Kriminalističke teme
Zbornik radova
Godina XIX, Broj 5, 2019.
ISSN 1512-5505

POSTUPCI KRIPTOGRAFIJE I NJIHOVA ULOGA
CRYPTOGRAPHY PROCEDURES AND THEIR ROLE

Pregledni naučni rad

Prof. dr. Jasmin Ahić
Kenan Hodžić, MA[181]

SAŽETAK

Inspiracija za rad i problem (i) koji se radom oslovljava (ju): Tehničko-tehnološki razvoj omogućava i pogoduje unapređivanju i inoviranju novih komunikacijskih kanala. U domenu kritičnih ljudskih djelatnosti osnovno je pitanje na koji način zaštititi čovjeka od savremenih prijetnji kojima je izložen. U raspoloživoj akademskoj literaturi ne postoji dovoljno informacija o metodama koje proučavaju skrivanje informacija što spada u skupinu postupaka kriptografije.

Ciljevi rada (naučni i/ili društveni): Cilj rada je analizirati historijsku ulogu kriptografije, ukazati na razloge njene pojave, primjenu i važnost u cilju unapređenja sigurnosti i zaštite ljudi u cjelini. Svakako da je popunjavanje praznina u dostupnoj građi iz ove oblasti dopunski cilj rada, uzimajući u obzir da će se u radu na sistematičan i jedinstven način zaokružiti zapaženo stanje.

Metodologija/Dizajn: U radu je primarno korištena tehnika iz kvalitativne istraživačke paradigme. Metodom analize sadržaja istraživat će se kriptografski sistemi i metode koje se koriste. Selekcija akademskih radova iz oblasti kriptografije je urađena na način da su odabrani samo oni radovi koji u svojoj sadržini imaju historijsku i razvojnu komponentu sigurnosti i kriptografije.

Ograničenja istraživanja/rada: Nedostatak naučnog diskursa i postojanje izraženog nesklada u teorijskim razmatranjima a u vezi sa interpretiranjem kripto postupaka.

Rezultati/Generalni zaključak: Rezultati se odnose na prikaz i klasifikaciju sistema i metoda kriptografije.

Opravdanost istraživanja/rada: Opravdanost istraživanja se ogleda u potrebi da se prizna važnost pogodnostima primjene kriptografije u današnje vrijeme.

Ključne riječi

historija kriptografije, kriptografija, područja primjene, kriptografske metode

ABSTRACT

Reason for writing and research problem (s)

Technical-technological development enables the improvement and innovation of new communication channels. In the field of critical human activities, the basic question is

[181] Fakultet za kriminalistiku, kriminologiju i sigurnosne studije Univerziteta u Sarajevu

how to protect a man from the modern threats he is exposed to. In the available academic literature, there is incomplete information about methods for analyzing hidden information and which belong under the category of cryptography.
Aims of the paper (scientific or social)
The aim of the paper is to analyze the historical role of cryptography, to indicate the reasons for its appearance, application, and importance in order to improve the safety and protection of people and society as a whole. Filling the gaps in the available material from this field is a supplementary goal of work, as it will work in a systematic and unique way to encircle the observed situation.
Methodology/ Design
The paper uses primarily the technique from a qualitative research paradigm. The method of content analysis will explore the cryptographic systems and methods. The selection of academic papers in the field of cryptography was done in a way that only works that have a history and development component of security and cryptography are selected.
Research/ Paperlimitation
Lack of scientific discourse and the existence of a pronounced disparity in theoretical considerations, regarding the interpretation of crypto operations.
General Conclusion
The results refer to the display and classification of systems and methods of cryptography.
Research/ Paper Validity
The justification of the research is reflected in the need to recognize the importance of the benefits of applying cryptography today.

Keywords
history of cryptography, cryptography, application areas, cryptographic methods

UVOD

Prema osnovnom modelu komunikacije pošiljatelj šalje poruku primatelju koja do njega putuje komunikacijskim kanalom, istu tumači na svoj način i koristi u svom vlastitom interesu ili potrebi. Temeljni proces komunikacije je stvaranje odnosa, odnosno stvaranje raznovrsnih socijalnih interakcija, dok je središnji element komunikacije upravo interakcija koja pomaže da se prihvaćene informacije interpretiraju prema namjeni i želji pošiljatelja (Rouse i Rouse, 2005).

"Poriv za otkrivanje tajni duboko je protkan kroz ljudsku narav; čak i krajnje neradoznali um uzbuđuje misao da bi mogao saznati nešto što je drugima uskraćeno."
John Chadwick

Svakako da današnji informacijsko-komunikacijski sistemi izuzetno smanjuju značaj prostornog i vremenskog faktora i time, možemo pretpostaviti, donose velike uštede uz povećanje efikasnosti informacijskih aktivnosti. Povećanje efikasnosti informacijskih aktivnosti donosi nove mogućnosti proširenja pristupa informacijskim sadržajima, kvalitetnije provođenje svih aktivnosti neposredno vezanih za korištenje informacijskih sadržaja.

Prema Reardonu (1998) šest je temeljnih karakteristika ljudske komunikacije koje uključuju sljedeće: 1. Ljudi komuniciraju iz mnoštva različitih razloga; 2. Komuniciranje rezultira namjeravanim, ali i nenamjeravanim učincima; 3. Komunikacija je obično obostrana; 4. Komuniciranje uključuje najmanje dvije osobe, koje jedna na drugu utječu u nejednakoj mjeri; 5. Komunikacija se dogodila i onda kada nije bila uspješna; 6. Komuniciranje uključuje upotrebu simbola.

Ljudi su od davnina željeli neometano i sigurno komunicirati,[182] s tim što su istovremeno bili svjesni da njihove poruke često putuju nesigurnim komunikacijskim kanalima kojima može pristupiti i treća osoba koja će vidjeti poruku iako joj nije namijenjena. Shodno tome, raste prijetnja da se otkriju važne informacije od kojih se očekuje da nas vode i da nam pomažu u pronalaženju alternativa i prijedloga, odnosno da reduciraju negativne efekte određenih problemskih situacija.

Uvijek aktuelna opasnost da bi neprijatelj mogao doći do informacije, potaknula je razvoj šifri i kodova. Zbog toga su naprimjer, mnoge zemlje počele osnivati odjele i institute za analizu i primjenu šifriranja. Kao rezultat pojave ovih aktivnosti, na neprijateljskim stranama istovremeno su započele mjere i aktivnosti za analizu kriptiranih sadržaja i razbijanje primijenjenih šifrarskih sistema kako bi se došlo do tih vrijednih informacija. Svaka je šifra snažna sve dok se ne otkrije njen ključ, te ista postaje beskorisna i mora se napraviti nova te tako sve u krug (Posavec, 2018). Kako su se kroz stoljeća promijenili načini prenošenja poruka, osnovni problem zapravo je ostao isti, a to je kako onemogućiti onoga tko može nadzirati komunikacijski kanal, kojim se prenosi poruka, da dozna njezin sadržaj. Načinima rješavanja ovog problema bavi se naučna disciplina koja se naziva *kriptografija*. Njezine su potencijale koristili vladari, ratnici, diplomate, uhode, mistici, kabalisti, alkemičari, nekromanti, policajci, ljubavnici, tragači za zakopanim blagom, naučnici, industrijalci, umjetnici i ljudi željni intelektualnih izazova. Ona je štitila državne, vojne, vjerske ali i privatne tajne.

Tokom posljednjih dvadeset godina akademska istraživanja o kriptografiji su doživjela veliku ekspanziju. U tom pravcu, autori ovog rada su postavili za cilj da ponude kratki historijski pregled i da ukažu na značaj kriptografije do danas, naročito obraćajući pažnju na određene pristupe razumijevanju savremenih postupaka koji se koriste u moderno doba. Naša zamisao i cilj će biti u cjelosti ostvaren ako barem u minimalnoj mjeri ojača svijest javnosti o važnostima korištenja sigurnih, zaštićenih i neometanih komunikacijskih usluga.

[182] Herodot u *Historijama* daje hroniku sukoba između Grčke i Perzije u 5. st. pr. Kr. i navodi da se već u tom razdoblju Grčka branila umijećem tajnog pisanja (Majić, 2015).

1. RAZLOZI NASTANKA KRIPTOGRAFIJE

Kako ćemo se u ovom radu baviti temama za koje je potrebno osnovno znanje, na samom početku ćemo ponuditi i obrazložiti osnovne elemente kategorijalno-pojmovnog aparata. Uzimajući u obzir da ljudi međusobno komuniciraju putem poruka važno je odrediti šta su poruke. Prema Reardonu (1998) sve poruke se sastoje od nizova simbola. Simboli su riječi, geste, slike, zvukovi ili pokreti, stoga što se ljudi više ili manje slažu u pogledu objekata, zbivanja ili osjećaja na koje se ti simboli odnose. Za potrebe izrade ovog rada, poruke ćemo razmatrati u kontekstu pisane komunikacije.

Prema Baueru (2002) kriptologija je starija više hiljada godina, i njen razvoj usko je vezan za razvoj matematike. Danas predstavlja interdisciplinarnu nauku koja obuhvata sve od matematike, statistike, logike, lingvistike, pa sve do elektromehanike, računarstva i umjetne inteligencije koje su više izražene danas nego u prošlosti. Ključ[183] je u kriptologiji naziv za informaciju koja onome koji tu informaciju posjeduje otkriva kojim je postupkom originalna poruka sakrivena, što mu omogućuje otkrivanje poruke. Kriptologija je u velikoj mjeri osnova za zaštitu informacija i cyber sigurnost.

Potreba za sakrivanjem poruka prisutna je otkako je ljudski rod iselio iz pećina, počeo živjeti u skupinama i odlučio ozbiljno shvatiti civilizacijsku ideju. Kako su postojale različite grupe ili plemena, pojavila se i ideja da, u cilju opstanka, moraju raditi jedni protiv drugih i raširiti se, zajedno s nasiljem, manipulacijama gomile i tajnošću. Načelno se razlikuju dva oblika skrivanja poruka u pisanoj komunikaciji. Naime, steganografija (grč. στεγανός, pokriven i γράφειν, pisati) pretpostavlja skrivanje same poruke, a kriptografija (grč. κρυπτός, skriven i γράφειν, pisati) skriveno, tajno pisanje, odnosno oblikovanje tajne, šifrirane poruke koja će biti razumljiva samo pošiljatelju i primatelju (Pawlan, 1998). Poruku koju pošiljatelj želi poslati primatelju zvat ćemo otvorenim tekst (engl. *plaintext*). To može biti tekst na bilo kojem jeziku, numerički iskazan tekst ili nešto drugo. Pošiljatelj transformira otvoreni tekst pomoću unaprijed dogovorenog ključa (engl. *key*). Taj postupak zove se šifriranje, a dobiveni rezultat zove se šifrat (engl. *ciphertext*) ili kriptogram.

Ponekad nije dovoljno samo zadržati tajnost sadržaja poruke, što čini kriptografija, nego treba sakriti i samo postojanje poruke. Tehnika kojom se skriva poruka zove se steganografija. Moderna steganografija, koja koristi prednosti digitalne tehnologije, najčešće podrazumijeva skrivanje tajne poruke unutar neke multimedijske datoteke, npr. slike, audio ili video datoteke. Multimedijske datoteke u pravilu sadrže neupotrijebljene ili nevažne podatkovne prostore koje različite steganografske tehnike koriste tako da ih

[183] Ključ također može biti i predmet koji je kao takav nositelj informacije o metodi zakrivanja poruke. U antičkoj Grčkoj poruke su bile ispisane na životinjskoj koži ili platnu koje bi se potom omotalo oko štapa tačno određene visine i debljine. Taj štap predstavljao je ključ - ako bi se poruka na platnu ili koži omotala oko bilo kojeg drugog štapa, bila bi nečitljiva. U tom smislu, predmet je bio ključ.

popune s tajnim informacijama. Takve datoteke se potom mogu razmjenjivati bez da itko bude svjestan prave svrhe dotične komunikacije (CARNet, 2006).

Kako navodi Posavec, steganografija se primjenjivala u mnogo različitih oblika. Vojskovođe su znali obrijati glasniku glavu i na nju napisati poruku, te su pričekali da kosa ponovno naraste, a zatim poslali glasnika na odredište. Kinezi su poruke pisali na tankoj svili, koju bi potom smotali u kuglicu zvanu *„la wan"* i obavili voskom, a zatim bi ju glasnik sakrio u odjeću ili jednostavno progutao. Jedan od načina skrivanja poruke je bila i upotreba nevidljive tinte iz biljaka ili organskih tekućina, koja je nevidljiva kad se osuši, ali pri zagrijavanju postane smeđa. Sve metode tajnog komuniciranja bile su jako opasne jer ih se lako moglo otkriti. Prednost kriptografije je što neprijatelj ne može saznati sadržaj čak ni uhvaćene poruke (2018). Zbog toga se, uz steganografiju, počinje razvijati kriptografija koja se dijeli na klasičnu i modernu.

Međutim, da bismo razumjeli razlike između klasične i moderne kriptografije, moramo shvatiti osnovnu supstancu obje. The Concise Oxford Dictionary (2006) kriptografiju definira kao umjetnost pisanja ili rješavanja šifara. Ova bi definicija mogla biti historijski tačna, ali ne obuhvata suštinu moderne kriptografije. Prvo, fokusira se isključivo na probleme tajne komunikacije. O tome govori činjenica da definicija određuje „šifre", dok je drugdje definirana kao „sistem unaprijed dogovorenih simbola, koji se posebno koriste za osiguravanje tajnosti u prenošenju poruka". Do 20. stoljeća stvaranje dobrih šifara ili probijanje postojećih oslanjalo se na kreativnost i lične vještine. Prema Bagiću (2018) ogromne su razlike između rane klasične i moderne kriptografije s obzirom na tehnike i metode šifriranja, ali i s obzirom na komplesnost kriptograma ili šifrata. Krajem 20. stoljeća kriptografija se radikalno promenila. Polje kriptografije sada obuhvata mnogo više od elemenata tajne komunikacija, uključujući autentifikaciju poruka, digitalni potpis, protokole za razmjenu tajnih ključeva, protokole za provjeru autentičnosti, elektronske aukcije i digitalni novac (Katz i Lindell, 2007), što sve zajednički opet ne zatvara krug. Kriptografija je prešla iz umjetničke forme koja se striktno bavila tajnom komunikacija za vojsku do nauke koja pomaže u osiguranju sistema za sve ljude širom svijeta. To u velikoj mjeri znači da je postala središnja tema informatike i informacijske sigurnosti.

Generalno posmatrano, a uključujući trendove koje nameće tehničko-tehnološki razvoj, pored rizika da sadržaj poruka bude razotkriven, paralelno je rasla potreba za zadržavanjem tajnosti. To dovodi do osmišljavanja metoda kojima bi poruka na svom putovanju od pošiljatelja do primatelja došla bez da je itko s treće strane primijeti i preuzme. Tako su se vremenom osmišljavali alati 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. Nije bilo dovoljno sakriti samo fizički zapis, ukazala se potreba ka orijentisanju i na značenje sadržaja samog zapisa. Kako su smišljane metode za očuvanjem tajnosti zapisa, tako su neprestano traženi i načini probijanja, odnosno dešifriranja istih.

2. SEGMENTI HISTORIJSKOG RAZVOJA

Dugo godina je kriptografija bila ekskluzivna vojna domena. Američka agencija za nacionalnu sigurnost (NSA) i agencije iz bivšeg Sovjetskog Saveza, Engleske, Francuske, Izraela i sl., potrošili su milijarde dolara u vrlo ozbiljnu igru osiguranja sopstvene komunikacije i razotkrivanja tuđe. Privatno pojedinci[184], sa daleko manje stručnosti i budžeta, nisu mogli zaštititi vlastitu privatnost od ovih vlada (Schneier, 1996). Mehanizmi zaštite u pravilu bi trebali biti pouzdani i jednostavni za korisnike. Da li je to uvijek bio slučaj, nastojat ćemo u nastavku prikazati kroz pregled određenih najznačajnijih historijskih razvojnih perioda ove izuzetne discipline.

Već 1900. godine prije Krista, u današnjem Egiptu korišteni su hijeroglifi na nestandardan način, vjerojatno kako bi sakrili značenje od onih koji nisu znali značenje (Whitman i Mattord, 2005). Rana kriptografija bavila se isključivo pretvaranjem poruka u nečitljive grupe simbola, brojeva i/ili slika radi zaštite sadržaja same poruke tokom prenošenja poruke s jednog mjesta na drugo.

Metode, koje su se najčešće tokom historije koristile za šifriranje poruka, bile su zamjena (supstitucija[185]) i premještanje (transpozicija[186]) osnovnih elemenata teksta (slova, blokova slova, bitova). Kombinaciju ovih metoda susrećemo i danas u najmodernijim simetričnim kriptosistemima. Asimetrični kriptosistemi s javnim ključem pojavili su se tek 70-tih godina 20. stoljeća. Kod njih se za šifriranje koriste funkcije koje su "jednosmjerne" i to znači da funkcija za šifriranje može biti javna, dok samo funkcija za dešifriranje mora biti tajna. U konstrukciji jednosmjernih funkcija koriste se "teški" matematički problemi, kao što su faktorizacija velikih prirodnih brojeva, te logaritmiranje u konačnim grupama (Dujella i Maretić, 2007).

U transpozicijskim[187] šiframa slova ishodišne poruke ili otvorenog teksta mijenjaju redoslijed pojavljivanja, ali zadržavaju svoj identitet. Što je poruka opsežnija, raste i broj

---

[184] Krug korisnika kriptografije uključuje i kriminalce. Vrijeme prohibicije u SAD-u pogodovalo je usponu kriptografije u službi kriminalnog miljea. Od tada, pa do danas u FBI-u postoji jedinica za kriptoanalizu (skr. CRRU) koja se bavi razbijanjem šifri koje koriste kriminalci.

[185] U sistemu supstitucije, kratki tekstovi poruke su sistematski zamijenjeni drugim znakovima. Nakon zamjene, redoslijed temeljnog konteksta je nepromijenjen, ali isti znakovi nisu više prisutni. U najjednostavnijim sistemima zamjene, zamjena je dosljedna; dati znak otvorenog teksta uvijek prima isti zamjenski znak. Sigurniji sistemi mijenjaju zamjene tako da imaju određene ekvivalente koji se mijenjaju svaki put kada se isti znak šifrira.

[186] U sistemu transponiranja, simboli otvorenog teksta se sistemski preuređuju. Nakon prenošenja poruke, isti su znakovi još uvijek prisutni, ali redoslijed slova je promijenjen.

[187] Transpozicijsko šifriranje je klica kriptografije. Naime na njezinu početku stoji skital, prvo poznato kriptografsko pomagalo. Radi se o tehnici tajne komunikacije za koju su bila potrebna dva drvena štapa jednake duljine i debljine, tj. dva skitala – jedan bi posjedovao pošiljatelj, a drugi primatelj poruke. Pošiljatelj bi oko štapa namotao vrpcu od pergamenta ili kože i na nju okomito napisao poruku. Kada bi se vrpcu odmotalo, kriptogram bi bio zgotovljen – na njoj se mogao vidjeti samo niz naizgled nepovezanih slova. Ako je

potencijalnih kombinacija njezinih dijelova. Tako primjerice rečenica od 30 slova omogućuje više od 50 milijardi kombinacija (Lunde 2010).

Kod supstitucijskih šifri slova otvorenoga teksta mijenjaju identitet, tj. bivaju zamijenjena drugim slovima ili znakovima, ali zadržavaju redoslijed pojavljivanja. Najstarija, a možda i najglasovitija supstitucijska šifra je ona koju je Julije Cezar koristio u Galskom ratu. Upotrijebljena je zamisao o prebacivanju slova na dogovoreni broj i tako je napisana poruka. Tada bi primatelj preusmjerio slova na isti broj i jednostavno dešifrirao poruku (Taylor, 2002). Cezarova šifra nazvana je monoalfabetskom šifrom. Budući da se temelji na jednostavnom pomaku, kombinacija je onoliko koliko i slova abecede. To je vrlo malen broj i takvu je šifru relativno lako dešifrirati. Međutim, monoalfabetska šifra može se oblikovati i određenim pomacima koji neće poštovati abecedni redoslijed slova, što do vrtoglavih granica uvećava broj potencijalnih kombinacija.

U nastavku, kako u arapskom svijetu dolazi do revolucije u području matematike, paralelno se izučava i razvija kriptologija. Arapski matematičari prikupili su veliku količinu znanja iz antičkih grčkih polisa i iskoristili ga za napredak civilizacije.[188] Teorija i praksa kriptoanalize tako je započela razvijanjem frekvencijske metode**,** koja se temeljila na proučavanju frekvencijskog pojavljivanja riječi, znakova ili simbola u tekstu (Wrickson, 1998). Matematičar, astrolog, psiholog i meteorolog Al–Kindi pojašnjava da se enkriptirana poruka na poznatom jeziku razrješuje tako da se potraži neki drugi otvoreni tekst na istom jeziku dovoljno dug da se može utvrditi učestalost pojavljivanja pojedinih slova (Bagić, 2018).

Frekvencijska analiza je ponudila jedinstven, nadasve dragocjen alat svima koji su nastojali proniknuti u smisao monoalfabetskih tajnih poruka. Ona se zasniva na tezi da je učestalost pojavljivanja važan element identiteta svakog slova te da nam upravo jednom utvrđeni identiteti omogućuju prepoznavanje tih slova, čak i kada su skriveni drugim znakovima. U daljnjem razvoju frekvencijske analize, uz istraživanje mogućih veza između podjednako učestalih slova i kriptografskih simbola, uspoređivale su se i relacije između podjednako učestalih dvoslova ili troslova u jeziku poruke i dvočlanih ili tročlanih dijelova šifrata. Frekvencijska analiza je podstakla kriptografe da traže druge i drukčije, tj. sigurnije načine šifriranja.

Cezarova šifra predstavljala je jedan od najpoznatijih postupaka kriptografije. Kasnije, istaknutiji postupci su sistemi koje je osmislio Leon B. Alberti, Blaise de Vigener i Gilbert Vernam.

---

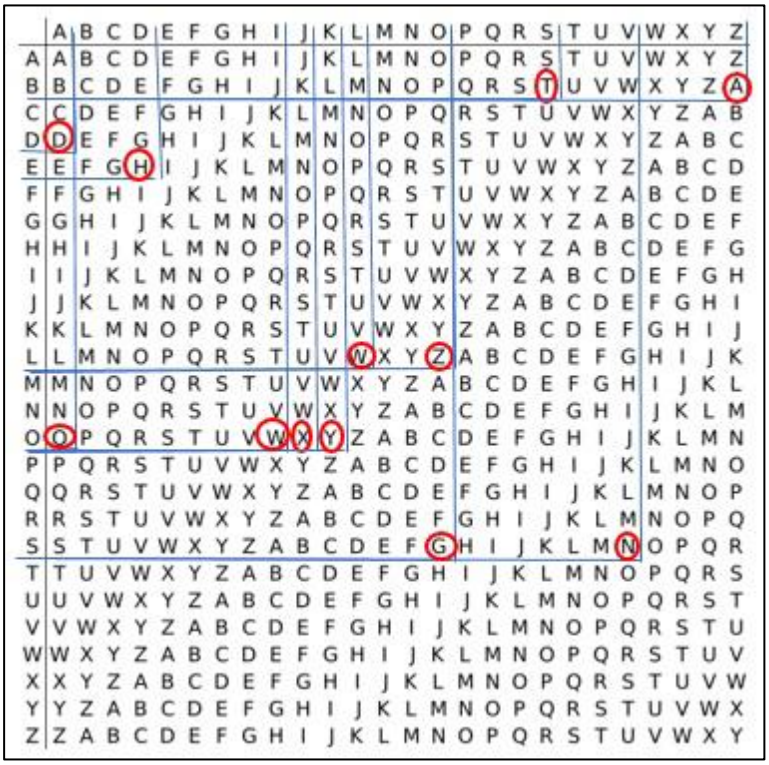
vrpca bila kožna, glasnik ju je mogao okrenuti naopako i opasati se njome. Kada bi poruka došla primatelju, on bi je namotao na svoj skital i pročitao (Bagić, 2018).

[188] Za razliku od Grka koji su se do tada bavili isključivo kriptografijom (npr. Spartanci, metodom korištenja platna omotanog oko štapa), Arapi su prvi krenuli razvijati kriptoanalizu.

Leon Battista Alberti umjesto monoalfabetske zamjene predlaže polialfabetski[189] sistem s dvije šifrarne abecede koje će oblikovati šifrat nedostupan frekvencijskoj analizi. Njegov se šifrirni brojčanik sastoji od dva diska, nepokretnog vanjskog (stabilis) na kojem je ispisana latinska abeceda bez slova H, K, J i Y te brojevi od 1 do 4, i pokretnog unutrašnjeg (mobilis) na kojemu su ispisana slova abecede prema slučajnom rasporedu i znak &. Poruka se enkriptira čas prema jednoj, čas prema drugoj abecedi, što rezultira time da isto slovo iz otvorenog teksta može biti zamijenjeno različitim slovima u šifratu. Mowry naglašava da sagovornici moraju imati identične diskove, a prije komuniciranja trebaju dogovoriti indeksno slovo u pokretnom unutrašnjem krugu (2014). Alberti je doprinio razvoju polialfabetičke supstitucije. Njegova metoda bila je upotreba dva bakrena diska koji se međusobno uklapaju. Svaka je na sebi imala upisanu abecedu. Nakon svakih nekoliko riječi, diskovi su rotirani kako bi promijenili logiku šifriranja, čime je ograničena upotreba frekvencijske analize za pucanje šifre (Cohen, 1990). Albertijev šifrarnik je nastao kao modifikacija, odnosno usavršeni postupak Cezarove šifre.

Slijedom razvoja kriptografskih postupaka, Bagić (2018) ističe da je francuski diplomat Blaise de Vigenére tokom službovanja u Italiji pomno proučio Albertieve spise, te oblikovao snažan kriptosistem koji se služi s 26 šifrarnih abeceda. Snaga ovog postupka je u činjenici da se ona služi ne jednom ili dvjema šifriranim abecedama, nego poruku enkriptira pomoću 26 abeceda, tačnije za svako slovo jednom. Prema istom autoru, punih 300 godina se vjerovalo da je kao takav posve siguran, toliko da je prozvan i neprobojnom šifrom (fr. *le chiffre indéchiffrable*). Vigenéreov kvadrat funkcionira tako da kriptograf odredi ključnu riječ (npr. SLOBODA) koja će, budući da je sedmoslovna, povezati sedam šifrarnih abeceda koje naizmjenično sudjeluju u šifriranju poruke. Škrobo (2017) u svom radu slikovito navodi da ključ pokazuje koji redak (počinje slovom iz ključa) treba upotrijebiti za šifriranje, a zatim se slovo spaja sa slovima obične abecede ispisane iznad stupca. Stoga bi početna poruka: „VOJSKADOLAZI“ nakon šifriranja glasila „NZXTYDHGWOAW“.

[189] Šifra koja jedno slovo otvorenog teksta mijenja sa više slova šifriranog teksta.



Slika 1: Vigenéreov kvadrat u kombinaciji s ključem SLOBODE (Škrobo, 2017).

Gilbert Vernam, inženjer američke kompanije Telephone & Telegraph (AT&T) radio je na poboljšanju šifre, stvarajući šifru Vernam-Vigenere 1918. godine. Njegov rad doveo je do jednokratne pločice, koja ključnu riječ koristi samo jednom, a pokazalo se da je gotovo neraskidiva (Rubin, 2008). U vrijeme Vernamovog rada, sve poruke koje se prenose preko AT&T-ovog teleprinter sistema bile su kodirane u *Baudot Code*[190], binarnom kodu u kojem kombinacija znakova i razmaka predstavlja slovo, broj ili drugi simbol (Britannica, 2020). Vernam je predložio način uvođenja izjednačavanja istom brzinom koji je smanjen suvišnim brojem simbola poruke, čime je zaštitio komunikaciju od kriptoanalitičkog napada. Uvidjelo se da se periodičnost (kao i informacije o frekvenciji i intersimbolna povezanost), na koju su se oslanjale ranije metode dešifriranja različitih Vigenèreovih sistema, može eliminirati ako se slučajna serija znakova i razmaka (tekući ključ) pomiješa s

[190] U digitalnoj telegrafiji (teleprinter, telex) standardni 5-bitni kod obično se koristi za predstavljanje znaka (slovo, broj ili interpunkcijski znak), poznat kao Baudot kod. Zvanični naziv za najnoviji telegrafski standard je ITA2 (Međunarodna telegrafska abeceda br. 2). Nadjačao ga je ASCII 1963. godine, ali i danas ga koriste amateri. Najčešći 'Baudot' kod poznat je i kao Murray kod, ili kao Baudot-Murray kôd. Standard ITA2 široko se koristi kod povijesnih šifrarskih strojeva (CryptoMuseum, 2020).

porukom tokom šifriranje da bi se dobilo ono što je poznato kao šifra niza[191] (engl. *stream cypher).*

Međutim, postojala je jedna ozbiljna slabost u Vernamovom sistemu. Zahtijevao je jedan simbol ključa za svaki simbol poruke, što je značilo da će korisnici morati unaprijed razmijeniti suviše veliki ključ, što praktično znači da su morali sigurno razmijeniti ključ ravnomjerne dužine poruke koju će na kraju poslati. Sam ključ sastojao se od probušene papirne vrpce koja se mogla automatski čitati dok su simboli upisani na tastaturi teleteksta i šifrirani za prijenos (Britannica, 2020).

Upravo je telegraf omogućio ogroman napredak u području kriptologije i kriptografije. Telegraf predstavlja uređaj za prenos kodiranih poruka. Prema Pađenu (2018) prenos skrivenih poruka postao je lakši i telegraf je omogućio nastanak elektromehaničkih enkripcijskih uređaja koji bi se koristili složenijim algoritmima za šifriranje ili dešifriranje poruka, a vrhunac ovog otkrića manifestirat će se za vrijeme Drugog svjetskog rata, izumima kao što su Enigma, SIGABA i mnogi drugi. U svojim počecima, telegraf je zahtijevao vezu između dva uređaja kako bi komunikacija bila moguća, no izumom radija omogućena je bežična komunikacija korištenjem električnih signala koje su uređaji mogli odašiljati.

Prijenos skrivenih poruka postao je lakši nego u početku, kada je trebala postojati fizička veza između dva telegrafska centra. No, loša strana je bila ta da su radio-signalu mogli pristupiti i oni koji nisu učestvovali u komunikaciji između dva operatera. Tako je došlo do potrebe za sve jačim kontramjerama koje bi spriječile pokušaje kriptoanalize presretanih radio-poruka. Ovakve novosti potaknule su na razmišljanje i donošenje novih pretpostavki o tome kako bi se kriptografija trebala shvatiti, razvijati, i na kraju krajeva koristiti. Pađen (2018) navodi da je jedan od tih teoretičara bio i Auguste Kerckhoffs, koji je u djelu "*La Cryptographie Militaire*" (fr. "Vojna kriptografija") napisao da:

a) šifrat u praksi mora biti neprobojan;
b) kriptosistem mora biti prikladan za komuniciranje;
c) ključ mora biti lako pamtljiv i lako promjenjiv;
d) šifrat mora biti moguće prenijeti telegrafom;
e) aparat za šifriranje mora biti lako prenosiv;
f) kriptografski stroj mora biti jednostavan za rukovanje.

Pored telegrafa, za revoluciju u području kriptografije u proteklom stoljeću zaslužna su upravo velika ratna zbivanja, gdje su brojni elektromehanički izumi korišteni često kao sredstvo za ostvarenje ratnog cilja i svrhe, a predstavljali su već sintezu određenih gore spomenutih realizacija različitih teorija i postupaka.

[191] Šifra kojom se šifrira čitav niz podataka.

Puno razumijevanje doprinosa kriptografije ali i same obavještajne djelatnosti uključuje mnoge događaje tokom prve polovine 20. stoljeća. Prema Tayloru (2010) uloga britanskih obavještajnih službi u ulasku Amerike u Prvi svjetski rat zbog afere sa Zimmermanovim telegramom, obavještajni neuspjeh koji je SAD uveo u Drugi svjetski rat (Pearl Harbor) i dramatični utjecaj kriptografije tokom Drugog svjetskog rata (razvoj „Enigme“) izuzetno su zanimljivi i važni slučajevi koji predstavljaju svojevrsne prekretnice u izučavanju ove teme.

Prvi svjetski rat se odvijao na teritoriju Europe, dok se neutralne Sjedinjene Američke Države zajedno s predsjednikom Thomasom Woodro Wilsonom nisu imale namjeru uplitati u sukob. To je odgovaralo građanima Amerike, zbog čega je 1917. Wilson dobio drugi mandat pod sloganom „On nas drži podalje od rata". Međutim, jedan izuzetno značajan događaj promijenit će stav cijele zemlje prema ratu, a osobito prema Njemačkoj. To je objavljivanje onoga, što je postalo poznato kao Zimmermannov telegram, nazvanog prema autoru, njemačkom ministru vanjskih poslova Arthuru Zimmermannu. Arthur Zimmermann u telegramu predlaže Meksiku savezništvo u slučaju da Sjedinjene Američke Države uđu u rat. Predlaže Meksiku da ukoliko do toga dođe, uspostavi rat sa SAD-om kako bi povratio ranije izgubljeni teritorij, te time ograniči broj američkih vojnika na evropskoj fronti. Zahvaljujući britanskim kriptoanalitičarima, taj plan je ubrzo razotkriven, a Amerika je proglasila rat. U neznanju, Nijemci su vjerovali kako je riječ o svojevrsnoj izdaji, te kako su kodovi kojima je telegram bio šifriran ostali povjerljivi. No, pogriješili su, dešifriranje Zimmermannovog telegrama bilo je najveće postignuće Prvog svjetskog rata. Zimmermanov telegram kodiran je pomoću šifrata „0075", dvodijelnog koda od 10 000 riječi i fraza s brojevima od 0000 do 9999. Brojevi su nasumično odabirani, kako bi se izbjegle analize frekvencija, te dodatno individualno kodirani jednostavnom supstitucijom. Šifrat je siguran sve dok knjiga kodova ostane tajna. Stariji kod „13040", već je ranije bio dešifriran od strane britanskih dešifranata, no kod „0075“ se smatrao pouzdanim. Međutim, Nijemci su podcijenili britanske dešifrante. Telegram su na putu za Washington presreli Britanci, a dešifrirali su ga u „Sobi 40", uredu za šifriranje, u kojem je radila nekolicina sposobnih kriptoanalitičara (Čavajda, 2017).

Neposredno prije Drugog svjetskog rata konstruišu se prve elektromehaničke mašine za šifriranje. Njemačka kriptografska mašina „*Enigma*“[192] predstavlja vjerovatno najpoznatiju svjetsku mašina za šifriranje poruka, uglavnom zbog vitalne uloge koju je odigrala tokom Drugog svjetskog rata. Pored Enigme, za sigurnu teleprinter komunikaciju (teleks) njemačka vojska je koristila i *Siemens T-52 Geheimschreiber* i *Lorenz SZ-40*[193]. Lorenz SZ-

[192] Sredinom 1930-ih njemačka vojska se očito pripremala za rat te je započela naručivanje strojeva Enigma-I u velikim količinama za *Wehrmacht* (vojsku) i *Luftwaffe* (zrakoplovne snage). Enigmu G koristi njemačka *Abwehr* (tajna služba). Za *Kriegsmarine* (njemačka mornarica) razvijen je model sličan kompatibilnom s Enigma-I. Postaje poznat kao Enigma M1 (1934), a kasnije slijedi Enigma M2 (1938) i konačno Enigma M3 (1940) (CryptoMuseum, 2020).

[193] Lorenz SZ-40/42 koristila je *Oberst-Kommando der Wehrmacht*, ili OKW (Visoka komanda njemačke vojske) za komunikaciju na najvišem nivou između Hitlera i njegovih generala. Stroj se zvao Schlüsselzusatz (SZ), što znači dodatak za šifriranje (CryptoMuseum, 2020).

40 bio je elektromehanički uređaj za šifriranje teleprinter signala i dešifriran je tokom Drugog svjetskog rata u Bletchley Park-u (CryptoMuseum, 2020). Za vrijeme Drugog svjetskog rata, Bletchley Park je bio glavni centar za kriptoanalizu, za razbijanje šifara. Alan Turing pridružio se GC&CS, prethodniku GCHQ[194] u septembru 1939. godine kako bi pomogao u pokušaju razbijanja koda tokom Drugog svjetskog rata, radeći zajedno s Gordonom Welchmanomi i drugim stručnjacima. 1940. Turing u saradnji sa poljskim kolegama dobio je na uvid komponente potrebne za dizajn *Bombe*[195].

Postoje i mnoge druge zanimljive mašine za šifriranje prikazane na slici ispod, o kojima se mnogo detaljnije može istražiti na stranici CyptoMuseum.com. WashingtonPost (2020) nudi uvid u operaciju „Rubikon" kojom su CIA i BND još od 1950-ih prisluškivali komunikaciju više od stotinu stranih vlada, tako što su im preko švicarske kompanije Crypto AG obezbjeđivale mašine za šifriranje poruka.[196] S druge strane, nisu rijetke pojave da pojedine države energiju usmjere na vlastito inoviranje kriptografskih uređaja.[197]

Slika 2: Izdvojeni kriptografski uređaji (CryptoMuseum, 2020)

Enigma je uređaj koji se sastoji od tipkovnice s 26 tipki poput pisaćeg stroja, zaslona s 26 žaruljica za prikaz šifriranog izlaza, tri mehanička rotora i električne prespojne ploče, a napaja se putem ugrađene baterije. Pritiskom na tipku kroz mrežu kontakata rotora i prespojne ploče zatvara se strujni krug i pali se odgovarajuća žaruljica koja označava šifrirano slovo (Posavec, 2018). Upotrebljavali su se višestruki diskovi za šifriranje posebno pozicionirani unutar Enigme, odakle su mogli simulirati različite šifrirane abecede, a sve

[194] Vladin štab za komunikacije Ujedinjenog kraljevstva Velike Britanije i Sjeverne Irske (engl. *Government Communications Headquarters*)
[195] Bomba je bila prva britanska kriptoanalitička mašina posebne namjene i dala je veliki doprinos u dešifriranju Enigme.
[196] „Bio je to najduži i najproduktivniji obavještajni projekt od Drugog svjetskog rata. Strane vlade plaćale su solidan novac SAD-u i Zapadnoj Njemačkoj kako bi dobile privilegiju da njihovu najtajniju komunikaciju čitaju barem dvije strane zemlje. Bio je to obavještajni potez stoljeća." (WashingtonPost, 2020).
[197] Kriptografski uređaj TelSec prvi je sklopovski kriptografski uređaj razvijen u Republici Hrvatskoj (Mreža.bug, 2020).

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 (Dsm, 2017).

Lienhard (2003) smatra da je glavna ideja njemačkog izumitelja Arthura Scherbiusa bila zamijeniti kriptografski sistem koji se koristio u Prvom svjetskom ratu, novim sigurnijim sistemom šifriranja. Već 1918. godine Arthur Scherbius i njegov prijatelj Richard Ritter osnivaju strojarsku tvrtku Scherbius & Ritter.

Lienhard nadalje pojašnjava kako je postupak izgledao. Naime, jedan od osnovnih dijelova Enigme je i premetačka jedinica koju čini rotor (engl. *scrambler*) koji predstavlja najvažniji dio stroja. Rotor je debeli disk isprepleten žicama koje određuju kako će se slova otvorenog teksta šifrirati. Šifrarna abeceda se poslije svake enkripcije mijenja, a zahvaljujući toj rotaciji, rotor stvara dvadeset i šest šifriranih abeceda. Dakle, stroj omogućava pisanje polialfabetskom šifrom. Enigma se sastojala od tri rotora i time je mogla zauzeti ukupno 17 576 položaja. Sigurnost se mogla povećati dodavanjem novih rotora, no time bi se istodobno povećavale i veličina i težina samog uredaja. Umjesto toga, Scherbius je odlučio povećati sigurnost povećanjem broja mogućih početnih postavki na dva načina: izmjenjivim rotorima i prespojnom pločom. Ona mijenja električne puteve između tipkovnice i prvog rotora, omogućujući inicijalnu zamjenu slova prije samog procesa šifriranja. Naprimjer, moguće je zamijeniti slova „B" i „F" tako da se pritiskanjem tipke „B" odašilje slovo „F" i obratno. Operator je imao šest kablova. Dakle, šest parova slova moglo je zamijeniti mjesta, a ostalih četrnaest slova ostalo je na istom položaju. Stoga, položaj rotora određuje 17 576 različitih ključeva, tri rotora mogu se zamijeniti na 6 različitih načina, te 6 parova slova od njih ukupno 26 mogu se prespojiti na prespojnoj ploči na ukupno 100 391 791 500 različitih načina. Množeći dobivene varijacije dobivamo ukupan broj ključeva od 10 000 000 000 000 000, što je fascinantan broj varijacija (2003).

3. OSNOVE RAZUMIJEVANJA SAVREMENIH KRIPTOGRAFSKIH POSTUPAKA

Određeni ranije prikazani postupci su poslužili kao odskočna daska za razvoj modernih sistema šifriranja. Dujella i Maretić (2007) ističu 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 kojem je poruka poslana zna ključ kojim je šifrirana poruka te može dešifrirati šifrat i učiniti tekst ponovno razumljivim. 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 je može samo pridruženi privatni ključ.

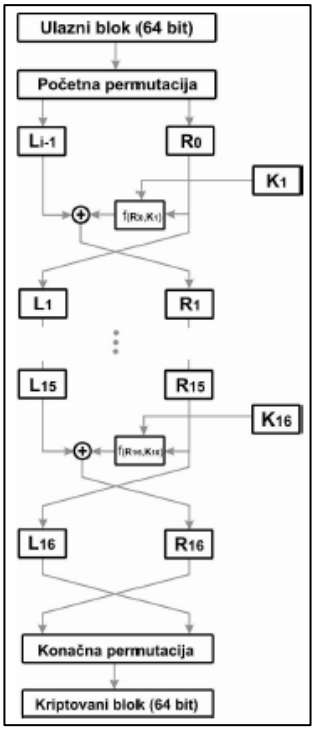
Također, Kuhn (2001) objašnjava osnovne vrste sistema šifriranja u savremenoj upotrebi: simetrični („privatni") i asimetrični („javni") sistem. U simetričnom sistemu koristi se isti ključ za obje funkcije, i za šifriranje i dešifriranje dokumenta. Čest primjer ovog oblika šifriranja je funkcija zaštite šifre obrađivača teksta, kao što je Microsoft Word, pomoću kojeg korisnik može zaključati dokument, a zatim ako isti dokument dostavi kolegi, isti će morati upotrijebiti identičnu šifru za otvaranje dokumenta. Ovaj oblik šifriranja je dovoljan za zaštitu ličnih dokumenata, gdje korisnik to želi kako bi spriječio da svi osim njega ne mogu pristupiti određenim datotekama. Međutim, simetrična enkripcija problematična je kada čovjek želi sigurno komunicirati s drugima, pri čemu stvara mogućnost da se prilikom razmjene ključeva sama komunikacija vrši preko nesigurnog kanala, čime se narušava sigurnost komunikacije prije nego što je do samog šifriranja uopće došlo. Kriptografija omogućava zaštitu osjetljivih podataka, bilo u pohrani ili u komunikaciji, i predstavlja nužnu pretpostavku bilo kojeg sigurnog e-poslovanja ili elektronskog komunikacijskog sistema (uključujući sigurnu e-poštu i glasovnu komunikaciju). Prema Posavec (2018) najpoznatiji algoritmi simetričnih kriptosistema koji se danas koriste su: DES, 3DES, DES-CBC, IDEA, RC5, RC6, AES.

Početkom šezdesetih godina prošlog veka, kompanija IBM je pokrenula istraživački projekat u cilju zaštite podataka pod nazivom *Lucifer*. Ovaj projekat okončan je 1971. godine i Lucifer je bio prvi šifrat sa blokovima veličine 64 bita koji je koristio ključ od 128 bita. Kompanija je kasnije komercijalizovala ovaj način kodiranja i nazvala ga DES (engl. *Data Encryption Standard*). 1976. godine DES je prihvaćen kao federalni standard za enkripciju podataka i korišten je u komunikacijama Američke vlade. DES je narednih dvadesetak godina bio najviše korišteni standard na svijetu. Tokom eksploatacije, DES standard je bio modifikovan i unapređivan svakih pet godina. Naslijedio ga je 2001. god. AES (engl. *Advanced Encryption Standard*), također poznat pod nazivom *Rijndael* algoritam. U poređenju sa DES, novi algoritam je bio dosta napredniji po pitanju sigurnosti podataka. Danas, DES algoritam i dalje koristi veliki broj organizacija u svijetu čime je nastavio život pružajući zaštitu u mrežnim komunikacijama, skladištenjima podataka ali i sistemima za kontrolu pristupa (Rhee, 2003).

DES suštinski predstavlja simetrični algoritam za kriptovanje blokovskog tipa, odnosno predstavlja direktnu upotrebu blok-šifre[198] (ECB mod). Kao ulaz u algoritam se koristi blok od 64-bita izvornog teksta i 56-bitni ključ. Izlaz iz algoritma je 64-bitni kriptovan tekst koji se dobija nakon 16 iteracija koje se sastoje od identičnih operacija. Ključ od 56 bita se formira od inicijalnog 64-bitnog ključa informacije ignorisanjem svakog 8 bita, tj.

[198] Šifra kojom se šifrira blok podataka fiksne dužine.

odsjecanjem ukupno 8 bitova. Na slici u nastavku prikazan je izgled DES algoritma za kriptovanje.[199]



Shema 1: DES algoritam (Buchman, 2002).

Problem s razmjenom ključeva riješen je 1970-ih pojavom asimetričnih ključnih sistema. Dok se u simetričnom sistemu ključeva isti ključ koristi za obje funkcije, u asimetričnom sistemu ključeva, jedan je ključ - *javni ključ* i koristi se za šifriranje, a za dešifriranje se koristi zasebni ključ - *privatni ključ* (Black, 2001). Vetter ističe da su i javni i privatni ključ matematički povezani (2010). Javni ključ korisnika može se učiniti općenito dostupnim (npr. objavljivanjem na web stranici) i svako ko želi korisniku poslati šifrirani dokument može preuzeti javni ključ i koristiti ga za šifriranje poruke. Međutim, poruka tada ne može

[199] Buchman (2002) objašnjava da se kriptovanje pomoću DES algoritma sprovodi u nekoliko koraka. Prvo se bitovi ulaznog bloka dužine 64 bita permutuju početnom permutacijom. Radi se o permutaciji koja vrši zamjenu bitova. Permutovan ulazni blok dijeli na dva dijela od po 32 bita, lijevi *L*i-1 i desni *R*0 deo. Nad desnim dijelom bloka se obavlja funkcija *f* (*R*0,*K*1) koja generiše 32-bitni rezultat. Nova 32-bitna vrijednost *R*1 se koristi za dalje operacije. Za lijevi dio *L*1 koristi se vrijednost *R*0 iz prethodne iteracije. Nakon ponavljanja 16 istovjetnih koraka, blokovi međusobno mijenjaju mjesta te se spajaju. Na kraju se obavlja konačna permutacija koja je inverzna početnoj. Konačna dobijena 64-bitna vrijednost čini kriptovani blok podataka.

biti dešifrovana od strane bilo koga - uključujući i originalnog pošiljaoca poruke, osim ako nema korisnikov privatni ključ, a ovaj ključ korisnik čuva (Black, 2001).

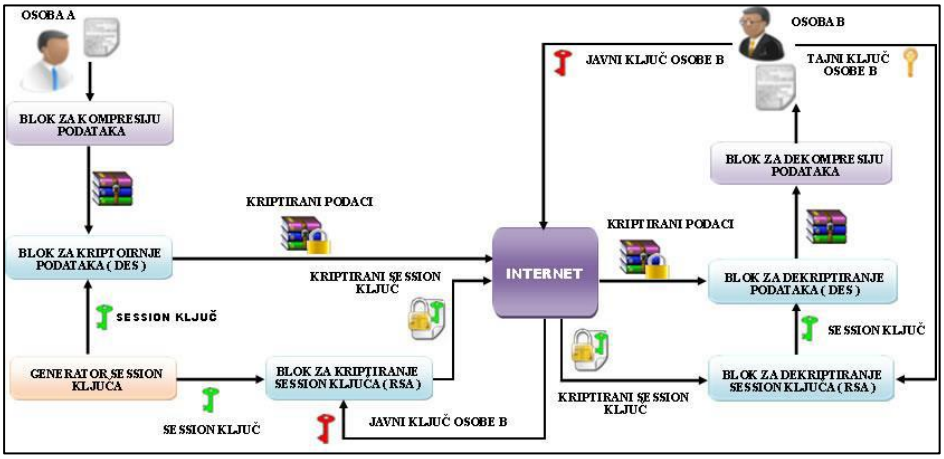
Godine 1977. dizajniran je RSA algoritam koji primjenjuje metodu šifriranja javnim ključem, te podržava šifriranje poruka i identifikaciju korisnika potrebnu za osiguravanje autentičnosti. Autori su američki kriptograf Ron Rivest, izraelski kriptograf Adi Shamir, te američki kriptograf Leonard Adleman po kojima je algoritam i dobio ime (Posavec, 2018). Prema istom autoru, najpoznatiji asimetrični algoritmi su RSA, Diffie-Hellman, ElGamal, Eliptične krivulje, Rabin.

Asimetrična kriptografija otvorila je potpuno nove vidike za šifriranje i olakšala razvoj mnogih aspekata modernog života. Sposobnost pokretanja sigurnog komunikacijskog kanala između dvije strane koje nikad dotad nisu komunicirale omogućio je, recimo, rast svih oblika e-trgovine na Internetu. Asimetrična kriptografija je u osnovi protokola *Hypertext Transfer Protocol - Secure* (u nastavku: HTTPS), koji omogućava sigurnu komunikaciju između poslužitelja i klijenata na cijelom svijetu. Bez asimetrične kriptografije sigurna komunikacija s dobavljačima e-trgovine ili dostupnost usluga internetskog bankarstva bile bi nezamislive kategorije nedostupne korisnicima.

Vetter (2010) naglašava da se sistemi šifriranja koji se danas koriste mogu učiniti izuzetno sigurnim, gdje jačinu sistema šifriranja karakteriziraju tri faktora: sigurnost šifrata, sigurnost osnovnog algoritma i dužina ključa. Sigurnost šifrata predstavlja odgovornost korisnika, i stoga je obično najmanje sigurna komponenta kriptografskog sistema.

Upotreba zajedničkog javnog ključa i privatnog ključa kojeg posjeduje samo pošiljalac danas se koristi kao oblik asimetrične enkripcije. Jedna od upotreba ove metode je da pošiljalac koristi privatni ključ za šifriranje poruke, a zatim svako ko primi poruku koristi javni ključ za dešifriranje. Na taj način primalac zna od koga je poruka morala doći. Prema Whitmanu i Mattordu (2005) ova metoda čini okosnicu digitalnog potpisa. Problemi nastaju kada komunikacija između više organizacija zahtijeva upotrebu mnogih javnih ključeva i kada se ne zna koji koristiti. Bez obzira koja metoda se koristi, kombinacija metoda koja se primjenjuju jedna za drugom će dati najbolji rezultat.

Posavec (2018) slikovito objašnjava hibridni postupak šifriranja. Osoba A izvornu poruku komprimira, radi lakšeg i bržeg slanja te dodatne zaštite. Takvu poruku šifrira nekom od metoda simetričnog šifriranja pomoću simetričnog ključa. Generiranje simetričnog ključa vrši generator pseudo-slučajnog broja u kombinaciji sa raznim korisničkim podacima unesenim tokom procesa generiranja. Tako dobiveni simetrični ključ se kriptira nekom od metoda asimetričnih algoritama pomoću javnog ključa osobe kojoj se poruka šalje te zajedno sa kriptiranom porukom šalje primaocu poruke. Dekriptiranje se vrši obrnutim postupkom. Osoba koja je primila poruku prvo dekriptira primljenu poruku koja sadrži simetrični ključ svojim tajnim ključem. Na taj način dolazi do simetričnog ključa kojim je kriptiran izvorni tekst. Kod hibridnih sistema koristi se duplo kriptiranje i tri ključa: javni i tajni ključ osobe kojoj se šalje poruka i simetrični ključ osobe koja šalje poruku.



Shema 2: Hibridni postupak šifriranja (Posavec, 2018).

Pobrojani postupci se koriste svuda u računarskim sistemima: za zaštitu pohranjenih podataka, u radu aplikacija, pri pristupu računarskim sistemima, te u mrežnim komunikacijama. U mrežnim komunikacijama koristi se već na drugom mrežnom sloju (WEP, WPA/WPA2) te na trećem i višim slojevima (IPSec, SSH, SSL, Kerberos, Radius, PGP, GPG). Za zaštitu podataka, pohranjenih na digitalnom mediju ili tokom prenosa komunikacijskim kanalom koriste se brojni algoritmi: RC4, IDEA, DES, 3DES, AES. Za zaštitu šifri, programskih aplikacija, a ponekad i podataka, koriste se hashing algoritmi koji daju jedinstveni, kratki "potpis" određenoj skupini podataka: MD5, Whirlpool, SHA-1, SHA-2 (CARNet, 2008).

4. MOGUĆNOSTI I VRSTE KRIPTOANALITIČKOG NAPADA

Kriptografija razvija algoritme koji trebaju osigurati povjerljivost i/ili tajnost, autentifikaciju i cjelovitost podataka. U načelu se zasnivaju na nekoj tajni, koju najčešće zovemo ključem i/ili posebnoj matematičkoj funkciji iskazanoj u vidu algoritma kojeg zovemo šifrom. Smisao kriptografije je sakriti otvoreni tekst (ili ključ, ili oboje) od prisluškivača[200]. Pretpostavlja se da prisluškivači imaju potpuni pristup komunikaciji između pošiljatelja i primatelja. Kriptoanaliza je upravo obrnuti napor, usmjeren na dešifrovanje tj. vraćanje kriptiranog sadržaja u otvoreni, čitljivi oblik. Prema Schneieru (1996) to je nauka o vraćanju otvorenog teksta poruke bez pristupa ključu. Uspješna kriptoanaliza može vratiti otvoreni tekst ili ključ. Također može pronaći slabosti u kriptosistemu koje na kraju vode do prethodnih rezultata. Kriptoanaliza nastoji dati rješenja u slučaju kad nemamo ključ ili šifru ili oboje. Prema tome, vodi se uvijek prisutan iscrpljujući rovovski rat između

[200] Često se nazivaju i protivnicima, napadačima, presretačima ili jednostavno neprijateljima.

napadača (kriptoanalitičara) i dizajnera (kriptografa). Pokušaj kriptoanalize naziva se napadom. Nisu rijetki slučajevi da se naruče napadi na sistem da bi se pokazala njegova slabost.

Temeljna pretpostavka u kriptoanalizi definisana od strane nizozemca A. Kerckhoffsa u devetnaestom stoljeću ističe da tajna mora biti u potpunosti u ključu. Kerckhoffs pretpostavlja da kriptoanalitičar zna sve detalje kriptografskog algoritma i postupak implementacije, što znači da je u određenoj mjeri posljedično i sigurnost takvog sistema ugrožena.

Prema Schneieru pretpostavka da kriptoanalitičar ima potpuno znanje o algoritmu šifriranja koji se koristi, predstavlja zajedničku kategoriju svim napadima (1996). Stoga, kategorizira nekoliko vrsta napada:

1. **Napad šifrata**. Kriptoanalitičar ima šifrat od nekoliko poruka, koje su sve kriptirane pomoću istog enkripcijskog algoritma. Zadatak kriptoanalitičara je da povrati otvoreni tekst što većeg broja poruka, ili još bolje da utvrdi ključ (ili ključeve) koji se koristio za kriptiranje tih poruka, kako bi se dekriptirale ostale poruke kriptirane istim ključevima.
2. **Napad poznatog otvorenog teksta.** Kriptoanalitičar ima pristup ne samo šifratu nekoliko poruka, već i otvorenom tekstu tih poruka. Njegov je zadatak izvući ključ (ključeve) koji se koristi za kriptiranje poruka ili algoritam za dekriptiranje novih poruka kriptiranih istim ključem (ili ključevima).
3. **Napad izabranog otvorenog teksta**. Kriptoanalitičar ne samo da ima pristup šifratu i otvorenom tekstu za nekoliko poruka, već također bira koji se otvoreni tekst kriptira. Ovo je snažnije od napada poznatog otvorenog teksta, jer kriptoanalitičar može izabrati određene blokove otvorenog teksta za kriptiranje, one koji mogu pružiti više informacija o ključu. Njegov je zadatak izvući ključ (ili ključeve) koji se koristi za kriptiranje poruka ili algoritam za dekriptiranje novih poruka kriptiranih istim ključem (ili ključevima).
4. **Napad prilagodljivog izabranog otvorenog teksta**. Ovo je poseban slučaj napada izabranog otvorenog teksta. Kriptoanalitičar ne samo da može izabrati otvoreni tekst koji je šifriran, već također može izmijeniti svoj izbor na osnovu rezultata prethodne enkripcije. U napadu izabranog otvorenog teksta kriptoanalitičar može samo odabrati jedan veliki blok otvorenog teksta za kriptiranje; u napadu prilagodljivog izabranog otvorenog teksta, on može odabrati manji blok otvorenog teksta, a zatim odabrati drugi na osnovu rezultata prvog, i tako dalje.
5. **Napad izabranog šifrata.** Kriptoanalitičar može izabrati različite šifrate za dešifriranje i ima pristup dekriptiranom otvorenom tekstu. Naprimjer, kriptanalitičar ima pristup neprobojnoj kutiji koja automatski dekriptira. Njegov je posao izvući ključ. Ovaj napad prvenstveno se odnosi na algoritme javnih ključeva. Napad izabranog šifrata ponekad je učinkovit i protiv simetričnog algoritma.
6. **Napad ključa.** Ovaj napad ne znači da kriptoanalitičar može odabrati ključ; znači da ima neko znanje o odnosu između različitih ključeva.

7. **Kriptoanaliza prijetnjom**. Kriptoanalitičar prijeti, ucjenjuje ili muči nekoga dok mu ne otkrije ključ. Podmićivanje se ponekad naziva napadom kupovine ključa.

Nije rijetko da kriptoanalitičar dobije šifrat u otvorenom obliku ili da podmiti nekoga da šifrira odabranu poruku. Mnoge poruke imaju standardne početke i završetke koji bi mogli biti poznati kriptoanalitičaru. Schneier naglašava da su napadi poznatog otvorenog teksta (pa čak i napadi izabranog otvorenog teksta) uspješno korišteni i protiv Nijemaca i Japanaca[201] tokom Drugog svjetskog rata.

5. OSNOVNE KARAKTERISTIKE I ULOGA KRIPTOGRAFIJE NA PRIMJERU KORIŠTENJA INTERNET PRETRAŽIVAČA I MOBILNOG TELEFONA

Prema Dooley (2018) iz kriptografske perspektive, najvažniji protokol na world wide webu je HTTPS (engl. *HyperText Transfer Protocol-Secure*). Kada web stranica koristi https: // prefiks sa URL-a (engl. *Uniform Resource Locator)*, to znači da bi preglednik trebao koristiti HTTPS protokol ali i šifrirati sav promet između pretraživača i web servera. HTTPS obično koristi jedan od dva kriptografska algoritma za kriptiranje prometa, TLS (engl. *Transport Layer Security*) ili SSL (engl. Secure Sockets Layer). Izvorna svrha HTTPS-a bila je olakšavanje komercijalnih transakcija putem svjetske mreže, ali od 2010. godine njegova upotreba raste kako bi se osigurala privatnost za sve komunikacije putem Interneta.

Kada browser želi uspostaviti vezu s web serverom, već tada započinje djelovanje TLS protokola. Prema riječima Dooleya (2018) unutar tog procesa odvijaju se sljedeće operacije:

1. Browser se povezuje na server i šalje zahtjev za vezu i spisak šifrarnih paketa (javni ključ, simetrične šifre i hash funkciju koju browser može koristiti);
2. Server bira šifrirani paket i šalje browseru poruku koja mu govori koji paket treba koristiti;
3. Server tada klijent browseru šalje svoj digitalni certifikat koji sadrži njegovo ime, vezu sa autoritetom certifikata i serverov javni ključ za šifriranje;
4. Klijent izvršava algoritam provjere valjanosti da provjeri jesu li ime i ključ servera tačni;

[201] Algoritam japanskog Purplea, podlegao je najjednostavnijim metodama kriptoanalize, kao što su *frekvencijska analiza* i *brute force* (engl. sirova sila). Koračni prekidač pokazao se vrlo predvidljivim, jer je nakon svakog 25. pritiska tipke (prilikom čega je svakim pritiskom teoretski nastajala nova abeceda) došlo do ponavljanja procesa. Cikličko ponavljanje algoritma bila je najveća mana stroja (Pađen, 2018).

5. Ako je certifikat servera potvrđen, tada će klijent započeti postupak generiranja ključa sesije za sistem simetričnog šifriranja. Da bi to učinili, klijent postupa na jedan od dva moguća načina:

a) Generira slučajni broj i kriptira ga serverovim javnim ključem za šifriranje. Onda klijent šalje šifrirani broj serveru. Server i klijent će tada koristiti nasumični broj za generiranje istog simetričnog ključa za šifriranje za odabrani simetrični šifrirani sistem.
b) Klijent i server koriste Diffie-Hellman algoritam za razmjenu ključeva da bi generirali simetrični ključ sesije.

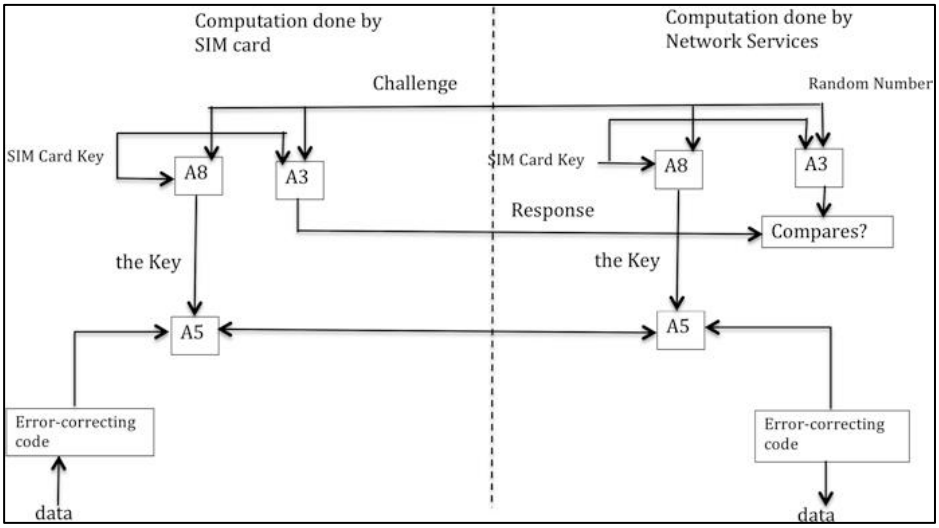
U ovom trenutku i klijent i server imaju isti simetrični šifrat ključa i započinju osigurani dio veze. Koristit će odabrani simetrični algoritam za svu komunikaciju dok veza ne bude gotova. U TLS je uključeno nekoliko sistema šifriranja javnih ključeva, uključujući RSA i Diffie-Hellman algoritam. Za simetrične algoritme, izbor uključuje AES, Camellia i ARIA, a svi koriste ili 128-bitne ili 256-bitne ključeve. Nakon uspostavljanja veze, sav se promet između browsera i web servera šifrira (Dooley, 2018).

Ova tehnika korištenja kriptografskog sistema javnog ključa i sekvence rukovanja radi uspostavljanja mrežne veze i dijeljenja simetričnog ključa, a zatim korištenja simetričnog ključa za sve preostale komunikacijske prijenose, funkcionira kao i svaka web lokacija za elektronsku trgovinu na Internetu. Svi mi koristimo šifriranje, iako toga često nismo svjesni, svaki put kada koristimo Internet za kupovinu knjige ili kada trebamo usluge internet bankarstva. Šifriranje omogućava slanje podataka o kreditnoj kartici i ostalih osjetljivih ličnih podataka putem Interneta bez otkrivanja tih podataka.

Šta se praktično dešava sa našim mobilnim telefonom? U mobilnom telefonu zapravo postoje dva „radija“. Prvi je radio koji pruža uslugu mobilne telefonije i podataka, dok je drugi radio koji će uređaj povezati s bežičnom lokalnom mrežom, a time i s Internetom (postoji mogućnost da se mobilni telefon poveže putem Bluetooth standarda kratkog dometa, no isti nije u fokusu ovog primjera).

Brookson (1994) navodi da globalni sistem za mobilne komunikacije (GSM) predstavlja najčešće korišteni digitalni protokol mobilne telefonije na svijetu. GSM postavlja pravila po kojima se mobilni telefoni povezuju s baznim stanicama mobilne telefonije, a potom i na globalnu telefonsku mrežu. GSM omogućuje šifriranu komunikaciju između mobilnog telefona i mobilne bazne stanice na koju je spojen. Iako GSM ne uključuje protokole podataka za mobilnu uslugu podataka od 1G do 4G (LTE), ti su protokoli usko povezani sa GSM-om. GSM je prvi put postao evropski standard 1987. godine i od tada se proširio po cijelom svijetu. U GSM sistemu postoje tri različita kriptografska algoritma koja omogućuju mobilnom telefonu da uspostavi vezu s mrežom, a zatim da prenosi podatke u obliku šifriranog glasa ili paketa podataka. Ova tri algoritma obavljaju tri različite funkcije: provjeru autentičnosti, stvaranje ključeva i enkripciju podataka. Prva dva algoritma, nazvana A3 i A8, pohranjena su na SIM kartici GSM telefona, dok je treći algoritam, A5

implementiran u hardveru samog telefona. Prema Dooleyu (2018) njihov odnos prikazan je na slici ispod.



Shema 3: Postupak provjere autentičnosti, stvaranja ključeva i enkripcija podataka u GSM sistemu (Dooley, 2018).

Kada se GSM mobilni telefon pokušava povezati s mrežom, u procesu autentifikacije uključene su dvije stvari, algoritam provjere autentičnosti, nazvan A3, i jedinstvena riječ spremljena na SIM kartici koja identificira telefon. Dooley (2018) prikazuje da postupak provjere autentičnosti podrazumjeva sljedeće korake:

1. Mobilni telefon pita mrežu da se pridruži. Kao dio zahtjeva, serveru šalje jedinstveni matični broj (koji se zove IMEI ili Međunarodni identifikacijski broj mobilne opreme).
2. Mrežni server generira nasumični broj i šalje ga telefonu kao "izazov."
3. Telefon koristi nasumični broj, ključnu riječ, i algoritam A3 i generira šifrirani "odgovor" koji šalje serveru.
4. Server također koristi algoritam A3, ključnu riječ telefona (koju dobiva od telefonske kompanije u kojoj korisnik ima uslugu, koristeći IMEI) i nasumični broj za generisanje šifrirane poruke.
5. Server zatim uspoređuje dvije šifrirane poruke i ako se podudaraju, uspostavlja vezu s mobilnim telefonom.

Dok mobilni telefon i mrežni poslužitelj „komuniciraju“, telefon i server također koriste nasumični broj i ključ SIM kartice zajedno s algoritmom generacije ključeva A8 za

generiranje jedinstvenog simetričnog ključa. Ovaj se ključ prosljeđuje trećem algoritmu A5[202] gdje se koristi za šifriranje prijenosa glasa i podataka nakon provjere autentičnosti veze. Niko od pružatelja usluga ili proizvođača mobilnih telefona ne otkriva koje algoritme koristi za provjeru autentičnosti i prijenos podataka.

UMJESTO ZAKLJUČKA

U ovoj specifičnoj genezi svog razvoja, kriptografija je od svojih najranijih pseudo-oblika, datiranih hiljadama godina prije nove ere, napredovala sve do kompleksne discipline u službi zaštite informacija. Osnovna kriptografska znanja su danas javno dostupna, što uključuje i postupke za mnoge moderne kriptografske metode. Neminovno je da će se ovaj trend razvitka nastaviti jer svaki primjer „neprobojne šifre" sazna svoj rok trajanja kada mu ga kriptoanaliza dodijeli.

Nemojmo zaboraviti da je kriptografija ključna za siguran rad gotovo svih organizacija i za zaštitu privatnosti pojedinaca širom svijeta. Unatoč važnosti, i uprkos činjenici da mnoge zemlje postavljaju snažna ograničenja za upotrebu kriptografija, mnogo organizacija zanemaruje razmatranje regulatornih implikacija za kriptografiju koju koriste. Sve međunarodno aktivne kompanije moraju poduzeti korake kako bi osigurali da su svi u skladu s propisima šifriranja zemlje u kojima posluju, a istovremeno moraju usvojiti najbolje prakse za maksimiziranje informacijske sigurnosti uprkos ograničenjima na korištenje kriptografije (Saper, 2013).

U prethodnom dijelu ponudili smo čitalačkoj publici osnovne informacije i kategorizacije koje mogu poslužiti kao osnova za dalja istraživanja ove izuzetno kompleksne discipline.

Razumljivo je da apsolutna zaštita bilo kojeg odabranog kriptosistema ne postoji, stoga preporučujemo da se više pažnje posveti čovjeku kao prenosiocu informacije i njegovoj povjerljivosti i lojalnosti. Također, smatramo da se treba potaknuti ulaganje u istraživanje ove oblasti i generalno u razvoj kriptografskih sistema prema svim sektorima i korisnicima za zaštitu podataka u mirovanju ali i u tranzitu.

---

[202] Zapravo postoje četiri A5 algoritma. A5/0 uopće nije algoritam, samo pokazuje da preneseni paketi podataka nisu šifrirani. A5/1 je 64-bitni algoritam šifriranja protoka koji šifrira i šalje pakete podataka (i prima i dešifrira pakete). A5/2 je slabija verzija A5/1 i izvorno se koristio za mobilne telefone koji su se prodavali izvan Europe. Od 2009. godine i A5/1 i A5/2 zastarjeli su jer se pokazalo da imaju ozbiljne kriptografske nedostatke koji ih ne čine sigurnima. Novi algoritam A5/3 uveden je 2009. godine i zasnovan je na verziji algoritma blok šifriranja nazvanoj KASUMI (koji je sam izveden iz algoritma Mitsubishi Electric Corporation pod nazivom MISTY) i namijenjen je da zamjeni A5/1 i A5/2 (Dunkelman, Keller i Shamir, 2010).

LITERATURA

1. Bagić, K. (2018). Kriptogram-vrlo kratak uvod, Croatica, XLII 62: 343–364
2. Bauer, F. (2002). Decrypted Secrets: Methods and Maxims of Cryptology. Treće izdanje, Berlin: Springer.
3. Black, T.E. (2001). Note, Taking Account of the World As It Will Be: The Shifting Course of U.S. Encryption Policy, 53 FED. COMM. L.J. 289, 292.
4. Brookson, C. (1994). GSM Security and Encryption. URL: http://brookson.com/ pristupljeno 20.11.2019. godine.
5. Buchmann, J.A. (2002). "Introduction to Cryptography", Technical University Dramstadt, New York.
6. CARnet. Kriptografija u službi napadača. URL: https://www.cert.hr/wp-content/uploads/2019/04/CCERT-PUBDOC-2008-04-226.pdf pristupljeno 30.11.2019.
7. CARNet: Steganografija, CCERT-PUBDOC-2006-04-154, URL: https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2006-04-154.pdf, pristupljeno 30.11.2019.
8. Cohen, F (1990). A short history of cryptography. URL: http://www.all.net/books/ip/Chap2-1.html pristupljeno 27.11.2019. godine.
9. Čavajda, A. (2017). Kriptografija u Prvom i Drugom svjetskom ratu. Osijek: Sveučilište J.J.Strossmayera u Osijeku.
10. Dooley, J.F. (2018). History of Cryptography and Cryptanalysis, History of Computing. Springer International Publishing AG, part of Springer Nature
11. Dujella, A. i Maretić M. (2007). Kriptografija. Zagreb: Element.
12. Dunkelman, O., Keller, N. and Shamir, A. (2010). A Practical-Time Attack on the A5/3 Cryptosystem Used in Third Generation GSM Telephony.
13. Group of authors (2006). Concise Oxford English Dictionary.Eleventh edition Hardcover
14. Katz J. and Lindell Y. (2007). Introduction to Modern Cryptography, CRC PRESS Boca Raton London New York Washington, D.C.
15. Kuhn, D. R. (2001). Nat'l inst. of standards & tech., introduction to public key technology and the federal pki infrastructure 10, URL: http://csrc.nist.gov/publications/nistpubs/800-32/sp800-32.pdf. pristupljeno 5.12.2019.
16. Lienhard, J. H. (2003). The Engines of Our Ingenuity, OUP USA.
17. Lunde, P. (2010). Tajne kodova. Razumijevanje svijeta skrivenih poruka. Prev.: D. Biličić. Zagreb: Znanje.
18. Majić, M. (2014). Šifrirne naprave. Osijek: Sveučilište J.J.Strossmayera u Osijeku.
19. Mathai, J. (2017). History of Computer Cryptography and Secrecy Systems. URL: http://www.dsm.fordham.edu/~mathai/crypto.html pristupljeno 2.12.2019.
20. Mowry, D. P. (2014). German Cipher Machines of World War 2, National Security Agency.
21. Pađen, L. (2018). Kriptologija u teoriji i praksi u prvoj polovici dvadesetog stoljeća, Zagreb: Filozofski fakultet.

22. Pawlan, M. (1998). Cryptography: the ancient art of secret messages. URL: http://www.pawlan.com/Monica/crypto/ pristupljeno 27.11.2019. godine.
23. Posavec, E. (2018). Zaštita podataka u kritičnim područjima ljudske djelatnosti-suvremene kriptografske metode. Karlovac: Veleučilište u Karlovcu.
24. Reardon, K. K. (1998). Interpersonalna komunikacija: gdje se misli susreću. Zagreb: Alinea,
25. Rhee, M. Y. (2003). "Internet Security Cryptographic principles, algorithms and protocols", School of Electrical and Computer Engineering Seoul, John Wiley & Sons, Wiltshire.
26. Rouse, M. J. i Rouse S. (2005). Poslovne komunikacije. Zagreb: Masmedia.
27. Rubin, J. (2008). Vigenere Cipher. URL://www.juliantrubin.com/encyclopedia/mathematics/vigenere_cipher.html pristupljeno 22.11.2019. godine.
28. Saper, N. (2013). International Cryptography Regulation and the Global Information Economy, Northwestern Journal of Technology and Intellectual Property, Volume 11 | Issue 7, Article 5.
29. Schneier, B. (1996). Applied Cryptography: Protocols, Algorithms, and Source Code in C. Vol. 2. Whole. New York: Wiley.
30. Singh, S. (2003). Šifre. Kratka povijest kriptografije. Zagreb: Mozaik knjiga.
31. Škrobo, M. (2017). Razumijevanje tajnih poruka. Osijek: Sveučilište J.J.Strossmayera u Osijeku.
32. Taylor, K. (2002). Number theory 1. URL: http://math.usask.ca/encryption/lessons/lesson00/page1.html pristupljeno 15.11.2019. godine.
33. Taylor, S. A. (2010). „Uloga obavještajne djelatnosti u nacionalnoj sigurnsoti", U suvremene sigurnosne studije, Alan Collins. Zagreb, Centar za međunarodne i sigurnosne studije Fakkulteta političkih znanosti Sveučilišta u Zagrebu.
34. Tilborg, Henk C.A. (2005). "Encyclopedia of Cryptography and Security", University of Technology Eindhoven.
35. Vetter, G. (2010). Patenting Cryptographic Technology, 84 CHI.-KENT L. REV. 757, 761-62.
36. Whitman, M. & Mattord, H. (2005). Principles of information security. University of Phoenix, Custom Edition e-text. Thomson Learning, Inc., rEsource, CMGT/432
37. Wrixon, F. (1998). Codes, Ciphers & Other Cryptic & Clandestine Communication: Making and Breaking Secret Messages from Hieroglyphs to the Internet. New York: Black Dog & Leventhal Publishers Inc.
38. https://www.britannica.com/topic/Vernam-Vigenere-cipher pristupljeno 15.1.2020. godine.
39. https://www.cryptomuseum.com/crypto/baudot.htm pristupljeno 15.1.2020. godine.
40. https://mreza.bug.hr/prvi-sklopovski-kriptografski-uredaj-razvijen-u-rh/ pristupljeno 15.1.2020. godine.

41. https://www.washingtonpost.com/graphics/2020/world/national-security/cia-crypto-encryption-machines-espionage/ pristupljeno 15.2.2020. godine.

Prilozi:

- Slika 1: Vigenéreov kvadrat u kombinaciji s ključem SLOBODE
- Slika 2: Izdvojeni kriptografski uređaji
- Shema 1: DES algoritam
- Shema 2: Hibridni postupak šifriranja
- Shema 3: Postupak provjere autentičnosti, stvaranja ključeva i enkripcija podataka u GSM sistemu