Filozofski fakultet Sveučilišta u Zagrebu
Odsjek za informacijske i komunikacijske znanosti
2017/2018.

Maja Mikac

Kako je Colossusom razbijena Lorenzova šifra

Završni rad

Mentorica: dr. sc. Vjera Lopina

Zagreb, 2018.

Sadržaj

Sažetak

Nepotrebno je naglašavati kako je tajnost informacija postala neizostavan dio komunikacije modernoga doba, a još je manje potrebno isticati da je krajnje bitna za vrijeme situacija u kojima nerijetko o sadržaju poruke ovise ljudski životi. Jedna od takvih situacija je i ratno stanje. Ovaj rad bavit će se kriptoanalizom Lorenzove šifre – ponekad u sjeni mnogo poznatije Enigme – koju je koristila njemačka vojska tijekom Drugog svjetskog rata. Prikazat će i objasniti strukturu i razvoj samog uređaja za šifriranje Lorenz SZ40 te britanskog kompjutera Colossus koji se koristio za razbijanje te šifre. Rad će se osvrnuti i na djelovanje kriptoanalitičara u Bletchley Parku te na posljedice kriptološkog djelovanja na ishod 2. svjetskog rata.

Ključne riječi: Colossus, Lorenzova šifra, Lorenz SZ40, Bletchley Park, Drugi svjetski rat, kriptologija, kriptoanaliza

Uvod

Od vremena kada su se ljudi počeli koristiti pismom te se na taj način sporazumijevali te razmjenjivali informacije koristeći se kako slovima i brojevima, tako i raznim simbolima i znakovima, tim istim alatima su s vremenom počeli prikrivati transparentnost podataka koje su razmjenjivali. Takva općeljudska potreba koja se kasnije proširila na mnoge sfere života, a danas postala uobičajen dio naših svakodnevica, rezultirala je razvojem nove znanstvene discipline. Kriptologija je znanost koja se bavi proučavanjem metoda kriptozaštite[1] i dekriptiranja[2] u svim vrstama poruka, a nama su najzanimljivije pisane iz kojih se razvila kriptografija.

Počeci kriptologije sežu još prije Krista, prvim poznatim dokazom o svojevrsnoj upotrebi kriptografije svjedoči natpis uklesan u odaji egipatske grobnice. Riječ je o neobičnim hijeroglifima kojima se vjerojatno pokušao promijeniti oblik poruke. Možemo reći da se radi o preobrazbi teksta, a slične metode bile su u uporabi i kasnije. Danas takve postupke smatramo relativno banalnima jer je jednostavno doći do ispravnog, originalnog značenja.

Dalje u radu bit će spomenuti još neki kreativni načini kojima su se služili uglavnom ljudi s određenim ovlastima, poput špijuna na dvorovima, a danas predstavljaju kriptologiju u povojima. Glavni naglasak ovog rada stavljen je na razdoblje Drugog svjetskog rata koji se naziva i ratom fizičara[3], no u sjeni nikako ne trebaju ostati izvanredni pothvati, izumi i uspjesi brojnih kriptoanalitičara čije je djelovanje imalo značajan utjecaj na ishod rata.

U jednu ruku upravo oružane snage i diplomatsku službu možemo smatrati najzaslužnijima za razvoj kriptologije, one koji su najbolje znali iskoristiti ponuđene potencijale, poslužiti se njima za veće ciljeve te ih tako unaprijedili. Onaj aspekt kojim će se ovaj rad detaljnije baviti pokriva specifičniji dio kriptologije pod imenom kriptografija. Naziv dolazi od grčkog pridjeva *kriptós* (κρυπτός) - "skriven" i glagola *gráfo* (γράφω) - "pisati" označavajući granu kriptologije koja se bavi logičkom promjenom podataka. Takvim izmjenama intenzivno su se služile obvještajne jedinice u Prvom i Drugom svjetskom ratu. Mehanizmi tada izumljeni bili su neusporedivo napredniji od onoga što smatramo povojima kriptografije, a kratki pregled izuma poput naprave *skital* bit će dan u sljedećem poglavlju sa ciljem prikazavanja veličine uspjeha i napretka koji je postignut u kasnijim stoljećima.

[1] Pojam označava zaštitu vlastitih šifriranih poruka od dešifriranja.

[2] Pojam označava dešifriranje tuđih šifriranih poruka bez prethodnog poznavanja šifre.

[3] Naziv za Drugi svjetski rat zbog atomske bombe, kao što se Prvi svjetski rat naziva „ratom kemičara“.

1. Kratki presjek razvoja kriptografskih sustava

Jedni od prvih pokušaja sakrivanja poruke bilo je doslovno prikrivanje njezina postojanja što danas nazivamo steganografijom. Steganografija[4] podrazumijeva prikrivanje poruke, ali ne i očite činjenice da A i B osoba komuniciraju. Povećanim potrebama za tajnost i sigurnost ta metoda je kasnije napredovala do prikrivanja samog sadržaja. Postojalo je nekoliko češće korištenih načina kako sakriti poruku, primjerice upotrebom simpatetičke tinte[5] koja može biti osjetljiva na toplinu, vodu, pudranje ili postaje vidljiva pod određenim kutem pod kojim pada svjetlost i slično. Osim raznih tekućina, korištene su i mikrodote. Tako stvorene poruke sadrže naizgled beznačajan tekst, no prava informacija krije se u prvim slovima. Osim navedenih bila su česta i fizička prikrivanja poput pisanja po ljusci kuhanoga jajeta, primatelju bi poruka bila vidljiva na stjenkama jajeta kada bi ga oljuštio. Slično tome glasnici bi nosili poruku na vlastitom tjemenu. Za potrebe poruke obrijali bi glavu te prije odlaska primatelju čekali da im kosa naraste kako bi prikrili važne informacije od nepoželjnih očiju. S obzirom na to da su navedeni načini postali relativno jednostavni za otkrivanje, a time i presretanje vrijednih informacija, počela se razvijati prava znanost tajne komunikacije.

Prvom kriptografskom napravom smatra se *skital* koji su koristili Spartanci još u 5. stoljeću prije nove ere.[6] Napravu je sačinjavao drveni štap oko kojega se omatala vrpca pergamene. Zakritak, odnosno tajna poruka, pisao bi se dok bi se vrpca omatala oko štapa, a potom bi se odmotala. Odmotana vrpca poslala se adresatu i u tom obliku nije bila čitljiva, smislena. Primatelj je trebao vrpcu namotati na štap jednake debljine kako bi pročitao tekst. Ovo je samo jedan od zastarjelih primjera sustava koji danas više ne mogu pronaći svoje mjesto u ozbiljnoj uporabi, ali je slikovit primjer za usporedbu sa sustavima koje je ljudski um kasnije zamislio, razvio te naposlijetku i izradio. Skitala funkcionira na principu transpozicije – premještajnog kritopisnog sustava u suvremenoj podjeli koji ujedno čini jedan od dva osnovna načina na koje ugrubo možemo podijeliti kriptografiju. Sama riječ označava svojevrsnu „zamjenu“, dakle slova koja sačinjavaju riječ ili rečenicu nalaze se u drugačijem redoslijedu od uobičajenog tvoreći anagram. S obzirom na to da zamjena mora slijediti neko dogovoreno pravilo, takve poruke obično je relativno jednostavno „probiti“ jer postoji određeni broj mogućih

[4] Naziv potječe od grčkih riječi *steganos* – u značenju prikriven i *graphein* – pisati.

[5] Simpatetička je tinta nevidljiva promatraču golim okom, zbog čega se naziva još i „nevidljiva tinta“.

[6] Singh, Simon. The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography. New York: Anchor Books, 2000. Str. 22.

kombinacija. Drugi način koji pruža više mogućnosti je supstitucija. Koristeći metodu supstitucije svaki element otvorenog teksta[7] (bio to bit, slovo ili grupa bitova, slova) preslikavamo u neki drugi element. Svako slovo jasnopisa zamjenjuje se nekim drugim znakom koje je određeno prema ključu. Za razliku od transpozicije koja sadrži originalno slovo, samo na drugačijoj poziciji, supstitucijom se zadržava pozicija, ali jedan znak se zamjenjuje drugim. Prvom upotrebom supstitucijske šifre smatramo „Cezarovu šifru", kako ju danas zovemo. Radi se o zamjeni slova slovom koje se nalazi tri mjesta dalje u abecedi. Upotrijebimo li taj princip, naziv postupka bi zvučao ovako: DHBČTSAČ VLITČ. Kako bismo se poslužili supstitucijiom, da otvoreni tekst pretvorimo u tajnopis potrebna su nam dva slovoreda[8] – zakritni (dolje) koji je šifriran i jasnopisni (gore) koji je uvijek jednak abecedi.

a	**b**	**c**	**č**	**ć**	**d**	**dž**	**đ**	**e**	**f**	**g**	**h**	**i**	**j**	**k**	**l**	**lj**	**m**	**n**	**nj**	**o**	**p**	**r**	**s**	**š**	**t**	**u**	**v**	**z**	**ž**
č	ć	d	dž	đ	e	f	g	h	i	j	k	l	lj	m	n	nj	o	p	r	s	š	t	u	v	z	ž	a	b	c

Supstitucijski kritopisni sustavi mogu biti monoalfabetski, poput Cezarove šifre ili polialfabetski koji koriste više zakritnih slovoreda.

Kako bismo šifrirali neki tekst, potrebno je u postupku upotrijebiti ključ. Ključevi zauzimaju vrlo važno mjesto u kriptografiji, sastavni su dio šifre. Ključ je proizvoljan, odnosno o njemu odlučuju pošiljatelj i primatelj. S obzirom na to da je riječ o razmjeni kriptiranih poruka koje naizgled nisu čitljive, od krucijalne je važnosti da ključ ostane tajan i isključivo u rukama ovlaštenih osoba jer se pomoću njega vrše postupci zakrivanja i, važnije, raskrivanja. Korištenjem ključa možemo vršiti i dvije vrste šifriranja: šifriranje s tajnim ključem ili šifriranje s javnim ključem. Postupci koji će ovdje biti spomenuti koriste metode šifriranja s jednim ključem. Broj ključeva nije beskonačan, već je ograničen brojem slova abecede koja se mogu kombinirati, stoga postoji i određen broj načina raskiravanja zakritka.

Kod simetričnih[9] ili konvencionalnih kriptosustava, ključ za dešifriranje i ključ za šifriranje u većini slučajeva su identični što dovodi do zaključka kako je sigurnost navedenih kriptosustava upravo u čuvanju tajnosti ključa. Zato ih i zovemo „kriptosustavi s tajnim ključem". No, to je ujedno njihov veliki nedostatak jer prije šifriranja pošiljatelj i primatelj moraju razmijeniti tajni

[7] Otvoreni tekst ili jasnopis (eng. plain text) predstavlja početnu poruku, njen izvorni oblik.

[8] Slovoredom podrazumijevamo bilo koji uređeni poredak slova.

[9] Postoje i asimetrični kritopisni sustavi poput RSA sustava koji koriste javni ključ za zakrivanje i tajni ključ za raskrivanje čime je povećana sigurnost podataka.

ključ putem odabranog sigurnog komunikacijskog kanala pri čemu uvijek postoji rizik da ga se domogne neovlaštena osoba.

U drugoj polovici petnaestog stoljeća Talijan Leon Battista Alberti svojim je revolucionarnim izumom unaprijedio razvoj kriptografije te je prvi upotrijebio polialfabetsku šifru[10]. Osnova je te šifre spomenuta supstitucijska Cezarova šifra, no nakon podužeg eseja u kojem Alberti objašnjava analizu frekvencije distribucije slova u zakritku i načine probijanja na temelju čestote pojavljivanja pojedinih slova, doskočio je pomno proučenom problemu. Za šifriranje poruka izumio je šifrirni disk koji je danas poznat pod njegovim imenom. Disk se sastojao od dva bakrena kruga različite veličine pri čemu je onaj veći bio statični, a manji pomični. Diskove je podijelio u 24 jednaka polja u koja su upisana slova abecede izuzevši H, K. U preostala 4 polja unio je brojeve od 1 do 4. Na manjem se disku također nalaze znakovi abecede, ali ovaj put njihov je redoslijed nasumičan, proizvoljan. Diskovi su spojeni iglom kroz sredinu koja služi kao os oko koje se manji disk okreće. Osobe koje komuniciraju moraju imati identične diskove te se dogovoriti oko indeksnog slova. Pošiljatelj pri stvaranju zakritka dogovoreno indeksno slovo namješta uz bilo koji znak vanjskog diska te o tome mora obavijestiti primatelja. Unutarnji disk predstavlja jasnopis, a zakritak ćemo dobiti čitanjem znakova sa statičnog diska. Revolucionarni dio ovog izuma bila je Albertijeva odluka da se zakritni slovored često mijenja, da nakon određenog vremena (par riječi ili rečenica) promijenimo indeksno slovo. Na taj način promijenit ćemo znak kojim smo zakrivali određeni znak jasnopisa što će uvelike otežati kriptoanalizu i probijanje šifre. Takvim učestalim mijenjanjem šifrirane abecede Alberti je utjecao na frekvenciju često pojavljivanih slova u jeziku koju je prethodno proučavao. Zbog upečatljivog doprinosa modernoj kriptografiji dobio je titulu „oca zapadne kriptografije“. Njegova šifra razbijena je tek krajem 19. stoljeća, lako je zaključiti kako je zadala podosta glavobolja kriptoanalitičarima.

[10] Singh, Simon. The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography. New York: Anchor Books, 2000. Str. 65-67.

L. B. Alberti bio je u punom smislu renesansni čovjek. Iskazao se na mnogim poljima kao humanist, pjesnik, slikar, kipar, glazbenik, arhitekt, pravnik, matematičar i kriptograf. Neka od njegovih najznačajnijih djela vezana su uz arhitekturu i kiparstvo, a svoj doprinos kriptologiji dao je izumom šifrirnog diska koji je poznat kao prvi primjer polialfabetske supstitucijske šifre. Također mu pripisujemo prvo zapadnjačko proučavanje kriptoanalize te prvo korištenje šifriranih kodova.

1.1. Kriptologija u Drugom svjetskom ratu

Spomenuti Spartanci predstavljaju prvi sistem vojne kriptografije. S godinama važnost kriptografije intenzivno raste, napose u vrijeme ratovanja među vojnim, obavještajnim, diplomatskim jedinicama kojima je primarni cilj bio komunicirati što izravnije, ali što tajnije kako neprijateljska strana ne bi došla u posjed vrijednih informacija. Promjene tog vremena sve su veće, posebno između svjetskih ratova, sukobi su masivniji, pa tako i potreba za tajnošću i čuvanjem raste. Kulminacija se događa za vrijeme Drugog svjetskog rata, a načini komuniciranja dobivaju na životnoj važnosti. U prilog toj tvrdnji svakako će govoriti dalje navedeni primjeri.

Vodeće sile koje su predstavljale okosnicu Drugoga svjetskog rata jedne su od najzaslužnijih za razvitak mehanizacije i kompjuterizacije. Primjerice, američka je mornarica za potrebe ratovanja razvila sustav za šifriranje za koji se smatralo da ga je nemoguće dešifrirati. Riječ je o stroju „Electronic Code Machine (ECM) Mark II“, poznat i pod nazivom SIGABA. SIGABA se sastojala od 15 rotora u završnoj inačici, a indeksni rotori nudili su 500 različitih vrijednosti. Stroj je bio kompleksniji od široko poznate Enigme koja je koristila tri rotora te je SIGABA ostala neprobijena tijekom rata[11]. Iako dosta sigurna s obzirom na to da je očuvala neprobojnost, sustav šifriranja odvijao se jako sporo što nije bilo praktično primjenjivo u borbi. Jedan ratni dopisnik opisao je poteškoće s kojima su se susreli rekavši kako se „komunacija morala odvijati brzo i precizno jednom kada je borba postala ograničena na malu površinu“[12]. Tada više nije bilo vremena čekati da stroj šifrira željeni tekst, već su se lukavo dosjetili kako iskoristiti navaho jezik[13] za međusobnu komunikaciju u stvarnom, trenutnom vremenu.

[11] Singh, Simon. The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography. New York: Anchor Books, 2000. Str. 226.

[12] Ibid, str. 227.

[13] Navaho jezik odigrao je važnu ulogu tijekom rata, možemo reći kako je bio jedan od najsigurnijih načina enkripicije korišten u tom periodu. Tim jezikom govorili su Indijanci koje je američka vojska obučila za posao slanja tajnih taktičkih poruka putem vojnog radija ili telefona koristeći kodove na navaho jeziku. Kodiranje se temeljilo na metodi susptitucije (imena za ptice označavala su avione), leksikon je na kraju sadržavao 274 riječi. Nijemci i Japanci nikada nisu dešifrirali kodove. Kriptoanalitičari koji su razbili najjači japanski stroj PURPLE, za navaho jezik rekli su da je to „čudan slijed nazalnih, jezičnih zvukova koji nisu mogli ni zapisati, a još manje dekodirati“. Tako je navaho jezik bio velika uspješnica.

Japanska vojska koristila se šifrirnim strojem pod nazivom „97-shiki –obun Inji-ki“, no poznatiji je pod imenom „PURPLE“ kako su ga Amerikanci nazivali. Japanci su stroj kupili od Nijemaca te su ga prilagodili vlastitim potrebama. Iako je princip na kojem je stroj radio, odnosno postupak modifikacije teksta stvarao izuzetno tešku šifru, američki su kriptoanalitičari razbili šifrirane poruke, a Japan je naposlijetku završio poražen u ratu.
Dvadeseto stoljeće i ratne godine iznjedrile su još mnogo različitih strojeva za šifriranje, kao i načina komunikacije, a pokušaji stvaranja drugačijih i neprobojnih šifri zaokupili su kapacitete kriptologa. Svakako danas najpoznatiji stroj toga vremena je Enigma koju se mnogo proučavalo, o njoj se pisalo, diskutiralo te je postala i česta metafora svakodnevne komunacije. No postoji još jedan stroj koji su koristili Nijemci tijekom rata, radio je slično kao Enigma, ali daleko kompleksnije, a nije ni izbliza tako poznat – riječ je o Lorenzu SZ40.

2. Lorenz

Lorenz SZ40 bio je njemački rotacijski elektromehanički uređaj za šifriranje[14] koji je radio na principu simetrične protočne šifre. Konkretno, implementirao je Vernamovu protočnu šifru.
Za razliku od Enigme, Lorenz nije bio zaseban stroj koji se neovisno koristio za šifriranje, već je bio postavljen između teleprintera i njegove linije. Tijekom komunikacije stroj je automatski šifrirao poruku odaslanu teleprinterom ili dešifrirao nadolazeću prije nego je bila ispisana, što je proces učinilo veoma brzim i laganim[15].

Lorenz su koristili Nijemci tijekom Drugog svjetskog rata za slanje poruka najveće važnosti između vrhovnog zapovjedništva njemačke vojske i ostatka vojnih zapovjedništava na području okupirane Europe. Britanski kriptoanalitičari koji su njemačke šifrirane teleprinterske poruke zvali kodnim imenom „Fish“ (hrv. riba), Lorenza su nazvali „Tunny“ (skraćeno od *tunafish*, hrv. tuna)[16].
Serija uređaja Lorenz SZ40 (njegova su poboljšanja SZ42a i SZ42b) razvijena je i proizvedena u njemačkoj tvornici „Lorenz AG“ u Berlinu, a specijalizirala se za proizvodnju uređaja za

[14] http://www.cryptomuseum.com/crypto/lorenz/sz40/index.htm (pristup 18.6.2018).

[15] Ibid.

[16] Hinsley, F. H. An introduction to Fish u: Hinsley, F. H. i Stripp, Alan. The Inside Story of Bletchley Park. Oxford: Oxford University Press, 1993. Str. 141–148.

telegrafiju i telefoniju te uređaja poput radija i radara. Ime modela SZ skraćeno je od Schlüssel-Zusatz, što bi označavalo nastavak za teleprinter koji šifrira njegove poruke[17].

Kako je već spomenuto, Lorenz je bio smješten između teleprintera i njegove linije. Dno uređaja bilo je metalno, dimenzija 48 x 39 cm, a visina je iznosila 43 cm kao što je prikazano na sljedećoj slici.[18]

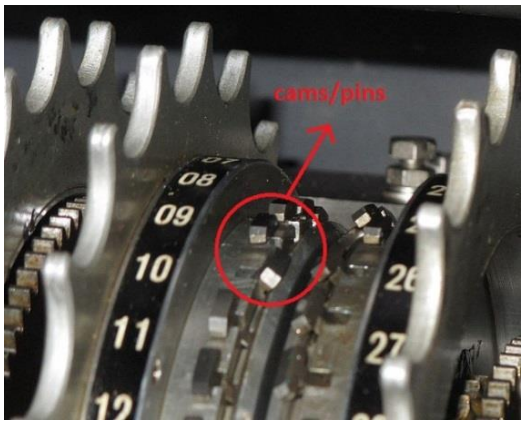
Slika 1. Uređaj Lorenz

Preuzeto sa: http://www.cryptomuseum.com/crypto/lorenz/sz40/

Kako bi primopredaja poruke funkcionirala kako je zamišljeno, uređaj koji je poruku odašiljao i onaj koji je poruku primao morali su koristiti iste postavke – zubi (eng. cams) na rotorima morali su biti postavljeni u identičan položaj (podignuti ili spušteni, odnosno aktivni ili neaktivni) na oba uređaja te su rotori morali biti postavljeni u odgovarajući početni položaj. Izgled i položaj zuba može se promotriti na slici ispod:

[17] eng. cipher attachment

[18] http://www.ellsbury.com/tunny/tunny-010.htm (pristup 9.7.2018).



Slika 2. Zubi na rotorima

Preuzeto sa: https://en.wikipedia.org/wiki/Lorenz_cipher

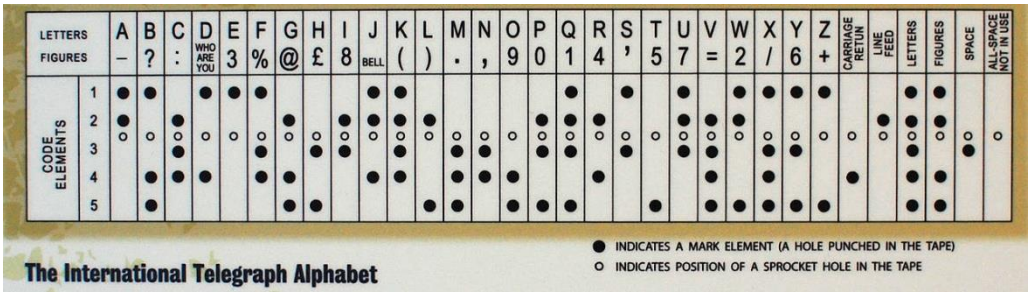
2.1. Vernamova šifra

U suštini Lorenz radi na principu simetrične protočne šifre – preciznije Vernamove protočne šifre. Kod nje se, koristeći Booleovu XOR funkciju, svakom slovu otvorenog teksta dodavalo jedno slovo ključa kojeg je generirao unutarnji Lorenzov mehanizam.
Vernamova šifra predstavlja simetrični algoritam budući da se isti ključ koristi i za zakrivanje jasnopisa i za raskrivanje šifriranog teksta.
Šifra počiva na pretpostavci da je svaki znak jasnopisa kombiniran s jednim znakom ključa. U teoriji, ako ključ sadrži isti ili veći broj znakova kao i jasnopis te ako je potpuno nasumičan, zakritak će također biti potpuno nasumičan, što bi značilo da ga je nemoguće raskriti. Po tome Vernamova šifra slična je jednokratnom ključu[19].

Za razliku od Enigme, teleprinteri nisu funkcionirali na principu abecede od 26 slova i Morseovog koda, već su koristili 32-simbolni Baudotov kod. Kao što vidimo na slici broj 3, svaki je znak zamijenjen digitalnim 5-bitnim kodom što je značilo da je znak bio sastavljen od različite kombinacije rupa u papirnoj traci koju su teleprinteri koristili. Te fizičke rupe na

[19] Šifriranje jednokratnim ključem (eng. one-time pad; OTP) naziv je za kriptografsku metodu koja se koristila od 1917. godine. Otvoreni tekst kombinira se sa slučajnim ključem i jednake su duljine. Ovaj se slučajni ključ u komunikaciji koristi isključivo jedanput, a s originalnim se tekstom spaja koristeći zbrajanje po modulu (XOR). Do sada je dokazano da je šifriranje na opisani način kao kriptografska metoda teoretski neslomljivo. Potpuna sigurnost sustava leži u činjenici da se svaki ključ koristi samo jednom (odakle i dolazi naziv).

papirnoj traci u digitalnom se obliku mogu smatrati jedinicama i nulama – 1 predstavlja rupu u traci, a 0 izostanak rupe.[20]



Slika 3. Baudot-Murray code

Preuzeto sa: https://commons.wikimedia.org/wiki/File:International_Telegraph_Alphabet_2.jpg

Zakritak nastaje tako da se na pojedine bitove jasnopisa i ključa primijeni XOR operacija, čiju istinitosnu tablicu vidimo ovdje, a primjer dobivanja zakritka i jasnopisa na slici ispod tablice:

A	B	A **XOR** B
0	0	0
0	1	1
1	0	1
1	1	0

Slika 4. Primjer XOR operacije

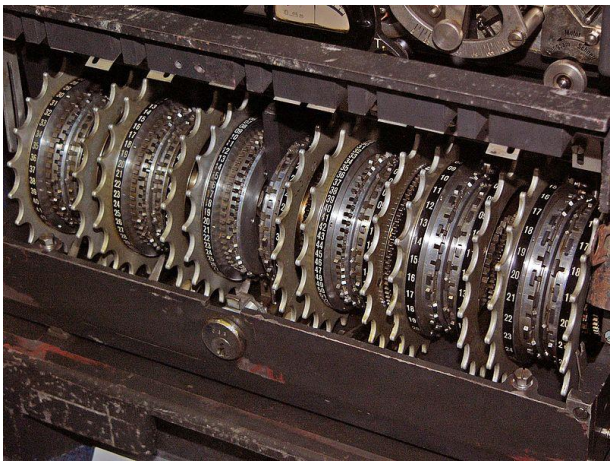
Preuzeto sa: http://www.cryptomuseum.com/crypto/img/mod2.png

[20] https://www.codesandciphers.org.uk/lorenz/fish.htm (pristup 15.7.2018)

U ovom primjeru slovo A, koje je prema Baudotovom kodu zapisano kao 00011, dodajemo slovu B koje je zapisano kao 11001, te primjenom XOR operacije dobivamo 11010, a koje je slovo G prema gore navedenoj tablici[21]. Isti postupak provodimo, samo obrnutim redosljedom, kada poruku raskrivamo.
U teoriji je zakrivanje i raskrivanje poruka ovom metodom jednostavno, ali proces generiranja ključa i držanje tog ključa u tajnosti kako ga savezнички kriptografi ne bi otkrili predstavljao je glavni izazov za Nijemce.

Princip rada stroja

Svaki od 5 bitova ključa za svako slovo jasnopisa kreiraju rotori u dva dijela stroja. Lorenz je imao dva seta rotora, a kriptografi u Bletchley Parku nazivali su te rotore χ ("chi") rotor i ψ ("psi") rotor. Svaki je od njih na sebi imao određen broj zuba koji su mogli biti postavljeni u spušteni (neaktivni) ili podignuti (aktivni) položaj. Izgled rotora prikazuje nam sljedeća slika, a stroj je sadržavao sveukupno 501 zub, dajući tako 10^{151} mogućih položaja zuba.[22]



Slika 5. Izgled rotora i zuba na Lorenzovom uređaju

Preuzeto sa: https://www.revolvy.com/page/Lorenz-cipher?

[21] Ibid.

[22] Churchhouse, Robert. Codes and Ciphers: Julius Caesar, the Enigma and the Internet. Cambridge: Cambridge University Press, 2002. Str. 158.

Rotori χ pomicali su se pravilno, za jedan zupčanik nakon šifriranja jednog znaka jasnopisa te su se svi pomicali odjednom. ψ rotori su se također pomicali zajedno, ali su se pomicali nepravilno, ne nakon svakog znaka jasnopisa. Kretnje ψ rotora kontrolirali su mu rotori. Rotor μ61 pomicao se za jedno mjesto nakon svakog znaka, ali μ37 rotor pomicao se samo kada je zub na μ61 bio u aktivnom položaju prije kretanja, a u tom se slučaju svih 5 ψ rotora pomicalo.[23]

Ključ generiran SZ uređajem sadržavao je komponentu χ i kompomentu ψ koje su združene XOR funkcijom:

$$\text{key} = \chi\text{-key} \oplus \psi\text{-key}$$

Svaki od 12 rotora sadržavao je različit broj zuba. Broj zuba na svakom je rotoru relativno prost s obzirom na sve ostale kako bi se omogućilo što više vremena prije nego što se kombinacija ponovila. Naziv rotora s pripadajućim brojem mu zuba nalazi se u sljedećoj tablici:

BP wheel name	ψ_1	ψ_2	ψ_3	ψ_4	ψ_5	μ_{37}	μ_{61}	χ_1	χ_2	χ_3	χ_4	χ_5
Number of cams (pins)	43	47	51	53	59	37	61	41	31	29	26	23

Slika 6. Ime rotora (u Bletchley Parku) i broj zuba na njemu

Preuzeto sa: https://bit.ly/2xPU5p4

[23] http://www.ellsbury.com/tunny/tunny-000.htm (pristup 17.7.2018).

2.2. Kriptoanaliza Lorenza

Kriptoanaliza Lorenza, kao i kriptoanaliza Enigme, pridonijela je Savezničkim naporima da, dešifrirajući njemačke tajne poruke, skrate trajanje rata. Dešifriranje Lorenza omogućilo je Saveznicima čitanje poruka između Njemačkog vrhovnog zapovjedništva (*Oberkommando der Wehrmacth*) i ostalih zapovjedništava diljem okupirane Europe. Informacije dobivene procesom razbijanja Enigme i Lorenza dobile su oznaku *Ultra* – podaci od najveće važnosti u britanskoj obavještajnoj službi.[24]

Prijašnje dešifriranje poruka koje su bile poslane Enigmom otkrilo je Saveznicima da Nijemci jedan od svojih teleprintera zovu „Sägefisch“[25] (eng. *sawfish*, hrv. pilan) pa su britanski kriptografi cjelokupnu njemačku šifriranu komunikaciju odaslanu radiotelegrafskim putem odlučili zvati „Fish“. Sam Lorenz dobio je oznaku „Tunny“ (od *tunafish*, hrv. tuna).

Iako izrazito kompliciran stroj, do prvog dešifriranja Lorenza te razumijevanja njegove logičke strukture naposljetku je dovela nepažnja njemačkih radiooperatora koji su prilikom prijenosa poruke u nekoliko navrata koristili iste postavke[26], odnosno isti ključ, što je kriptografima omogućilo da ručno dešifriraju poruke i naposljetku otkriju logičku strukturu stroja. Za poruke poslane na taj način govorilo se da su *in depth*.

Kasnije se kriptoanaliza odvijala uz pomoć ručnih te automatiziranih metoda. Prvi savezнички uređaj koji je pomagao pri kriptoanalizi Lorenza bio je Heath Robinson[27], no kako je bio spor i nepouzdan, razvijen je napredniji i felksibilniji stroj, Colossus[28] – prvi programabilni digitalni kompjuter na svijetu.

S obzirom na to da su njemački odašiljači za slanje teleprinterskih poruka koristili usmjerene antene, većina signala koji su dospjeli do Britanije bili su slabi, a postojalo je i 25 različitih frekvencija na kojima se odašiljanje odvijalo. Zbog toga su diljem Britanije postavljene Y-stanice, poput one u Knockholtu u Kentu[29], koje su presretale poruke odaslane teleprinterom.

---

[24] Uredili: Hinsley, F.H. & Stripp, Alan. Codebreakers: The inside story of Bletchley Park. Oxford University Press, 1993. Str. 1.

[25] Ibid. Str. 149.

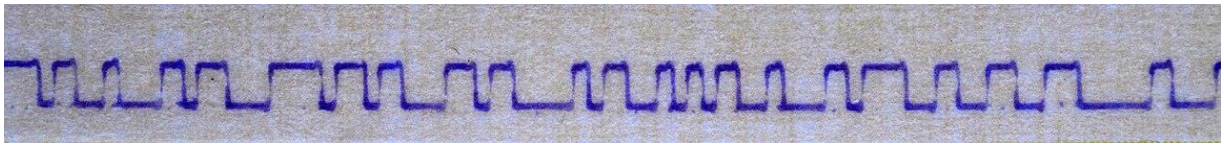
[26] https://www.codesandciphers.org.uk/lorenz/fish.htm (pristup 20.7.2018).

[27] Copeland, B. Jack. Colossus: The Secrets of Bletchley Park's Codebreaking Computers. Oxford: Oxford University Press, 2006. Str. 71.

[28] http://www.colossus-computer.com/colossus1.html#section10 (pristup 21.7.2018).

[29] http://www.ellsbury.com/tunny/tunny-000.htm (pristup 21.7.2018).

Svaka poruka je uz pomoć undulatora, uređaja koji je impulse odaslane teleprinterom vizualno bilježio, otisnuta na papirnu traku u obliku vrhova i udubina. Naknadno su takve poruke „prevedene“ u Baudotov kod tako da su vrhovi postali rupe, odnosno manjak istih na papirnoj traci kakve su koristili teleprinteri.[30] Vizualni trag zabilježen undulatorom vidljiv je na ovoj slici:



Slika 7. Undulator

Preuzeto sa: https://bit.ly/2y5DP2m

2.3. Logika stroja

Kako bismo dešifrirali neku novu šifru, prvo je potrebno otkriti logiku iza procesa enkripcije i dekripcije. U slučaju Lorenza to je podrazumijevalo mehaničku, odnosno logičku strukturu samog uređaja, što bi na kraju dovelo i do shvaćanja njegovog načina rada.
Kako bi nastavak rada bio razumljiviji, donosim tablicu simbola koje su kriptografi u Bletchley Parku koristili pri dešifriranju zakritka i objašnjavanja procesa Lorenzovog rada.[31]

P	**jasnopis**
K	ključ
χ	*chi* dio ključa
ψ	*psi* dio ključa
Ψ'	prošireni *psi* – stvarna sekvenca znamenaka proizvedena psi-rotorima
Z	zakritak
D	*de-chi* – zakritak bez *chi* komponente ključa
Δ	bilo koji od gore navedenih elemenata nad kojima je provedena operacija XOR s nadolazećim znakom
$\oplus$	operacija XOR

Tablica 1. Objašnjenje simbola

[30] Gannon, Paul. Colossus: Bletchley Park's Greatest Secret. Great Britan: Atlantic Books Ltd, 2006.

[31] Tablica napravljena prema podacima sa: http://www.ellsbury.com/tunny/tunny-000.htm

Zakritak Z nije sadržavao nikakve statističke ni lingvističke karakteristike koje bi ga razlikovale od nasumičnog seta znamenaka, ali to nije bilo istinito za K, χ, Ψ' i D. To je bila slabost koja je na kraju dovela do otkrivanja Lorenzovih ključeva.

John Tiltman, kriptoanalitičar koji je radio na dešifriranju Lorenza za vrijeme njegove eksperimentalne faze, zaključio je da stroj radi na prinicpu Vernamove šifre. Kada su dvije poruke, a i b, odaslane istim ključem, kažemo da su *in depth* – kombiniranjem tih dvaju poruka poništava se efekt ključa. Na primjer, recimo da postoje dva zakritka, Za i Zb, ključ K te dva jasnopisa Pa i Pb. Tada vrijedi:

$$Za \oplus Zb = Pa \oplus Pb$$

Ako je moguće doći do dva jasnopisa, ključ je moguće otkriti iz bilo kojeg para zakritak-jasnopis.[32] Na primjer:

$$Za \oplus Pa = K$$

U kolovozu 1941. Saveznici su presreli dvije dugačke poruke s istim indikatorom - HQIBPEXEZMUG. Prvih sedam znakova zakritka bilo je identično, ali je druga poruka bila kraća. Tiltman je uspoređivao nekoliko mogućih jasnopisa s obzirom na Za $\oplus$ Zb string te je otkrio da prvi jasnopis počinje njemačkom riječju „SPRUCHNUMMER“. U drugome je jasnopisu njemački operater za tu istu riječ koristio skraćenicu „NR“. U tom je jasnopisu također bilo dodatnih skraćenica te razlikovanja što je Tiltmanu omogućilo da otkrije jasnopis obje poruke. Dijelovi jasnopisa *Pa* mogli su se usporediti s jasnopisom *Pb* i obrnuto, što je otkrilo 4000 znamenaka ključa[33].

Istraživačka sekcija probala je uz pomoć tog ključa i jasnopisa matematički opisati način na koji Lorenz generira ključ, no bezuspješno. U listopadu 1941. sekciji se pridružio Bill Tutte, koristeći Kasiski test[34] otkrio je ponavljanja u ključu koji je mehanizam Lorenza proizvodio.

---

[32] Copeland, B. Jack. Colossus: The Secrets of Bletchley Park's Codebreaking Computers. Oxford: Oxford University Press, 2006. Str. 50-51.

[33] Copeland, B. Jack. Colossus: The Secrets of Bletchley Park's Codebreaking Computers. Oxford: Oxford University Press, 2006. Str. 50.

[34] Kasiski test naziv je za metodu kojom tražimo ponavljanja istih skupova slova u zadanom šifratu i gledamo koliko su mjesta ponavljanja međusobno udaljena. Zatim uspoređujemo dobivene brojeve i tražimo im zajedničke djelitejlje. Metoda počiva na činjenici da će pojedine česte riječi vjerojatno biti šifrirane istim slovima ključa pa će se u šifratu pojaviti ponovljene grupe slova. Ime je dobila po Friedrichu Kasiskom koji je prvi napravio uspješan napad na Vigenerovu šifru 1863.g.

Tehnika je podrazumijevala ispisivanje ključa na papir te prelazak u novi red nakon određenog broja znamenaka s obzirom na pretpostavljenu frekvenciju ključa. Ako je broj znamenaka u redu bio točan s obzirom na ključ, nakon vremena uočila bi se ponavljanja određenih znamenaka.

Ključ koji je generirao Lorenz bio je veoma dugačak pa je Tutte isprobao tehniku na samo jednom impulsu, odnosno bitu ključa. Lorenzovi indikatori koriste 25 slova za 11 pozicija, ali samo 23 za dvanaestu, pa je Tutte primijenio Kasiski tehniku za prvi bit ključa koristeći broj ponavljanja 25x23=575. To nije proizvelo veliki broj ponavljanja po redovima, ali je uočeno ponavljanje po dijagonali. Tada je pokušao ponovno s 574, što je doista i dovelo do ponavljanja nizova znamenaka po redovima. Prepoznao je da su prosti faktori tog broja 2, 7 i 41 pa je pokušao opet te dobio „četverokut točaka i križeva koji je bio pun ponavljanja.“[35]

Bilo je očito da je prvi bit ključa složeniji od onoga kojeg je proizvodio jedan rotor s 41 mogućom pozicijom. Tutte je tu komponentu ključa nazvao *chi* – χ_1. Zaključio je da postoji i druga komponenta nad kojom je provedena XOR operacija, a koja se nije uvijek mijenjala sa svakim novim znakom te je to bio rezultat rotora kojeg je nazvao *psi* - ψ_1. Sve prethodno spomenuto bilo je primjenjivo na svih 5 bitova ključa pa se tako ključ sastojao od dvije komponente:

$$K = \chi \oplus \psi$$

Stvaran niz znamenaka koje je dodavao psi-rotor nazvan je prošireni *psi*:

$$K = \chi \oplus \psi'$$

Tutte je do toga došao zbog činjenice da je iza točke najčešće došla druga točka, a iza križa najčešće drugi križ. Sve to dovelo je do konačnog zaključka da se svih 5 psi-rotora pomiče istovremeno, a kontroliraju ih dva μ (mu) rotora.

Budući da je Lorenz bio izrazito složena naprava te da ga kriptografi nisu uživo vidjeli sve do kraja rata, otkrivanje njegova načina rada smatra se jednim od najvećih intelektualnih postignuća 2. svjetskog rata.[36]

[35] Copeland, B. Jack. Colossus: The Secrets of Bletchley Park's Codebreaking Computers. Oxford: Oxford University Press, 2006. Str. 50-51.

[36] http://www-history.mcs.st-and.ac.uk/Biographies/Tutte.html (pristup 4.8.2018)

2.4. Turingery

Tijekom 1942. Alan Turing proveo je nekoliko tjedana u Istraživačkoj sekciji Bletchley Parka. Zanimao ga je problem dešifriranja Lorenza uz pomoć ključeva dobivenih *from depths*.[37] Razvio je metodu otkrivanja postavki zuba na rotorima iz određenih ključeva. Ta je metoda postala znana kao „Turingery", a uvela je metodu diferenciranja na kojoj se baziralo otkrivanje ključeva u nedostatku *depthova*.[38]

Kriptoanaliza često podrazumijeva pronalaženje neke vrste uzoraka kako bi se eliminirao veći broj mogućih ključeva te brže pronašli oni ispravni. Kriptografi su se trudilli pronaći proces kojim bi se manipuliralo zakritkom ili ključem kako bi se dobila frekvencijska distribucija znakova koji su odstupali od uniformne distribucije koju je Lorenz nastojao postići. Turing je niz, nastao provođenjem XOR metode nad dvama susjednim znakovima ključa, nazvao razlika (eng. difference), jer je XOR metoda isto što i modulo 2 zbrajanje, a bio je označen grčkim slovom Δ. Za niz znakova u ključu K, gdje podcrtana vrijednost označava nadolazeći znak u nizu, razlika je dobivena po formuli:

$$\Delta K = K \oplus \underline{K}$$

Diferenciranje je pridonijelo razbijanju Lorenza jer, iako je frekvencijsku distribuciju znakova u zakritku bilo nemoguće razlikovati od nasumičnog niza znakova, to nije bilo istinito za zakritak iz kojega je *chi* element ključa bio uklonjen. Kada je jasnopis sadržavao znak koji se ponavlja, što je u njemačkom jeziku relativno često (npr. u riječi wetter), te se psi-rotori nisu pomicali, znak dobiven metodom diferenciranja bi uvijek bio *null character* – '/ '. Kada se na njega i bilo koji drugi znak primijeni XOR operacija, *null character* nema nikakvog učinka na proces.

Turingova metoda otkrivanja postavki zuba na rotorima uz pomoć ključa dobivenog iz *deptha* bila je iterativan proces. Kada je Δψ znak bio /, pretpostavka ΔK=Δχ bila je točna u 50 posto slučajeva. Proces je započeo pretpostavkom da za pojedini ΔK znak vrijedi da je Δψ za određenu poziciju rotora. Tako nastao uzorak križeva i krugova (s obzirom na Baudotov kod) bio je zapisan na papir koji je sadržavao onoliko stupaca koliko je bilo znakova u ključu, a 5 redova predstavljalo je pet bitova Δχ.

---

[37] Copeland, B. Jack. Colossus: The Secrets of Bletchley Park's Codebreaking Computers. Oxford: Oxford University Press, 2006.

[38] General Report on Tunny: With Emphasis on Statistical Methods / Reeds, James A; Diffie, Whitfield; Field, J. V.

Set od 5 listova papira, po jedan za svaki chi-rotor, također je bio pripremljen. Oni su sadržavali stupce koji su brojčano odgovarali zubima pojedinog chi-rotora, a zvali su se „kavezi". Npr. χ_3 kavez imao je 29 takvih stupaca.[39]

Daljnji „pogoci" $\Delta\chi$ vrijednosti dali su ostale pretpostavljenje postavke zuba na rotorima. Ti se pogoci jesu ili nisu slagali s prijašnjim pretpostavkama, a kada su neslaganja bila daleko veća od slaganja, kriptografi su pretpostavili da u tom slučaju $\Delta\psi$ znak nije bio *null character*. Nastavkom tog procesa sve postavke pinova na chi rotorima bile su dokučene, a iz njih i postavke psi i mu rotora.

2.5. Testery

Od srpnja 1942. godine količina poruka odaslanih Lorenzom značajno se povećavala, što je rezultiralo potrebom za novim kriptografima, zapravo novim odjelom u Bletchley Parku. Pukovnik Ralph Tester vodio je novoosnovanu sekciju koja je po njemu dobila naziv „Testery", a obavljala je veliku većinu posla vezanog za dešifriranje Lorenzovih poruka.[40] Sekcija se sastojala od bivših članova Istraživačke sekcije, primjerice Peter Ericsson, Peter Hilton, Denis Oswald i Jerry Roberts. Dešifriranje poruka obavljalo se uglavnom ručno, čak i nakon uvođenja elektroničkih pomagala poput Robinsona i Colossusa.[41]

Prva faza rada tog odjela trajala je od srpnja do listopada 1942. godine, a dekripcija poruka ovisila je o *depthovima*. Nažalost, ubrzo je uobičajen standardizirani početak svih njemačkih poruka zamijenio nasumičan set znamenaka pa je dekricpija postala teža te je trajala puno dulje. Srećom, u rujnu su Saveznici presreli poruku s *depthom* koji je omogućio razvitak prije spomenute Turingove metode otkrivanja postavki rotora. Nakon što je u lipnju 1943. osnovana Sekcija Newmanry, dešifriranje u Testeryju se više nije oslanjalo na *depthove*.

Dio Sekcije Testery bio je i britanski Tunny (prikazan na slici 8) – elektromehanički stroj koji je funkcionirao na istom principu kao i originalni njemački uređaj, a koristio se za dobivanje jasnopisa nakon što su se odredile postavke rotora.[42] Dizajnirali su ga i sastavili Gil Hayward,

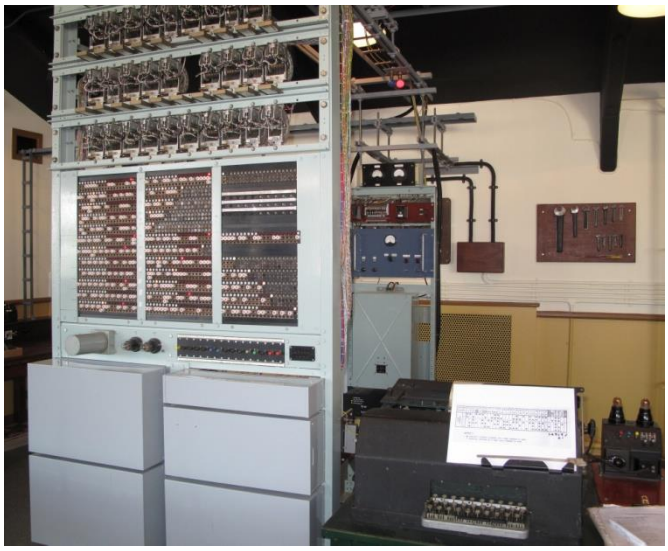
[39] Copeland, B. Jack. Colossus: The Secrets of Bletchley Park's Codebreaking Computers. Oxford: Oxford University Press, 2006. Str. 372.

[40] Roberts, Jerry My Top-Secret Codebreaking During World War II: The Last British Survivor of Bletchley Park's Testery, 2009.

[41] Ibid.

[42] Hayward, Gil. Operation Tunny u: Hinsley, F. H. i Stripp, Alan. The Inside Story of Bletchley Park. Oxford: Oxford University Press, 1993. Str. 175–192.

Allen William Mark Coombs, Bill Chandler i Sid Broadhurst u laboratoriju Tommyja Flowersa, a koji će biti instrumentalan za kasniju izradu Colossusa.



Slika 8. Britanski Tunny

Preuzeto sa: https://bit.ly/2y55hgC

2.6. Newmanry

Bill Tutte razvio je metodu dešifriranja koja je iskorištavala neuniformnost bigrama (susjednih slova) u njemačkom jasnopisu koristeći diferencirani zakritak i dijelove ključa. Ta se metoda zvala „dvostruki delta napad“ (eng. double delta attack).[43] Poanta metode bila je otkrivanje inicijalnih postavki *chi* komponente ključa tako što bi se isprobale sve kombinacije između *chi* komponente i zakritka te tražili primjeri neuniformnosti karakteristične za jasnopis.[44] S obzirom na to da je bilo nepraktično generirati 22 milijuna znakova od svih 5 chi-rotora, u početku se to radilo samo za prva dva.

S obzirom na to da za prva dva bita, tj. impulsa vrijedi Z_i=$\chi_i \oplus \psi_i \oplus P_i$ te stoga vrijedi P_i=$Z_i \oplus \chi_i \oplus \psi_i$ za prva dva impulsa $(P_1 \oplus P_2) = (Z_1 \oplus Z_2) \oplus (\chi_1 \oplus \chi_2) \oplus (\psi_1 \oplus \psi_2)$

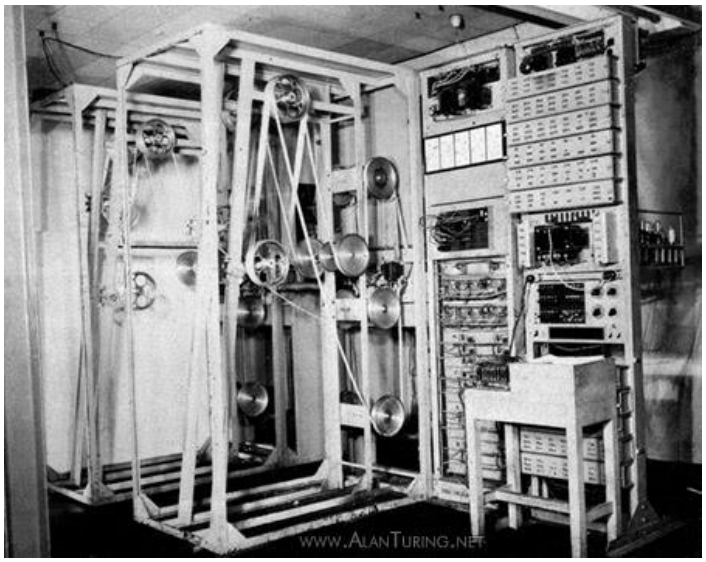
Izračunavanje mogućeg rezultata $P_1 \oplus P_2$ na ovaj način za svaku početnu točku sekvence $\chi_1 \oplus \chi_2$ rezultiralo bi križevima i točkama te na kraju većom zastupljenošću točaka (po Baudotovom kodu) kada je pravilna početna točka bila korištena za izračunavanje. Tutte je znao

[43] https://cs.stanford.edu/people/eroberts/courses/soco/projects/2008-09/colossus/doubledelta.html

[44] Copeland, B. Jack. Colossus: The Secrets of Bletchley Park's Codebreaking Computers. Oxford: Oxford University Press, 2006. Str. 52–63.

da će korištenje metode diferenciranja dodatno pojačati taj efekt jer bi svaki znak koji se ponavlja u jasnopisu uvijek generirao točku, a $\Delta\psi_1 \oplus \Delta\,\psi_2$ bi generiralo točku svaki put kad se psi-rotori ne bi pomicali te u 50% slučajeva kad bi se pomicali. Tutte je analizirao dešifrirani zakritak s diferenciranom verzijom gore opisane funkcije te otkrio da se točka generirala u 55% slučajeva[45]. S obzirom na funkcioniraje psi-rotora te njihov doprinos u procesu šifriranja, ono poravnavanje *chi* seta znamenaka sa zakritkom koje je dalo najveći broj točaka bilo je najvjerojatnije točno.[46] Taj je prinicp, koji se još zvao i „1+2 break in", bio temelj kasnijeg automatiziranog procesa kako bi se dobila *de-chi* (D) komponenta zakritka iz koje bi se potom ručno uklonila *psi* komponenta.

Ta metoda bila je korisna samo ako bi ju se moglo automatizirati. S tim je ciljem Tutte pristupio Maxu Newmanu koji je u prosincu 1942. utemeljio sekciju Newmanry. Prvi uređaj koji se koristio kao automat za provođenje Tutteove novorazvijene metode bio je Heath Robinson čiji se jedan dio vidi na niže priloženoj slici, ime je dobio po Williamu Heathu Robinsonu[47]. Frank Morell bio je glavni inženjer pri izradi Robinsona, a pomagao mu je Tommy Flowers koji je radio na Kombinirajućoj jedinici (eng. Combining Unit). Izrada je započela u siječnju 1943, prototip je u Bletchley Park dostavljen u lipnju.[48]



Slika 9. Heath Robinson

Preuzeto sa: http://www.colossus-computer.com/colossus1.html

[45] Copeland, B. Jack. Colossus: The Secrets of Bletchley Park's Codebreaking Computers. Oxford: Oxford University Press, 2006. Str. 50-51.

[46] Carter, Frank. Codebreaking with the Colossus Computer: Bletchley Park Reports. Bletchley Park Trust, 2008.

[47] Britanski ilustrator koji je crtao komplicirane naprave za izvršavanje jednostavnih zadatka.

[48] General Report on Tunny: With Emphasis on Statistical Methods / Reeds, James A; Diffie, Whitfield; Field, J. V.

Uređaj se sastojao od nekoliko dijelova – mehanizma zaduženog za čitanje poruka u Baudotovom kodu na probušenim vrpcama, kombinirajuće jedinice koja je automatizirala Tutteovu metodu te jedinice koja je bilježila broj točaka na papirnoj vrpci. Iako efektivan, Robinson je imao značajne nedostatke. Nije bio dovoljno brz za pojmove kriptografa, jedinica za brojanje nije bila potpuno pouzdana, a pogreške pri ručnoj izradi probušene papirne vrpce dodatno su otežavale rad stroja.[49] Robinson je uvelike skratio vrijeme dešifriranja poruka poslanih Lorenzom, ali zbog brojnih pogrešaka u radu ukazala se potreba za boljim, bržim i preciznijim strojem.

Tommyju Flowersu nije se dopao princip rada Robinsona, poglavito činjenica da je papirna vrpca s ključem morala biti savršeno sinkronizirana s papirnom vrpcom na kojoj je bila poruka jer je to otvaralo, kako se pokazalo u praksi, mjesto brojnim pogreškama. Na vlastitu inicijativu dizajnirao je stroj kojim bi eliminirao potrebu papirne vrpce s ključem jer bi taj stroj u sebi sadržavao elektroničku verziju Lorenza. S obzirom na to da se uređaj sastojao od tisuća vakuumskih cijevi koje su u to vrijeme bile nepouzdane te su često sagorijevale zbog promjene napona, njegova je ideja izazvala sumnje kod Maxa Newmana.[50] Ustrajući na ideji, Flowers je dobio potporu direktora W. Gordona Radleyja te je stroj napravljen tijekom idućih 11 mjeseci, počevši od siječnja 1943. godine.

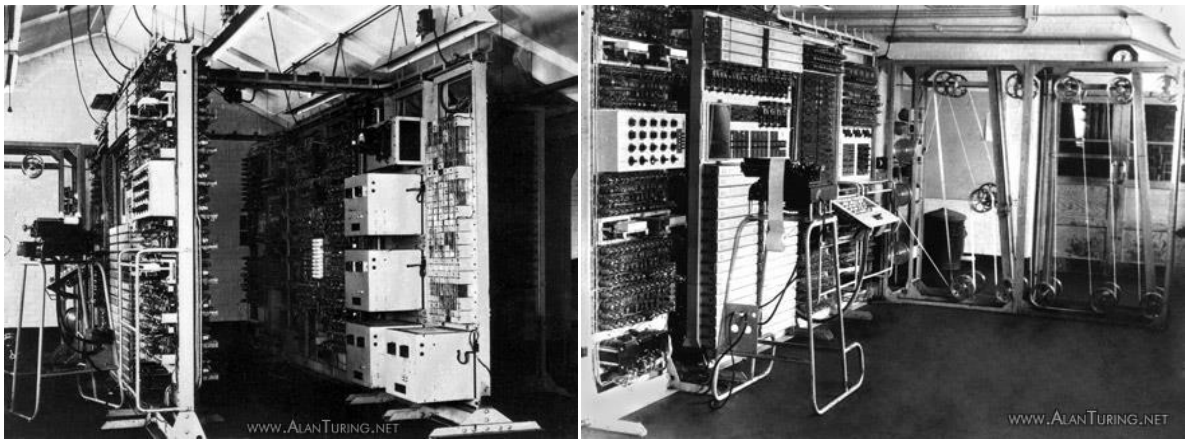
Mark I Colossus (na slici broj 10), kako se stroj zvao, dostavljen je u Bletchley Park, a svoju prvu poruku dešifrirao je 5. veljače 1944. godine.[51] Uvidjevši korisnost i revolucionarnost Colossusa, naročito nakon što je razvijen i Mark II, naručeno ih je nekoliko pa je tako na Dan pobjede u Europi u Bletchley Parku radilo 10 Colossusa.[52]

[49] http://www.colossus-computer.com/colossus1.html#section08

[50] Flowers, Thomas H. The Design of Colossus. Annals of the History of Computing. Str. 239–252.

[51] Copeland, B. Jack. Colossus: The Secrets of Bletchley Park's Codebreaking Computers. Oxford: Oxford University Press, 2006. Str. 76.

[52] General Report on Tunny: With Emphasis on Statistical Methods / Reeds, James A; Diffie, Whitfield; Field, J. V.



Slika 10. Colossus

Preuzeto sa: http://www.colossus-computer.com/colossus1.html

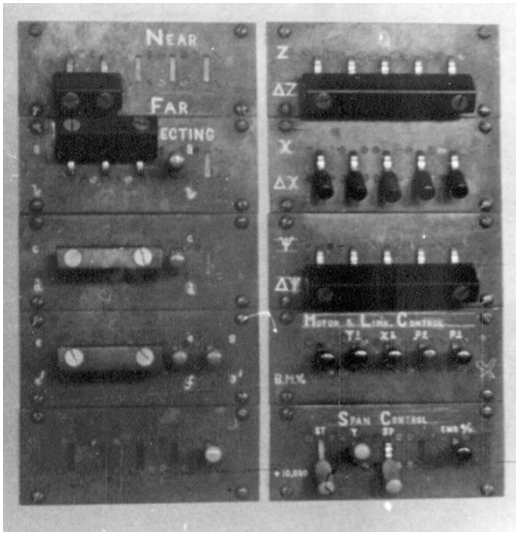
Mark II Colossus sastojao se od otprilike 2400 vakuumskih cijevi, a njegovi glavni dijelovi bili su: mehanizam za očitavanje poruke na papirnoj vrpci; brzina čitanja 5000 znakova po sekundi, elektronska jedinica koja je simulirala Lorenzov rad, 5 paralelnih procesirajućih jedinica, programabilne za velik broj Booleovih operacija, 5 jedinica za brojanje koje su printale i brojale broj križeva i rupa na papirnoj vrpci.

Colossus je bio dio sekcije Newmanry, njime je rukovalo 299 ljudi. Posao je počeo tako da se papirna vrpca sa zakritkom stavila na postolje. Njeni su krajevi bili spojeni tako da se ona konstantno vrtila tvoreći petlju, što je Colossusu omogućilo da nad istom porukom konstantno provodi različite operacije.[53] Nakon što se učvrstila napetost papirne vrpce i nakon što se uređaj kalibrirao, u Colossusa je unesen odgovarajući „program“ te je pušten u rad.

Iako Colossus nije bio računalo u današnjem smislu riječi – nije bio programiran uz pomoć pohranjenog programa na njemu samom već uz pomoć prekidača, a nije ni imao mogućnost pamćenja prijašnjih operacija – smatramo ga prvim programabilnim elektronskim digitalnim računalom.[54] Jedan dio prekidača na ploči pomoću kojih je bio programiran vidi se na sljedećoj slici:

[53] Flowers, Thomas H. The Design of Colossus. Annals of the History of Computing. Str. 239–252.

[54] Citirano prema: Rojas, Raúl. The First Computers: History and Architecture. Cambridge, Massachusetts: The MIT Press, 2000. Str. 351–364.



Slika 11. Prekidači na Colossusu

Preuzeto sa: https://bit.ly/2QlSvlp

Po završetku rata, svi Colossusi su rastavljeni i uništeni zajedno s mnogim nacrtima te je njihovo postojanje bilo tajno još trideset godina poslije, što je onemogućilo pravodobno priznanje svima koji su radili na tom projektu za postignuća koja su ostvarili.[55] Zbog toga se još dugo smatralo da je ENIAC prvo programabilno računalo, iako je nastao tri godine nakon Colossusa i u usporedbi imao ograničene mogućnosti programiranja.

3. Bletchley Park

Žarište događanja i ujedinjenog rada kriptoanalitičara i informatičara događalo se upravo u Bletchley Parku, mjestu čija je prava funkcija ostala sakrivena od javnosti sve do sedamdesetih godina dvadesetoga stoljeća. Smješten na strateškoj poziciji između dvaju sveučilišnih gradova, Oxforda i Cambridgea, u Buckinghamshireu predstavljao je dom mnogim vrsnim matematičarima, kriptografima, kriptoanalitičarima, lingvistima, znanstvenicima i prvim informatičarima koji su „u tišini“ razbijali njemačke sustave šifriranja i tako naposlijetku utjecali na ishod rata. Već spomenuti Colossusi bili su vodeći strojevi Bletchley Parka. Iako je Colossus imao puno važniju zadaću jer je dešifrirao poruke koje su se slale unutar njemačke

[55] http://www.alanturing.net/turing_archive/pages/Reference%20Articles/BriefHistofComp.html#ACE (pristup 2.9.2018).

vojske, prvo mjesto pri pomisli na Bletchley Park zauzima činjenica da je tamo probijena njemačka Enigma. Jedan od vodećih zaslužnih ljudi koji je radio na tom zadatku, a danas ga smatramo ocem moderne informatike, bio je Alan Turing. Zahvaljujući njemu postalo je moguće razbiti Enigminu šifru pod najtežim mogućim okolnostima. Poznato je njegovo djelovanje u baraci broj osam, a nakon rata i dalje je radio na temeljima računarstva. Uz Turinga i ranije spomenutoga Billa Tuttea, u periodu od pet godina u sklopu Bletchley organizacije bilo je zaposleno 7000 muškaraca i žena.[56] Potreba za tajnošću bila je ogromnih razmjera pa su svi zaposlenici Parka bili primorani potpisati „The Official Secrets Act"[57] koji im nije dopuštao govoriti o prirodi svog posla ni pod kojim okolnostima što je jedan od razloga zašto su se tako kasno otkrila stvarna događanja u Bletchleyju. Osim njemačkih šifri, na udaru kriptoanalize našle su se i japanske i talijanske poruke.

Bletchley Park bio je jedna od najbolje čuvanih tajni u Britaniji; tijekom rata Nijemci su ga pogodili bombom samo jednom i to najvjerojatnije pogreškom. Posjetitelji koji su dolazili poslovno u prostore Parka govorili su da idu u lov kako bi sačuvali tajnu o stvarnoj ratnoj namjeni kompleksa.

Danas Bletchley Parkom upravlja organizacija „Bletchley Park Trust" kojoj možemo zahvaliti što je devedesetih cijeli kompeks spašen od rušenja te je preuređen u muzej posvećen kriptografiji.

[56] Singh, Simon. The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography. New York: Anchor Books, 2000. Str. 193.

[57] McKay, Sinclair. The Secret Life of Bletchley Park: the WWII Codebreaking Centre and the Men and Women Who Worked There. London: Aurum Press Ltd, 2010. Str. 296.

Zaključak

Rijetko da postoje okolnosti u kojima je kriptografija toliko važna kao u ratnom razdoblju gdje stotine tisuća života, ponekad i milijuni, ovise o tajnosti podataka, a što je kulminaciju doživjelo tijekom Drugog svjetskog rata. Njemački je Lorenz bio veoma komplicirana naprava za šifriranje te je Saveznicima priuštio značajne izazove pri dešifriranju, počevši od osnovne logike stroja koju je uz pomoć samo dvije presretnute poruke otkrio Bill Tutte, preko cjelokupnog truda svih kriptologa i zaposlenika u Bletchley Parku – između kojih su se uz Tuttea isticali John Tiltman, Alan Turing i Max Newman – a koji su svojim znanjem i kreativnošću razbili Lorenza, čak i kada su ga poboljšali sigurnosnim promjenama. Brojni inženjeri dali su neosporiv i trajan doprinos svojim tehnološkim izumima kako bi se dešifriranje Lorenza odvilo što brže i efikasnije, a od kojih se naročito ističe Tommy Flowers i njegov Colossus, prvo programabilno računalo u povijesti.

Iako to isprva možda nije tako očito, funkcioniranje modernoga svijeta sazdano je na kriptologiji i njenom doprinosu u zaštiti naših podataka. Kada bankovnim karticama platimo račune, kada provodimo vrijeme na raznim internetskim stranicama ili kada mobilnim uređajem zovemo drugu osobu u pozadini se odvija proces šifriranja i dešifriranja, najčešće uz pomoć javnoga ključa. Zakrivanje se tako preselilo iz svijeta elektromehaničkih rotora u računalnu sferu jedinica i nula – proces koji ne vidimo i o kojem većina nas ni ne razmišlja, ali je nužan za zaštitu naših osobnih podataka u vrijeme kada nam je rapidnim razvojem interneta i društvenih mreža sve postalo dostupno jednostavnim pritiskom nekoliko tipaka.

Literatura

1. Carter, Frank. Codebreaking with the Colossus Computer: Bletchley Park Reports. Bletchley Park Trust, 2008.
2. Churchhouse, Robert. Codes and Ciphers: Julius Caesar, the Enigma and the Internet. Cambridge: Cambridge University Press, 2002.
3. Flowers, Thomas H. The Design of Colossus. Annals of the History of Computing.
4. Gannon, Paul. Colossus: Bletchley Park's Greatest Secret. Great Britan: Atlantic Books Ltd, 2006.
5. General Report on Tunny: With Emphasis on Statistical Methods / Reeds, James A; Diffie, Whitfield; Field, J. V.
6. Hinsley, F. H. i Stripp, Alan. The Inside Story of Bletchley Park. Oxford: Oxford University Press, 1993.
7. McKay, Sinclair. The Secret Life of Bletchley Park: the WWII Codebreaking Centre and the Men and Women Who Worked There. London: Aurum Press Ltd, 2010.
8. Rojas, Raúl. The First Computers: History and Architecture. Cambridge, Massachusetts: The MIT Press, 2000.
9. Sale, Tony. The Colossus of Bletchley Park – The German Cipher System
10. Singh, Simon. The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography. New York: Anchor Books, 2000.

Popis slika