Proučavajući broj slova između ponavljanih dijelova, uz korištenje pomoćnih statističkih metoda, uspio je procijeniti duljinu ključne riječi. Zatim je šifrirani tekst podijelio u

[52] Usp. Kotas, William August. Nav. dj.
[53] Usp. Cohen, Fred. Nav. dj.
[54] Usp. Sihegee: Evolution of Cryptography – Are you really protecting your Data?, 2013. URL: https://sihegee.wordpress.com/2013/03/24/evolution-of-cryptography-are-you-really-protecting-your-data/ (2017-09-17)

nekoliko dijelova što se tako podijeljeno moglo sagledati kao jednostavna abeceda cezarove šifre. Daljnjom frekvencijskom analizom odredio je slova ključne riječi, a potom dekodirao i cijelu šifru.[55] S obzirom da su se zbog mračnih ureda i frekvencijske analize gotovo svi kriptografi okrenuli Vigenereovim šiframa, ovakvo otkriće zatreslo bi tada djelomično stabilno područje kriptologije. No, Babbage svoje otkriće nikada nije objavio. Tek kasnije je to umjesto njega učinio Francuz Friedrich Wilhelm Kasiski, uzimajući sve zasluge koje su trajale do dvadesetog stoljeća kada je otkrivena istina o autoru.[56]

U prvoj polovici dvadesetog stoljeća Lester Hill izumio je kriptosustav kod kojeg se određeni broj uzastopnih slova otvorenog teksta zamjenjuje s jednako određenim brojem slova u šifratu. Ukoliko broj slova u otvorenom tekstu nije djeljiv s određenim brojem, poruka se mora nadopuniti da bi se mogla podijeliti u blokove određenog broja slova. Hillova poligramska šifra uspješno je skrivala i informacije o frekvencijama slova i informacije o frekvencijama bigrama. Sustav je ipak imao propuste koje su određeni napadi mogli iskoristiti te nije ušao u širu upotrebu. Ono poznato je da se šifra kratko vrijeme koristila za šifriranje pozivnih signala radio-stanica.[57]

15. Utjecaj kriptografije na zbivanja u Prvom svjetskom ratu

Već je samim početkom dvadesetog stoljeća bilo vjerojatno da će ratna zbivanja zahvatiti Europu. Ogromna su se sredstva ulagala u užurbani razvoj kriptografije i kriptoanalize. Najveći pomak učinila je Engleska koja je u početku rata uspijevala probiti većinu neprijateljskih šifri (posebice šifre njemačke mornarice). Osim Engleza, presretanjem radio poruka intenzivno su se bavili i Francuzi i Amerikanci.[58]

Sa kriptografske strane se odvijala nešto drugačija situacija. Mnoge su nove šifre razvijane, ali su se temeljile na permutacijama ili kombinacijama starijih šifri koje se već znalo dešifrirati. Poseban problem stvarao je ubrzan razvoj komunikacijskih kanala. Materijal koji se trebao šifrirati više nije bio samo papir. Ogromna količina informacija prenosila se putem radijskih kanala. Neke od razvijanih metoda uspjele su otkriti informacije o poruci bez da ju zapravo dekriptiraju, što je označilo početak analize prometa. Shvaćajući odakle su poruke

[55] Usp. Kotas, William August. Isto.
[56] Usp. Kotas, William August. Isto.
[57] Usp. Dujella, Andrej. Klasična kriptografija: Hillova šifra. URL: https://web.math.pmf.unizg.hr/~duje/kript/hill.html (2017-09-17)
[58] Usp. Kriptografija. URL: http://archive.cnx.org/contents/6c69c406-cf73-4520-86ef-6a6db4bd317c@1/kriptografija (2017-09-17)

poslane i kamo te tko ih je poslao pomoglo je u određivanju smjera kretanja neprijateljske vojske. Tijekom Prvog svjetskog rata Saveznici su pokazali kriptografsku nadmoć, osnivajući i razvijajući svoje kriptografske odjele čak i prije rata (poznati engleski Room 40), dok su Nijemci u rat ušli nepripremljeno, osnivajući kriptografski odjel tek dvije godine nakon početka rata.[59]

Doprinos kriptografa tijekom ratnih zbivanja se najbolje može prikazati na primjeru Zimmermanova telegrama. Arthur Zimmerman imenovan je njemačkim ministrom vanjskih poslova 1916. godine. Američki predsjednik Woodrow Wilson nadao se mirnom rješenju rata kako se SAD postavio neutralno, na distanci, no to ipak nije bio slučaj. Utvrđeno je da bi njemačka mornarica mogla stegnuti blokadu Britanije i odnijeti laku pobjedu. Njemački zapovjednici su procijenili da bi takav čin bio moguć prije nego bi SAD stigao oformiti mornaricu, te su, u konačnici, odobrili akciju. Zimmerman je osmislio kako osigurati da SAD ne uđe u rat, čak i ako pobjeda ne dođe tako brzo kako je planirana. Predložio je savezništvo s Meksikom i poticao njihova predsjednika da napadne američki teritorij te povrati Teksas i druge teritorije. Također im je predložio da ohrabre Japance za istovremeni napad na američki teritorij, čime bi SAD odvratili od zbivanja u Europi. Telegramom je poslao poruku njemačkom ambasadoru u Washingtonu o svom planu s uputama da proslijedi poruku njemačkom ambasadoru u Meksiku, koji bi tu poruku zatim prenio meksičkom predsjedniku. Enkriptirao je poruku jer je znao da Saveznici presreću kompletnu diplomatsku komunikaciju te je, kao što je pretpostavio, enkriptirana poruka isti dan došla u posjed britanskih kriptografa. No, ono što nije pretpostavio je to da su tu poruku dekriptirali već idući dan i došli do cijelog sadržaja poruke. Poruku nisu predstavili predsjedniku Wilsonu sve dok nisu presreli i drugu poruku koja je išla ambasadoru u Meksiku. Zatim su pustili Nijemce da vjeruju kako je došlo do sigurnosnog propusta u meksičkom kraju, a ne da su im uspjeli dekriptirati šifru. Nakon čitanja Zimmermanovog pisma i njegova priznanja o autentičnosti, predsjednik Wilson je uveo SAD u rat kako bi ga okončao.[60]

Nijemci su počeli intenzivno presretati pozive Saveznika, čime su se doveli u prednost poznavajući svaki njihov idući potez. Američki zapovjednik Lewis osmislio je plan uvođenja američko-indijanskoga jezika u komunikaciju. Pronašao je osmero vojnika koji su bili u srodstvu s plemenom Choctaw, koji su preuzeli komunikaciju putem radija i poziva, a za to su imali jedinstveni jezik. Kodovi i šifre na zajedničkim jezicima su se mogli lagano probiti, no kodovi bazirani na jedinstvenom jeziku bi se prvo morali iscrpno proučiti da bi se mogli shvatiti i zatim

[59] Usp. Kotas, William August. Nav. dj.
[60] Usp. Isto.

dekodirati. Koristeći indijanski jezik kao enkripciju, Saveznici su unutar 24 sata vratili prednost nad Nijemcima. Unutar 72 sata, Saveznici su krenuli u napad, a Nijemci su bili prisiljeni povući se.[61]

16. Kriptografija na primjeru Enigme u Drugom svjetskom ratu

Nedugo nakon Prvog svjetskog rata, 1919. Godine, Nijemac Arthur Scherbius razvio je sustav za kriptografsku zaštitu informacija i nazvao ga Enigma. S obzirom da je Njemačka tražila kriptografsko rješenje upotporeno automatizacijom i uređajima za šifriranje, njemačka vojska ubrzo uvodi Enigmu kao standardni način kriptiranja u mornarici, a kasnije ga usvajaju i zrakoplovstvo te kopnena vojska.[62]

Enigma se sastojala od osnovne tipkovnice, zaslona na kojem bi se prikazale šifrirane poruke i mehanizma za šifriranje pomoću kojega se svako uneseno slovo putem tipkovnice šifriralo u njemu odgovarajuće drugo slovo. Upotrebljavali su se višestruki diskovi za šifriranje posebno pozicionirani unutar Enigme, odakle su mogli simulirati različite šifrirane abecede, a sve s ciljem sprječavanja uspješnog frekvencijskog analiziranja. Da bi se poruka dešifrirala, bila je potrebna knjiga kodova (koju imaju samo primatelj i pošiljatelj poruke) s pojedinostima o specifičnim postavkama za šifriranje, i to na dnevnoj bazi.[63] Enigmin kompleksno razrađeni kriptosustav uzdrmao je dotad poznato područje kriptoanalize, koje se s takvim izazovom još nije susrelo (u svojoj standardnoj verziji Enigma je pružala milijarde mogućih kombinacija što je bilo nemoguće ispitati[64]). Dešifriranje je bilo presudno za okončavanje rata, a vremena nije bilo na pretek.

Poljski statističar, matematičar i kriptoanalitičar Marian Rejewski je proučavao Enigmu i, iako ju nikad nije uspio razbiti, prenio je cijelo svoje istraživanje Englezima i Francuzima tjednima prije nego je Njemačka napala Poljsku. U konačnici je njegovo istraživanje pomoglo Alanu Turingu i kriptoanalitičarima kod Bletchleya za izgradnju elektromehaničkih strojeva, tzv. bombi, dizajniranih isključivo u svrhu razbijanja Enigme.[65] Strojevi su uspjeli pronaći Enigmin

[61] Usp. McDonald, Nicholas. Nav. dj.
[62] Usp. Galinović, Andro. Nav. dj.
[63] Usp. Mathai, Jacob. Nav. dj.
[64] Usp. Dujella, Andrej. Teorija brojeva i kriptografija. URL: https://bib.irb.hr/datoteka/870211.novigrad-dujella-rev2.pdf (2017-09-17)
[65] Usp. Mathai, Jacob. Nav. dj.

ključ u roku sat vremena od slanja poruke[66], što je Saveznicima bilo dovoljno da shvate idući potez njemačke vojske i okrenu ishod rata u svoju korist.

Unatoč nevjerojatnom postignuću, sve su informacije oko dešifriranja Enigme držane u strogoj tajnosti i nisu bile otkrivane do 1974. godine, kada je objavljeno djelo „The Ultra Secret“ u kojem je opisan cijeli Enigmin slučaj.[67]

17. Zaključak

Razvojem pismenosti je fizičkim objektima pridodana funkcija podloge za pisanje poruka. Kako su objekti vidljivi oku, zapisana misao na njima također poprima istu karakteristiku. Proširile su se mogućnosti komunikacije, posebice između pošiljatelja i primatelja poruke na udaljenim lokacijama, što je rezultiralo pojavom mogućnosti presretanja poruke i otkrivanja sadržaja iste.

Iz primjera tijekom cijele povijesti je vidljivo da se svaka nova kriptografska metoda za očuvanjem sigurnosti podataka razbila popratnom kriptoanalitičkom metodom koja je tim podacima htjela pristupiti. Analizom takvih primjera proizlazi informacija da se tajnost poruka treba temeljiti na sigurnosnom tajnom ključu, a ne na samom kriptosustavu. U svakom primjeru u kojem se zaštita podataka temeljila na korištenju kriptosustava samom po sebi, uslijedilo je, sa kriptoanalitičke strane, identificiranje tog određenog kriptosustava i razotkrivanje sadržaja svih poruka koje su tim sustavom bile zaštićene. U tom slučaju, kriptosutav je generalno jednako štitio sve poruke te ih ujedno sve zajedno ugrožavao. S druge strane, upotreba posebnog tajnog ključa postavila je opravdane izazove kriptoanalizi, koja u slučaju probijanja tajnog ključa, probija sadržaj samo one poruke za koju je taj ključ namijenjen.

U svom razvitku, kriptografija je od svojih najranijih pseudo-oblika, datiranih tisućama godina prije nove ere, napredovala do kompleksne znanosti u službi zaštite informacija, a sigurno će se i nastaviti razvijati jer svaki primjer 'neprobojne šifre' sazna svoj rok trajanja kada mu ga kriptoanaliza dodijeli.

[66] Usp. Kotas, William August. Nav. dj.
[67] Usp. Isto.

Literatura

1. Anderson, Ross. Security Engineering: A Guide to Building Dependable Distributed Systems. URL: https://www.cl.cam.ac.uk/~rja14/Papers/SE-05.pdf (2017-09-17)
2. Bushra et al. Cryptoanalysis of Arabic Poetry: Ibn Tabata Treatise. // Scholars Journal of Engineering and Technology 2, 5(2017), str. 62-29. URL: http://saspublisher.com/wp-content/uploads/2017/03/SJET5262-69.pdf (2017-09-17)
3. CivilWarSignals. URL: http://www.civilwarsignals.org/pages/crypto/cryptotl.html (2017-09-17)
4. Cohen, Fred. A Short History of Cryptography, 1995. URL: http://web.itu.edu.tr/~orssi/dersler/cryptography/Chap2-1.pdf (2017-09-17)
5. Cruise, Brit. Ancient Cryptography: The Caesar cipher, 2012. URL: https://www.khanacademy.org/computing/computer-science/cryptography/crypt/v/caesar-cipher (2017-09-17)
6. Dujella, Andrej. Klasična kriptografija: Hillova šifra. URL: https://web.math.pmf.unizg.hr/~duje/kript/hill.html (2017-09-17)
7. Dujella, Andrej. Klasična kriptografija: osnovni pojmovi. URL: https://web.math.pmf.unizg.hr/~duje/kript/osnovni.html (2017-09-17)
8. Dujella, Andrej. Klasična kriptografija: Playfairova šifra. URL: https://web.math.pmf.unizg.hr/~duje/kript/playfair.html (2017-09-17)
9. Dujella, Andrej. Teorija brojeva i kriptografija. URL: https://bib.irb.hr/datoteka/870211.novigrad-dujella-rev2.pdf (2017-09-17)
10. Đuraković, Adriana. Klasična kriptografija, 2014. URL: http://www.mathos.unios.hr/~mdjumic/uploads/diplomski/%C4%90UR80.pdf (2017-09-17)
11. Galinović, Andro. Povijest kriptografije, 2005. URL: http://web.zpr.fer.hr/ergonomija/2005/galinovic/PovijestKriptografije.pdf (2017-09-17)
12. History of Encryption, 2001. URL: https://www.sans.org/reading-room/whitepapers/vpns/history-encryption-730 (2017-09-17)
13. IBM Knowledge Center. URL: https://www.ibm.com/support/knowledgecenter/hr/ssw_i5_54/rzahu/rzahurzahu0cmcryptogco.htm (2017-09-17)
14. Kotas, William August. A Brief History of Cryptography, 2000. URL: http://trace.tennessee.edu/cgi/viewcontent.cgi?article=1398&context=utk_chanhonoproj (2017-09-17)

15. Kriptografija. URL: http://archive.cnx.org/contents/6c69c406-cf73-4520-86ef-6a6db4bd317c@1/kriptografija (2017-09-17)
16. Kriptografija, 2009. URL: http://www.cert.hr/sites/default/files/CCERT-PUBDOC-2009-08-275.pdf (2017-09-17)
17. Machinae: Cryptology. URL: http://www.machinae.com/crypto/ (2017-09-17)
18. Mathai, Jacob. History of Computer Cryptography and Secrecy Systems. URL: http://www.dsm.fordham.edu/~mathai/crypto.html (2017-09-17)
19. McDonald, Nicholas. Past, present, and future methods of cryptography and data encryption. URL: http://www.eng.utah.edu/~nmcdonal/Tutorials/EncryptionResearchReview.pdf (2017-09-17)
20. Origin of cryptography. URL: https://www.tutorialspoint.com/cryptography/pdf/origin_of_cryptography.pdf (2017-09-17)
21. Pommerening, Klaus. Cryptology: Some Notes on Early history, 2015. URL: https://www.staff.uni-mainz.de/pommeren/Cryptology/Classic/1_Monoalph/EarlyHist.html (2017-09-17)
22. Red hat. A brief History of Cryptography, 2016. URL: https://access.redhat.com/blogs/766093/posts/1976023 (2017-09-17)
23. Sidhpurwala, Huzaifa. Cipher writing of ancient India was called mlecchita vikalpa, pre-alphabetic, pre-syllabic cryptography of Indus Script Corpora, 2014. URL: http://www.academia.edu/12160041/Cipher_writing_of_ancient_India_was_called_mlecchita_vikalpa_pre-alphabetic_pre-syllabic_cryptography_of_Indus_Script_Corpora (2017-09-17)
24. Sihegee: Evolution of Cryptography – Are you really protecting your Data?, 2013. URL: https://sihegee.wordpress.com/2013/03/24/evolution-of-cryptography-are-you-really-protecting-your-data/ (2017-09-17)
25. Simon Singh: Arab Code Breakers. URL: https://simonsingh.net/media/articles/maths-and-science/arab-code-breakers/ (2017-09-17)
26. Simon Singh: The Black Chamber. URL: https://www.simonsingh.net/The_Black_Chamber/index.html (2017-09-17)
27. Steganografija, 2006. URL: http://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2006-04-154.pdf (2017-09-17)
28. Šaban, Josip. Povijesni pregled računalne sigurnosti. URL: http://sigurnost.zemris.fer.hr/ostalo/2002_saban/index.htm (2017-09-17)
29. Weber, Ralph. United States Diplomatic Codes and Ciphers. Routledge, 2010. Str. 633