

SVEUČILIŠTE U ZAGREBU
FILOZOFSKI FAKULTET
ODSJEK ZA INFORMACIJSKE I KOMUNIKACIJSKE ZNANOSTI
Ak. God. 2017./2018.

Luka Pađen

Kriptologija u teoriji i praksi u prvoj polovici dvadesetog stoljeća

Diplomski rad

Mentor: dr. sc. Vjera Lopina

Zagreb, 2018.

Sadržaj

Sažetak	2
Abstract	3
1. Uvod.....	4
2. Kriptologija - tisućljetna znanost	5
3. Kriptologija kroz povijest do početka 20. stoljeća.....	8
3.1. Stari vijek	8
3.2. Srednji vijek	9
3.3. Od Srednjeg vijeka do početka 20. stoljeća	10
4. Kriptologija uoči Drugog svjetskog rata.....	11
4.1. Prvi svjetski rat.....	11
4.2. Prvi elektromehanički kriptografski strojevi.....	14
4.3. Situacija na početku Drugog svjetskog rata.....	17
5 Elektromehanički strojevi Sila Osovine.....	18
5.1. Enigma	18
5.2. T-52	27
5.3. Lorenz SZ.....	29
5.4. Red	31
5.5. Purple	32
6. Elektromehanički strojevi Saveznika.....	33
6.1. Typex.....	34
6.2. Sigaba.....	36
6.3. Combined Cipher Machine	39
7. Ostale vrste tajne komunikacije	40
8. Kriptoanaliza prve polovice 20. stoljeće.....	42
8.1. Kriptoanaliza u Drugom svjetskom ratu	43
9. Utjecaj na suvremenu kriptologiju.....	50
10. Zaključak.....	53
11. Literatura	54

Sažetak

Kriptologija, ta vrlo kompleksna i stara znanost, od svojih najranijih početaka bila je interdisciplinarna, i služila se dostignućima drugih znanosti kako bi razvila nove načine sigurne komunikacije. Matematika, logika i fizika samo su neke od znanosti koje su pomogle u teoretskom napretku kriptologije, koja je svoju najveću revoluciju doživjela potpomognuta modernim električnim i mehaničkim inženjerstvom pomoću kojeg su konstruirani prvi elektromehanički enkripcijski strojevi, a koji su također otvorili put suvremenom računalstvu. Drugi svjetski rat je najbolje dokumentiran i istražen dio povijesti kriptologije, a to vrijeme svjedočilo je i praktičnim implementacijama različitih teorija ove znanosti. Kriptografija i kriptanaliza obje su doživjele vrlo velike promjene u periodu Drugog svjetskog rata, a izumi korišteni u tom vremenu postali su temeljem budućeg razvoja kriptologije. Znanstvenici kao što su Alan Turing, Arthur Scherbius, Marian Rejewski i William Tutte samo su neki od najpoznatijih stručnjaka tog vremena, a bez njihovih zasluga današnja bi znanost zasigurno bila puno siromašnija.

Ključne riječi: kriptologija, Drugi svjetski rat, Enigma, kriptanaliza, kriptografija, Alan Turing

Abstract

Cryptology, an old and complex science, was from the very beginning composed of different scientific disciplines and used the achievements of other sciences to develop new methods of secure communication. Mathematics, Logic, and Physics are a few out of many sciences that helped develop Cryptology, which in the end lived through its greatest revolution based on modern electrical and mechanical engineering, used to construct the first electromechanical cypher machines that also opened the way to the modern Computer science. The Second World War was the most documented and investigated part of Cryptology's history, and those times have also witnessed the practical implementations of different cryptological theories. Cryptography and cryptanalysis both witnessed great changes during the Second World War period, and the inventions used during that time became the basis of the later advancement of Cryptology. Scientists such as Alan Turing, Arthur Scherbius, Marian Rejewski and William Tutte are just a few of the great people who worked during that period, but without their efforts modern science as a whole would surely not be as great and advanced as it is today.

Ključne riječi: Cryptology, Second World War, Enigma Cryptanalysis, Encryption, Alan Turing

1. Uvod

Kriptologija je znanost koja, iako stara nekoliko tisućljeća, u suvremenom svijetu nimalo ne gubi svoju važnost, štoviše, mogli bismo reći da je postala važnija nego ikad. Kriptologija svoju primjenu danas pronalazi u širokom spektru ljudske djelatnosti, od bankarstva, informatike (hardvera i softvera), vojne industrije, pa sve do ekonomije, u vidu osiguravanja kriptovaluta. Međutim, kriptologija kakvu je poznajemo danas, počela se formirati tek početkom prošlog stoljeća, zaslugama nekoliko ključnih znanstvenika koji su posjedovali izvanredne matematičke vještine, a koje su im omogućile da započnu razvoj složenih algoritama koji su stvorili pravu revoluciju u području kriptologije. Ovaj rad bavit će se upravo tim periodom prve polovice prošlog stoljeća, a istražiti će ključne teorijske pretpostavke i njihovu praktičnu realizaciju do kraja Drugog svjetskog rata, kao i slikovitu povijest koja je dovela do tih spoznaja. Kako su za revoluciju u području kriptologije u proteklom stoljeću zaslužna upravo ratna zbivanja, naglasak će također biti na brojnim elektromehaničkim izumima koji su korišteni u ratne svrhe, a predstavljali su već spomenutu realizaciju različitih teorija.

Algoritmi razvijeni u ovom periodu poslužili su kao odskočna daska za razvoj modernih sustava šifriranja, a želimo li se baviti suvremenim algoritmima, bilo bi vrlo korisno upoznati se i s poviješću koja je dovela do njihova razvoja.

2. Kriptologija - tisućljetna znanost

Kako će se sljedeća poglavlja baviti temama za koje je potrebno znati osnovne pojmove kojima se ova znanost bavi, valjalo bi ih najprije obrazložiti. Kriptologija je znanost koja obuhvaća širok spektar različitih djelatnosti, stoga je teško izvesti sveobuhvatnu definiciju koja bi odgovarala svim metodama i djelatnostima ove kompleksne znanosti. Jednostavne definicije ponekad su ujedno i najbolje, a jedna od njih koju donosi Oxford Dictionary kaže da je kriptologija "postupak proučavanja kodova, ili umijeće njihova pisanja i odgonetavanja"¹. Sama riječ "kriptologija" dolazi od kombinacije grčkih riječi *kryptos* (zakriti, skriven) i *logos* (govor, riječ). Iz prethodno spomenute definicije odmah se može zaključiti da je osnova kriptologije, ali i glavni predmet njena izučavanja - kôd. Kodovi dolaze u raznim oblicima, a predstavljaju dogovorenu metodu kojom se poruka napisana čitljivim tekstom (jasnopisom) pretvara u nečitljiv, skriven oblik (zakritak). Ovaj proces koji se odvija korištenjem koda naziva se zakrivanje (šifriranje, enkripcija) poruke, a obrnuti proces, kojim se nečitljiva poruka pretvara u čitljivu naziva se raskrivanje (dešifriranje, dekripcija) poruke². Postoje dvije vrste raskrivanja poruke - jedna se odvija uz posjedovanje ključa (raskrivanje), dok se druga odvija bez posjedovanja ključa i naziva se kriptozanalizom³. Ključ je u kriptologiji naziv za informaciju koja onome koji tu informaciju posjeduje otkriva kakvom je metodom originalna poruka zakrivena, što mu omogućuje raskrivanje poruke⁴. Osim ovakve podjele, nerijetko se pojavljuje i podjela na kriptografiju i kriptozanalizu kao glavne dvije grane kriptologije. Kriptografija predstavlja primijenjenu kriptologiju, odnosno proces proučavanja i sastavljanja zakritnih algoritama te njihovu primjenu u pisanju poruka⁵.

Međutim, kada govorimo o zakrivanju poruke, kodovi nisu jedini način kojim se ono može postići. Druga metoda kojom se poruka može zakriti je šifra (arapski "*sifr*" - "ništa")⁶. Razlika između šifre i koda je jasna - šifra se sastoji od slova (uglavnom njihove supstitucije), dok kod može biti sačinjen od slova, simbola ili slogova. Šifre također mogu zamijeniti samo jedan znak (slovo) drugim znakom, dok se kodom veće jedinice mogu zamijeniti manjima, npr. jednim simbolom može se

1 Oxford Dictionaries Online. Pristup: 2018.

2 Hrvatska enciklopedija (online izdanje). Pristup: 2018.

3 Kriptozanaliza se često definira kao odvojen pojam, jer spada u posebnu kategoriju koja se veže uz informacijsko ratovanje.

4 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 točno 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.

5 Kriptografija (en. "*cryptography*") se također koristi kao sinonim za kriptozanalizu, i to najčešće u literaturi pisanoj na engleskom jeziku.

6 Wrixon (1998.), str. 21.

zamijeniti čitava jedna riječ, i to je temeljna razlika između šifre i koda⁷. Primjer jedne jednostavne šifre je "Cezarova šifra", koju prikazuje sljedeća slika:

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
V Z Ž 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
DANAS JE SUNČAN DAN = CVLVO GD OSLAVL CVL

Slika 1 - Primjer Cezarove šifre

U slučaju Cezarove šifre koriste se dvije abecede - jedna pomoću koje se piše jasnopis, i druga koja predstavlja ključ za pisanje zakritka (i raskrivanje poruke). Prilikom šifriranja koristi se pomak od 3 znaka, prilikom kojeg se abeceda ključa potpisuje pod abecedu jasnopisa, ali tako da se prvo slovo pomakne za tri mjesta udesno i tako pretvori u novo slovo. Cezarova šifra jedna je od najjednostavnijih, što je ujedno i prednost i mana. Loša strana šifri je to što se konstrukcija šifrirane poruke ne razlikuje previše od jasnopisa. Vidljivo je da je duljina riječi ostala ista, što je vrlo loše ukoliko se neka treća strana odluči probiti šifru i doznati što je originalna poruka. Šifre se, za razliku od kodova, metodama kriptanalize mogu lakše razotkriti upravo zbog tog nedostatka, a lakše ih je razumjeti i kad posjedujemo jasnopis i zakritak, a ne posjedujemo ključ. Poruka se tada može jasno razotkriti zamjenom slova u zakritku slovima jasnopisa.

Što se tiče šifri, zakrivanje poruka je nešto teže, ali produkt njihova korištenja je poruka koja je sigurnija i teža za razbiti metodama kriptanalize. Spomenuli smo već da se korištenjem kodova mogu zamijeniti čitave riječi pojedinačnim znakom, slovom ili simbolom, što dodatno skraćuje konačni zakritak, ali takvu poruku lakše je razbiti metodama kriptanalize. Kodovi se koriste prema dogovoru onog koji poruku zakriva (pošiljatelja), i onoga tko ju raskriva (primatelja), a taj dogovor najčešće je zapisan u obliku knjige kodova (en. "*codebook*"), o čemu će biti više riječi u jednom od sljedećih poglavlja. Knjiga kodova ujedno predstavlja i ključ za raskrivanje ili zakrivanje poruke, a u slučaju da takva knjiga padne u ruke nekome kome poruka nije namijenjena, ta osoba bi bez problema mogla otkriti originalnu poruku⁸.

⁷ Isto, str. 674.

⁸ Za vrijeme Drugog svjetskog rata, Saveznici su uspjeli zarobiti nekoliko takvih knjiga, što im je na kraju omogućilo da shvate algoritam njemačkih elektromehaničkih strojeva koji su se koristili u tajnoj komunikaciji (npr. Enigma),

"kod", on nije shvaćen u istom smislu kao što ga definira kriptologija¹¹. Morseov kod zapravo bi bio bliži šifri nego kodu, zbog načina na koji se odvija supstitucija jednog slova jednim Morseovim znakom.

Koncepti i pojmovi predloženi u ovom poglavlju temelj su za razumijevanje kriptologije kao znanosti, a pojavljuju se čak i u današnjoj, modernoj kriptologiji, iako su im značenja nerijetko proširena kako bi se mogli primijeniti na suvremene algoritme i metode.

3. Kriptologija kroz povijest do početka 20. stoljeća

Nakon upoznavanja temeljnih koncepata i pojmova na kojima se temelji kriptologija kao znanost, možemo dati pregled njene povijesti do početka 20. stoljeća, čime će se baviti ostala poglavlja. Kao što je ranije navedeno, kriptologija je starija više tisuća godina, i njen razvoj usko je vezan uz razvoj matematike. a danas predstavlja znanost koja je vrlo interdisciplinarna - obuhvaća sve od matematike, statistike, logike, lingvistike, pa sve do elektromehanike, računalstva i umjetne inteligencije koje su više izražene danas nego u prošlosti¹². No, kriptologija je u svojim počecima bila vrlo skromna. Smatra se da se potreba za kriptologijom pojavila već za vrijeme drevnih carstava, kada su poljoprivreda i trgovina postale osnova ekonomije takvih carstava.

3.1 Stari vijek

Većina dokaza upućuje na to da se kriptologija počela razvijati prije gotovo četiri tisuće godina. Vjeruje se da su se prve šifre počele koristiti već u Egipatskom, Babilonskom i Sumerskom carstvu, a čak je i u Bibliji zapisano da su stari Hebreji običavali šifrirati svoje poruke¹³. Hebreji su također razvili i svojevrstu igru pamćenja židovskog pisma (abecede), nazvanu jednostavno "Jeremijina igra"¹⁴. Jeremijina igra sastojala se u tome da se rečenica pisana jasnopisom jednostavnom supstitucijom korištenjem ključa pretvori u sličnu rečenicu koja bi imala drukčije

11 Morseov kod je specifičan i po tome što se koristi kao osnova u nekim algoritmima kriptografije, a prvenstveno je vezan uz elektromehaničke kriptografske strojeve kao što je Enigma, gdje se koristio u komunikaciji za slanje zakritka.

12 Bauer (2002.), str. 2.

13 Primjeri stare hebrejske enkripcije mogu se pronaći u Starom Zavjetu - u knjizi Jeremija, gdje se neka ključna imena zamjenjuju onima koja se dobiju zakrivanjem pomoću jednostavnog ključa.

14 Hoskisson (2010.), str. 3.

značenje. Sustav supstitucije bio je vrlo jednostavan, čak jednostavniji od Cezarove šifre, uz razliku da nije postojao pomak od tri znaka, već se, na primjer, prvo slovo abecede zamjenjivalo posljednjim, drugo preposljednjim i tako do kraja. Hebreji su ovu metodu supstitucije nazvali "athash"¹⁵. Osim jednostavnih supstitucijskih šifri, ništa značajno vezano uz kriptologiju nije se dogodilo prije Srednjeg vijeka. Dominacija kultura i civilizacija Male Azije i Sjeverne Afrike osjetila se i u znanosti, iako su i kulture Dalekog istoka također razvijale vlastite kriptografske metode, a Indija je bila predvodnica takvih pokušaja toga vremena.

3.2 Srednji vijek

Kriptologija i metode zakrivanja poruka razvijale su se relativno sporo, uz minimalnu evoluciju na području matematičkih modela zakrivanja poruka. Takva situacija održavala se tisućama godina, sve do dolaska osvajačkih arapskih plemena na područje Sjeverne Afrike i Malu Aziju u sedmom i osmom stoljeću. Do dolaska Arapa, kriptologiju su uglavnom razvijali stari Grci (koji su toj znanosti i osmislili ime) i Egipćani¹⁶. Dolaskom Arapa dolazi do svojevrsne revolucije u području matematike, a samim time i kriptologije. Arapski matematičari prikupili su veliku količinu helenskog znanja i iskoristili ga za napredak vlastite civilizacije. Za razliku od Grka koji su se do tada bavili isključivo kriptografijom (npr. Spartanci, već spomenutom metodom korištenja kože ili platna omotanog oko štapa), Arapi su prvi krenuli razvijati kriptanalizu. Teorija i praksa kriptanalize tako je započela razvijanjem **frekvencijske metode** - metode koja se temeljila na proučavanju frekvencijskog pojavljivanja riječi, znakova ili simbola u tekstu¹⁷. Za razvoj ove metode zaslužan je arapski intelektualac Al-Kindi, koji je pri analizi muslimanskih vjerskih tekstova primijetio učestalo pojavljivanje nekih znakova ili riječi. Ova tehnika postala je vrlo rasprostranjenom, a nastavila se koristiti čak i u moderno vrijeme¹⁸, prvenstveno za vrijeme Drugog svjetskog rata, gdje je pod rukovodstvom Alana Turinga korištena u pokušajima razbijanja njemačkih kriptografskih algoritama. Arapska osvajanja i trgovina naposljetku su dovela i nova otkrića u Europu, gdje su se ona usavršila do početka dvadesetog stoljeća.

15 Wrixon (1998.), str. 19.

16 Nimalo čudno, s obzirom na to da su upravo ovi narodi bili prvaci matematičkih otkrića tokom više tisućljeća, a samim time omogućili su i razvoj kriptologije.

17 Isto, str. 21.

18 Osim u području kriptologije, frekvencijska metoda koristila se i u ostalim znanostima, na primjer, statistici i informacijskim znanostima.

3.3. Od Srednjeg vijeka do početka 20. stoljeća

Tijekom Srednjeg vijeka, potreba za tajnom komunikacijom u Europi znatno je porasla, što možemo pripisati usponima i padovima brojnih carstava i kraljevstava, osnivanjima tajnih društava (Masoni), porastu trgovačkog prometa i politici. Međutim, razvoj kriptologije i u tom periodu tekao je dosta sporo. U periodu Renesanse, međutim, ponovno dolazi do revolucije u području kriptologije (konkretnije, kriptografije). Revolucija u kriptografiji ogledala se u osmišljavanju novih šifri i metoda zakrivanja teksta, kao i korištenju ključeva koji su bili mnogo kompleksniji nego u dotadašnjoj povijesti. Primjer jednog takvog, kompleksnijeg sustava, je šifra koju je u šesnaestom stoljeću razvio francuski diplomat Blaise de Vigenère, a sama šifra nazvana je "Vigenèreovom šifrom". Vigenère je odlučio unaprijediti Cezarovu šifru, i to tako što je umjesto ključa koji je u slučaju Cezarove šifre bila abeceda s pomakom od tri znaka, razvio tzv. "Vigenèreovu tablicu" - tablicu koja je sadržavala okomito i vodoravno ispisane abecede i čija je svrha bila onemogućiti kriptanalizu zakritka frekvencijskom metodom, koja je tada već bila raširena metoda razbijanja šifri. Vigenèreu je uspjelo stvoriti "nerazrješivu šifru" (kako su je nazvali njegovi suvremenici, a nije razbijena sve do devetnaestog stoljeća. Njegove zasluge stavile su nove prepreke pred kriptanalizu, a frekvencijska metoda privremeno je postala neučinkovita.

Kriptologija se nastavila razvijati smjerom koji su zacrtali Vigenère i njegovi suvremenici sve do devetnaestog stoljeća. Zanimljivo je da je kriptologija sredinom 17. stoljeća postala i službeno zanimanje na kraljevskim dvorovima, osnivanjem tzv. "Crnih odaja" (en. *Black Chamber*)¹⁹.

Sljedeći izum koji je omogućio ogroman napredak u području kriptologije je **telegraf** - uređaj za prijenos kodiranih poruka. Telegraf je omogućio nastanak elektromehaničkih enkripcijskih uređaja koji bi se koristili složenijim algoritmima za zakrivanje ili raskrivanje poruka, a vrhunac ovog otkrića manifestirat će se za vrijeme Drugog svjetskog rata, izumima kao što su Enigma, SIGABA i slično. 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. Kao i gotovo sva značajna otkrića modernog doba, i ovo je nastalo u vojne svrhe, a postat će najrasprostranjenija metoda komunikacije do kraja prve polovice dvadesetog stoljeća.

Sve ove revolucije, ili postepene evolucije, dovest će u prvoj polovici dvadesetog stoljeća do uspostavljanja kriptologije kao jedinstvene znanosti i dati joj okvir za razvoj koji će joj omogućiti da postane ono što ona jest danas.

¹⁹ Isto, str. 36.

4. Kriptologija uoči Drugog svjetskog rata

Početak dvadesetog stoljeća obilježen je prvim pokušajima da se konstruiranju primitivni elektromehanički strojevi koji bi teoretski bili sposobni realizirati složene algoritme zakrivanja poruka. što bi se postiglo uključivanjem pomičnih mehaničkih dijelova stroja u sam algoritam.

Na samom kraju devetnaestog stoljeća, izum radija postavio je nove mogućnosti, ali i izazove pred kriptologiju. Prijenos zakrivenih poruka postao je lakši nego u početku, kada je trebala postojati fizička veza između dva telegrafskih centra. No, loša strana je bila ta da su radio-signalu mogli pristupiti i oni koji nisu sudjelovali u komunikaciji između dva operatera. Tako je došlo do potrebe za sve jačim protumjerama koje bi spriječile pokušaje kriptanalize presretanih radio-poruka. Ovakve novosti potaknule su neke teoretičare na razmišljanje i donošenje novih pretpostavki o tome kako bi se kriptologija trebala shvatiti, razvijati, i na kraju krajeva koristiti. Jedan od tih teoretičara bio je i Auguste Kerckhoffs, koji je u svojem djelu "*La Cryptographie Militaire*" (franc. "Vojna kriptografija")²⁰ napisao da:

- a) zakritak u praksi mora biti neprobojan
- b) kriptosni sustav mora biti prikladan za komuniciranje
- c) ključ mora biti lako pamtljiv i lako promjenjiv
- d) zakritak mora biti moguće prenijeti telegrafom
- e) aparat za šifriranje mora biti lako prenosiv
- f) kriptografski stroj mora biti jednostavan za rukovanje

Temelji koje je Kerckhoffs postavio bit će osnova elektromehaničke kriptografije koja je započela u Prvom svjetskom ratu, a vrhunac doživjela za vrijeme Drugog svjetskog rata.

4.1. Prvi svjetski rat

Prvi svjetski rat je bio prvi veliki vojni sukob u kojem su se aktivno upotrebljavali mehanički kriptografski strojevi. Iako su se takvi strojevi pokušali koristiti i ranije, njihov ulazak u vojnu upotrebu dogodio se tek u Prvom svjetskom ratu. Nažalost, strojevi (ili, bolje rečeno, uređaji)

²⁰ Cohen, F. (1990.). URL: <http://all.net/edu/curr/ip/Chap2-1.html> (5.9.2018.).

korišteni u ovom periodu bili su vrlo primitivni. Pošto je telegraf i dalje bio osnova za prenošenje poruka na bojišnici i komunikaciju u ratu, to se odrazilo i na dizajn samih kriptografskih uređaja, koji su uglavnom bili dizajnirani kao teleprinter koji je istovremeno omogućavao jednostavno pisanje poruka i slanje putem telegrafske veze. Naime, iako je radio izumljen otprilike dvadeset godina prije početka Prvog svjetskog rata, telegraf je i dalje bio glavna osnova za komunikaciju. Prvi svjetski rat bio je rovovski rat u kojem se oružje dvadesetog stoljeća koristilo uz taktike devetnaestog stoljeća, što će reći da je tehnologija tadašnjeg naoružanja prestigla teoriju (doktrinu). Samim time, bojište je bilo vrlo statično, što je pogodovalo sigurnoj fizičkoj vezi koju je zahtijevao telegraf. Radijski signal bio je nesiguran jer se mogao presretati, a potreba za njime pojavila se tek u Drugom svjetskom ratu, kada je pokretljivost vojske i brza promjena crte bojišta zahtijevala komunikaciju čija veza nije ovisila o fizičkoj povezanosti, koju je zahtijevao telegraf²¹.

Iako je kriptologiju Prvog svjetskog rata obilježila pojava primitivnijih kriptografskih strojeva, u tajnoj komunikaciji i dalje su prevladavali kodovi i šifre koji bi bili korišteni da se zakritak zapiše i pošalje na papiru (ili kao što je ranije spomenuto, telegrafom)²². Jedna od najpoznatijih šifri Velikog rata je njemačka šifra korištena na zapadnom bojištu, nazvana jednostavno "ADFGVX", a predstavljala je nastavak u razvoju metode zvane "Polibijeva kutija"²³. Jednostavna Polibijeva kutija predstavljala je algoritam **bipartitne supstitucije**, što znači da se jedno slovo jasnopisa zamjenjivalo dvama slovima koji predstavljaju položaj toga slova u tablici. Na primjer:

	1	2	3	4	5
1	a	b	c	č/ć	d
2	dž/đ	e	f	g	h
3	i	j	k	l/lj	m
4	n/nj	o	p	r	s
5	š	t	u	v	z/ž

21 Iako je radio korišten u pomorskim bitkama, velika većina bitki Prvog svjetskog rata odvijala se na kopnu, stoga je postotak ovakve komunikacije zanemariv.

22 U Prvom svjetskom ratu, za razliku od Drugog svjetskog rata, velik dio poruka i dalje su prenosili pismonoše ili kuriri, koji su, zbog nedostatka modernih vozila i oklopnih vozila bili prisiljeni poruke dostavljati biciklom ili konjima.

23 Bauer (2002.), str. 51.

Možemo odmah zaključiti da bi ovakva tablica bila vrlo nepogodna za hrvatski jezik, zbog prevelikog broja znakova u hrvatskoj abecedi, no to je omogućeno ADFGVX algoritmom koji je proširio tablicu za još jedan redak i stupac²⁴.

Ako bismo zakrili neku poruku ovom tablicom, na primjer:

Danas je petak

poruka bi izgledala ovako:

1511411145 3222 4322521133

Vidljivo je da je ovo vrlo jednostavna šifra koja koristi jednostavniji Vigenereov model, što se pokazalo i lošom karakteristikom u praksi. Njemačka vojska pokušala je doskočiti ovom problemu proširivanjem ADFGVX algoritma dodatnim stupcem i retkom, ali i uvođenjem više tablica i više koraka zakrivanja, no britanski tim i dalje je uspio razbiti njihovu šifru²⁵. Glavni problem ove šifre predstavljala je frekvencija, pojavljivanja nekih znakova, u gornjoj poruci prvenstveno znakova "a" i "e". Algoritam je stoga vrlo slab protiv nekih modela kriptanalize koji su se temeljili na frekvencijskoj analizi koju je utemeljio Al-Kindi.

Krajem Prvog svjetskog rata, britanski vojnik **Gilbert Vernam** pokušao je riješiti problem sigurnosti kriptografije tako što je izmislio metodu nazvanu "*One-time pad*" (eng. "Jednokratni ključ")²⁶. Ova metoda uključuje odabir jednog ključa, koji mora biti jednako dug kao i jasnopis, te korištenje toga ključa za jednokratno zakrivanje poruke. I pošiljatelj i primatelj moraju posjedovati ključ, kako bi se poruka mogla i zakriti i raskriti. Ova metoda pokazala se najsigurnijom, zato što je posjedovanje ključa samo dvojice operatora garantiralo da su šanse gotovo nikakve da će ključ pasti u ruke neprijatelja, što je bio čest slučaj s knjigama koje su sadržavale ispisane kodove. One-time pad je najučinkovitija vrsta šifre koju je nemoguće razbiti konvencionalnim metodama, a snaga šifre ovisi o sigurnosti ključa - ako neprijatelj ne posjeduje ključ, razbijanje poruke je nemoguće, jer je ključ uistinu nasumičan. Ključ se također mora mijenjati nakon razmjenjivanja svake poruke, što znači da frekvencijska analiza dvije različite poruke nikad neće dati iste rezultate. Ovakva metoda koristila se i kasnije, u Drugom svjetskom ratu, i to upravo u njemačkoj kriptografiji za koju se

24 Iako je tablica proširena, njemačka vojska u algoritam je ubacila brojeve, tako da bi za hrvatski jezik i takav algoritam bio nedovoljan.

25 Cohen, F. (1990.). URL: <http://all.net/edu/curr/ip/Chap2-1.html> (5.9.2018.).

26 Schneier (1996.), str. 15.

smatralo da je nerazrješiva. Možda je uistinu i bilo tako, no više riječi o tome bit će u jednom od narednih poglavlja.

4.2. Prvi elektromehanički kriptografski strojevi

Prvi svjetski rat, iako najveći globalni sukob dotadašnje ljudske povijesti, proizveo je i nekoliko pozitivnih otkrića ili spoznaja, od kojih je jedna bila i ta da je sigurnost komunikacije, enkripcija poruka i potreba za novim modelima i uređajima koji bi to omogućili od presudne važnosti. Samim time, u poslijeratnim godinama u raznim dijelovima Europe pojavili su se izumitelji sa sličnim idejama - proizvesti moderni uređaj ili stroj koji bi omogućio sigurnosno prenošenje poruka bez straha od nepoželjnih akcija treće strane. Iako se može pretpostaviti da su takvi izumi nastali u vojne svrhe, ili financirani novcem vojne industrije, to nije bio slučaj²⁷. Prvi takav uređaj patentiran je u Švedskoj, od strane švedskog znanstvenika zvanog Arvid Gerhard Damm²⁸. Nažalost, o ovom uređaju ne zna se mnogo, osim da je princip rada tog uređaja bio temeljen na sudjelovanju pomičnih mehaničkih rotora u algoritmu zakrivljanja poruke²⁹, te da je uređaj bio namijenjen u komercijalne svrhe. Damm je svoj izum patentirao 1919. godine, no takav uređaj nikad nije proizveden, a zbog financijskih neprilika Damm je privremeno morao napustiti kriptologiju.

Dammov patent i utjecaj ostavio je vrlo dubok trag na sljedeće desetljeće, a utjecaj koji je zamisao o elektromehaničkim strojevima baziranim na radu pomičnih rotora ostavio bit će vidljiv gotovo do kraja dvadesetog stoljeća. Godine 1921. Edward Hugh Hebern, američki kriptolog, uspio je realizirati svoju zamisao na kojoj je radio godinama. Njegov elektromehanički stroj za potrebe šifriranja poruka prezentirao je američkoj vojsci (konkretnije, mornarici), uz komentar da je proizveo "neprobojni" kriptografski alat³⁰. Za razliku od Damma, Hebern je osigurao dovoljno sredstava, i čak registrirao vlastito poduzeće za proizvodnju kriptografskih strojeva, ali na kraju se zbog loših poslovnih odluka njegovo poduzeće moralo zatvoriti. Međutim, američka ratna mornarica ipak je uspjela osigurati dovoljno njegovih strojeva kako bi se mogli zaposliti stručnjaci koji bi nastavili istraživanja u tom području.

27 Za razliku od europskih kriptologa, koji su svoje izume namijenili komercijalnoj upotrebi, američki su ih pokušavali prodati isključivo vojsci.

28 Kahn (1967.), str. 214.

29 Elektromehanički strojevi korišteni u Drugom svjetskom ratu uglavnom će se bazirati na radu pomičnih rotora, što znači da je Damm bio na tragu vrlo revolucionarne metode kriptografije.

30 Isto, str. 212.

U Europi je pak, Damm utjecao na daljnji razvoj elektromehaničkih kriptografskih strojeva. Hugo Koch, nizozemski znanstvenik, konstruirao je sličan uređaj i uspio dobiti patent nizozemskih vlasti, ali ni njegov stroj, kao ni Dammov, nije zaživio u upotrebi. I jedan i drugi uređaj bili su zamišljeni kao pisaći stroj koji je posjedovao dodatne dijelove koji bi omogućili jednostavno, ali učinkovito zakrivanje poruka.

Vjerojatno najvažnije ime dvadesetih godina prošlog stoljeća u području elektromehaničke kriptografije predstavljao je **Arthur Scherbius**, njemački kriptolog koji je zaslužan za stroj koji će obilježiti Drugi svjetski rat, ali i kriptologiju dvadesetog stoljeća uopće - **Enigma**³¹. Scherbius je, kao i njegovi europski suvremenici, Enigmu izradio kako bi se mogla koristiti u komercijalne ili političke svrhe (prvenstveno, poštansku upotrebu, trgovinu i diplomaciju). Scherbius je također uspio patentirati svoj izum, preuzevši Kochovo pravo na patent. Enigma je u upotrebu ušla 1923. godine, a temeljne ideje i princip rada Scherbius je osobno predstavio u obliku članka u časopisu *Elektronische Zeitschrift*. Enigma je, sukladno tradiciji kriptologije 1920-ih godina, izgledala kao pisaći stroj. Glavna ideja koju je Scherbius izložio bila je jedinstven kriptografski stroj koji bi bio sposoban ispisivati zakrivene poruke na papir - korisnik bi trebao jednostavno napisati poruku onakvu kakva je ona u svom originalnom obliku (jasnopis), a stroj bi sam obavio proces zakrivanja poruke. Na papiru bi se, na kraju, ispisao zakritak³². Scherbius je stroj zamislio kao vrlo jednostavan za korištenje, ali u praksi nemoguć za razbiti. Enigma je posjedovala nekoliko temeljnih dijelova, a neki od njih su bili uključeni u sam algoritam zakrivanja. Kako je prva inačica Enigme koju je Scherbius predstavio u svojem članku posjedovala manji broj dijelova koji su sudjelovali u algoritmu zakrivanja poruke, tako je i njen algoritam bio slabiji. Osim uobičajenih dijelova koje je posjedovao svaki pisaći stroj, Scherbiusov je stroj posjedovao četiri pomična rotora koji su radili na elektromehaničkom principu. Pritiskom tipke na ploči s tipkama električni signal poslao bi se, kroz pomične rotore, do pisaće glave koja bi zapisala znak na papir. U posebnom poglavlju o Enigmi bit zakritni algoritam bit će detaljno objašnjen, uz dodatne pojedinosti o novim elementima koje je uvela njemačka vojska. Bitno je napomenuti da je Enigma u svojim počecima bila vrlo loš stroj za potrebe vojske - vrlo teška i zahtjevna za korištenje, a kasnije je pojednostavljena i napravljena tako da stane u manju drvenu kutiju.

Što se tiče ideja kojima su izumitelji elektromehaničkih kriptografskih strojeva bili rukovođeni, one su uglavnom predstavljale reakciju na dotadašnja dostignuća metoda kriptanalize. Uvjerivši se u nepouzdanost kodova i supstitucijskih šifri koje je bilo lako razbiti korištenjem suvremenih metoda razvijenih na osnovi frekvencijske analize, izumitelji suvremenih strojeva nastojali su se približiti

31 Njemačka i engleska riječ za zagonetku.

32 Scherbius (1923.).

"pravoj" nasumičnosti i nerazrješivosti koje se dosjetio Vernam u obliku one-time pad metode. Neki strojevi, poput Enigme, posjedovali su rotore koji bi prolaskom električnog signala mijenjali položaj. U slučaju Enigme, jedan rotor pomicao bi se svakim pritiskom tipke na ploči s tipkama, njemu susjedni rotor pomicao bi se svakih osam pomaka početnog rotora i tako dalje do posljednjeg rotora. Ovakav sustav omogućavao je konstantni *scramble* (eng. miješanje) slova u zamišljenom zakritnom slovoredu³³.

Osim europskih i američkih kriptografskih strojeva, koji su se razvijali u vrlo sličnom pravcu, dvadesete godine prošlog stoljeća obilježio je i razvoj kriptologije na Istoku - doduše, sa sličnim fokusom na razvoj kriptografskih elektromehaničkih strojeva. O sovjetskoj kriptografiji nema gotovo nikakvih informacija³⁴, osim da su ruski kriptolozi uspjeli izraditi stroj temeljen na radu pomičnih rotora, koji je bio sličan Hagelinovu³⁵ patentu. Stroj kodnog imena K-27, od američkih znanstvenika nazvan "Crystal", proizvodnju je započeo tek 1940. godine i sudeći prema izvještaju njemačke vojske koja je tijekom Drugog svjetskog rata uspjela zarobiti nekoliko primjeraka, njegov algoritam bio je vrlo slab. Također, za razliku od zapadnih sila, Sovjeti su se znatno manje oslanjali na kriptologiju, koja je u toj zemlji zaživjela tek u tridesetim godinama prošlog stoljeća³⁶.

Osim Sovjetskog slučaja, i Japan se također uključio u izradu kriptografskih strojeva, prvenstveno za potrebe svoje vojske i diplomacije (kao i Sovjetski Savez). Japanski su diplomati, prilikom posjeta Europi za vrijeme mirovnih pregovora u poslijeratnim godinama Prvog svjetskog rata, uvidjeli važnost sigurne komunikacije za budući razvoj vojske i diplomacije. Novoostvarenim vezama pokušali su i sami postići uspjehe tadašnjih zapadnih saveznika, i to kroz suradnju s Poljskom. Međutim, zbog nedovoljne suradnje, ili zbog same prirode japanskog jezika i pisma, Japan nije uspio doći do dobrih rješenja, te su japanski strojevi običavali biti lošije kvalitete, a posjedovali su vrlo loše algoritme za zakrivljanje poruka. Veliki problem bio je i taj što su japanski kriptolozi smatrali da posjeduju jedan od najboljih sustava supstitucije, no kako je japansko pismo bazirano na slogovima (a ne pojedinačnim slovima), to je svaki algoritam zakrivljanja učinili mnogo jednostavnijim za razbijanje putem kriptanalize. Kao što će se vidjeti i za vrijeme Drugog svjetskog rata, japanska kriptografska mreža prva je razbijena od strane Saveznika, što će imati katastrofalne posljedice za Japan na Pacifičkom bojištu.

33 Zamislimo Cezarovu šifru, ali uz ključ koji se stalno mijenja.

34 Ruske vlasti do danas nisu otvorile arhive u kojima se čuvaju podaci o aktivnostima njihovih znanstvenika zaduženih za razvoj kriptologije i kriptanalize.

35 Boris Hagelin - Dammov idejni nasljednik i znanstvenik koji je nastavio s razvojem švedske kriptologije i kriptanalize.

36 Argenta.ru: Sovjetska enkripcijska služba 1920-1940-e.

URL = <http://www.agentura.ru/press/about/jointprojects/inside-zi/sovietcryptoservice/> (10.5.2018.).

Iz ovih primjera vidljivo je da su elektromehanički kriptografski strojevi postali osnova tajne komunikacije prve polovice dvadesetog stoljeća. Sukladno tome, vrhunac njihove upotrebe predstavljao je upravo Drugi svjetski rat, u kojem je potreba za sigurnom komunikacijom postala od najveće važnosti.

4.3. Situacija na početku Drugog svjetskog rata

Suvremena povijest pokazala je da je konvencionalni način ratovanja nezamisliv bez informacijskog ratovanja, a to se potvrdilo i u slučaju Drugog svjetskog rata. Za razliku od Prvog svjetskog rata, Drugi svjetski rat predstavio je novi model ratovanja gdje su pokretljivost i potreba za konstantnom komunikacijom unutar vojske postale nužnima. To je, naravno, potaknulo potrebu za posjedovanjem velikog broja elektromehaničkih kriptografskih strojeva, koji su tridesetih godina prošlog stoljeća ušli u vojnu upotrebu. Najznačajnije uspjehe u području kriptologije tog razdoblja možemo podijeliti na dvije skupine - one Sila Osovine (na čelu s Njemačkom i Japanom kao glavnim korisnicima enkripcijskih strojeva), te one koje su postigli Saveznici (predvođeni, u području kriptologije, Velikom Britanijom, Poljskom i Sjedinjenim Američkim Državama). Njemački Reich pokazao se, na početku rata, kao zemlja najjačeg enkripcijskog sustava za koji su i Nijemci i Saveznici smatrali da je nemoguće riješiti (no, na kraju se takvo mišljenje ipak pokazalo pogrešnim). Japan je, doduše, bio u vrlo lošem položaju što se kriptografije tiče, a zaslugama britanskih kriptanalitičara je već i prije početka rata japanski kriptografski sustav razbijen.

Saveznici su se u ovom ratu pokazali kao vrsni kriptanalitičari, jer je većina napora njihovih znanstvenika bila uložena u razbijanje Enigme i kriptografije Sila Osovine³⁷, a manje na stvaranje vlastitog sustava zakrivanja poruka. Naime, Poljaci su tijekom tridesetih godina došli u posjed nekoliko Enigmi koje su bile u komercijalnoj upotrebi, i već 1932. matematičkim analizama uspjeli shvatiti način na koji je zakritni algoritam funkcionirao. Međutim, do početka rata njemački su kriptolozi dodatno otežali kriptanalizu Enigme izmjenom unutarnjeg mehanizma koji je također promijenio i algoritam, otežavši tako postupak kriptanalize i do deset puta no što je bio prije izmjena.

Sva dotadašnja otkrića stavit će se u vojne i diplomatske svrhe početkom rata i napadom na Poljsku, a sigurnost komunikacije postat će jednom od glavnih problema Drugog svjetskog rata.

³⁷ Ovo prvenstveno vrijedi za poljske kriptologe .

5. Elektromehanički strojevi Sila Osovine

Dizajn elektromehaničkih kriptografskih strojeva Sila Osovine temeljio se na Scherbiusovu prototipu Enigme, s dodatno modificiranim mehanizmom kako bi se spriječilo, ili barem znatno otežalo mogući postupak kriptanalize. Wehrmacht (vojska nacističke Njemačke) koristio je različite inačice Enigme u svim rodovima vojske - kopnenoj vojsci (*Heer*), mornarici (*Kriegsmarine*)³⁸ te avijaciji (*Luftwaffe*). S druge strane, Japan je svoje strojeve koristio uglavnom u mornaričkom rodu vojske (*Nippon Kaigun*), ali i diplomaciji, za komunikaciju veleposlanika s japanskom vladom. Iako je Drugi svjetski rat također obilježila rekordna upotreba špijuna, čak su i oni u velikoj mjeri koristili strojeve za sigurnosnu komunikaciju.

Iako su i sateliti Sila Osovine posjedovali neke elektromehaničke strojeve za zakrivanje poruka, najvažniji i najrašireniji stroj ipak je bio - Enigma.

5.1. Enigma

Enigma će tijekom rata biti u središtu pozornosti, bilo da se radi o kriptografiji ili kriptanalizi. Nakon Scherbiusova članka iz 1923. godine Enigma je ušla u komercijalnu upotrebu, no prošlo je neko vrijeme prije no što je vojska prepoznala da bi se takav alat mogao vrlo dobro iskoristiti i u vojne svrhe. Prisjetimo se prvog modela Enigme koji je Scherbius predstavio u časopisu *Elektronische Zeitschrift*³⁹. Prema tom nacrtu, Enigma je bila stroj koji je bio najsličniji običnom pisaćem stroju, uz dodatak rotora koji su sudjelovali u algoritmu zakrivanja poruke. Kako su Poljaci već u ranim tridesetim godinama uspjeli razriješiti algoritam na temelju kojeg je Enigma zakrivala poruke, u vojsci se pojavila potreba da se taj stroj dodatno modificira, kako bi u slučaju rata komunikacija ostala sigurna, ali i kako bi se eventualno osigurala komunikacija s diplomatima izvan zemlje.

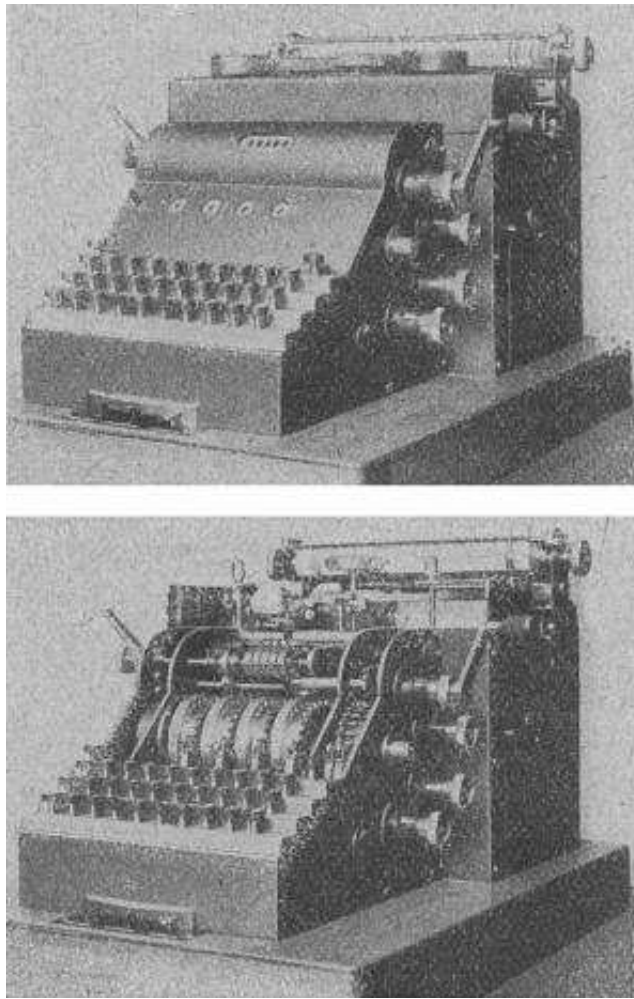
Prvi model Enigme, bez izmjena koje je predložila njemačka vojska, naziva se Enigma tipa A, ili **Enigma A**⁴⁰. Enigma A, ili "pisaća Enigma" je bio velik i nezgrapan stroj, koji je bio namijenjen stacionarnom korištenju. Osim pisaćeg dijela koje je posjedovao i bilo koji pisaći stroj, sastojao se od četiri rotora, od kojih je svaki imao 28 kontaktnih točki, te različit broj zupčanika.

38 Mornarica je tijekom rata razvila najnapredniju inačicu Enigme.

39 Scherbius (1923.).

40 Crypto Museum. URL = <http://www.cryptomuseum.com/crypto/enigma/a/index.htm> (11.5.2018.).

Na sljedećoj fotografiji prikazana je prva inačica stroja:



Slika 3 - Enigma tip A (Crypto Museum)

Prilikom tipkanja na ploči s tipkama, električni impulsi slali bi se kroz zupčanike, a oni bi se nakon određenog broja pritisnutih tipki pomicali, dok se broj pritisaka tipki mjerio na analognoj traci iznad ploče s tipkama⁴¹. Različit broj zupčanika na svakom rotoru samim time omogućio je da se rotori razlikuju po broju pomaka, tako da su se neki pomicali više puta od drugih, što je razbijalo uzorak koji se teže mogao uočiti. Osim pomičnih rotora, stroj je sadržavao ručicu kojom se mogao obrisati broj pritisaka tipki na traci koja ih je mjerila, a stroj je također bio sposoban promijeniti način rada - pritiskom na tipku mogao se promijeniti u "Enkripcija", "Dekripcija" ili "Jasnopis" način rada⁴². Ova metoda bila je revolucionarna, jer se Enigma mogla koristiti kao običan pisači stroj, kao stroj

41 Isto.

42 Scherbius (1923.).

za zakrivanje poruka, ili kao stroj za zakrivanje poruka - sve u jednom. Budući da se enkripcija i dekripcija nisu mogle obavljati istovremeno, bilo je nužno da se uvedu ovi načini rada. Kada bi stroj bio postavljen u "Enkripcija" načinu rada, električni signal putovao bi normalno kroz rotore, no kada bi se način rada prebacio u "Dekripcija", tada bi se događao obrnut proces, jer korisnik sam nije mogao mijenjati položaj rotora, što će biti mogućnost novijih revizija Scherbiusova izuma⁴³. Također, Scherbius je kao glavnu prednost svog stroja istaknuo nevjerovatno snažan algoritam koji je omogućavao rad temeljen na zakrivanju pomoću rotora - prema njegovim tvrdnjama, bilo je potrebno milijun pritisaka tipki kako bi se uzorak počeo ponavljati, odnosno kako bi se položaj rotora vratio na početni položaj u kojem su rotori bili prije prvog pritiska tipke. Takvim dizajnom, Scherbius se jako približio nasumičnosti, iako je ona u slučaju Enigme još uvijek bila pseudonasumičnost (pošto je rad stroja baziran na rotaciji rotora koji kad-tad moraju doći na nultu točku s koje su krenuli i početi ponavljati proces, iako se on u praksi činio nedostižnim). Ovaj prvi model Enigme je još uvijek bio donekle robustan, a zbog čestih kvarova na mehanizmu (prvenstveno pisačem dijelu), zahtijevao je stalne revizije. U dvadesetim godinama postojale su dvije revizije Enigme u komercijalnoj domeni korištenja, no ubrzo se stroj počeo koristiti i u ostalim europskim zemljama, i to za potrebe diplomacije.

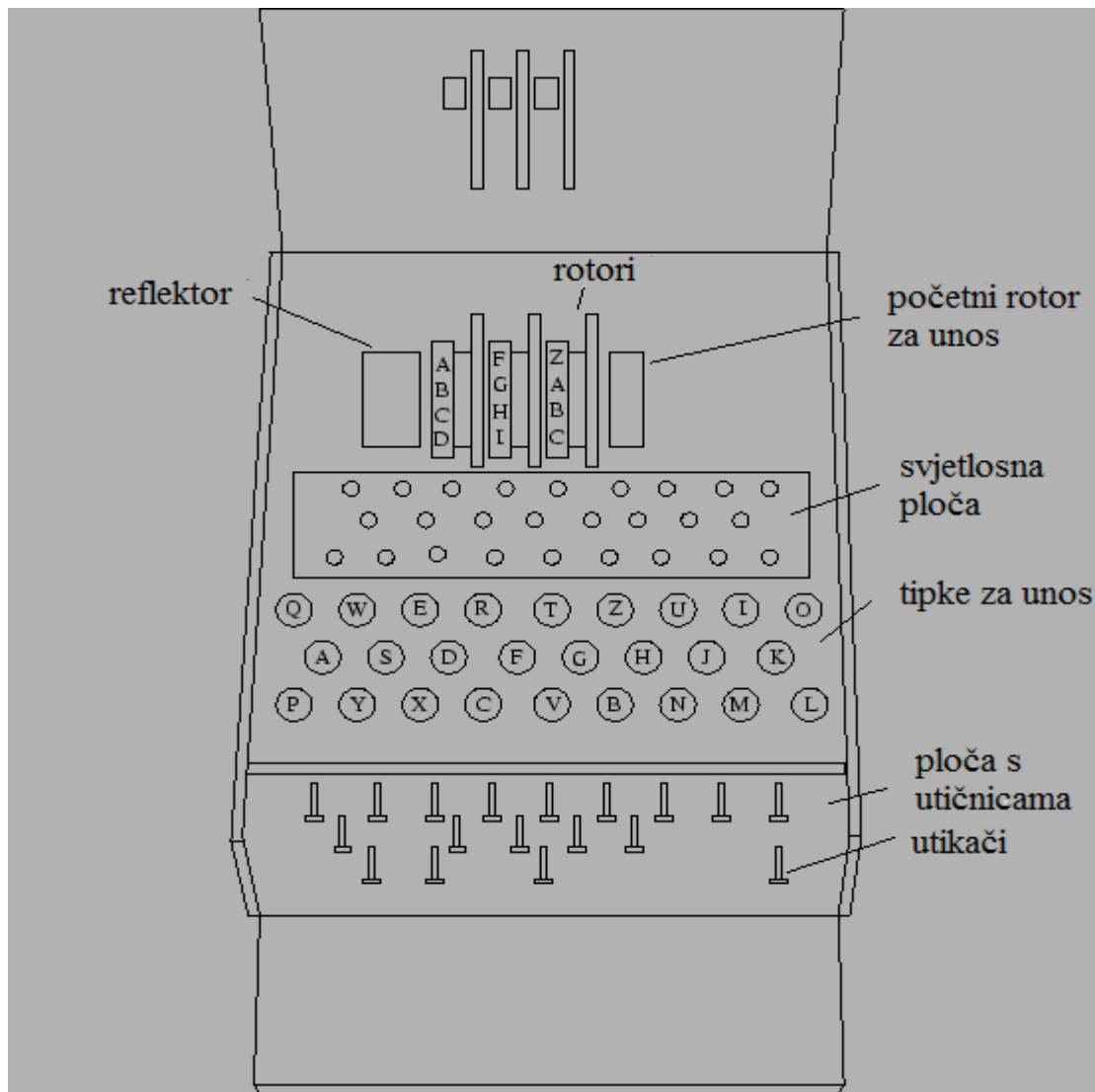
Nakon nekoliko revizija Enigme za potrebe komercijalne upotrebe, vojska je krenula s ulaganjima u stroj koji bi bio lako prenosiv, imao daleko jači algoritam za zakrivanje, i bio višestruko otporniji na napore kriptanalitičara koji bi pokušali prodrijeti u sustav tajne komunikacije. Tako je došlo do razvoja najpoznatije inačice Enigme, jednostavno nazvane **Enigma I**⁴⁴ (ili *Reichswehr D*). Ovaj stroj temeljen je na dizajnu prethodnog stroja namijenjenog komercijalnoj upotrebi, a imao je drastično drukčiji dizajn od prve verzije Enigme, i to već na prvi pogled. Na prvi pogled, stroj je bio puno manji, i bio je oblika omanje drvene kutije u koju su stali svi najvažniji elementi, ali zbog prenosivosti stroj je morao žrtvovati mehanički dio koji je ispisivao poruke na papir.

Ovaj model Enigme daje najbolji prikaz elektromehaničkog kriptografskog stroja kakav se koristio u Drugom svjetskom ratu. Iako su Saveznici, pa čak i Sile Osovine koristile razne modele, njihov dizajn bio je uvijek vrlo sličan ovom modelu Enigme.

Sljedeća slika daje prikaz Enigme tipa I, s označenim najvažnijim dijelovima. Kao što se može primijetiti, razlike ovog i prethodnog modela (Slika 3) vidljive su već pri samom eksternom dizajnu, ali glavne promjene dogodile su se u samom algoritmu:

43 Isto.

44 Rimski broj 1.



Slika 4. - Ilustracija Enigme I

Enigma I sastojala se od sljedećih dijelova:

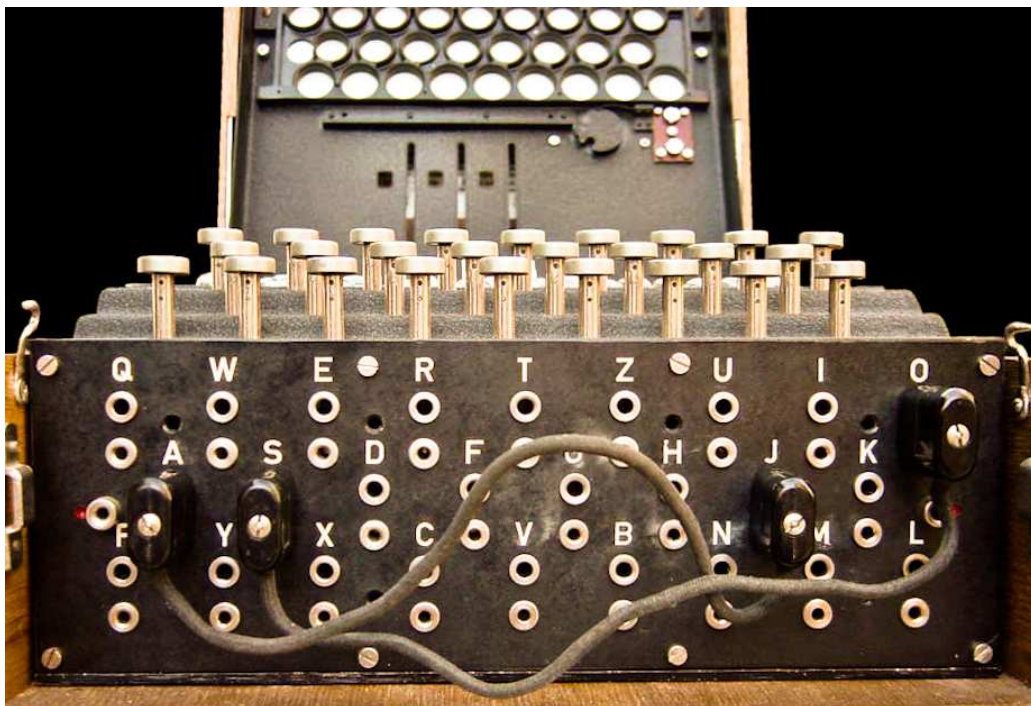
a) drveno kućište - ovaj model Enigme prvi je uveo drveno kućište kao zamjenu za tešku metalnu konstrukciju, a logika tog izbora bila je prenosivost - prethodne inačice ovog stroja bile su vrlo teški i stacionarni strojevi koji nisu odgovarali potrebama vojske koja je zahtijevala mogućnost lakog prenošenja, ali loša strana je bila to što je stroj morao žrtvovati dio za ispis poruke na papir.

b) rotori - najmanji, a ujedno i najvažniji dio stroja, Enigma I sastojala se od pet mehaničkih rotora, od kojih su tri bila pomična, a dva (početni rotor - stator, i završni rotor - reflektor) statična. Rotori su se, kao i kod prethodnih modela Enigme, pomicali s obzirom na pritisak tipke i unos znaka (odnosno, pri prolasku električnog signala kroz njih).

c) **tipke za unos i svjetlosna ploča** - tipke za unos znakova dio je koji je na stroju bio prisutan još od početne verzije, ali razlika u odnosu na prijašnje strojeve je ta da tipke nisu bile povezane s pisačim dijelom koji bi ispisivao unos na papir, već su bile povezane sa svjetlosnom pločom koja se nalazila iznad tipki. Svjetlosna ploča služila je za prikaz zakritka, a slovo koje bi zasvijetlilo na svjetlosnoj ploči nakon pritiska tipke predstavljalo je *output* (izlaznu jedinicu); na primjer, ako bi korisnik pritisnuo slovo A, algoritam bi zakrio slovo i ono bi na svjetlosnoj ploči zasvijetlilo kao slovo X - više takvih slova predstavljalo je poruku koja se slala primatelju, koji bi je onda sličnim ali obrnutim procesom pretvorio u jasnopis.

d) **ploča s utičnicama i utikači** (njem. *Steckerbrett*) - ova ploča također predstavlja novost u odnosu na prethodne verzije Enigme (ali i enkriptijskih strojeva uopće), a predstavljala je dodatni *scrambler* čija je funkcija bila višestruko otežati mogući postupak kriptanalize. Ploča s utičnicama predstavljala je dodatni slovored i dodatni postupak u procesu zakrivljanja poruke, a utikači su korišteni kako bi se povezala dva slova na ploči - npr. ako bi korisnik utikačem povezo slova B i N, pritiskom na tipku B to slovo najprije bi se zakrilo kao N, a tek onda bi djelovanjem rotora prešlo u treće slovo.

Na sljedećoj fotografiji prikazana je navedena ploča:



Slika 5 - Prikaz Enigme sa *scrambler* pločom (Wikipedia)

Zakritni algoritam Enigme bio je vrlo kompleksan za tadašnje shvaćanje, ali poslužio je kao temelj za razvoj svih budućih kriptografskih strojeva, a neke inačice takvih strojeva nastavile su se koristiti čak i do početka sedamdesetih godina.

Algoritam je, kao što je ranije spomenuto, temeljen na radu rotora, ali za potrebe primjera objasniti ćemo ga na primjeru stroja Enigma I, kako bi se također pokazao i rad svjetlosne ploče. No, prije objašnjenja samog algoritma, treba prikazati konstrukciju rotora, kako bi se algoritam mogao bolje razumjeti. Sljedeća slika prikazuje jedan pomični rotor korišten u Enigmi:



Slika 6: Rotor (Crypto Museum)

Utor u sredini rotora koristio se kako bi se rotor povezao sa susjednim rotorima, a malene žice korištene su za usmjeravanje električnog signala, i bile su povezane na svaki od 26 kontakata. U inačicama Enigme kakve su se koristile tijekom Drugog svjetskog rata, korišteno je pet rotora - dva nepomična (stator - početni rotor, te reflektor - posljednji rotor), a tri pomična rotora bila su konstruirana kao rotor na slici 6. U kasnijim inačicama Enigme, Scherbius je izbacio zupčanike i oslanjao se na usjeko (zareze) u metalnom prstenu, čija je funkcija bila pomicanje susjednih rotora. Algoritam je u osnovi bio polialfabetni supstitucijski algoritam, a rotacija pomičnih rotora odvijala se na sljedeći način:

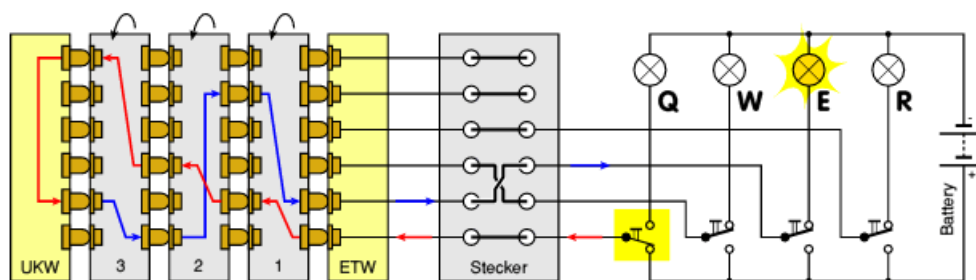
a) strujni krug - pritiskom na tipku na ploči s tipkama, strujni signal šalje se od ploče do rotora. Prolaskom kroz stator, početni rotor, struja dolazi do prvog rotora zdesna, koji je ujedno i najbrži (najčešće se okreće)⁴⁵.

⁴⁵ Bauer (2002.), str. 134.

b) prolazak kroz rotore - u ovom koraku odvija se rotacija pomičnih rotora. Kod prolaska električnog signala kroz početni pomični rotor, on se pomiče za jedan kontakt u smjeru obrnutom od kazaljke na satu. "Najbrži" rotor pomiče se svaki put kada kroz njega prođe električni signal, odnosno pomakne se 26 puta⁴⁶ u punom okretaju. Nakon što napravi puni okretaj (26 pomaka), sljedeći (srednji) rotor pomakne se jednom, a posljednji, "spori" rotor pomaknut će se jednom kada srednji rotor napravi 26 pomaka⁴⁷. Na prvi pogled, ovaj sistem čini se lošim zato što bi se mogao razbiti nekom metodom kriptanalize koja bi predviđjela regularne pomake svakih 26 znakova. No, inženjeri koji su radili na Enigmi dosjetili su se da svaki rotor dizajniraju tako da se na istom urezu ne nalazi isto slovo. Međutim, prema Khanovu mišljenju, ova praksa bila je kontraproduktivna i samo stvorila iluziju kompliciranosti sustava jer je dovela do vrlo loše mane koja je na kraju pomogla u razbijanju sustava - a to je da se niti jedno slovo nije moglo zakriti kao to slovo⁴⁸. Kriptanalitičari su stoga, nakon što su shvatili ovu manu, jednostavno eliminirali jedno slovo iz abecede prilikom razbijanja algoritma, što im je na kraju olakšalo postupak razbijanja.

c) povratak kroz rotore - nakon prolaska kroz sve rotore i "reflektiranja" od konačnog rotora, električni signal ponovno se vraća kroz sve rotore, no ovaj put izlazi kao "output" na svjetlosnoj ploči, i očituje se u novom slovu koje predstavlja zakritak početnog znaka koji je korisnik pritisnuo.

Ovo velikim dijelom opisuje i čitav proces enkripcije poruke. Pojednostavljen model enkripcije može se vidjeti na sljedećoj slici:



Slika 7: Grafički prikaz algoritma Enigme (Crypto Museum)

46 Zbog toga što je Enigma omogućavala unos 26 znakova, odnosno na svakom rotoru bilo je 26 ureza (zarez) koji su služili pri rotaciji.

47 Isto.

48 Isto, str. 135.

Na prvi pogled može se uočiti da cijeli proces predstavlja jedan strujni krug, koji se zatvara pritiskom na tipku na ploči s tipkama (u ovom slučaju je to slovo Q), uz dodatak ploče s utičnicama i utikačima (na slici *Stecker*) koja je u slučaju ove slike uključena u algoritam zakrivanja. Crvena linija prikazuje inicijalni put električnog signala, a plava označava povratak električnog signala nakon prolaska kroz reflektor. Prilikom dolaska do ploče s utičnicama i utikačima, električni signal se, umjesto do ulaska na svjetlosnu ploču kod slova W, zakriva u slovo E, jer je taj supstitucijski par povezan na ploči (prisjetimo se, ploča određuje zamjenu konačnog izlaznog znaka za neko drugo slovo).

Sigurnost Enigme je, osim o zakritnom algoritmu, mnogo ovisila i o ljudskom faktoru, odnosno o operatorima koji su se njome služili za vrijeme rata. Nakon što je postalo izvjesno da bi Saveznici mogli pokušati razbiti algoritam Enigme, njemačko zapovjedništvo odlučilo je da je potrebno uvesti još jedan sigurnosni korak u proces tajne komunikacije. Taj korak bio je uvođenje izmjenjivih rotora u mehanički sustav stroja, i popratne knjige kodova (eng. *codebooks*). Ideja koja je stajala iza ovog postupka bila je ta da se ključ u procesu enkripcije i dekripcije trebao svakodnevno izmjenjivati. Knjige kodova su stoga sadržavale velik broj različitih ključeva - a pojedini ključ predstavljao je početni položaj rotora (ili čak izbor rotora) koje je svaki operator trebao slijediti. Na primjer, u ponedjeljak u ponoć rotori bi se podesili tako da se kontakti nalaze u određenom položaju, kako bi se zakrivanje poruke (i njeno raskrivanje) na svim strojevima odvijalo jednako. Sljedećeg dana u ponoć, rotori bi se postavili u drukčiji položaj, ovisno o tablicama koje je knjiga kodova propisivala. Knjige kodova obično su se ispisivale (tiskale) na papiru koji se mogao lako otrgnuti i uništiti, kako ključ eventualno ne bi pao u neprijateljske ruke. Osim početnog položaja rotora, knjiga kodova također je propisivala parove koje je trebalo povezati na *Steckerbrett* ploči. Također, propisan je bio i odabir rotora - za vrijeme rata razvila se nova tehnika komunikacije, pri kojoj je svaki operator koji se koristio Enigmom posjedovao pet pomičnih rotora koje je mogao izmjenjivati po potrebi (npr. danas su se mogli koristiti rotori I, III, II, a sutra IV, II, VI itd.). Operatori su također birali i dodatni ključ od tri slova, uz koji bi još proizvoljno dodali dva slova, kao još jednu sigurnosnu mjeru (taj set ključeva nazivao se *Kenngruppen*). Osim tih ključeva, operatori su običavali slati i "ključ poruke", koji je svaki operator odabirao po vlastitom izboru kao dodatnu sigurnosnu mjeru.

Primjer slanja poruke izgledao je ovako: operator bi postavio rotore u položaj koji za taj dan propisuje knjiga kodova, a zatim bi proizvoljno postavio prstene na rotorima tako da odgovaraju nekim trima znakovima, npr. ADX. Nakon toga bi proizvoljno odabrao ključ poruke, recimo DBF, koji bi zakrio i dobio neka druga tri znaka, na primjer GTR. Zatim bi operator namjestio rotore u novi početni položaj, tako da oni odgovaraju trima slovima DBF, nakon čega bi prema tako

namještenim rotorima zakrio poruku. Nakon zakrivanja, zakrivenu poruku poslao bi primatelju skupa s početnim položajem rotora ADX i ključem poruke GTR. Primatelj bi tako morao namjestiti rotore na svojoj Enigmi kako bi oni odgovarali početnom položaju ADX, a zatim bi raskrio ključ poruke GTR, nakon čega bi dobio novi položaj rotora DBF, na koji bi morao namjestiti svoj stroj kako bi konačno raskrio poslan mu zakritak⁴⁹.

Ovako izgleda primjer jedne poslanske poruke:

```
1230 = 3tle = 1tl = 250 = WZA UHL =  
  
FDJKM LDAHH YEOEF PTWYB LENDP  
MKOXL DFAMU DWIJD XRJZY DFRIO  
MFTEV KTGUY DDZED TPOQX FDRIU  
CCBFM MQWYE FIPUL WSXHG YHJZE  
AOFDU FUTEC VVBDB OLZLG DEJTI  
HGYER DCXCV BHSEE TTKJK XAAQU  
GTTUO FCXZH IDREF TGHSZ DERFG  
EDZZS ERDET RFGTT RREOM MJMED  
EDDER FTGRE UUHKO DLEFG FGREZ  
ZZSEU YYRGD EDFED HJUIK FXNVB
```

Slika 8 - Primjer Enigma poruke (Dirk Rijmenants)

Na slici, 1230 označava da je slika poslana u 12:30 sati, 3tl znači da se poruka sastoji od 3 dijela, a ovo je prvi dio - 1tl; poruka se sastoji od 250 znakova (uključujući i *Kenngruppe* ključ na početku poruke - ključ JKM koji se nalazi u tablici uz proizvoljno odabrana slova FD). Naposljetku, poslan je i početni položaj rotora WZA kojim treba raskriti UHL, kako bi se dobio ključ poruke za raskrivanje ostatka poruke⁵⁰.

Ovo predstavlja postupak zakrivanja poruke kako ga je koristio Wehrmacht nakon 1940. godine. Unutar njemačke vojske postojale su i neke razlike u zakrivanju poruke, ali i samim strojevima. Mornarica je, na primjer, koristila Enigmu s jednim pomičnim rotorom više, te je stoga takav model bio i najsigurniji. U sljedećem poglavlju predstaviti ćemo jedan napredniji stroj, koji je ipak vrlo sličan Enigmi.

49 Rijmenants. URL = <http://users.telenet.be/d.rijmenants/en/enigmaproc.htm> (13.5.2018.).

50 Isto.

5.2. T-52

Tijekom godina koje su dovele do Drugog svjetskog rata, vojska je uvidjela da komunikacija putem telegrafске mreže omogućuje komunikaciju niske razine sigurnosti. Iako je izum telegrafa otvorio mogućnost izradi enkripcijskih strojeva, oni su pak, zbog nemogućnosti uspostavljanja linijske veze poruke običavali slati putem radija, Morseovim kodom (što se činilo i u slučaju Enigme). Međutim, telegraf i dalje nije potpuno izbačen iz upotrebe. Naprednija verzija telegrafije - radiotelegrafija, omogućila je slanje zakrivenih poruka putem radiovalova⁵¹. Istraživanja u ovom području naposljetku su iznjedrila izum teleprinter-a - stroja koji je bio sposoban komunicirati putem modela telegrafije, uz znatno brži prijenos podataka.

Jedan takav stroj bio je i njemački T-52, nazvan još i *Geheimschreiber* (njem. "tajni pisac"), a među Britanskim kriptanalitičarima poznat pod imenom *Sturgeon* (jesetra). Ovaj stroj bio je vrlo velik, i težio je gotovo stotinu kilograma, te samim time nije bio pogodan za korištenje na terenu gdje je mobilnost bila od presudne važnosti⁵². Težina i veličina stroja nisu nimalo začeđujuće, s obzirom na to da je, za razliku od modela Enigme opisanog u prethodnom poglavlju, glavna funkcija ovog stroja osim zakrivanja i raskrivanja poruka bila ubrzavanje procesa komunikacije, što se postizalo uključivanjem tiskarskog dijela u stroj, što je omogućavalo ispisivanje poruke na papir. Komunikacija među T-52 strojevima obavljala se putem radio-veze, ali i putem linijske telegrafске veze.

Što se tiče algoritma na temelju kojeg je ovaj stroj obavljao enkripciju, on je mnogo kompleksniji od Enigme, a temeljio se na radu čak deset rotora. Komunikacija među rotorima odvijala se na principu bitova (5-bitne kodne grupe), a pomak svakog rotora odgovarao je uvjetima XOR logike, kumulativno producirajući 960 zakritnih alfabeta. Stroj je također dizajniran tako da se pomak rotora odvija nelinearno, što se pokazalo vrlo dobrom odlukom s obzirom na uspješnost kriptanalize (a stroj se također nastavio koristiti u poslijeratnoj Europi, što dokazuje kvalitetu njegovog vrlo kompliciranog algoritma)⁵³.

Algoritam za vrijeme rata nije nikad razbijen, osim nekoliko poruka koje su razbijene zbog lijenosti kriptografa koji su se služili istim ključem poruke⁵⁴.

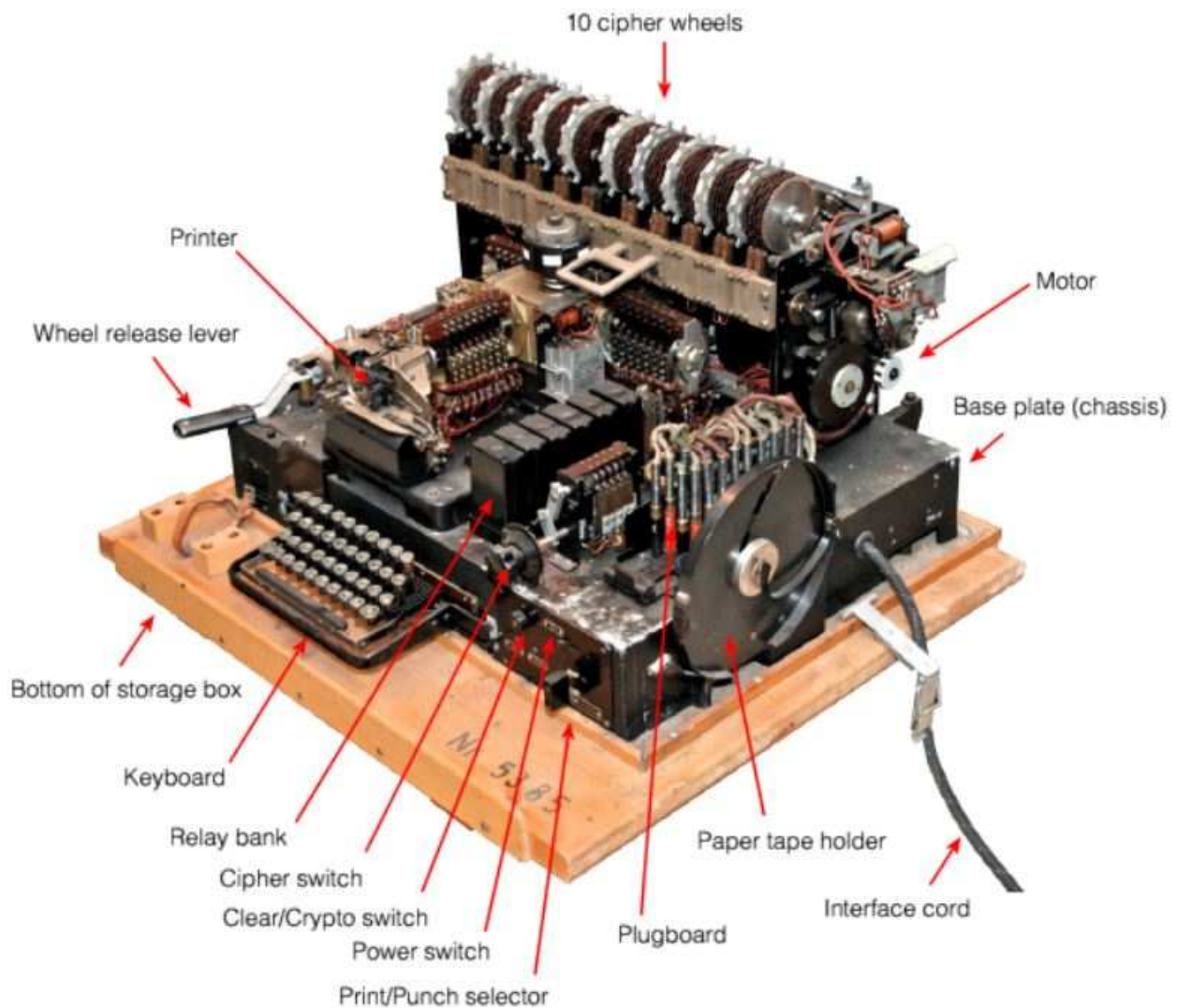
51 Hrvatska enciklopedija. "telegrafija". URL = <http://www.enciklopedija.hr/natuknica.aspx?ID=60720> (pristup: 14.5.2018.).

52 T-52 strojevi uglavnom su se koristili u podmornicama, gdje su bili stacionirani u posebnim prostorijama i nisu zahtijevali prenošenje.

53 Proc (2012.). URL = <http://jproc.ca/crypto/sturg.html> (pristup: 14.5.2018.).

54 Savard (1999.). URL = <http://www.quadibloc.com/crypto/te0302.htm> (pristup: 14.5.2018.).

Na sljedećoj slici prikazan je jedan model T-52, konkretnije, T-52 model "d":



Slika 9 - T-52 (Crypto Museum)

Ako usporedimo veličinu tipkovnice (*keyboard*) prikazane na gornjoj slici s ostatkom stroja, vidjet ćemo koliko je stroj zapravo bio velik.

Zbog algoritma koji nije uspješno razriješen godinama nakon Drugog svjetskog rata, ovo predstavlja jedan od najučinkovitijih (ako ne i najučinkovitiji) elektromehanički kriptografski stroj Sila Osovine.

5.3. Lorenz SZ

Kako je Drugi svjetski rat sve više napredovao, njemačka vojska shvatila je da Enigma strojevi ipak nisu bili imuni na postupke kriptanalize britanskih kriptanalitičara, stoga je odlučeno da je potrebno izumiti stroj koji bi bio sigurniji od Enigme, a služio u komunikaciji na najvišoj razini - među samim Hitlerom i njegovim generalima. Tako je nastao *Lorenz Schlüssel-Zusatz* - stroj za čiji su algoritam tadašnje njemačke vlasti pretpostavljale da je mnogo jači od algoritma Enigme, no u praksi je i dalje brzo razbijen od strane britanskih kriptografa, koji čak nikad nisu došli u dodir sa samim strojem, već je kriptanaliza obavljena presretanjem radio-signalu kojim su se poruke odašiljale.

Lorenz je u osnovi bio stroj sličan prethodnom opisanom stroju. Također je bio teleprinter koji je mogao poruke ispisivati na papir i tako ubrzati postupak komunikacije. Algoritam enkripcijskog stroja Lorenz mehanički je bio uvjetovan radom deset pomičnih i dva nepomična rotora. Pet rotora s lijeve strane spadali su u grupu takozvanih *Psi* rotora, srednja dva rotora (nepomični rotori) nazivali su se *Mu* rotorima, dok je pet rotora s desne strane svrstano u grupu *Chi* rotora. Ovu podjelu utvrdili su britanski kriptanalitičari koji su razbili Lorenzov algoritam⁵⁵.

Algoritam je također bio sličan, iako manje kompleksan i siguran u odnosu na T-52. Oba algoritma bila su temeljena na XOR logici i bitovima. Poruke bi se Lorenzom odašiljale u "bitnom" obliku koji je pojednostavljeno, mogao biti 0 ili 1⁵⁶. U slučaju XOR logike, operacija bi se kod zakrivanja poruke provodila nad bitovima jasnopisa i ključa (odnosno, nad zakritkom i ključem u slučaju raskrivanja poruke). XOR nalaže da sud između jasnopisa (ili zakritka) te ključa može biti 1 ukoliko je isključivo jedna vrijednost između dvije vrijednosti 1:

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

55 Grime (2014.), URL = <https://www.youtube.com/watch?v=GBsfWSQVtYA> (pristup: 15.5.2018.).

56 Originalna zamisao bila je koristiti točkice i križice umjesto nula i jedinica, no za potrebe ovog primjera uzet ćemo te brojeve.

Zakrivanje poruke odvijalo se na ovakvom principu, a treba nadodati da su se logičke vrijednosti svakog slova raspisivale po sistemu Baudotovog koda.

Kako je tekao proces zakrivanja poruke sa strane zakritnog algoritma? *Chi* rotori proizveli bi jedan ključ od pet vrijednosti, koji bi se zatim usporedio sa *Psi* ključem kojih je generiralo ostalih pet rotora, i na kraju bi se dobivenom binarnom vrijednošću zakrila originalna poruka u jasnopisu⁵⁷.

Chi rotori imali su standardni linearni pomak nakon unosa svakog slova, dok su *Psi* rotori rotirali iregularno, što je ovaj algoritam učinilo vrlo teškim za razbijanje od strane britanskih kriptanalitičara. Iregularnu rotaciju određivali su *Mu* rotori koji su se nalazili u sredini, a osim toga, svaki rotor mogao se podesiti na zaseban početni položaj (slično kao u slučaju Enigme), no dodatna prednost bila je i ta što je svaki rotor imao drukčiji broj mogućih startnih položaja, tako da se uzorak ponavljanja, barem u teoriji, nije mogao primijetiti⁵⁸.

Colossus, stroj koji se smatra prvim elektroničkim programabilnim digitalnim računalom, konstruiran je kako bi se razbio Lorenzov zakritni algoritam, a bio je sposoban obavljati operacije vezane uz Booleovu logiku i prebrojavanja. Znanstvenik Martin Gillow je uspio potpuno digitalizirati Colossusov sistem razbijanja Lorenzova algoritma, a usput je digitalizirao i Lorenzov algoritam u interaktivnom obliku. Na web stranici *Virtual Colossus* moguće je tako pronaći interaktivno okruženje u kojem se može isprobati rad Lorenza, od postavljanja rotora i testiranja veze, pa sve do zakrivanja poruke, uz rezultate koje bi stroj ispisivao na papiru kao *output*⁵⁹. Ova web stranica također nudi i neke zanimljivosti, na primjer, u koji je položaj rotore bilo zabranjeno postaviti prije slanja poruke, kako se ne bi naštetilo sigurnosti cjelokupnog komunikacijskog sustava.

Lorenz, iako vrlo kvalitetan enkripcijski stroj, doživio je jednaku sudbinu kao Enigma. Zbog nepažnje i nemara operatora koji je dvije slične poruke zakrio istim ključem, britanski kriptanalitičari uspjeli su razbiti ovaj složeni algoritam, i samim time stroj učiniti beskorisnim bez da su ga ikad vidjeli uživo.

57 Isto.

58 Isto.

59 Gillow. URL = <http://www.virtualcolossus.co.uk/index.html> (pristup 15.5.2018.).

5.4. Red

Angō Kikai Taipu-A (jap. Enkripcijski stroj tip A) prvi je japanski stroj za zakrivanje poruka koji je isključivo korišten u diplomatske svrhe u tridesetim godinama prošlog stoljeća. Ovaj stroj vrlo je specifičan, što može zahvaliti i jeziku za čije korištenje je namijenjen. Japanski jezik vrlo je poseban u odnosu na indo-europske jezike, a glavni razlog je taj što je ovaj jezik skupa s njegovim pismom zasnovan na slogovima - posebnost za koju će Japanci smatrati glavnom preprekom u razbijanju ovog stroja, no na kraju će se pokazati da to nije bio problem za zapadnjačke kriptanalitičare.

Red (eng. crven, crveno) je stroj koji se sastojao od pisaćeg dijela vrlo sličnog pisaćem stroju (koji je služio za *input* znakova jasnopisa), jednog rotora, posebne ploče s utičnicama i utikačima, kotačića od 47 zubaca (kao na zupčanicima rotora ostalih strojeva), te još jednog pisaćeg dijela koji je vraćao zakritak kao *output*⁶⁰. Zakritni algoritam sastojao se u djelovanju rotora s 26 kontaktnih točki koje su propuštale električnu struju, a sam rotor rotirao se pomoću ranije spomenutog kotačića. Protok struje kroz ploču s utičnicama i utikačima odvijao se dvaput prilikom jednog pritiska tipke za unos slova - prvi put nakon pritiska, te drugi put prije *outputa*, pri čemu je ploča proizvodila dodatni polialfabetni *scramble* zakritka⁶¹.

Nažalost, o stroju nema previše podataka, jer se njegovom istraživanju nije posvetilo toliko pozornosti koliko i njemačkim strojevima. Red je razbijen u nekoliko navrata te od nekoliko različitih grupa, od kojih su najznačajnije bile britanska kriptanalitičarska grupa koja je stroj razbila 1934. godine, a 1936. godine algoritam je razbijen i od strane američkih kriptanalitičara. Glavna mana stroja bila je ta što je koristio *rōmaji* stil pisanja, koji predstava romanizaciju japanskih simbola (zapisuje se latinicom), a nakon što su zapadnjački kriptanalitičari shvatili da funkcionira na tom principu, kriptanaliza u kasnijim navratima bila je mnogo lakša.

Ovaj stroj polako je izišao iz upotrebe uoči Drugog svjetskog rata, kada je postepeno zamijenjen novim kriptografskim strojem kodnog imena Purple⁶², da bi se od Red strojeva konačno odustalo tijekom 1938. godine.

60 Wrixon (1998.), str. 267.

61 Isto.

62 Ovo ime stroju su dali američki kriptanalitičari.

5.5. Purple

Drugi japanski stroj koji se koristio u vrijeme Drugog svjetskog rata⁶³ je *97-shiki O-bun-Injiki*, poznat također pod nazivom "Enkripcijski stroj tip B" ili jednostavno Purple, kako su ga nazvali američki kriptanalitičari. Stroj je uveden u upotrebu početkom 1939. godine, a prve službene poruke zakrivene ovim strojem odaslane su 20. veljače 1939. godine⁶⁴. Nažalost, Purple također nije dovoljno istražen, kao niti prethodni japanski stroj. Algoritam zakrivanja poruke ovog stroja ne temelji se na rotoru, što ga razlikuje od ostalih strojeva koje smo do sada objasnili. Purple koristi takozvani koračni prekidač (eng. *stepping switch*), za koji su japanski kriptolozi smatrali da će pružiti puno veću sigurnost od rotora kakav je koristio Red.

Kao i Red, i Purple se sastojao od dijela za *input* poruke (tipkovnica) i dijela za *output* (ispis poruke na papir), a također su dijelili i dodatni *scramble* mehanizam u obliku ploče na koju se moglo povezati bilo koji unos tipkovnice na bilo koje od 26 slova⁶⁵. Unutar stroja, slova su bila podijeljena na "šestice" i "dvadesetice". "Šestice" su predstavljale grupu samoglasnika (uključujući slovo y), a "dvadesetice" su predstavljale suglasnike. Prilikom povezivanja na ploči s utičnicama i utikačima, slova su se mogla povezati bez obzira na ovu podjelu, a zatim bi se zakrivala u jednoj od tih grupa slova. Ako bi se povezali samoglasnik na tipkovnici i suglasnik na ploči, onda bi se taj znak zakrivao u grupi "dvadesetice". Također, slova koja ne postoje u japanskom jeziku i pismu, zakrivala su se kao bigrami (kombinacije dvaju slova): tako je L postalo "ai"; X se zakrivalo kao "ei"; P je predstavljalo "ni"; V je zakrivano kao "u" s dugim naglaskom, a postojale su i kombinacije od tri slova koje bi se mogle zakriti kao tri riječi i slično⁶⁶. Algoritam je, kako su pokazale analize američkih kriptanalitičara, bio izrađen s namjerom da eliminira sve mogućnosti ponavljanja koje su se mogle dogoditi u sustavima koji su koristili rotore, kako bi se izbjegla bilo kakva mogućnost da se frekvencijskom analizom shvati o kakvom je algoritmu riječ. No, američki kriptanalitičari uspjeli su shvatiti upravo to - da stroj ne koristi rotore, te da mora postojati neki početni položaj od kojeg stroj kreće. Amerikanci su deduktivno uspjeli razbiti algoritam, kao i u slučaju Lorenza, bez da su ikad došli u fizički doticaj s tim strojem. Iako je namjera bila eliminirati ponavljanja, Amerikanci su ipak primijetili vrlo visoko frekvencijsko ponavljanje šest slova, što je značilo da Purple nije ispravio neke od glavnih propusta koje su krasile prethodnu inačicu, tip A.

63 Ovo nipošto ne znači da se u Japanu nije koristio niti jedan drugi enkripcijski elektromehanički stroj, no Red i Purple bila su dva najpoznatija i najkorištenija. Japan je za kratke suradnje s Poljskom uspio napraviti pomak u kriptološkim istraživanjima, no ova zemlja je po tom pitanju i dalje ostala primitivna, a većina komunikacije i dalje se obavljala zakrivanjem poruka kodovima te njihovim prenošenjem putem radio-veze.

64 Wrixon (1998.), str. 268.

65 Weierud. URL = <http://cryptocellar.org/simula/purple/index.html> (16.5.2018.).

66 Friedman (1940.), str. 2-3.

Japanski su se kriptografi, kao i u slučaju njemačke kriptologije Drugog svjetskog rata, uvođenjem Purplea odlučili koristiti dogovorene početne pozicije za zakrivanje poruka, koje su trajale devet dana (a nisu se mijenjale na dnevnoj bazi kao što je bio slučaj s njemačkim kriptografima). Ovo pokazuje koliku je vjeru Japan polagao u svoju kriptografsku mrežu, i snagu ovog stroja.

Ideja koračnog prekidača u svojoj osnovi lošija je od uvođenja više rotora. Kao što su brojni primjeri pokazali, Saveznicima je mnogo muke zadavala pseudonasumična priroda njemačkih enkripcijskih strojeva, koja je bila uvjetovana iregularnim pomakom rotora, što je dovelo do nemogućnosti razbijanja nekih od strojeva (T-52). Algoritam japanskog Purplea, iako u teoriji nije trebao biti razrješiv, na kraju je ipak podlegao najjednostavnijim metodama kriptanalize, kao što su frekvencijska analiza i *brute force* (eng. sirova sila). Koračni prekidač pokazao se vrlo predvidljivim, jer je nakon svakog 25. pritiska tipke (prilikom čega je svakim pritiskom teoretski nastajao nova zakritna abeceda) došlo do ponavljanja procesa. Cikličko ponavljanje algoritma bila je najveća mana stroja, čiji je algoritam gotovo potpuno razbijen već dva mjeseca nakon što je poslana prva poruka.

Kao što brojni primjeri pokazuju, kriptologija Sila Osovine bila je ili vrlo učinkovita, ili gotovo beskorisna, a mnoštvo Savezničkih enkripcijskih strojeva nastalo je upravo iz želje da se razbiju neprijateljski strojevi.

6. Elektromehanički strojevi Saveznika

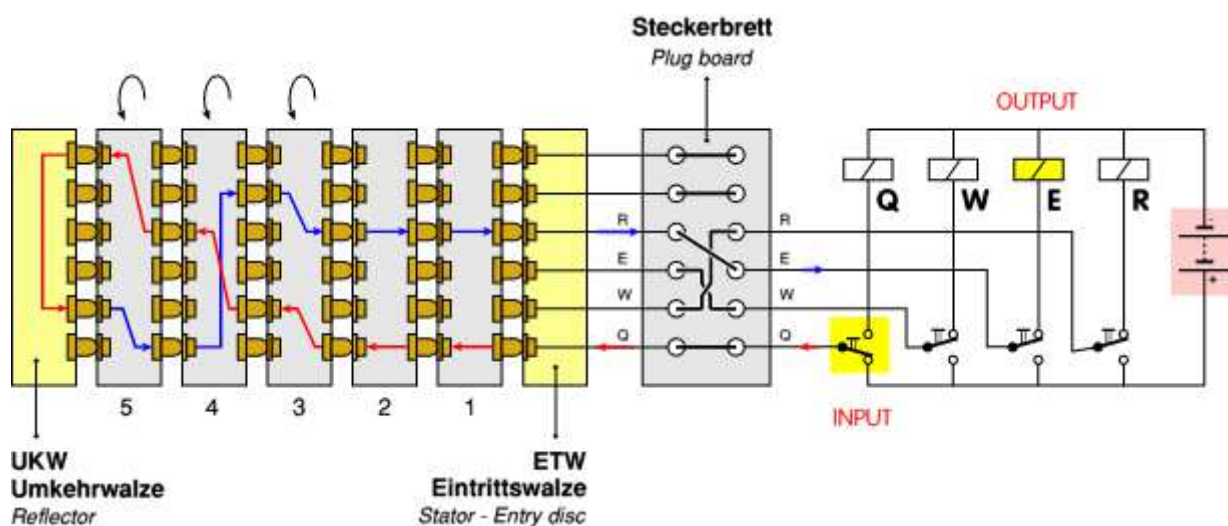
Velike zemlje (poput Amerike, Francuske i Velike Britanije) koje su u Drugom svjetskom ratu pripadale strani Saveznika imale su dugu tradiciju istraživanja u području kriptologije. Osim toga, Američki građanski rat i Prvi svjetski rat poslužili su kao poligon za uspostavu odjeljenja čiji je cilj bio istraživati nove mogućnosti kriptologije, a ta praksa nastavila se i u poslijeratnim godinama. Kao što su pokazali primjeri Sila Osovine, Saveznici su tijekom rata uglavnom bili usmjereni na razbijanje neprijateljskih šifri i kodova, ali imali su i svoju mrežu tajne komunikacije. Zasluge savezničkih kriptologa dovele su također do izuma prvog računala (Colossus), a većina njihovih strojeva ostala je u upotrebi i u poslijeratnim godinama, što su omogućili kvalitetni algoritmi koji su također bili bazirani na radu rotora.

6.1. Typex

Britanska kriptologija tijekom Drugog svjetskog rata bila je vrlo napredna, a i danas obično predstavlja prvu asocijaciju na kriptologiju tog perioda. Alan Turing, Colossus, Bombe, Bletchley Park i razbijanje Enigme često su glavne teme kada se govori o britanskoj kriptologiji, no zaboravlja se na jedan vrlo važan elektromehanički enkripcijski stroj koji je odigrao veliku ulogu tijekom rata, a to je Typex. Typex je dizajnom podsjećao na Enigmu, što nije začuđujuće s obzirom na to da je taj stroj nastao kao britanska interpretacija komercijalne inačice Enigme koju je predstavio Scherbius. Samim time, stroj je zadržao sličnost s njemačkim inačicama korištenima u Drugom svjetskom ratu, ali od njih se razlikovao ponešto izmijenjenim modelom zakrivanja poruka, ali zakritni algoritam i dalje je bio vrlo sličan onome Enigme I.

Mehanički dizajn ovog stroja također je bio vrlo sličan Enigmi, iako je i Typex imao mnogo revizija nakon što je prvi model uveden u vojnu upotrebu u drugoj polovici tridesetih godina. Svaki Typex stroj, bez obzira na inačicu, imao je pet rotora, od kojih su dva susjedna koja su "prihvaćala" električni *input* signal bila nepomična (slično kao i stator u slučaju Enigme, iako je Typex posjedovao i takav ulazni rotor)⁶⁷. Međutim, ta dva nepomična rotora moglo se postaviti u određeni početni položaj, ali oni nisu sudjelovali u rotaciji prilikom prolaska električne struje.

Iz sljedećeg grafičkog prikaza Typexova algoritma vidljivo je koliko su taj stroj i Enigma bili slični:



Slika 10 - Grafički prikaz Typex algoritma (Crypto Museum)

⁶⁷ Bauer (2002.), str. 136.

Osim rasporeda rotora, glavna razlika također je bila i u ploči s utičnicama (na slici *Steckerbrett*). Ploča koju je posjedovao Typex bila je bolja od one koju je posjedovala Enigma, a glavna razlika između te dvije ploče je ta da je Typex omogućavao povezivanje bilo koja dva slova, što se pokazalo kao snažnijom sigurnosnom mjerom od ploče na Enigmi koja je dozvoljavala povezivanje parova slova. Na slici 10 prikazan je algoritam inačice Typex Mk. 22, koji je najpoznatiji model stroja Typex.

Osim ranije spomenutih razlika u broju rotora i ploči, Typex i Enigma razlikovali su se i po još nekoliko elemenata:

a) ispisivanje poruka na papir - Typex strojevi bili su dizajnirani s mogućnošću ispisa poruke na papir, što ih je također učinilo manje prenosivima od Enigme, ali ne toliko kao u slučaju T-52 i Lorenz strojeva. Ovo je ubrzalo proces komunikacije jer je za rukovanje stroja bio potreban samo jedan operator, dok je u slučaju Enigme zakrivanje zahtijevalo dvojicu - jednog koji će poruke unositi i drugog koji će ih zapisivati.

b) mogućnost priključivanja na teleprinter - ova mogućnost također je ubrzala proces komunikacije jer se poruke, kao u slučaju Enigme, nisu morale pretvarati u Morseov kod kako bi bile poslone radio-vezom, već se proces pojednostavnio izravnim priključivanjem na teleprinter⁶⁸.

c) dizajn rotora - Enigma I, koja je obrazložena u jednom od prethodnih poglavlja, koristila je regularni pomak rotora, što je značilo da će njihovo pomicanje uvijek biti isto - prvi rotor pomicat će se 26 puta, susjedni rotor pomaknut će se jednom na svakih 26 pomaka prvog rotora i tako dalje. Ovakvi pomaci bili su uvjetovani zupčanicima, a britanski kriptolozi algoritam Typexa su odlučili dodatno osigurati tako što su za svaki rotor uveli različit broj "zarezova" koji su utjecali na pomicanje. Tako za jedan pomak drugog rotora nije trebalo 26 pomaka njemu susjednog rotora, već se jedan pomak mogao dogoditi već nakon pet pomaka početnog rotora, a sljedeći pomak mogao se dogoditi nakon 9 pomaka⁶⁹. Iako je i ovakav pomak rotora također smatran regularnim, predstavljao je napredak u odnosu na Enigmu I čiji je pomak bilo lakše uočiti prilikom kriptanalize koju su proveli britanski matematičari i kriptanalitičari na čelu s Alanom Turingom.

68 Crypto Museum. URL = <http://www.cryptomuseum.com/crypto/uk/typex/index.htm> (pristup: 17.5.2018.).

69 Isto.

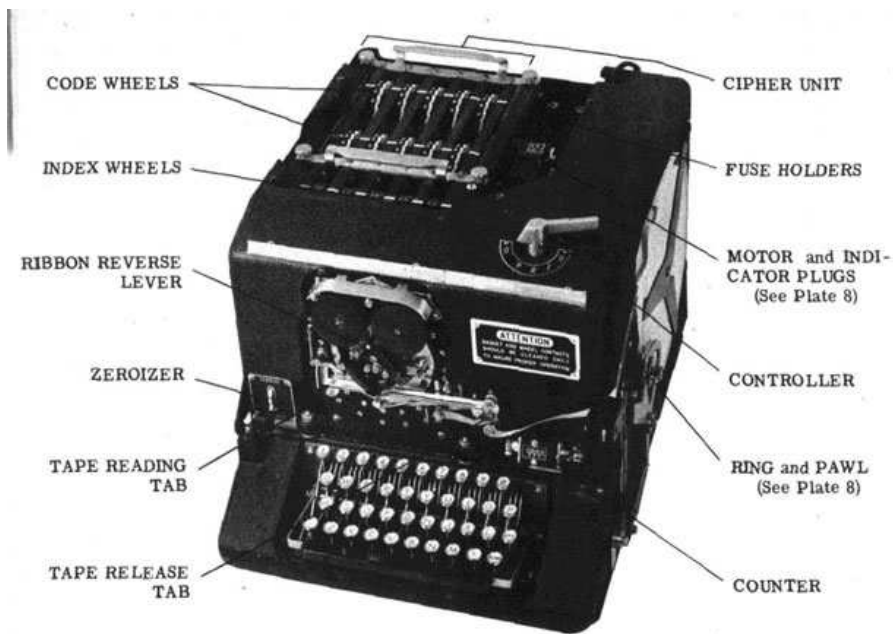
Typex je kao britanska inačica Enigme bio vrlo kvalitetan, a nije dokazano je li tijekom rata razbijen ili je ostao siguran medij za komunikaciju tajnih poruka. Njegovo korištenje nastavljeno je i tijekom rata, što je dovoljan dokaz kvalitete ovog stroja.

6.2. Sigaba

Kao i u slučaju britanske kriptologije, i američka kriptologija uoči Drugog svjetskog rata uglavnom se doticala samo kriptanalize. Američki kriptanalitičari najviše su se bavili kript analizom japanskih strojeva, i u tom području ostvarili su velike uspjehe. Međutim, kada je postalo izvjesno da će uskoro doći do mogućeg oružanog sukoba na globalnoj razini, američke vlasti pokrenule su razvoj novog sustava koji bi omogućio sigurnu komunikaciju, što je rezultiralo izumom stroja nazvanog SIGABA, čije ime predstavlja tvorenicu stvorenu od kratice SIG (*Signal Intelligence* ili SIGINT, naziv za djelatnost koja pokriva presretanje poruka i prikupljanje digitalnih informacija i podataka) te ABA (tajni naziv za ime nekog položaja). Sigaba je trebao biti stroj baziran na radu rotora koji će ispraviti sve nedostatke i propuste koje su tadašnji enkripcijski strojevi posjedovali, a Amerikanci su, poučeni dugim godinama kriptanalize, u tome i uspjeli. Sigaba se pokazao jednim od najboljih strojeva namijenjenih enkripciji poruka, i nastavio se koristiti dugo nakon završetka Drugog svjetskog rata, te nije poznato je li njegov algoritam ikad uspješno razbijen.

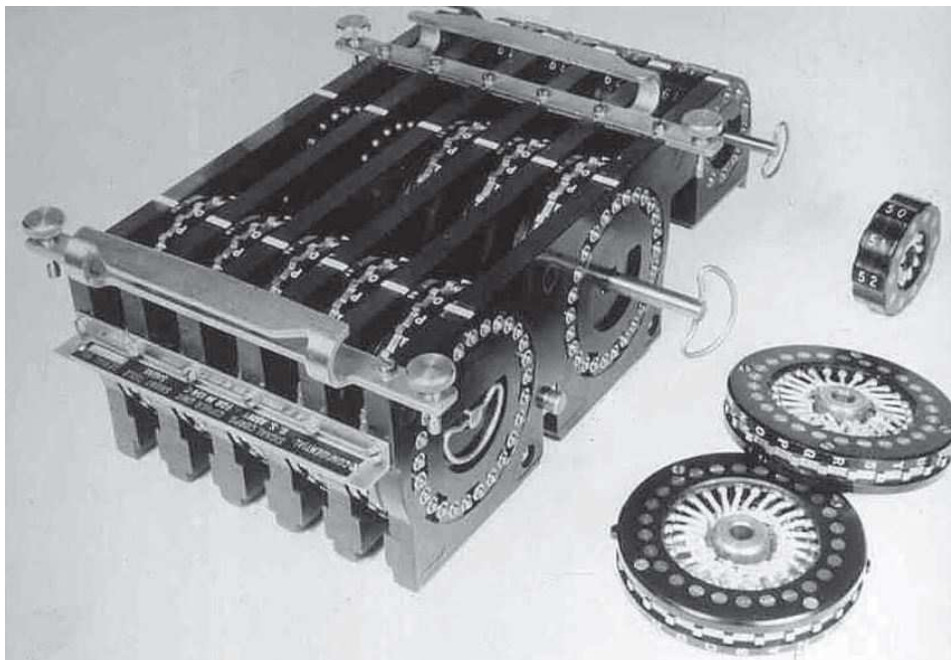
Dizajnom je stroj jako podsjećao na pisaći stroj, i mogao je ispisivati poruke na papir kao i Typex, što je svakako bila napredna mogućnost za tadašnje vrijeme. Osim toga, posjedovao je i ostale elemente koji su bili zajednički većini elektromehaničkih enkripcijskih strojeva toga doba - poseban odjeljak namijenjen za postavljanje i kontrolu rotora, ploču s tipkama (tipkovnicu), posebnu ručicu koja je dozvoljavala promjenu načina rada stroja (ispisivanje jasnopisa, enkripciju, dekripciju i isključivanje stroja), brojač pritisaka tipki (unosa znakova) i tako dalje. Najveća razlika između Sigabe i Typexa bila je u tome što je Sigaba posjedovao 15 rotora svrstanih u tri skupine, što će se znatno odraziti na kvalitetu zakritnog algoritma.

Na sljedećoj stranici prikazan je stroj s pripadajućim označenim dijelovima.



Slika 11 - Sigaba s označenim glavnim dijelovima (Wikipedia)

Zakritni algoritam koji je posjedovao ovaj stroj bio je vrlo kompleksan, a predstavljao je razvikanje ideja koje su se prethodno manifestirale u obliku Enigme, Typexa i sličnih elektromehaničkih strojeva baziranih na radu rotora. Za razliku od ovih strojeva, Sigaba je posjedovao sveukupno 15 rotora i nije imao reflektor:



Slika 12 - Tri skupine Sigaba rotora (NSA)

Tri skupine rotora bile su podijeljene na sljedeći način⁷⁰:

a) indeksni rotori - ovi rotori nalazili su se sprijeda, i nisu sudjelovali u rotaciji. Indeksne rotore bilo je moguće ručno podesiti, ovisno o dnevnom ključu. Američka kriptološka praksa tijekom Drugog svjetskog rata bila je jednaka njemačkoj, u smislu da su obje zemlje propisale dnevne ključeve zbog cikličkog sustava rotora⁷¹ (proces se ponavljao nakon određenog broja pomaka rotora, što je bila loša strana algoritma s obzirom na to da se mogao razbiti *brute force* metodom pokušaja i pogreške).

b) kontrolni rotori - ovi rotori sudjeluju u zakritnom algoritmu i, skupa sa sljedećom skupinom rotora (abecednim rotorima) tvore polialfaberski sustav koji sudjeluje u rotaciji i supstitucijskom zakrivljanju znakova na principu zamjene jednog slova drugim. Krajnje lijevi i krajnje desni kontrolni rotor bili su statični, a ostali rotori nisu se pomicali linearno već nelinearno. Treći rotor s lijeva pomicao se nakon svakog pritiska tipke, rotor koji je njemu s lijeva (desno od statičnog rotora) pomicao se nakon svakih 676 pritisaka tipke, a četvrti rotor (trećem s desna) pomicao se svakih 26 pritisaka tipke, odnosno svaki put kada bi treći rotor napravio puni krug (rotori su imali 26 kontaktnih točki kao i rotori ostalih strojeva).

c) abecedni rotori - treća skupina rotora, koja obavlja završni *scramble* slova prije ispisa na papir. Ovi rotori zamijenili su ploču s utičnicama i utikačima kakvu su posjedovali svi ostali strojevi, a to se na kraju pokazalo boljim rješenjem jer je stroj, kako se ispostavilo, posjedovao vrlo snažan zakritni algoritam.

Algoritam stroja u osnovi je bio vrlo sličan ranije prikazanim enkripcijskim strojevima, uz dodatke i izmjene koje su došle uvođenjem većeg broja rotora i većom mogućnošću njihove kontrole (neki su se mogli izvaditi tako da se koristi manje rotora u jednoj skupini).

Sigaba se pokazao kao najbolji saveznički enkripcijski stroj u razdoblju Drugog svjetskog rata, i dokazao da enkripcijski strojevi bazirani na radu rotora vrlo dobro rješenje za potrebe sigurnosne komunikacije, ukoliko su takvi strojevi kvalitetno konstruirani. Tijekom Hladnog rata, Sigaba je stroj koji je ostao u upotrebi, a tajne njegova dizajna dugo godina čuvane su zbog velike vrijednosti i kvalitete ovakvog algoritma.

70 Mucklow (2015.), str. 33.

71 I u američkoj praksi također se, osim dnevnog ključa, koristio i ključ poruke.

6.3. Combined Cipher Machine

Combined Cipher Machine (eng. "Mješoviti zakritni stroj", skraćeno CCM) bio je zajednički enkripcijski stroj koji je nastao suradnjom britanskih i američkih kriptologa. Ove dvije zemlje ostavile su suradnju u proučavanju novih kriptografskih metoda, a početkom rata postigle su dogovor prema kojem su trebale ostvariti ideju izuma zajedničkog enkripcijskog stroja koji bi bio kompatibilan s britanskim Typexom. Do ove ideje došlo je napretkom rata i sve većom suradnjom britanske i američke vojske. Međutim, nakon razvoja originalnog stroja nazvanog CCM/Sigaba, razvila se potreba i za britanskom inačicom, nakon čega je došlo do izuma CCM stroja baziranog na osnovi Typex stroja, čime je nastala CCM/Typex inačica.

Razlike među ovim modificiranim strojevima bile su sljedeće⁷²:

a) CCM/Typex - ovaj stroj zapravo je nazvan "Typex Mk. 23", što znači da je predstavljao sljedeći korak u modifikaciji prethodno opisanog Typex uređaja (koji je bio model 22). Promjena u algoritmu zakrivanja nije bilo, jer je prema dogovoru Typex poslužio kao temelj za razvoj ove modifikacije. Samim time, razlike u ovom modelu nisu bile velike u odnosu na prethodnu inačicu Typexa, osim fizičkih izmjena u vidu promjene konstrukcije i dodavanja novih konektora kojima se mogao spojiti dio namijenjen za univerzalno zakrivanje kompatibilno s američkim strojem.

b) CCM/Sigaba - za razliku od Typex inačice CCM stroja, Sigaba model doživio je veće izmjene, i to u samom algoritmu. Kao prvo, cjelokupni sustav rotora izmijenjen je i prilagođen tako da je ostalo samo pet pomičnih rotora koji su sudjelovali u zakritnom algoritmu, kako bi se stroj sveo na model koji je koristio Typex. Ovakva izmjena predstavljala je drastičan pad sigurnosti zakritnog algoritma u odnosu na originalni Sigaba model, ali omogućena je komunikacija s britanskim strojem (kojeg njemačka kriptološka služba ionako nije uspjela razbiti, ako je za suditi po nedostatku dokaza).

Gotovo svi saveznički kriptografski strojevi nastavili su se koristiti po završetku rata, a kriptologija anglo-saksonskog govornog područja od tad je postala dominantnom u svijetu tajne komunikacije.

⁷² Proc (2012.), URL = <http://jproc.ca/crypto/ccm.html> (pristup: 19.5.2018.).

7. Ostale vrste tajne komunikacije

Prvi svjetski rat bio je poligon za testiranje raznih inovacija u području kriptologije koje nisu uspjele zaživjeti u praksi kao što je bio slučaj s Drugim svjetskim ratom. Prvi svjetski rat obilježili su kodovi, a Drugi svjetski rat bio je pravi informacijski rat, koji je po prvi put izjednačio važnost informacija i važnost vojske i oružja. Međutim, i Drugi svjetski rat također je bio prepun slučajeva tajne komunikacije temeljene na dogovorenim kodovima, a veliku važnost predstavljala je i špijunaža, koja je do tada već bila tisućljetna profesija. Sovjetska kriptologija u periodu uoči i za vrijeme Drugog svjetskog rata do danas je ostala nepoznanicom, bez dovoljno informacija o onome što se događalo, i kakve su Sovjeti uređaje koristili prilikom tajne komunikacije. No, podaci koji jesu dostupni govore o jakoj mreži sovjetske špijunaže koja je, u odnosu na tadašnju suvremenu kriptologiju, možda bila primitivna, ali je svakako bila jednako učinkovita. Primjer koji su pružili Richard Sorge i slični špijuni dokaz je da je špijunaža i dalje ostala jednako važnim aspektom informacijskog ratovanja kao i moderne metode. Sorge je, kao sovjetski špijun u Japanu, otkrio nacističke planove za invaziju Sovjetskog Saveza, kao i dokaze za odustajanje Japana od napada sovjetskog Dalekog istoka. Prilikom komunikacije s Moskvom, Sorge je koristio takozvanu "knjišku šifru" (eng. *book cipher*)⁷³. Ovakva vrsta šifre vrlo je primitivna, a kao ključ uzima neku nasumičnu riječ iz određene knjige, te preko te riječi zakriva poruku. Unatoč tome, šifra se pokazala dovoljno sigurnom za slanje poruka, ali Sorge je na kraju ipak uhapšen i obješen kao sovjetski špijun. Špijunaža je također bila glavno obilježje Prvog svjetskog rata, gdje je povijest također ispisala imena poput Mate Hari.

Što se tiče kodova, oni su ostali u upotrebi do kraja Drugog svjetskog rata. Carska Japanska Mornarica uz kriptografske strojeve oslanjala se podjednako i na sustav kodova. Kodovi su uglavnom bili ostavština starih istraživanja iz područja kriptologije, i bili su obilježje Prvog svjetskog rata, tako da je za prilike Drugog svjetskog rata komunikacijama bazirana na kodovima predstavljala zastarjeli sustav koji nije garantirao jednaku sigurnost kao i kriptografski strojevi (iako, kodovi su i dalje često ostali u upotrebi u obliku koji je omogućivao njihovu integraciju u praksu korištenja kriptografskih strojeva). No, jedan slučaj korištenja kodova ipak je ostao vrlo jedinstven za prilike Drugog svjetskog rata, a usto se pokazao i jednim od najjačih kriptoloških sustava korištenih u tom razdoblju. Takav sustav proizveli su Amerikanci, a temeljio se na jeziku američkog indijanskog plemena Navajo. Američki Indijanci koji su sudjelovali u takvoj komunikaciji nazvani

⁷³ Kaspersky Lab Daily (2015.),

URL = <https://www.kaspersky.com/blog/ww2-zorge-book-cipher/8638/> (pristup: 19.5.2018.).

su *Navajo code talkers*. Ovaj sustav komunikacije bio je vrlo jedinstven jer se temeljio na jeziku plemena Navajo, koji nije bio poznat niti jednom drugom narodu izvan Sjeverne Amerike. Bitno je napomenuti da Navajo Indijanci nisu bili jedini narod koji je bio uključen u ovakav sustav komunikacije. Američka vojska eksperimentirala je i s ostalim indijanskim plemenima, ali i ostalim etničkim skupinama koje su govorile jedinstvenim jezikom koji se razlikovao od ostalih poznatih jezika (npr. baskijski jezik). Doduše, Navajo Indijanci pokazali su se kao najbolje rješenje s obzirom na to da posjeduje nekoliko glasova koji se ne pojavljuju u drugim poznatim jezicima, nije pisani jezik (što je predstavljalo ogroman problem prilikom kriptanalize koda, kad bi se kod pokušao transkribirati), a također ima vrlo ograničenu bazu govornika.

Sustav kodova kojim su Navajo Indijanci komunicirali bio je vrlo jednostavan, no zbog jezičnih posebnosti ujedno i vrlo siguran način komunikacije. Prema dogovorenom sustavu koji je razvila američka vojska, pojedina riječ odgovarala je pojedinom slovu abecede:

Alphabets (English)	Code Language (English)	Code Language (Navajo)	Modern spelling
A	Ant	Wol-la-chee	Wóláchíí'
B	Bear	Shush	<i>Shash</i>
C	Cat	Moasi	<i>Mósí</i>
D	Deer	Be	<i>Bííh</i>
E	Elk	Dzeh	<i>Dzeeh</i>
F	Fox	Ma-e	Mą'ii
G	Goat	Klizzie	T'í'í'í'
H	Horse	Lin	łíí'
I	Ice	Tkin	<i>Tín</i>
J	Jackass	Tkele-chogi	Téllícho'í
K	Kid	Klizzie-yazzi	T'í'í'í' yázhí
L	Lamb	Dibeh-yazzi	<i>Dibé yázhí</i>
M	Mouse	Na-as-tso-si	Na'asts'qqsí
N	Nut	Nesh-chee	Neeshch'íí'
O	Owl	Ne-ash-jah	Né'éshjaa'
P	Pig	Bi-sodih	<i>Bisóodi</i>
Q	Quiver	Ca-yeiith	k'aa'yeiftííh
R	Rabbit	Gah	<i>Gah</i>
S	Sheep	Dibeh	<i>Dibé</i>
T	Turkey	Than-zie	<i>Tązhii</i>
U	Ute	No-da-ih	Nóóda'í
V	Victor	a-keh-di-glini	Ak'ehdidlíní
W	Weasel	Gloe-ih	Dlǫ'ii
X	Cross	Al-an-as-dzoh	Alná'ázdzoh
Y	Yucca	Tsah-as-zih	Tsá'ászi'
Z	Zinc	Besh-dogliz	Béésh doot'í'izh

Slika 13 - Kod Navajo Indijanaca (Wikipedia)

Što se tiče procesa zakrivanja odnosno raskrivanja poruka, on je također bio vrlo jednostavan. Pošiljalac poruke jednostavno bi zakrio poruku korištenjem tablice prikazane na slici 13, a zatim bi tu poruku poslao radio-vezom do primatelja. Primatelj bi potom raskrio poruku korištenjem te iste tablice. Uz ovu tablicu, korišteni su i neke dogovorene kodne riječi, poput naziva različitih brodova ili vojnih postrojbi koje su nazivane imenima životinja, biljaka i slično. Sve takve riječi bile su propisane posebnim knjigama kodova.

Kod Navajo Indijanaca nikad nije razbijen od strane japanskih kriptanalitičara, a na europskom ratištu nije se koristio.

8. Kriptanaliza prve polovice 20. stoljeća

Kriptanaliza se u periodu Drugog svjetskog rata pokazala disciplinom koja je odlučivala ne samo bitke, već i čitav rat. Međutim, ona je također bila važna i u Prvom svjetskom ratu. I jedan i drugi sukob okupljali su znanstvenike raznih područja čija je zadaća bila prodrijeti u tajne komunikacije kojom se služila neprijateljska strana, a u toj zadaći prednjačile su matematika i njoj srodne znanosti, zbog već otprije spomenutih metoda baziranih na frekvencijskoj analizi, statističkim modelima proučavanja pojavljivanja uzoraka, te kombinatorici kao *brute force* metodi koja se uglavnom temeljila na procesu pokušaja i pogrešaka kako bi se došlo do konačnog rezultata. Jedan od najpoznatijih primjera uspješnosti kriptanalize u Prvom svjetskom ratu je takozvani "Zimmermanov telegram", tajni telegram koji je zakriven brojevanim kodom, a koji je poslan Meksiku od strane njemačkog ministarstva vanjskih poslova. Namjena telegrama bila je Meksiko uvući u rat protiv Sjedinjenih Američkih Država, što se nije dogodilo zaslugama britanskih kriptanalitičara koji su kodiranu poruku presreli i uspjeli razbiti, te nakon toga prosljedili američkim saveznicima⁷⁴. Kod je uspješno razbijen zbog već ranijeg napora britanskih kriptanalitičara da se razbije prethodna poruka komunicirana između pomorskih jedinica. Zimmermanov telegram označio je prvu veliku pobjedu britanskih kriptanalitičara, ali i početak ozbiljnijeg informacijskog ratovanja. Kada su vlasti velikih sila prepoznale koliku važnost i vrijednost kriptanalitičari mogu predstavljati, ova disciplina dobila je veliku pažnju. Naposljetku, tradicija kriptanalize anglo-saksonskih zemalja postat će dominantnom upravo po završetku rata, o

⁷⁴ NSA, URL = https://www.nsa.gov/news-features/declassified-documents/cryptologic-quarterly/assets/files/the_zimmermann_telegram.pdf (pristup: 20.5.2018.).

čemu svjedoči rano razbijanje komercijalne inačice Enigme i japanskih enkripcijskih strojeva, ali i ogromne zasluge u Drugom svjetskom ratu.

8.1. Kriptoanaliza u Drugom svjetskom ratu

Sile Osovine u predratno vrijeme nisu ulagale previše napora u kriptoanalizu postojećih enkripcijskih strojeva, što pogotovo vrijedi za carski Japan. I nacistička Njemačka i Japan razvijali su enkripcijske strojeve s ciljem ostvarenja potpuno sigurne komunikacije, i prije početka rata obje zemlje smatrale su da su dosegle vrhunac izumima kao što su Purple i Enigma tipa I. Problem ovakvog pristupa kriptologiji je taj što se koncentracijom na jedan aspekt znanosti postižu polovični rezultati - smatrati neki sustav savršenim bez testiranja loših strana dovodi do katastrofa kao što su razbijanje Enigme ili Purple (i to još prije no što je rat započeo). Kako su enkripcijski strojevi Saveznika uglavnom bili još strože čuvana tajna, i kako su nastali djelomično kao reakcija na enkripcijske strojeve Sila Osovine, Japan i Njemačka nisu imali priliku razviti snažno odjeljenje kriptoanalitičara kao što je bio slučaj sa zemljama Saveznika.

Britanski kriptoanalitičari (uz suradnju s poljskim kriptoanalitičarima) u Drugom svjetskom ratu predstavljali su najbolji primjer te discipline u navedenom periodu. Njihovi najveći uspjesi vezani su uz razbijanje Enigme, a potom i razbijanje Lorenza. **Razbijanje Enigme** započelo je već tridesetih godina, kada je Britansko Carstvo kupilo komercijalnu inačicu Enigme i započelo izučavanje njena zakritnog algoritma. Britanci su uspješno razbili algoritam komercijalne Enigme, i na temelju tog stroja kasnije razvili Typex. Međutim, to ne bi bilo moguće bez ranijih otkrića poljskih kriptoanalitičara, koji su prvi uspješno razbili taj algoritam. Poljski matematičari Marian Rejewski, Jerzy Rózycki i Henryk Zygalski uspješno su razbili algoritam zakrivanja poruka bez da su ikad došli u doticaj sa samim strojem, korištenjem nekoliko radio-poruka koje su presrele poljske službe (ovdje se govori o ranijoj vojnoj inačici Enigme - vojna Enigma tipa I, koja je razvijena kasnije, posjedovala je mnogo sigurniji i jači algoritam koji je razbio Alan Turing)⁷⁵. Uz to, Poljaci su izradili stroj nazvan "Bomba", koji je posjedovao algoritam specifično namijenjen razbijanju poruka zakrivenih Enigmom. Poljski kriptoanalitičari godinama su u tajnosti razbijali algoritam Enigme, bez znanja Britanskog Carstva. Invazijom nacističke Njemačke na Poljsku 1938. godine

⁷⁵ Crypto Museum. URL = <http://www.cryptomuseum.com/crypto/enigma/hist.htm> (pristup: 20.5.2018.).

znatno je onemogućena kriptanaliza Enigme, ali ostale zemlje nastavile su ono što je Poljska započela.

Britanska Vlada početkom rata inzistirala je na okupljanju grupe matematičara i znanstvenika srodnih znanosti kako bi se takvi znanstvenici stavili u funkciju budućih kriptanalitičara koji bi predvodili kriptanalizu usmjerenu protiv njemačke tajne komunikacije, a odluke Vlade trebala je sprovesti britanska obavještajna služba MI6, koja se bavila špijunažom i kriptologijom. Potraga za takvim osobama uglavnom je svedena na prestižna britanska sveučilišta i bivše kriptanalitičare, i rezultirala je okupljanjem najvećih znanstvenika iz područja kriptologije koji su služili u razdoblju Prvog svjetskog rata, ali pojavili su se i novi znanstvenici koji će obilježiti novo razdoblje, kao što su Alan Turing, Dillwyn Knox i William Tutte. Ovaj tim, predvođen zapovjednikom Dennistonom, preselio se sjeverno od Londona, na imanje u blizini sveučilišta Oxford i Cambridge, nazvano **Bletchley Park**. Lokacija je odabrana vrlo pažljivo, i to iz dva razloga. Prvi je bio blizina sveučilišta Oxford i Cambridge, što je značilo da će pribavljanje novih znanstvenika koji će posjedovati novije znanje i perspektivu biti lako. Drugi razlog je sjecište telekomunikacijskih kanala u blizini kojeg se imanje nalazilo, što je omogućilo uvježbavanje i osposobljavanje novopridošlog osoblja koje je trebalo izučiti kriptanalitičke metode poput presretanja poruka⁷⁶. Okupljeno je oko 150 članova, a projekt je čuvan u najvećoj tajnosti, čak i od britanske javnosti.

Prve operacije koje je Bletchley Park provodio bile su vezane uz presretanje poruka, a na samom imanju uspostavljena je stanica za presretanje radijskih signala, nazvana *Station X*. Osim ove stanice, osnovane su i brojne druge stanice identične namijene diljem cijelog svijeta, od Indije (gdje je bila stanica za presretanje signala japanske komunikacije), pa do europskih stanica (gdje su se presretali signali talijanskih i njemačkih signala). Ovakve stanice nazvane su *Station Y*⁷⁷.

Prve značajne operacije koje je grupa kriptanalitičara iz Bletchley Parka poduzela vežu se uz razbijanje Enigme, a takve operacije ostvarile su napredak već 1940. godine. Zbog suradnje s poljskim kriptolozima uoči (ali i za vrijeme) Drugog svjetskog rata, britanski kriptanalitičari imali su vrlo dobre početne uvjete za razbijanje Enigme, a razbijanje komercijalne inačice poslužilo je kao dobra praksa i dobro teoretsko polazište za nastavak informacijskog ratovanja. Osim toga, britanski kriptanalitičari bili su u velikoj prednosti time što su posjedovali kopiju Enigme koju su razvili Poljaci, a koji su je donirali britanskim kriptanalitičarima zbog postojeće suradnje. Britanski stručnjaci počeli su odvajati poruke koje su presreli putem Stanice X i Stanica Y, tako da su sve poruke važnijeg značaja grupnim imenom nazvali "Ultra" (od engleskog *Ultra Secret*). Ove poruke bile su isključivo poruke zakrivene strojevima Enigma. Kako je zakritni algoritam vojnih

76 URL = <https://bletchleypark.org.uk/our-story> (pristup: 25.5.2018.).

77 Isto.

inačica Enigme bio vrlo kompleksan i različit u odnosu na algoritam komercijalne Enigme koju su uspjeli razbiti, britanski kriptanalitičari odlučili su konstruirati stroj sličan Bombi koji je izmislio Rejewski godinu dana ranije. Alan Turing predložio je takvu ideju zapovjedništvu, a kako je stroj bio temeljen na poljskom stroju, namjena im je bila ista. Turing je svoj stroj nazvao "Bombe", slično kao i Poljaci. Turingove Bombe bile su vrlo veliki strojevi čiji je zadatak bio matematičkim pokušajima odgonetnuti ključeve kojima su njemačke poruke zakrivene korištenjem Enigme. Pojedinačni stroj težio je oko tonu, bio je širok približno 215 cm i visok 200 cm, a u konstrukciju su bile ugrađene tri ploče, od kojih je svaka sadržavala tri reda, i u svakom redu po dvanaest "bubnjeva" (cilindara, valjaka)⁷⁸. Ovi "bubnjevi" predstavljali su osnovu stroja, a povezivali su se vertikalno u parovima po tri, te je svaki od njih imao 26 kontaktnih točki kao i rotori korišteni u algoritmu Enigme. Razlog zbog kojeg se cilindre na Bombama povezivalo na taj način bio je simulirati rad njemačke Enigme, što znači da je svaki pojedinačni stroj mogao simulirati rad 36 Enigmi istovremeno.

Proces kriptanalize Bombi je moguće pojednostavniti na sljedeći način:

1) presretanje poruke - sigurnosna komunikacija njemačke vojske odvijala se radio vezom putem koje bi se zakritak slao Morseovim kodom. Stanica X i razne Stanice Y prikupljale su ovakve poruke i slale ih operaterima koji su koristili Bombe.

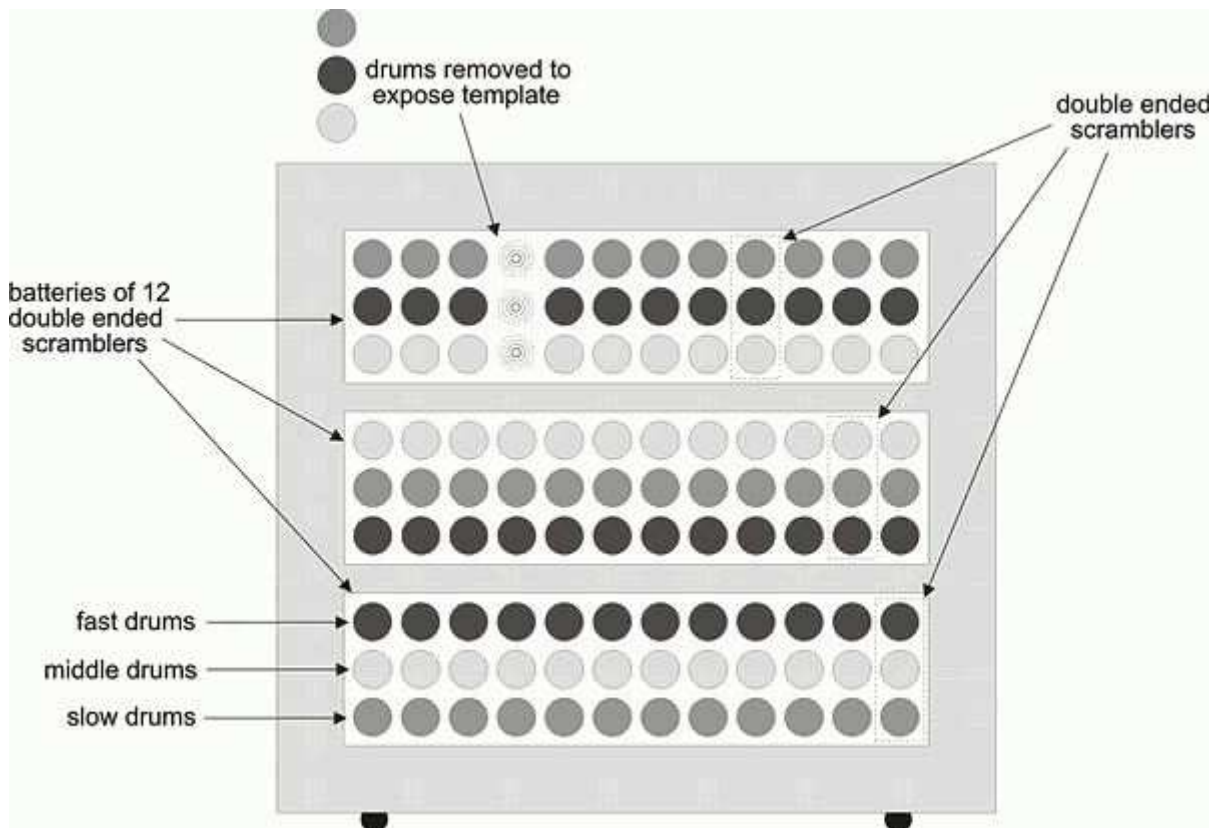
2) odgonetavanje zakritka - britansko presretanje poruka bilo je vrlo sistematično, a brojne stanice za presretanje poruka su, osim bilježenja sadržaja poruka, također pokušavale doznati otkud signal potječe, te kome je namijenjen. Ovo znanje pokazalo se ključnim za ovaj korak, jer je omogućavalo precizniju pretpostavku što bi poruka mogla sadržavati. Ako bi se sadržaj poruke (ili barem dio te poruke) uspješno pogodio (to jest, jasnopis te poruke, ili "šalabahter" kako su ga zvali kriptanalitičari), tada je bilo moguće podesiti cilindre na Bombi koji su prema tome mogli odrediti položaj rotora na Enigmi koja je sudjelovala u komunikaciji te poruke. Kriptanalitičarima je veliko olakšanje pružila ključna pogreška Enigme - niti jedno slovo nije se moglo zakriti u samo sebe, tako da je određivanje (pogađanje) eventualnog zakritnog slovoreda bilo znatno olakšano.

3) pronalaženje parova na ploči s utičnicama i utikačima - u ovom koraku zadatak kriptanalitičara bio je pronaći odgovarajuće parove koji su bili povezani na *Steckerbrett* ploči, koju su Enigma strojevi na početku rata već koristili kao dodatnu sigurnosnu mjeru. Kada bi set od tri

78 Ellsbury (1998.), URL = <http://www.ellsbury.com/index.htm> (pristup: 26.5.2018.).

uparena cilindra pronašao mogući početni položaj rotora bez ikakvih kontradikcija (mogući ključ), ta tri cilindra trenutno bi prestala funkcionirati dok operater nije provjerio rezultat i, u slučaju pogrešnog rezultata koji nije predstavljao korišten ključ originalne poruke, potom bi ga resetirao kako bi ti cilindri novim procesom producirali drukčiji rezultat. U pronalasku *Steckerbratt* postavki također je pomogao propust koji se sastojao u tome da se na ploči Enigme moglo povezivati parove od dva jedinstvena slova (npr. slovo A i C), što je također smanjilo broj operacija pronalaska takvih kombinacija. Unatoč tome, pronalazak ovih parova predstavljao je vrlo složen proces i najteži korak u razbijanju zakrivenih poruka.

Na sljedećoj slici grafički je prikazan izgled Bombe, s pripadajućim kombinacijama od po tri rotora:



Slika 14 - Grafički prikaz stroja Bombe (Ellsbury)

Bombe su, kao i ostali elektromehanički strojevi korišteni u informacijskom ratovanju i tajnoj komunikaciji, doživjele nekoliko izmjena ili revizija (pogotovo izumom Enigme bazirane na radu

četiri rotora). Zajedničkim naporom britanskih i poljskih kriptanalitičara, uz pomoć nekoliko zarobljenih tablica ključeva i doprinos savezničkih špijuna kao i operativnu lijenost nekih njemačkih kriptografa, došlo je do razbijanja mnoštva poruka te naposljetku i savezničku pobjedu u informacijskom ratovanju tijekom Drugog svjetskog rata.

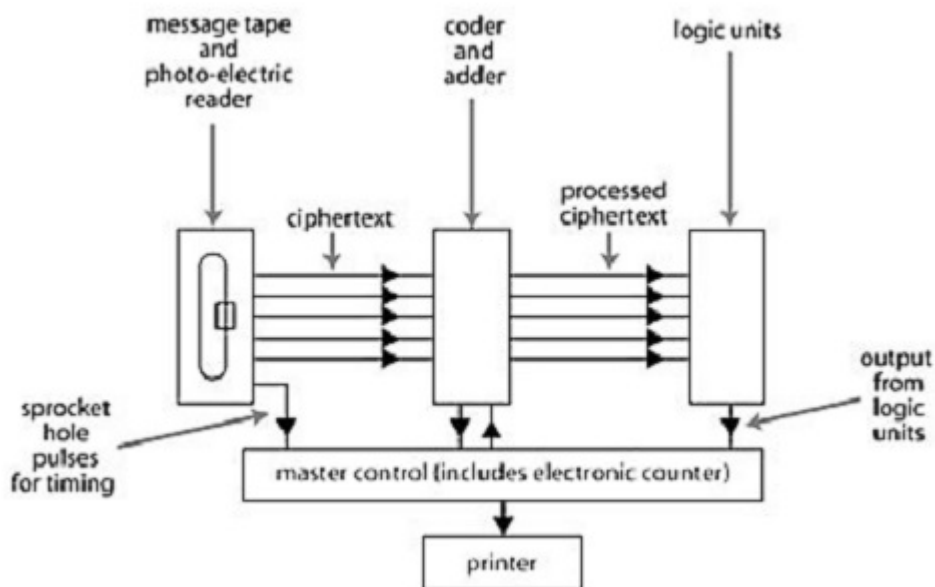
Kao i u slučaju razbijanja Enigme, kada je za potrebe kriptanalize izumljen poseban stroj namijenjen kriptanalizi, i za **razbijanje Lorenza** također je došlo do potrebe za takvim strojem. Lorenz je u upotrebu ušao nešto kasnije nakon Enigme, a predstavljao je velik skok u sigurnosti zakritnog algoritma u odnosu na Enigmu. Taj uređaj, izumljen sa svrhom razbijanja njemačkog stroja Lorenz nazvan je **Colossus**, i predstavljao je prvo elektroničko digitalno programabilno računalo. Međutim, Colossus je izumljen tek 1944. godine, a do tada je razbijanje Lorenza bilo utemeljeno na matematičkim operacijama koje je osnovao Alan Turing, a koje su se provodile ručno, bez pomoći nekog stroja. Turing je nedugo nakon što su britanske stanice presrele poruke zakrivene Lorenzom razvio posebnu metodu kriptanalize ovog stroja, pri čemu su mu pomogle pretpostavke koje su razvili ostali članovi tima koji je sudjelovao u razbijanju Lorenza, a koje su se pokazale točnima. Turingova metoda temeljila se na dedukciji mogućih ključeva kojima je poruka mogla biti zakrivena, slično radu Bombi. Velika prednost za britanske kriptologe predvođene Turingom bila je, opet, lijenost njemačkih kriptografa, koji su zakrivali više različitih poruka istim ključem, što je olakšalo proces dedukcije jer se za više različitih poruka koristio identičan položaj rotora. Turingova metoda bila je dominantna sve do 1944. godine, kad je napokon došlo do izuma Colossusa sa svrhom ubrzavanja procesa razbijanja Lorenza. Colossus je izumio Tommy Flowers, a dimenzijama je računalo bilo veće i od samih Bombi⁷⁹. Ukratko, računalo se sastojalo od nekoliko temeljnih dijelova, od kojih su najbitniji kontrolna ploča, S-postolja koje je simuliralo rad pisaćeg stroja, postolja koja su sadržavala razne prstenove ili jedinice zadužene za provođenje XOR logike nad ulaznom porukom, ali i ulaze i izlaze za pisane poruke ili upute (Colossus je prihvaćao naredbe za analizu pojedinog teksta na papiru koji je sadržavao tekst i bio probušen na način sličan bušenim karticama). Svrha Colossusa zapravo je bila prebrojavanje i analiza datog mu teksta, i to tako da je računalo trebalo uočiti uzorak u nepravilnosti zakrivanja poruka. Britanski kriptanalitičari shvatili su unutarnju logiku i dizajn Lorenza bez da su ikad došli u doticaj s tim strojem, a samim time mogli su zaključiti i da će dva seta rotora (*psi* i *chi* rotori) zakrivati tekst na različit način, što je otvorilo mogućnost frekvencijskoj analizi i implementaciji matematičkih modela kombinatorike kojima se mogao analizirati zakritak⁸⁰. Colossus se programirao vrlo primitivno u usporedbi s

79 Sale, URL = <http://www.codesandciphers.org.uk/lorenz/colossus.htm> (pristup: 27.5.2018.).

80 Isto.

današnjim računalima - korištenjem raznih utikača i poluga, a djelovao je na principu elektronskih cijevi koje su kontrolirale logiku (propuštajući električni signal).

Sljedeća slika prikazuje pojednostavljen proces obrade poruke na način koji je to radio Colossus, prema skici koju je izradio Flowers:



Slika 15 - Logika računala Colossus (Copeland)

Razlike Colossusa i Bombe ovdje su prilično očite. Turingove Bombe nisu mogle ispisivati poruke ili prihvaćati *input* u obliku teksta na papiru, a također nisu mogle prebrojavati moguće kombinacije (ključeve), za što su korišteni specifični strojevi korišteni za obradu popisa stanovništva.

Zbog toga što su se u ovom ratu zatekle na istoj strani, američki i britanski kriptolozi mnogo su surađivali na razvijanju novih sustava zakrivanja poruka (prisjetimo se već spomenutog CCM standarda i pripadajućih strojeva), ali također su surađivali i u domeni kriptanalize. Međutim, ova suradnja nije bila aktivna od samog početka rata, već je do nje došlo kasnije, kada se SAD uključio u rat⁸¹.

81 Zanimljivo je da su se britanski i američki kriptolozi zapravo zatekli na "suprotnim" stranama uoči rata, jer su britanske obavještajne agencije prisluškivale i nadzirale američku vojsku i diplomaciju i obrnuto (SAD je uoči rata provodio politiku neutralnosti).

Američka kriptanaliza početkom Drugog svjetskog rata uglavnom je bila orijentirana na razbijanje japanskih enkripcijskih strojeva, gdje je postigla velike uspjehe vrlo rano. Nesretna okolnost je za američke kriptologe, za razliku od britanskih, bila ta što američko vodstvo nije polagalo prevelike nade u informacijski rat kao novu stranu rata koja će biti jednaka (ako ne i važnija) konvencionalnom načinu ratovanja. Tridesete godine prošlog stoljeća stoga su američku kriptanalizu obilježile okolnostima kao što su nedostatak financiranja, razumijevanja i interesa za razvoj posebnih metoda i strojeva koji bi služili takvoj svrsi. Unatoč tome, američki kriptanalitičari postigli su vrlo dobre rezultate i uspjeli razbiti sve enkripcijske strojeve koje su Japanci koristili, čak i prije izbijanja rata između te dvije zemlje. Američki program provođenja kriptanalize nad japanskom komunikacijom nazvan je "*Magic*", a započeo je još za vrijeme dvadesetih godina kada je grupa kriptanalitičara započela s analizom strojeva tipa Red, koji su uspješno i do kraja razbijeni tek 1936. godine (što je opet moguće pripisati raznim ranije navedenim faktorima).

Tijekom rata su Amerikanci, zbog suradnje s britanskim kriptanalitičarima, uspjeli i sami izraditi nekoliko Turingovih Bombi, ali uz dodatne revizije, zbog čega se različite američke inačice Bombi razlikovale od britanskih. Na kraju su se ti strojevi posudili skupini britanskih kriptanalitičara koja je radila u Bletchley Parku, što je dokaz da su američki strojevi bili kvalitetniji i predstavljali napredak u odnosu na britanske strojeve istog tipa. Američke inačice Bombi također su bile namijenjene razbijanju Enigme, dok se program Magic zasnivao na razbijanju isključivo japanske tajne komunikacije. Američka se kriptanaliza, kao i britanska, pokazala vrlo korisnom u odlučujućim trenucima. Jedan takav primjer predstavlja i bitka za Midway, gdje je zahvaljujući naporima grupe kriptanalitičara razbijeno nekoliko poruka među kojima je bila i ona o datumu i mjestu napada, što je Američka Mornarica vrlo dobro iskoristila te na kraju i pobijedila u bitci. O važnosti uloge kriptanalitičara posvjedočio je i general George Marshall: "Zbog kriptanalize smo uspjeli koncentrirati naše ograničene snage kako bi spriječili njihov (japanski) napad na Midway kada bi inače bili 3000 milja izvan položaja."⁸².

Što se tiče kriptanalize Sila Osovine, ona jest postojala ali u znatno manjoj mjeri nego na strani Saveznika, stoga ne postoji dovoljno dokaza o uspješnosti kriptanalitičara Sila Osovine.

82 Weadon (2016.), URL = <https://www.nsa.gov/about/cryptologic-heritage/historical-figures-publications/publications/wwii/battle-midway.shtml> (pristup = 28.5.2018.).

Teorijske pretpostavke koje su postavili kriptolozi ovog perioda (npr. Alan Turing i njegov "Turingov stroj") i realizacija određenih ideja u praksi (Colossus i Bombe) poslužile su kao dobar uvod u ono što će se tijekom narednih godina formulirati kao suvremena računalna znanost.

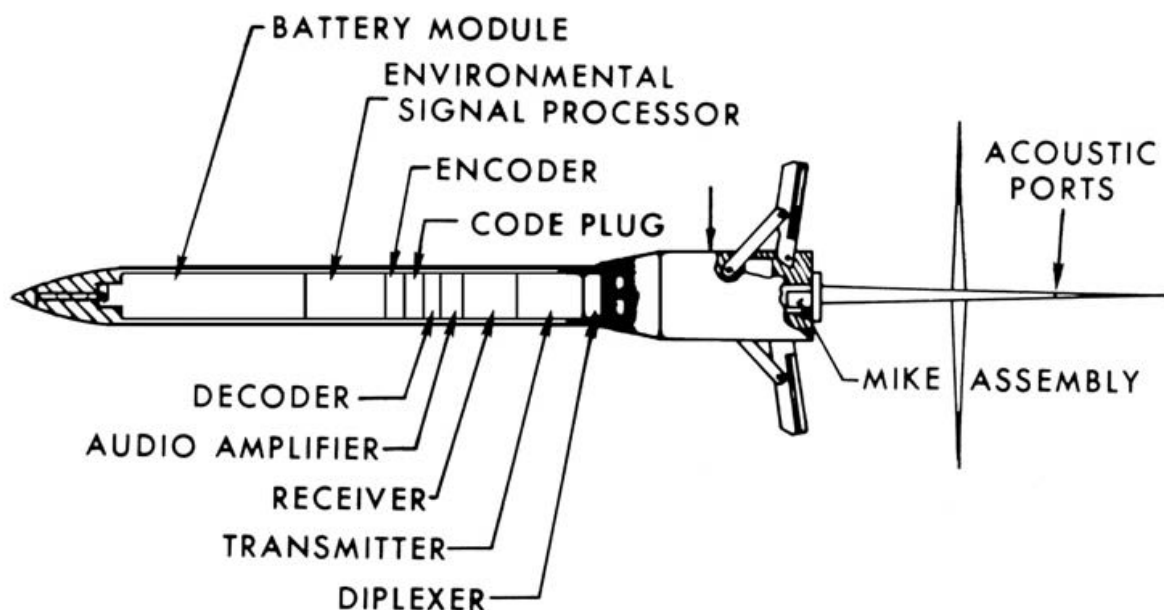
9. Utjecaj na suvremenu kriptologiju

Iako kriptologija Prvog svjetskog rata nije imala prevelik utjecaj na poslijeratno razdoblje, ona je poslužila kao uvod u istraživanja vezana uz elektromehaničke strojeve za zakrivanje poruka, koji su definitivno ostavili najveći trag u suvremenoj kriptologiji. Ovo ne znači da su sami strojevi kao alati ostavili taj trag, već se on očitovao i u novom načinu razmišljanja i teorijama komunikacije koji su obilježili informacijski rat Drugog svjetskog rata.

U poslijeratnom periodu velik broj elektromehaničkih strojeva koji su služili u razdoblju Drugog svjetskog rata uništen je. Jedan od razloga bio je da za takvim strojevima više nije postojala potreba, rat je bio okončan, a samim time i svrha takvih strojeva. Drugi razlog bio je sigurnosne naravi, a ticao se uglavnom strojeva koji su služili u kriptanalizi (npr. Colossus). Takvi strojevi bili su uništavani kako bi se tajna njihova postojanja sačuvala od ostatka svijeta, a za neke od njih nije se saznalo jako dugo. Colossus je tako ostao strogo čuvana tajna sve do sedamdesetih godina prošlog stoljeća, a originalni stroj skupa s nacrtima bio je uništen. O nekim strojevima nema gotovo nikakvih informacija. Pretpostavlja se da je Sovjetski Savez također koristio elektromehaničke strojeve za potrebe tajne komunikacije u razdoblju Drugog svjetskog rata, ali postojanje takvih strojeva i dalje je strogo čuvana tajna, tako da o kriptologiji te zemlje za vrijeme rata znamo vrlo malo. Zna se za postojanje samo jednog modela baziranog na radu rotora, ali poslijeratne godine pokazale su da su Sovjeti bili itekako sposobni kriptolozi. Sovjetski Savez nastavio je koristiti enkripcijske strojeve temeljene na radu rotora, koji su bili vrlo rašireni na području Istočne Europe u razdoblju Hladnog rata.

Osim Sovjeta, i ostale zemlje u većoj ili manjoj mjeri i dalje su se oslanjale na strojeve čiji su se algoritmi temeljili na radu rotora. Velika Britanija svoje strojeve koristila je za obučavanje budućih kriptanalitičara, što je osiguralo važnost i primjenu Turingovih Bombi i u poslijeratnim godinama. Ostali strojevi, poput raznih inačica Typexa, također su ostali u upotrebi. Štoviše, ti strojevi proširili su se cijelim svijetom, odnosno ostali su u upotrebi u gotovo svim zemljama koje su nekoć pripadale Britanskom Carstvu. Može se smatrati pomalo čudnim što su takvi strojevi ostali u funkciji sve do sedamdesetih godina, kada su računala i ostali napredni strojevi već ušli u vojnu

upotrebu, no prisjetimo se da su neki od tih strojeva (konkretno, Sigaba i Typex) posjedovali vrlo snažan algoritam zakrivljanja, a vjerojatno nikad nisu niti razbijeni od strane neke druge zemlje. Američka kriptologija nastavila je sada već formiranu tradiciju snažne kriptologije i u Hladnom ratu, a financiranje takvih projekata više nije bio problem kao uoči Drugog svjetskog rata. Također, Sjedinjene Američke Države su se razlikovale od ostalih velikih zemalja po tome što su prošle kroz dva veća vojna sukoba koja su slijedila Drugi svjetski rat - Korejski rat i Vijetnamski rat. Ova dva rata potvrdila su ono što se vidjelo i u prošlom velikom ratu, a to je značaj vojnog sukoba za razvoj kriptologije. Kao i Drugi svjetski rat, i Koreja i Vijetnam poslužili su kao poligon za ispitivanje novih komunikacijskih teorija primjenjivih u informacijskom ratovanju. Prikupljanje i pohrana informacija postala je jednom od najvažnijih aktivnosti, čiji se začetci mogu vidjeti u britanskim stanicama X i Y koje su služile za presretanje radijskih signala. Jedan od takvih projekata u Vijetnamskom ratu bio je *Operation Igloo White*, američki projekt nadzora kretanja vijetnamskih vojnih postrojbi. Grafički prikaz uređaja korištenih u tom projektu može se vidjeti na sljedećoj slici⁸³:



Slika 16 - Akustički senzor (Novak)

83 URL = <https://paleofuture.gizmodo.com/how-the-vietnam-war-brought-high-tech-border-surveillance-1694647526> (pristup: 1.6.2018.).

Ovakav uređaj bio bi ispušten iznad predviđenog smjera kretanja neprijateljske vojske, a slao bi podatke do najbliže stanice (antene) koja je takav signal slala dalje na obradu. Obrada ovih podataka odvijala se pomoću računala. Računala su u sedamdesetim godinama služila za analizu i obradu podataka, a posebni enkripcijski strojevi i dalje su bili korišteni za zakrivljanje odnosno kriptanalizu poruka.

Što se tiče američke kriptografije, ona je i dalje u određenoj mjeri bila temeljena na strojevima kao što su Sigaba. Kao što je iz brojnih primjera vidljivo, enkripcijski strojevi koji su se temeljili na radu rotora bili su vrlo revolucionaran izum koji je ostao u upotrebi dugo nakon što je ušao u funkciju. Međutim, brzim napretkom tehnologije došlo je do razvoja ostalih vrsta uređaja i strojeva koji su služili za osiguravanje tajne komunikacije. Takvi strojevi postajali su sve sličniji računalu, a mehanički analogni rotori su polako zamijenjeni digitalnim algoritmima. Neki od takvih uređaja bili su takozvani "*voice scrambleri*", uređaji slični telefonu (ponekad i sami telefoni) koji su bili sposobni glas pretvoriti u nerazumljiv i razlomljen signal koji bi se na primateljevoj strani opet posložio u razumljiv "jasnopis" (u zvučnom obliku). Enkripcija zvuka temeljila se na razlamanju poruke na manje dijelove i njihovoj pretvorbi u "zakriven" oblik, koji bi bio nerazumljiv presretaču kojem ona nije namijenjena. Ponekad bi se tako razlomljeni djelići poruke slali drukčijim redoslijedom, tako da ih presretač nije mogao sastaviti čak i ako bi ih uspio presresti. Takvi uređaji uglavnom su koristile tajne službe, policija, diplomacija, ali i državni vrh i vlade. Zanimljivo je za primijetiti da su gotovo sve takve uređaje proizvodile tvrtke koje i danas posluju, poput Motorole, Siemens, i drugih. Krajem dvadesetog stoljeća u upotrebu ulaze i suvremena računala, koja su napokon dosegla visoku procesorsku snagu i količinu memorije dovoljnu da se procesi kriptografije ili kriptanalize obavljaju na manjem i prenosivom računalu, za razliku od računala korištenih u Drugom svjetskom ratu koja su zauzimala prostor čitave jedne oveće sobe. Krajem devedesetih godina računalo je postalo vodeće sredstvo u tajnoj komunikaciji i informacijskom ratovanju, a pravac tog razvoja možemo još bolje vidjeti danas kad su računala postala ne samo glavni alat u tajnoj komunikaciji, već i glavni alat i medij komunikacije uopće. Digitalni algoritmi polako su zamijenili analogne i elektromehaničke, a popratni uređaji namijenjeni osiguravanju komunikacije postaju sve rjeđi. Međutim, uvijek se treba prisjetiti kako je sve počelo, te gdje leže izvori moderne kriptologije. Bez genijalnih izuma koji su popratili teoriju kriptologije prve polovice dvadesetog stoljeća komunikacija u suvremenom svijetu možda nikad ne bi izgledala ovako, a brojni izumi koji su doprinijeli ubrzanom razvoju tehnologije možda se nikad ne bi pojavili.

10. Zaključak

Kriptologija je kao znanost ostvarila svoj najveći utjecaj i ostavila svoj najveći trag u svjetskoj povijesti i znanosti općenito upravo u prvoj polovici dvadesetog stoljeća. Od revolucije koje su predstavili elektromehanički strojevi za raskrivanje poruka, do pojave prvih računala koji su se koristila baš u svrhe kriptologije, možemo vidjeti koliko je utjecajna ova znanost bila na daljnji razvoj i napredak komunikacije, sigurnosti komunikacije, ali i napredak znanosti uopće. Kao što je kriptologija u osnovi interdisciplinarna znanost, tako je i njen utjecaj vrlo opipljiv i vidljiv i u ostalim znanostima - od matematike, logike, mehanike, računalne znanosti, pa sve do umjetne inteligencije, te nove znanosti budućnosti. Zbog tog utjecaja važno je prepoznati kriptologiju prve polovice dvadesetog stoljeća kao iznimno važnu znanost koja je zasigurno promijenila tijek ljudskog razvoja i osigurala osnove za neviđen napredak tehnologije. Neki od najvećih znanstvenika u vrijeme Drugog svjetskog rata bili su uključeni u razvoj i realizaciju novih ideja kriptologije, a zbog svojih zasluga njihova imena zauvijek će biti urezana u povijesti tehnologije, informacijskih i računalnih znanosti.

11. Literatura

Bauer, F. *Decrypted Secrets: Methods and Maxims of Cryptology*. Treće izdanje, Berlin: Springer, 2002.

Bletchley Park. <https://bletchleypark.org.uk/our-story> (20.6.2018).

Cohen, F. *Introductory Information Protection*. 1990, all.net/edu/curr/ip (17.6.2018.).

Crypto Museum. <http://www.cryptomuseum.com/> (20.6.2018).

Ellsbury, G. *The Enigma and the Bombe*. (1998).

<http://www.ellsbury.com/index.htm> (20.6.2018).

Fraser, A. *Mary Queen of Scots*. London: Weidenfeld and Nicholson, 1969.

Friedman, W. *Preliminary Historical Report on the Solution of the "B" Machine*. 1940, https://www.nsa.gov/news-features/decclassified-documents/friedman-documents/assets/files/reports-research/FOLDER_211/41760789079992.pdf (17.6.2018.).

Gillow, M. *Virtual Colossus*. <http://www.virtualcolossus.co.uk/index.html> (20.6.2018).

Grime, J. *Lorenz: Hitler's "Unbreakable" Cipher Machine*,

<https://www.youtube.com/watch?v=GBsfWSQVtYA> (15.5.2018.).

Hoskisson, P. *Jeremiah's Game*. // *Insight*. 30/1(2010), str. 3-4.

Kahn, D. *The Codebreakers*. New York: The Macmillan Company, 1967.

Leksikografski Zavod Miroslav Krleža: *Hrvatska Enciklopedija*, <http://www.enciklopedija.hr/>

Mucklow, T. *The SIGABA / ECM II Cipher Machine: "A Beautiful Idea"*. (2015).

https://web.archive.org/web/20170515064250/https://www.nsa.gov/about/cryptologic-heritage/historical-figures-publications/publications/assets/files/sigaba-ecm-ii/The_SIGABA_ECM_Cipher_Machine_A_Beautiful_Idea3.pdf (20.6.2018).

Novak, M. *How the Vietnam War Brought High-Tech Border Surveillance to America.* // Paleofuture (web stranica) (2015).

<https://paleofuture.gizmodo.com/how-the-vietnam-war-brought-high-tech-border-surveillan-1694647526> (20.6.2018).

NSA. *Zimmermanov telegram.*

https://www.nsa.gov/news-features/declassified-documents/cryptologic-quarterly/assets/files/the_zimmermann_telegram.pdf (20.6.2018).

Oxford Dictionaries Online: *cryptology.* (20.6.2018).

Proc, J. *Crypto Machines.* (2012). <http://jproc.ca/crypto/index.html> (20.6.2018).

Rijmenants, D. *Cipher Machines and Cryptology: Enigma Messages Procedures.*

<http://users.telenet.be/d.rijmenants/en/enigmaproc.htm> (13.5.2018).

Sale, T. *The Colossus: Its purpose and operation.*

<http://www.codesandciphers.org.uk/lorenz/colossus.htm> (20.6.2018).

Savard, J. *A Cryptographic Compendium.* (1999).

<http://www.quadibloc.com/crypto/te0302.htm> (20.6.2018).

Schneier, B. *Applied Cryptography: Protocols, Algorithms, and Source Code in C.* New York: John Wiley and Sons, 1996.

Service, R. *Lenin: A Biography.* Cambridge, Massachusetts: Harvard University Press, 2000.

Scherbius, A. "*Enigma*" *Chiffriermaschine.* // *Electrotechnische Zeitschrift.* 47/48 (1923).

Weadon, P. *The Battle of Midway: How Cryptology enabled the United States to turn the tide in the Pacific War*. (2016).

<https://www.nsa.gov/about/cryptologic-heritage/historical-figures-publications/publications/wwii/battle-midway.shtml> (20.6.2018).

Weierud, F. *Cryptology and its History*, <http://cryptocellar.org/simula/purple/index.html> (16.5.2018.).

Wikipedia, The Free Encyclopedia, <https://www.wikipedia.org/>

Wrixon, F. *Codes, Ciphers & Other Cryptic & Clandestine Communication: Making and Breaking Secret Messages from Hieroglyphs to the Internet*. New York: Black Dog & Leventhal Publishers Inc, 1998.