Enigma

Simona Ipša
Fakulteta za matematiko in fiziko
Ljubljana, 15.12.2004

Povzetek

Enigma je šifrirna naprava, ki so jo uporabljali Nemci v času 2. svetovne vojne. Naprej je opisana zgradba in delovanje Enigme. Sledi še opis njenega razbitja. Prvi jo je razbil poljski matematik Marian Rejewski leta 1932. Nato so Nemci posodobili napravo in povečali varnost pri pošiljanju sporočil. Posodobljeno različico je razbil britanski kriptograf Alan Turing. Sporočila so začeli razbijati leta 1940 s pomočjo naprave, ki se je imenovala bomba. V nadaljevanju je opisana tudi njena zgradba in delovanje.

Abstract

Enigma is a cipher machine that was used by the Germans during World War II. First, the structure and the function of Enigma are described, and then the process of its breaking. The first man who broke Enigma was Marian Rejewski, a Polish mathematician, in 1932. After that, The Germans updated the device and increased the security of sending the messages. The updated version of Enigma was broke by the British cryptoanalyst Alan Turing. They started to broke messages in 1940 with the help of a device, the so-called "bombe". Finally, the structure and the function of bombe are described.

Kazalo

1 Uvod

Kriptografija že od nekdaj igra pomembno vlogo pri varovanju skrivnosti. Predvsem v času vojn postane prenos informacij, za katere sovražnik ne sme izvedeti, še pomembnejši. Proti koncu 1. svetovne vojne so v kriptografiji začeli uporabljati vrtljive elektro-mehanske šifrirne naprave. Kmalu po koncu 1. svetovne vojne je Arthur Scherbius izdelal šifrirno napravo, ki jo je poimenoval Enigma. Enigma je bila na začetku namenjena v komercialne namene. Kasneje je nastalo več raličic, ki so jih Nemci času 2. svetovne vojne uporabljali predvsem v vojne namene.
Enigma je bila sestavljene iz petih osnovnih komponent: tipkovnice, stikalne plošče, vrtljivih diskov, reflektorja in zaslona, na katerem so se osvetljevale zašifrirane črke sporočila. Varnost Enigme je temeljila na velikem številu možnih začetnih nastavitev naprave. Ko so britanski, francoski in drugi kriptoanalisti začeli prejemati Enigmina sporočila, so se lotili razbitja. Po zaslugi francoskega vohuna so celo vedeli, kako je Engima sestavljena, kjub temu pa se jim je zdelo nemogoče, poiskati začetno nastavitev posameznega sporočila. Podrobneje so se z razbitjem začeli ukvarjati Poljaki, saj so bili ogroženi s strani sosedov Nemcev. Tako je Marianu Rejewskemu leta 1932 uspelo razbiti Enigmina sporočila. Njegovo razbitje je temeljilo na ciklih črk, ki so bile odvisne le od nastavitve diskov in ne od nastavitev v stikalni plošči. S tem je zelo zmanjšal število razporeditev, ki jih je bilo potrebno pregledati.
Tako so Poljaki vse do leta 1939 razbijali Enigmina sporočila, drugi narodi pa niso o tem ničesar vedeli. Nato pa so Nemci vpeljali nekatere posodobitve in varnostne ukrepe. Poljaki tako niso imeli dovolj sredstev za razbitje in o svojih dosežkih so povedali še ostalim narodom. Razbitje so tedaj prevzeli Angleži. Med njimi je bil najpomembnejši Alan Turing. Ker so takrat že imeli veliko razbitih Enigminih sporočil, je lahko za določene dele tajnopisa domneval, kaj je ustrezni čistopis. V teh parih čistopis - tajnopis je iskal zanke, na podlagih katerih je potem nekaj naprav zaporedoma povezal med sabo. Če je bil par pravilen in Enigme prav nastavljene, se je v enem izmed možnih krogov tokokrog sklenil. Izdelali so napravo, ki je avtomatično preverjala različne nastavitve. Naprava se je imenovala *bomba*.
S pomočjo bombe so Angleži dolgo razbijali Enigmina sporočila. Kljub bombi je bilo razbijanje Enigminih sporočil še zmeraj zahtevno delo, ki pa je zaradi svoje pomembnosti ostalo v veliki tajnosti še dolgo po koncu 2. svetovne vojne.

2 Opis delovanja Enigme

Enigmo je leta 1918 izdelal Arthur Scherbius v komercialne namene. Ker je napravo lahko kupil kdorkoli, varnost njenih sporočil ni bila odvisna od naprave same, ampak od ogromnega števila možnih nastavitev naprave pred pričetkom šifriranja.

Slika 1: Enigma

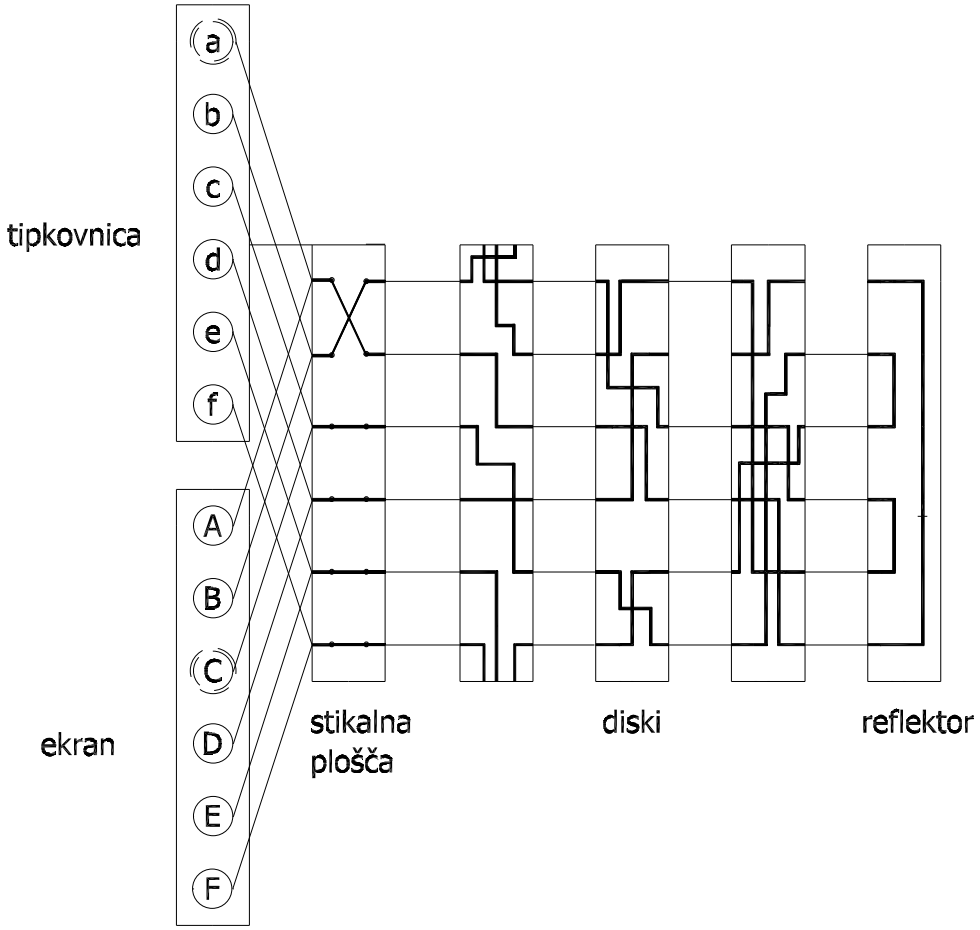
Kasneje so jo začeli uporabljati tudi v vojne namene, vendar se je ta nekoliko razlikovala od komercialne oblike. V tem poglavju je podrobneje opisana zgradba Enigme in njeno delovanje. Osnovne komponente Enigme so bile tipkovnica, stikalna plošča, v kateri je operater s pomočjo kablov lahko zamenjal dve črki med sabo, trije diski, ki so se zavrteli ob vsakem pritisku na tipkovnico, in zaslon, na katerem se je osvetlila ustrezna zašifrirana črka. Če je hotel operater, ki mu je bilo sporočilo namenjeno, odšifrirati sporočilo, je moral imeti na začetku isto nastavitev kot operater, ki je sporočilo pošiljal. V ta namen so si Nemci omislili knjigo ključev. Na koncu tega poglavja je primer zapisa v knjigi ključev za dnevno nastavitev Enigme in izračunano število možnih začetnih nastavitev osnovne in posodobljene različice Enigme.

Osnovna oblika Scherbiusove Enigme je bila sestavljena iz treh komponent, povezanih z žicami. Prva komponenta je bila tipkovnica, druga je bila sestavljena iz diskov, ki so vsako črko čistopisa, ki jo je operater pritisnil na tipkovnici, spremenili v ustrezno črko tajnopisa, tretja pa zaslon z abecedo, na katerem se je osvetlila ustrezna črka tajnopisa.

Iz tipkovnice je bilo speljanih 26 žic (za vsako črko abecede po ena žica) do diska. V notranjosti diska so se te žice med seboj prepletle, preden so prišle do določenih 26 točk na drugi strani diska, od koder so potem potekale žice do posameznih črk abecede na ekranu. Ko je tako operater pritisnil določeno tipko, je s tem poslal električni tok po žici in na ekranu se je osvetlila ustrezna črka. To je prikazano na sliki 2, zaradi lažje predstave s samo šestimi črkami. V Scherbiusovi Enigmi si bili trije diski. Vsakič, ko se je zašifrirala ena črka, se je prvi disk premaknil za en položaj, položajev pa je bilo toliko kot je črk angleške abecede, torej 26. Če je operater večkrat zaporedoma pritisnil isto črko, se je ta zašifrirala vsakič drugače. Ko je prvi disk naredil cel krog, se je premaknil še drugi disk, in ko je tudi drugi disk naredil cel krog, se je premaknil še tretji disk. Tako je bilo skupaj možno $26^3 = 17576$ različnih položajev diskov. Diski so se lahko med sabo tudi zamenjali, tako da so lahko bili pred pričetkom šifriranja razporejeni v poljubnem vrstnem redu. Tri diske lahko razporedimo na svoja mesta na šest različnih načinov, torej je s tem povečal število razporeditev za faktor 6.
Vsak disk je bil obkrožen z obročem, ki ga je operater lahko vrtel in ga nastavil v eno izmed 26 možnih položajev. Obroč je imel na obodu vgravirano abecedo ali v nekaterih različicah številke od 01 do 26. Prav tako je imel zarezo, v katero je v določenem položaju skočilo zatikalo. Disk 1 je imel zarezo pri črki *Y*, disk 2 pri črki *M* in disk 3 pri črki *D*. To je pomenilo, da je bilo zatikalo v zarezi, ko so navzgor gledale črke *Q,E,W*, torej 8. črka pred zarezo. Ko je torej na disku 1 gledala navzgor črka *Q*, je bilo zatikalo v zarezi in to je pomenilo, da se pri naslednji črki obrne tudi disk desno od diska 1.

Med tipkovnico in prvi disk je Scherbius vstavil še stikalno ploščo. Ta je omogočala, da je operater lahko vstavil kable, s katerimi je zamenjal dve črki med seboj, preden so prišle do diskov. Recimo, da je operater zamenjal a z b. Če je nato pritisnil tipko a, je električni tok potoval po poti, ki je prej pripadala črki b. Operater je imel šest kablov, torej je lahko med sabo zamenjal šest parov črk.

Slika 2: Prikaz notranje zgradbe Enigme, zaradi lažje predstave s samo šestimi črkami



Tako je operater nastavil obroče na diske, razporedil diske na svoja mesta in jih orientiral. Nato je odtipkal določeno sporočilo, si zapisoval osvetljene črke in jih nato po radijski zvezi sporočil svojemu zavezniku. Zašifriran tekst so Nemci pošiljali v Morsejevi abecedi. Enigma pa je seveda morala biti sestavljena tako, da je operater, ki je prejel tajnopis, znal sporočilo odšifrirati. V ta namen je

Scherbius dodal t.i. reflektor. Ta je podoben disku, vendar se ne vrti. V notranjosti ima prav tako žice, ki pa vstopajo in izstopajo na isti strani. Ko električni tok prispe skozi vse tri diske do reflektorja, pošlje ta tok nazaj skozi iste tri diske, vendar v nasprotni smeri in po drugi poti, kot je prikazano na sliki 2. Scherbius je z reflektorjem dosegel, da če se npr. črka b zašifrira v D, se črka d zašifrira v B. Ko dobi torej operater zašifriran tajnopis, odtipka na tipkovnico črke tajnopisa, na zaslonu pa se mu osvetlijo črke čistopisa. Tako lahko prebere sporočilo. Seveda pa mora biti njegova Enigma pred pričetkom odšifriranja nastavljena isto kot od operaterja, ki mu je sporočilo poslal.

Poglejmo najprej , koliko je bilo možnih začetnih nastavitev Enigme:
- iz orientacije diskov dobimo $26^3 = 17576$ razporeditev,
- diske lahko razporedimo na 6 načinov,
- šest parov črk, ki jih bomo med sabo zamenjali, lahko izberemo na

$$\frac{1}{6!}\binom{26}{2}\binom{24}{2}\binom{22}{2}\binom{20}{2}\binom{18}{2}\binom{16}{2} = 100391791500$$

načinov. Skupaj dobimo tako

$$17576 \cdot 6 \cdot 100391791500 = 10586916764424000 \approx 10^{16}$$

možnih razporeditev.

Kasneje je Scherbius uvedel še nekaj izboljšav. Najprej je dodal še dva diska, tako da je lahko oprater izmed skupno petih diskov izbiral, katera dva bo vstavil v napravo. Izmed pet diskov lahko izberemo tri in jih razporedimo na svoja mesta na $5 \cdot 4 \cdot 3 = 60$ načinov, torej se je s tem število začetnih nastavitev povečalo za faktor 60. Disk 4 je imel zarezo pri črki R, disk 5 pa pri črki H. Torej je bila zareza zasedena, ko sta navzgor gledali črki J in Z in ob naslednji črki se je premaknil tudi disk desno od njiju. Nato je še povečal število kablov v stikalni plošči, tako da jih je bilo skupno deset. Tako je število razporeditev v stikalni plošči naraslo na

$$\frac{1}{10!}\binom{26}{2}\binom{24}{2}\binom{22}{2}\binom{20}{2}\binom{18}{2}\ldots\binom{8}{2} = 150738274937250 \approx 1.5 \cdot 10^{15},$$

skupno število razporeditev pa je s tem naraslo na

$$26^3 * 60 * 150738274937250 = 158962555217826360000 \approx 159 \cdot 10^{18}.$$

Nemška mornarica je dodala še tri diske, tako da jih je imela skupno osem. Dodala je še četrti disk, ki se je vrtel, ni pa bil nastavljiv. Naprava se je imenovala M4.

Ostane še vprašanje, kako je operater na drugi strani, ki je dobil zašifrirano sporočilo, vedel, katero izmed mnogih možnih nastavitev je kot začetno izbral

operater, ki je pisal sporočilo. V ta namen je obstajala knjiga ključev, ki so jo vohuni vsak mesec dostavili vsem svojim operaterjem. V njej je bil za vsak dan naveden dnevni ključ. Dnevni ključ je izgledal npr. tako:

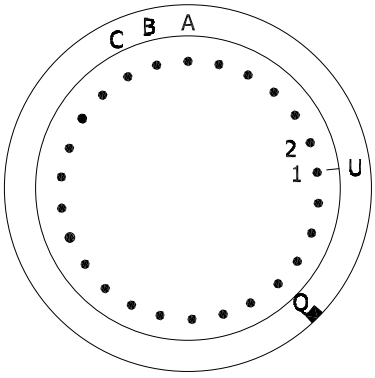
1. nastavitev stikalne plošče: *A/L - P/R - T/D - B/W - K/F - O/Y*
2. razporeditev diskov: 2 - 3 - 1
3. nastavitev obročev: *Q - C - U*
4. orientacija diskov: *M - F - J*

To je pomenilo:

1. Operater mora najprej kable v stikalni plošči namestiti tako, da zamenja med sabo črki A in L, nato zamenja črki P in R in tako naprej.
2. Disk z oznako 2 namesti kot prvega v Enigmo, disk z oznako 3 namesti kot drugega, disk z oznako 1 pa kot zadnjega.
3. Na disku 2 obrne operater obroč tako, je pri oznaki 0 črka Q, disk 3 obrne tako, da je pri oznaki 0 črka C, disk 1 pa tako, da je pri oznaki 0 črka U.
4. Prvi disk operater obrne tako, da je gledala navzgor črka Q, drugega tako, da je gledala navzgor črka C in zadnjega s črko W navzgor.

Tako so bile vse Enigme na isti dan pred začetkom vsakega sporočila isto nastavljene.

Slika 3: Skica diska. Disk ima zarezo pri črki Q, nastavitev obroča je U, orientacija diska pa A. Točke, do katerih so vodile žice, so označene s številkami 1 do 26. Oznaka za nastavitev obroča je pri številki 1.



V katero črko je Enigma zašifrirala določeno črko, lahko opišemo s permutacijami. Zamenjave v stikalni plošči opišemo s permutacijo, ki je produkt šestih

transpozicij: $\pi_0 = (x_1y_1)(x_2y_2)\dots(x_6y_6)$. V notranjosti vsakega diska in reflektorja so se žice prepletle. Te permutacije označimo s π_1 za disk, ki je v trenutni nastavitvi najhitrejši, s π_2 za srednji, s π_3 za počasni disk in s π_4 za reflektor. Ker so diski nastavljivi in se med šifriranjem obračajo, bomo permutacije posameznih diskov v nekem koraku označili s Π_1, Π_2, Π_3, ki pa jih bomo izrazili s π_1, π_2, π_3. Permutacija π_4 je fiksna, permutacija π_0 sicer ni fiksna, se pa med šifriranjem ne spreminja. Črkam abecede priredimo številke od 1 do 26. Označimo nastavitve obročev z z_i, orientacije diskov s s_i, črke, ki so gledale navzgor, ko je bilo zatikalo v zarezi, pa z r_i. Zanima nas, v katero črko se zašifrira črka z zaporedno številko x. To je odvisno seveda tudi od tega, koliko črk smo že zašifrirali. Označimo s t_1 število korakov. Za hitri obroč potem velja

$$\Pi(x, t, z_1, s_1) = \pi(x + t + s_1 - z_1 \ mod\ 26),$$

Srednji obroč , se bo obrnil korak zatem, ko bo na hitrem obroču gledala navzgor črka r_1. Torej se drugi obroč prvič obrne po $r_1 - s_1$ korakih, nato pa naslednjič šele po 26-tih korakih. Torej bo na srednjem disku število obratov po t_1 korakih enako

$$t_2 = (t_1 + 26 - r_1 + s_1)\ div\ 26.$$

Število obratov na tretjem disku je potem enako

$$t_3 = (t_2 - 26 - r_2 + s_2)\ div\ 26.$$

Tako lahko šifriranje črk na posameznem disku opišemo s permutacijo

$$\Pi(x, t_i, z_i, s_i, r_i) = \pi(x + t_i + s_i - z_i).$$

Celotno šifriranje črke z Enigmo tako opišemo s permutacijo

$$\pi_0 \circ \Pi_1 \circ \Pi_2 \circ \Pi_3 \circ \pi_4 \circ {\Pi_3}^{-1} \circ {\Pi_2}^{-1} \circ {\Pi_1}^{-1} \circ {\pi_0}^{-1}.$$

Ker so Nemci v času druge svetovne vojne dnevno poslali zelo veliko sporočil, so uvedli še en varnostni ukrep. Tako so na začetku vsakega sporočila najprej poslali novo orientacijo diskov, ki si jo je vsak operater za vsako sporočilo sam izbral. Recimo, da si je operater izbral orientacijo *PGH*. Potem je v Enigmo, ki je bila seveda nastavljena v skladu z dnevnim ključem, vtipkal najprej *PGH*. Zaradi napak, ki so lahko prišle pri prenosu sporočil preko radijske zveze, so nov ključ vsakič odtipkali dvakrat, torej *PGHPGH*. To se je zašifriralo npr. v *KIVBJE*. Ko je operater na drugi strani dobil to zašifrirano orientacijo diskov, jo je vtipkal v Enigmo z dnevno nastavitvijo in dobil novo orientacijo. Potem je tudi svojo Enigmo nastavil v skladu s to novo orientacijo in odšifriral še preostalo sporočilo. Tako je imelo vsako sporočilo svojo orientacijo diskov. Vendar pa je ravno ponovitev novega ključa na začetku sporočila pripomogla k temu, da so nasprotniki uspeli razbiti Enigmo.

3 Marian Rejewski in razbitje Enigme

V tem poglavju je opisano, kako je Marian Rejewski s pomočjo ponovitve orientacije diskov na začetku sporočila razbil Enigmo. S pomočjo te ponovitve je poiskal zveze med črkami. Na podlagi teh zvez je tvoril cikle črk, katerih število in dolžina je bila neodvisna od zamenjav v stikalni plošči. S tem je zelo zmanjšal število nastavitev, ki jih je bilo potrebno pregledati.

Leta 1926 so britanski kriptoanalisti začeli sprejemati sporočila, zašifrirana z Enigmo. To jih je popolnoma zmedlo. Tudi Američani in Francozi so se lotili razbitja, vendar so hitro obupali. Edino Poljaki so vztrajali, saj so na novo vzpostavili samostojno državo, z leve in desne pa so jim grozili Rusi in Nemci. Novembra leta 1931 je Hans-Thilo Schmidt, ki je bil zaposlen v najbolj tajnem centru za Enigmo, za takratnih 10.000 DM dovolil francoskemu vohunu, imenovanemu Rex, da je fotografiral dva pomembna dokumenta: Navodila za uporabo za Enigmo in Navodila za ključe za Enigmo. V teh dokumentih je bilo zapisano, kako je Enigma sestavljena, iz njih pa so lahko tudi sklepali o razporeditvi žic v notranjosti diskov. Kljub temu se je Francozom zdelo nemogoče poiskati dnevne ključe in tako dnevno razbijati Enigmina sporočila. Fotografije so dali Poljakom, ki so bili bolj zainteresirani. Tako je Biuro Szyfrow poklical na pomoč matematike iz univerze Poznan. Najuspešnejši med njimi je bil Marian Rejewski. Rejewskijeva strategija je temeljila na ponavljanju. Najbolj očitna ponovitev v sporočilih je bil ključ na začetku vsakega sporočila. Vsak dan je Rejewski prejel ogromno sporočil, vsako pa se je začelo s ključem iz treh črk, ki se je dvakrat ponovil. Rejewski si je zapisoval te zašifrirane ključe. Recimo da je dobil naslednje zašifrirane ključe:

	1	2	3	4	5	6
1. sporočilo	L	O	K	R	G	M
2. sporočilo	M	V	T	X	Z	E
3. sporočilo	J	K	T	M	P	E
4. sporočilo	D	V	Y	P	Z	Y

V vseh primerih je 1. in 4. črka enkripcija iste črke, prav tako 2. in 5. ter 3. in 6. črka. Rejewski je tako lahko določil povezave med pari črk, ki jih je zapisoval v tabele. Opazimo, da gre pravzaprav za permutacijo rk. Poglejmo najprej tabelo za 1. in 4. črko:

1. črka:	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
4. črka:	F	Q	H	P	L	W	O	G	B	M	V	R	X	U	Y	C	Z

1.črka:	R	S	T	U	V	W	X	Y	Z
4.črka:	I	T	N	J	E	A	S	D	K

V zgornjo vrsto je zapisal abecedo. Iz prvega sporočila je dobil povezavo med črko L na 1. mestu in črko R na 4. mestu. Zato je v drugo vrsto pod črko L zapisal R. Iz preostalih treh sporočil je dobil še zveze med črkami M in X, J in M ter D in P. Torej je v drugo vrsto pod M zapisal črko X, pod J črko M in pod D črko P. Ko je prejel zadosti sporočil, je tabelo lahko dokončal. Nato je začel iskati vzorec v tej tabeli. Črka A v zgornji vrsti je povezana s črko F v spodnji vrsti. Nato je pogledal črko F v zgornji vrsti in ta je povezana s črko W v spodnji vrsti. Nato je pogledal še W, ta je povezana z A in tako je krog zaključen. Nato je pogledal še ostale črke in dobil cikle:

A→F→W→A 3 črke
B→Q→Z→K→V→E→L→R→ I→B 9 črk
C→H→G→O→Y→D→P→C 7 črk
J→M→X→S→T→N→U→J 7 črk

Isto je ponovil še z 2. in 5. ter 3. in 6. črko. Rejewski je tako vsak dan sestavljal te cikle in opazil, da se število in dolžina ciklov vsak dan spreminja. Ugotovil pa je tudi, da je število in dolžina ciklov odvisna le od nastavitve diskov in ne od kablov v stikalni plošči. Saj če npr. v stikalni plošči zamenjamo črki S in G, se s tem zamenjata črki S in G v 3. in 4. ciklu, nič pa se ne spremeni število ciklov in dolžina posameznih ciklov. Tako je Rejewski ločil nastavitve diskov od nastavitev v stikalni plošči. Možnih razporeditev diskov je 6, možnih orientacij diskov pa $26^3 = 17576$, torej skupaj 105456 možnih razporeditev diskov. Torej je sedaj Rejewski namesto skupno 10^{16} možnih dnevnih ključev moral preveriti le 105456 nastavitev diskov.

Tako je njegova ekipa začela preverjati vseh 105456 razporeditev diskov. V enem letu so naredili katalog s številom in dolžinami ciklov ob vsaki nastavitvi. Katalog je bil sestavljen za obroče z nastavitvijo Z - Z - Z. Ko je bil katalog narejen, so lahko začeli z razbijanjem Enigminih sporočil. Vsak dan so pogledali zašifrirani dnevni ključ vsakega sporočila, zapisovali zveze v tabelo in ko je bila tabela končana, so določili cikle. Tako so npr. za nek dan dobili podatke:

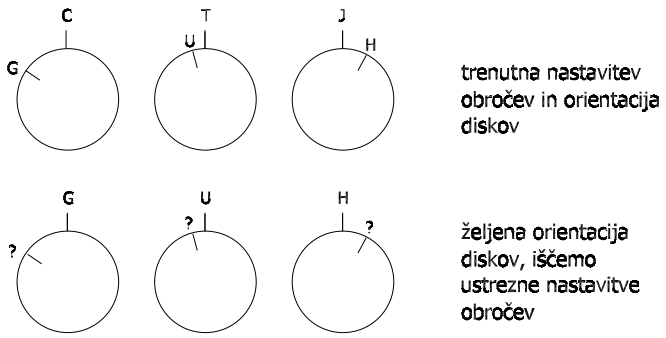
1. in 4. črka: 4 cikli dolžine 3,9,7 in 7 črk,
2. in 5. črka: 4 cikli dolžine 2,3,9,in 12 črk,
3. in 6. črka : 5 ciklov dolžine 5,5,5,3 in 8 črk.

Nato so pogledali v katalog, katere nastavitve diskov ustrezajo tem ciklom, in jih pregledali. Seveda so dobljene nastavitve bile dnevne nastavitve diskov in so se tako nanašale le na prvih šest črk. S pomočjo teh so nato morali določiti še zamenjave v stikalni plošči. Pri določanju le-teh so uporabjali ugotovitev, da so nemški operaterji za ključ sporočila večkrat izbrali kar tri iste črke ali tri zaporedne črke na tipkovnici, čeprav bi naj bile te črke popolnoma naključne. Tako so nastavili diske v skladu z orientacijo iz kataloga in odšifrirali ključ sporočila. Recimo, da se je *GUH BIS* odšifriralo v *yyy ylr*. Torej je ključ sporočila bil verjetno *yyy*. Tako so Enigmo nastavili nazaj v začetni položaj in dvakrat odtipkali *yyy*. Recimo, da

so dobili *GUH BZE*. To je pomenilo, da je v stikalni plošči bil *I* zamenjan z *Z* in *E* zamenjan s *S*. Nato so pogledali še drugo sporočilo, in recimo, da se je zašifriran ključ *BHG DBG* odšifriral v *bam bam*. Pogledali so na tipkovnico in sklepali, da je bil izbran ključ sporočila *bnm*. Torej je v stikalni plošči bil *A* zamenjan z *N*. Tako so nadaljevali še z drugimi sporočili in njihovimi ključi, dokler niso določili vse zamenjave v stikalni plošči.

Morali pa so določiti še nastavitev obročev. Od tega je bilo odvisno, kdaj se aktivirata tudi sredinski in počasni disk. Torej je bilo prvih nekaj črk pravilnih, tudi če nastavitev obročev ni bila dobra. Tako to največkrat ni vplivalo na prej opisano iskanje nastavitev v stikalni plošči.
Da bi dobili pravilno nastavitev obročev, so najprej odšifrirali ključ sporočila z uporabo nastavitve obročev *Z - Z - Z* in iz kataloga dobljeno orientacijo. Recimo, da so dobili ključ *GUH*. Sedaj so obroče nastavili v skladu s tem ključem. Vedeli so, da se skoraj vsa sporočila začnejo z *ANX*(AN pomeni nemško za, torej komu je bilo sporočilo namenjeno, *X* pa je bil znak za presledek). Sedaj so morali poiskati orientacijo, ki zašifrira prve tri črke sporočila v *ANX*. Pri taki orientaciji je bil torej disk prav obrnjen. Ker pa je bil ključ sporočila *GUH*, bi morale navzgor gledati te črke in obroč je potrebno zarotirati temu primerno.

Recimo, da so se prve tri črke sporočila zašifrirale v *ANX* pri orientaciji *CTJ*, iz kataloga dobljen ključ pa je *GUH*. Primer ja narisan na spodnji sliki:



Tako dobimo formulo:

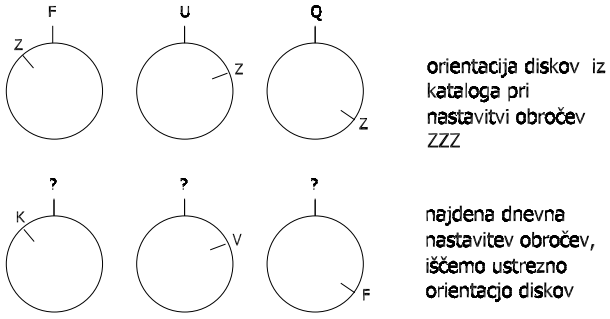
črke ključa sporočila - črke najdene orientacije =
iskane črke nastavitve obročev -črke ključa sporočila

Oziroma

iskane črke nastavitve obročev = 2·(črke ključa sporočila) - črke najdene orientacije

V tej formuli smo črkam abecede pripisali zaporedoma števila 0d 0 do 25, odštevanje pa opravili po modulu 26.

Iskana nastavitev obročev v našem primeru je torej:
Prvi disk: $2 \cdot G - C (= 2 \cdot 7 - 3 = 11) = K$
Drugi disk: $2 \cdot U - T (= 2 \cdot 21 - 20 = 22) = V$
Tretji disk: $2 \cdot H - J (= 2 \cdot 8 - 10 = 6) = F$
Iskana nastavitev obročev je torej KVF. Seveda moramo sedaj še poiskati ustrezno dnevno orienatcijo diskov. Recimo, da je po tabelah orientacija diskov FUQ. To velja za nastavitev obročev ZZZ. Primer je narisan na spodnji sliki:



Po podobni formuli kot prej dobimo iskano dnevno orientacijo:

ZZZ - črke orientacije iz kataloga = najdene črke nastavitve obročev - črke dnevne orientacije

oziroma

črke dnevne orientacije = črke nastavitve obročev + črke orientacije iz kataloga

Ker odštevamo po modulu 26, lahko ZZZ izpustimo.

V našem primeru torej dobimo za črke dnevne orientacije:

$$KVF+FUQ=QQW$$

Tako so imeli vse potrebne podatke in so lahko brali vsa Enigmina sporočila tistega dne.

Ker je bilo možnih šest različnih razporeditev diskov, so imeli šest naprav, ki so predstavljale vsaka eno razporeditev diskov. Skupaj so lahko našli dnevni ključ v dveh urah.
Tako so poljski kriptografi nekaj let uspešno iskali dnevne ključe, ostali narodi pa o tem niso vedeli ničesar. Vendar pa je bilo veliko njihovega dela nepotrebnega. Schmidt se je namreč še naprej srečeval z francoskim vohunom Rexom in mu dostavljal knjige z dnevnimi ključi. Tako je dnevne kjluče dobil tudi vodja Biuroja, Gwido Langer. Vendar tega ni hotel povedati Rejewskemu in njegovi ekipi, saj je hotel, da so pripravljeni na čas, ko ključev več ne bodo dobivali.
Decembra leta 1938 so nemški kriptografi povečali varnost Enigme. Vsi Enigmini operaterji so dobili dva dodatna diska. Tako so izmed skupno petih izbrali tri, ki so jih nato vstavili v napravo. Tako je število možnih razporeditev diskov naraslo na 60. Sedaj bi moral Rejewski najprej rekonstruirati razporeditev žic v notranjosti obeh novih diskov. Poleg tega je sedaj potreboval 60 Enigem, da bi vsaka predstavljala eno razporeditev diskov. To bi Biuro stalo petnajstkrat toliko, kot so imeli na razpolago. V naslednjih mesecih so Nemci povečali tudi število kablov v stikalni plošči, tako da jih je bilo sedaj deset parov. Rejewski je v prejšnjih letih dokazal, da je Enigmo mogoče razbiti, ampak brez sredstev za dodatne naprave ni mogel več iskati dnevnih ključev. Poleg tega pa je ravno pred uvedbo novih diskov Schmidt pretrgal zveze z Rexom. Sedem let je Schmidt dostavljal knjige z dnevnimi ključi, sedaj, ko pa bi jih Poljaki res potrebovali, jim več niso bile dosegljive. Če Poljaki niso mogli brati Enigminih sporočil, niso imeli nobenega upanja, da bi ustavili napad Nemcev, ki je sledil že čez nekaj mesecev. Tako so se odločili, da bodo za svoja odkritja povedali Britancem in Francozom, saj bodo mogoče z večjimi sredstvi lahko oni nadaljevali njihovo delo.

4 Alan Turing

Poleg nekaj posodobitev same naprave so leta 1940 nemški operaterji začeli na začetku sporočila pošiljati le enkrat zašifrirano orientacijo diskov. Razbijanje Enigminih sporočil so tedaj prevzeli Angleži, med katerimi je bil najpomembnejši Alan Turing. V tem poglavju je opisana njegova ideja za razbitje Enigme. Njegovo razbitje je temeljilo na delih besedila, za katere je mogoče domnevati, kaj je ustrezni čistopis. Iz teh parov čistopis - tajnopis je dobil povezave med črkami in iskal tiste črke, ki so tvorile zanke. Nato je med sabo povezal toliko Enigem, kolikor je bilo črk v zanki. Tem Enigmam je lahko odstranil stikalne plošče, saj se je njihov učinek med sabo izničil. S tem je, podobno kot Rejewski, zelo zmanjšal število razporeditev, ki jih je bilo potrebno pregledati.

Polnih 13 let so Francozi in Angleži mislili, da je Enigma nezlomljiva, delo Poljakov pa jim je dalo upanje. Poljaki so jim pokazali, kako pomembno je delo matematikov pri razbijanju šifer. Tako so Angleži zbrali matematike in druge znanstvenike v Bletchley Parku v Buckinghamshire-u. Jeseni leta 1939 so se matematiki in znanstveniki v Bletchley Parku seznanjali z odkritji Poljakov. Proučevali so že razbita sporočila in začeli iskati nove poti pri iskanju dnevnih kljlučev. Ugotovili so nekaj pravil o diskih. Odgovorni za sestavljanje knjig ključev so se trudili, da bi razporeditev diskov bila nepredvidljiva in tako niso pustili nobenega diska dva dni na istem mestu. Če je bila torej nek dan razporeditev diskov 134, je naslednji dan lahko bila 215, ne pa 214, saj je potem bil disk 4 dva dni na zadnjem mestu. Če so tako ugotovili razporeditev diskov za nek dan, je za naslednji dan bilo število možnih razporeditev le $60 - 3 \cdot (4 \cdot 3) + 3 \cdot 3 - 1 = 32$. Poleg tega je veljalo pravilo, da v stikalni plošči nikoli nista bila zamenjani med sabo dve sosednji črki, npr. S ni bila nikoli zamenjana z R ali T, saj so Nemci menili, da je taka zamenjava preveč očitna. Tako je število možnih razporeditev v stikalni plošči iz prejšnjih $1.5 \cdot 10^{15}$ padlo na približno

$$\frac{1}{10!}\left(\frac{26*23}{2}\right)\left(\frac{24*21}{2}\right)\left(\frac{22*19}{2}\right)\left(\frac{20*17}{2}\right)\left(\frac{18*15}{2}\right)\left(\frac{16*13}{2}\right)$$

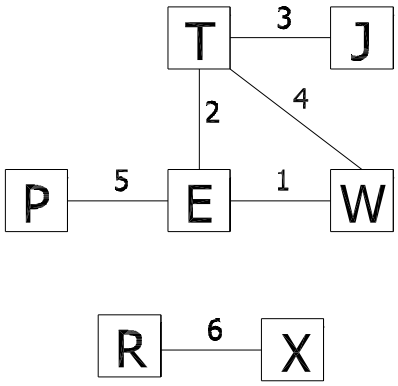
$$\left(\frac{14*11}{2}\right)\left(\frac{12*9}{2}\right)\left(\frac{10*7}{2}\right)\left(\frac{8*6}{2}\right) = 30147654987450 \approx 3 \cdot 10^{13}.$$

Izmed mnogih kriptoanalistov v Bletchley Parku je bil najbolj zaslužen za razbitje Enigme Alan Turing, ki je prišel v Bletchley Park septembra leta 1939. Angleži so domnevali, da bodo Nemci v kratkem nehali ponavljati ključ sporočila na začetku vsakega sporočila. Turing se je ukvarjal s problemom, kako razbiti Enigmina sporočila, v katerih je ključ sporočila zašifriran le enkrat. Takrat so v Bletchley Parku imeli že veliko odšifriranih sporočil, ki jih je Turing proučeval. Ugotovil je, da lahko v nekaterih sporočilih za določeni del tajnopisa predvideva, kaj je ustrezni čistopis. Tak par čistopis - tajnopis so v Bletchley Parku imenovali crib.

Crib je bil odvisen od časa in izvora sporočila. Nemci so npr. vsak dan okrog šeste ure zjutraj pošiljali vremenska obvestila. Tako so Angleži lahko predvidevali, da to sporočilo vsebuje besedo *wetter*, kar pomeni v nemščini vreme. Ponavadi je to bilo kar prvih šest črk vsebine sporočila. Turing se je osredotočil le na nekatere cribe, in sicer tiste, ki so vsebovali notranje zanke. Recimo, da je domneval, da beseda *wetter* ustreza tajnopisu ETJWPX.

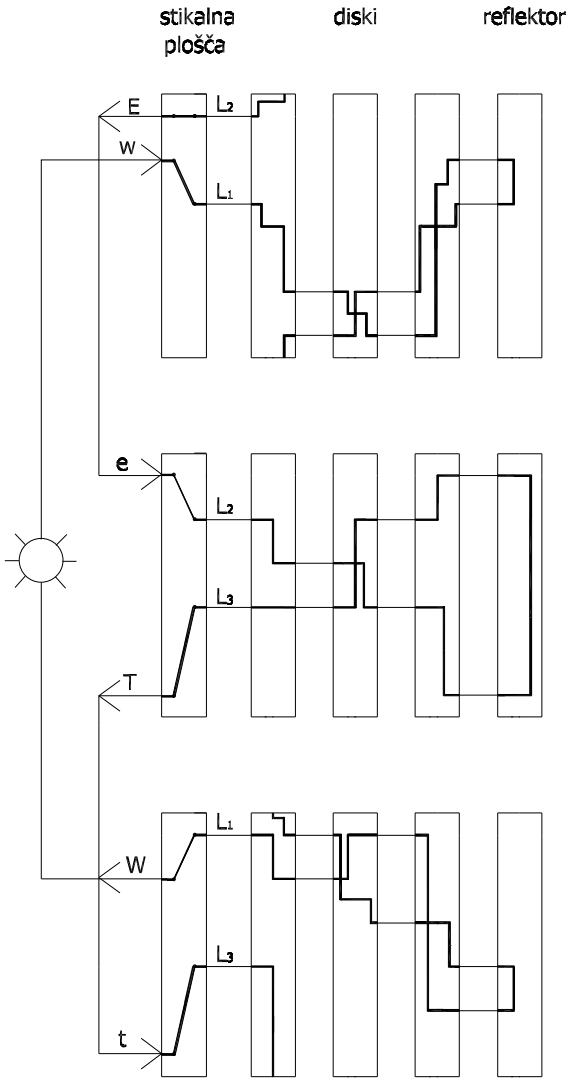
1	2	3	4	5	6
w	e	t	t	e	r
E	T	J	W	P	X

Te povezave lahko predstavimo tudi v diagramu.



Ker sta na mestu 1 v zvezi črki E in W, ju v diagramu povežemo in povezavo označimo z 1. Nato narišemo in označimo še vse ostale povezave. Iz diagrama takoj vidimo, če crib vsebuje kakšne zanke. Naš crib vsebuje zanko $W \rightarrow E \rightarrow T \rightarrow W$. Turingova ideja je bila, da je povezal tri naprave, eno za drugo. Vse so imele isto razporeditev diskov in v stikalni plošči zamenjane iste črke. Razlika je bila le v orientaciji diskov. Če je bila prva Enigma v nekem stanju 1, potem je bila druga v našem primeru v stanju 2 in tretja v stanju 4. Seveda so stanja bila odvisna od criba.

Slika 4: Skica Turingove ideje

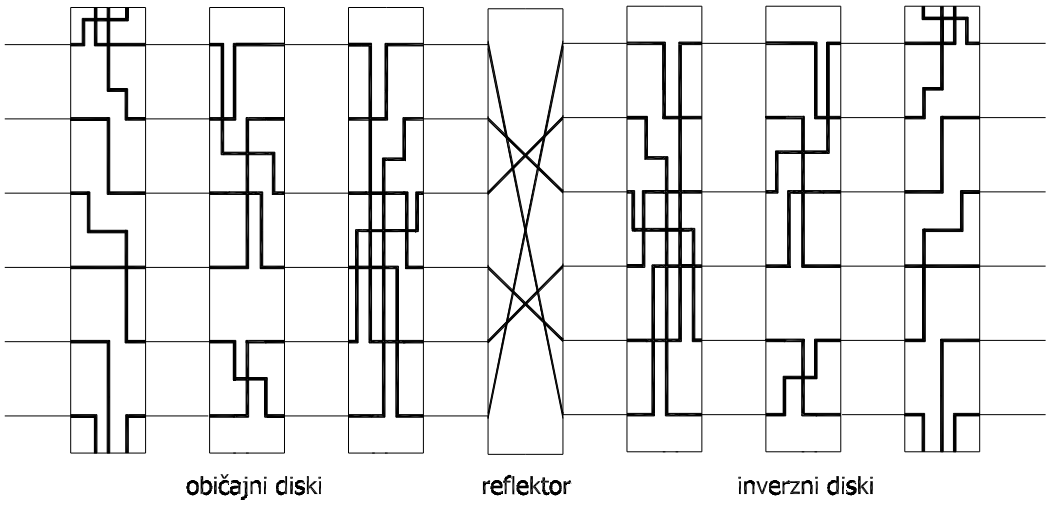


Črka w se v stikalni plošči zamenja v neko drugo, imenovali jo bomo L_1. Ko tok, ki ustreza tej črki, pripotuje skozi vse tri diske, reflektor in nazaj skozi diske do stikalne plošče, ustreza neki drugi črki, imenujmo jo L_2. Vemo, da potem stikalna plošča to črko zamenja z E . Ta črka je potem z žico povezana s črko e na naslednji Enigmi. Stikalna plošča zamenja črko e nazaj v črko L_2, saj so nastavitve v stikalni plošči v obeh Enigmah enake. Stikalni plošči se tako med sabo izničita. Tok poteka potem skozi vse tri diske, reflektor in spet skozi diske in pride nazaj do stikalne plošče kot črka L_3. Ta se v stikalni plošči zamenja v T, črka T pa je povezana s črko t na tretji Enigmi. Ta stikalna plošča črko t zamenja

nazaj v L_3 in tako se stikalni plošči spet izničita. Tok poteka skozi vse tri diske in reflektor ter pripotuje nazaj kot črka L_1, ki se zamenja z W, ta pa je povezana z prvo Enigmo in krog je sklenjen. Da bi Turing vedel, kdaj je krog sklenjen, je vmes vezal žarnico in če je krog bil sklenjen, je ta zagorela.

Stikalne plošče so se tako med sabo izničile in Turing jih je lahko kar odstranil. Tako je, podobno kot Rejewski, ločil nastavitve diskov od nastavitev v stikalni plošči. Ker pa ni poznal vrednosti L_1, L_2, L_3, je moral povezati vseh 26 izhodov prve Enigme z ustreznimi 26 vhodi druge Enigme. Tako je dobil 26 krogov in vsak je imel svojo žarnico. Turing si je zamislil še elektromotor, ki bi avtomatično preverjal vse razporeditve.
V Enigmi, ki ji je Turing odstranil stikalno ploščo, je električni tok vstopal in izstopal na istem mestu na disku. Tako je Turing moral konstruirati Enigmo z različnim vhodom in izhodom. Na sliki 4 je skica te dvoizhodne Enigme.

Slika 5: Dvoizhodna Enigma



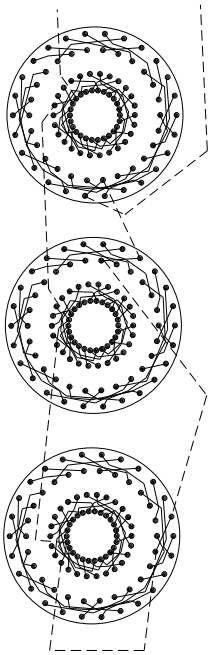
Reflektor je na sredini in ima dve strani. Na vsaki strani so trije diski. Tisti na desni strani so inverzni levim in predstavljajo povratni tok skozi diske. Tako dobimo vhodno stran na levi in izhodno stran na desni in lahko brez težav povežemo več Enigem zapored.
Praktična izvedba celotne naprave je bila zahtevna in je zahtevala še nekaj izboljšav.

5 Izdelava bombe

V tem poglavju je opisana praktična izdelava naprave za razbijanje Enigminih sporočil, ki se je imenovala bomba. Diske so nadomestili z bobni, ki so bili v skladu s parom čistopis - tajnopis povezani z diagonalno ploščo. Diagonalna plošča je bila sestavljena iz 26 kablov, za vsako črko abecede en kabel, v vsakem kablu je bilo 26 žic, za vsako črko abecede ena žica. Žice so bile med sabo povezane in so predstavljale zamenjave v stikalni plošči. S pošiljanjem toka po različnih žicah so se tako preverjale različne zamenjave črk v stikalni plošči. Elektromotor je avtomatično preverjal različne zamenjave.

Po Turingovi ideji je napravo izdelala British Tabulating Machine factory iz Letchwortha. Tam so namesto Enigme z dvema izhodoma izdelali boben. En boben je predstavljal en disk, v njem pa so bile žice za običajni in inverzni disk. Tako so trije bobni predstavljali dvoizhodno Enigmo.

Slika 6: Trije bobni predstavljajo dvoizhodno Enigmo. Na sliki je narisana tudi po ena žica med bobni.



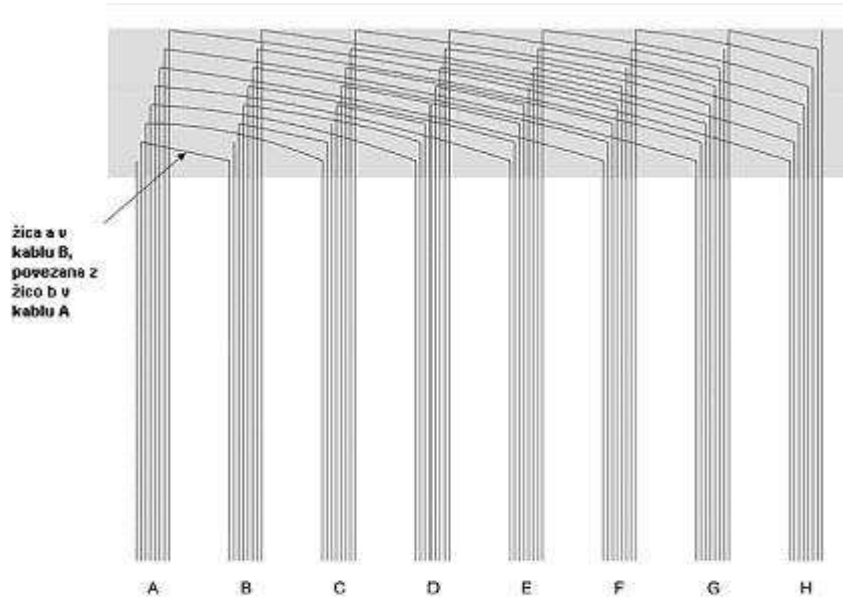
V enem bobnu so bili v koncentričnih krogih raporejeni kontakti, v vsakem krogu po 26 kontaktov. Zunanji krog je predstavljal vhodno stran običajnega diska, tretji od znotraj pa izhodno stran istega diska. Podobno sta notranja dva

kroga predstavljala vhodno in izhodno stran temu disku inverznega diska. Na bobnu sta torej bila z žicami, ki so predstavljale žice v disku, povezana zunanji in tretji krog ter notranja dva kroga. Trije bobni so bili med seboj povezani preko žic. Te so bile razporejene v obliki žične krtače s koncentričnimi krogi za vsakim bobnom. Vsak žica te krtače je potem bila povezane z ustrezno žico krtače sosednjega bobna. Bobni so bili eden nad drugim, in sicer se je zgornji boben zavrtel ob vsaki zašifrirani črki in je tako predstavljal najhitrejši disk, ko je ta naredil cel krog se je zavrtel še sredinski boben, ko pa je še ta naredil cel krog se je zavrtel še spodnji boben, ki je tako predstavljal najpočasnejši disk. Tako so bobni bili med seboj povezani na naslednji način.

• tretji krog zgornjega bobna z zunajim krogom sredinskega bobna
• tretji krog srediskega bobna z zunajim krogom spodnjega bobna
• tretji krog spodnjega bobna preko žic, ki so predstavljale žice v reflektorju z drugim krogom spodnjega bobna
• notranji krog spodnjega bobna z drugim krogom sredinskega bobna
• notranji krog sredinskega bobna z drugim krogom zgornjega bobna

Zgornji disk ni bil priključen direktno na naslednjo dvoizhodno Enigmo v zanki, pač pa sta bila zunanji in notranji krog zgornjega bobna povezana z diagonalno ploščo.

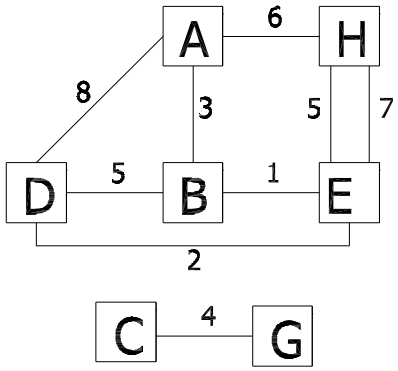
Slika 7: Skica diagonalne plošče, zaradi lažje predstave s samo osmimi črkami



Zamisel o diagonalni plošči je dobil Gordon Welchman, bila pa je posledica dejstva, da če je črka B zamenjana s črko G, potem je tudi G zamenjana z B. Sestavljena je bila iz 26 kablov, ki je vsak vseboval 26 žic.
Žica a v kablu B je bila trajno povezana z žico b v bloku A, žica a v kablu C je bila trajno povezana z žico c v bloku A in tako naprej.
Na tak način so bile povezane vse črke, torej je bilo skupno $26 \cdot 25 = 325$ povezav.
Oba izhoda zgornjega bobna dvoizhodne Enigme sta bila povezana vsak z enim kablom diagonalne plošče. S katerim, je bilo odvisno od criba.
Oglejmo si npr. crib

1	2	3	4	5	6	7	8	9
b	e	a	c	h	h	e	a	d
E	D	B	G	E	A	H	D	B

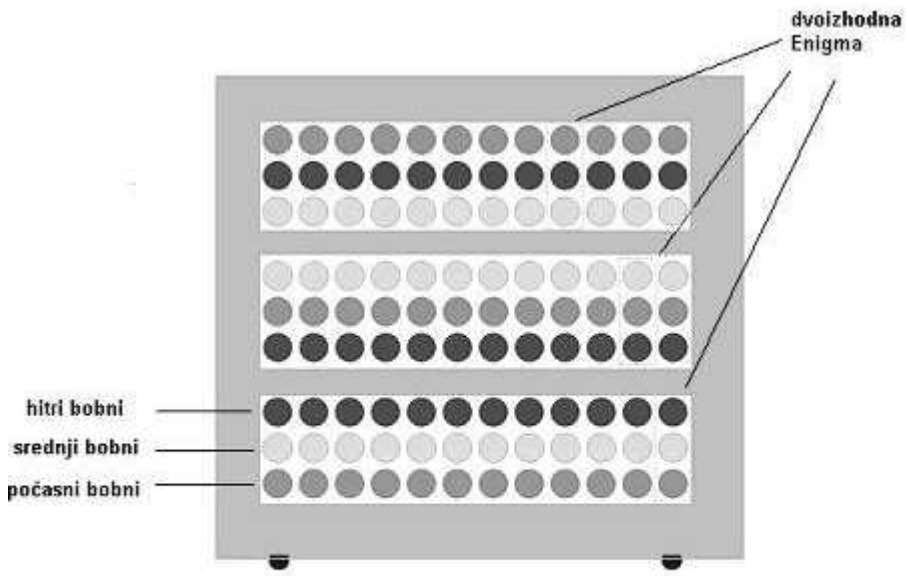
Zaradi poenostavljene diagonalne plošče smo izbrali crib, ki vsebuje le prvih devet črk angleške abecede. Povezave v cribu lahko predstavimo tudi v diagramu.



Namestimo najprej bobne v skladu s tem cribom. Bomba je imela $12 \times 3 = 36$ setov bobnov, ki so vsak predstavljali dvoizhodno Enigmo.
Recimo, da najprej preizkusimo diske 1,2 in 3. Namestimo 9 diskov(ker je v cribu 9 črk), ki predstavljajo disk 1, v zgornjo vrsto. V drugo vrsto namestimo devet bobnov, ki predstavljajo disk 2 in v tretjo vrsto devet bobnov, ki predstavljajo disk 3. Bobne v prvem setu nastavimo tako, da gledajo navzgor črke AAA, v drugem setu so bobni premaknjeni za en položaj naprej, torej AAB in tako naprej. Ker delamo s samo osmimi črkami, je deveti disk nastavljen na ABA, v pravi Enigmi se to seveda zgodi šele po 26. črki. V spodnjih dveh vrstah izberemo drugi vrstni red bobnov, recimo 132 in 213, sicer pa bobne nastavimo isto

kot v zgornji vrsti.

Slika 8: Sprednja stran bombe

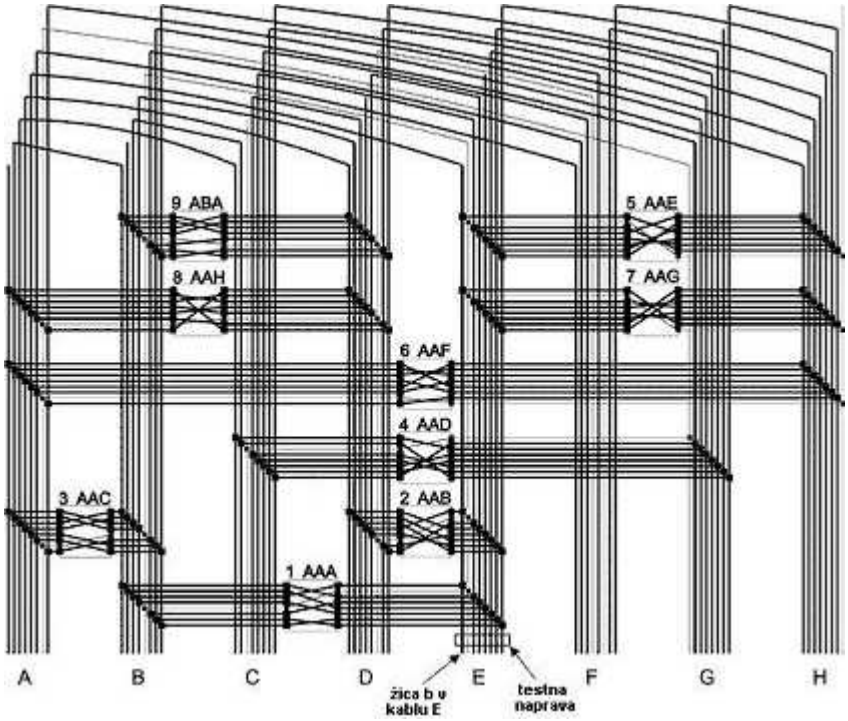


V tem cribu je na mestu 1 črka B povezana s črko E, zato en izhod dvoizhodne Enigme na prvem mestu priključimo na kabel B, drugega pa na kabel E. Nato povežemo še naslednjih osem dvoizhodnih Enigem z ustreznimi kabli diagonalne plošče. Zanke v cribu so sedaj predstavljene zankami v bombi.

Oglejmo si npr. zanko B-E-H-A. Boben na mestu 5 smo na enem koncu priklopili na kabel E. Preveriti hočemo predpostavko, da je E zamenjana v stikalni plošči z B. To naredimo tako, da pošljemo tok po kablu E, žica b ob različnih orientacijah bobnov.

Tok poteka skozi dvoizhodno Enigmo na mestu 5, ki je na drugi strani priključena na kabel H. V orientaciji na sliki pride tok v žico h. Na kabel H je priključena tudi dvoizhodna Enigma na mestu 6, in tok pride preko nje v kabel A, v žico g. Na kabel A je priključena dvoizhodna Enigma na mestu 3, in preko nje pride tok v kabel B, žica e. Na kabel B je priključena še dvoizhodna Enigma na mestu 1 in preko nje pride tok v kabel E, žica b in krog je sklenjen. Seveda pride tok tudi do drugih žic, ki so z njimi povezane. Žice, do katerih pride tok, imenujemo žive žice.

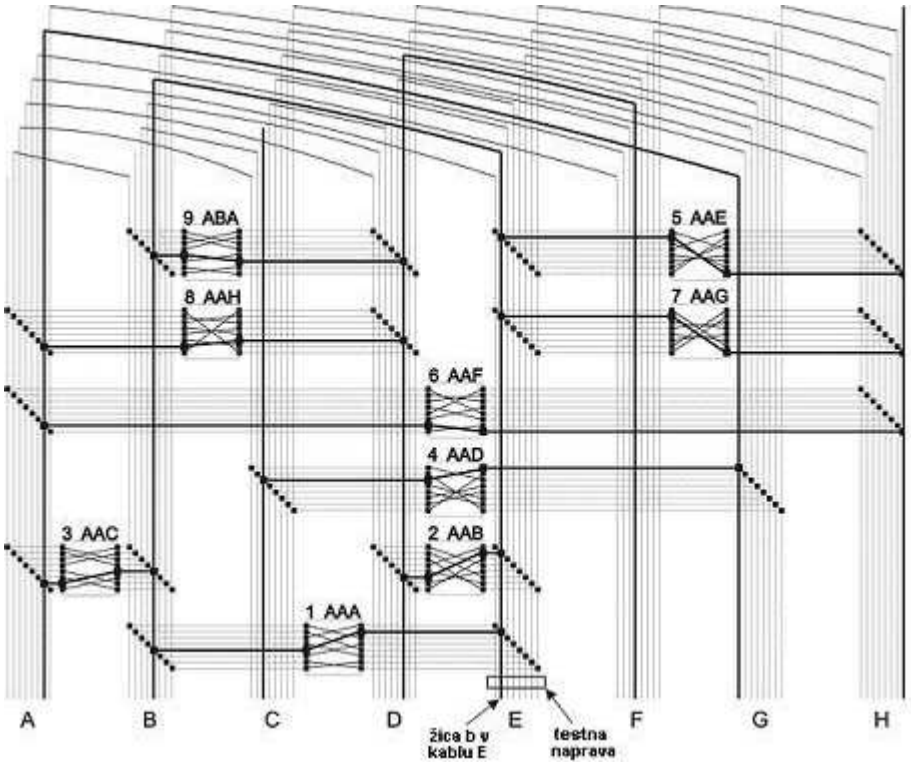
Slika 9: Dvoizhodne Enigme so vezane na diagonalno ploščo v skladu s cribom. S črno barvo so označene žive žice ob preverjanju predpostavke, da je E v stikalni plošči zamenjan z B.



Če je bila naša predpostavka, da je črka E zamenjana v stikalni plošči s črko B, pravilna, mora biti v vsakem kablu le ena žica živa. Če bi npr. v kablu E bila živa tudi žica h, bi to pomenilo, da je črka E zamenjana v stikalni plošči z B, pa tudi s H, torej z dvema naenkrat, kar pa seveda ni mogoče. Te žive žice nam tako povedo, katere črke so zamenjane v stikalni plošči. Živa žica g v kablu A nam tako pove, da je črka A zamenjana z G. Naprej lahko razberemo, da je črka E zamenjana z B, črka C ni zamenjana, črka D je zamenjana s F in črka H ni zamenjana.
Pravilna razporeditev in orientacija diskov je seveda tista, v kateri so v tem trenutku bobni v bombi.
Poglejmo še primer, ko preverjamo napačno predpostavko, npr, da je E zamenjan z A. Torej pošljemo tok po kablu E, žica a. Tok pride nato v kadel H, žica e, nato v kabel A, žica a, nato v kabel B, žica c in še v kabel E, žica d. Torej se krog ne sklene in tok se širi še naprej po žicah. Vendar pa tok ne pride do žic, ki predstavljajo zanko v cribu ob pravilni zamenjavi v stikalni plošči, saj so te sklenjene v zanko. Torej so sedaj žive vse žice razen tistih, ki predstavljajo zanko v cribu ob pravilni zamenjavi. Tako nam sedaj mrtve žice povedo, katere

zamenjave so pravilne.

Slika 10: S črno barvo so označene žive žice ob preverjanju napačne predpostavke, da je A zamenjan z E.



Oba primera seveda nastopita le, če je orientacija in razporeditev diskov pravilna. Če ta ni pravilna, se ponavadi tok razširi na vseh 26 žic. V tem primeru nam ni treba preverjati še drugih zamenjav, pač pa takoj vemo, da ta orientacija ni pravilna in lahko preverjamo naprej še druge orientacije. V bombi niso bile vezane žarnice za preverjanje, katera žica je mrtva in katera živa, ampak je bomba preverjala žive in mrtve žice s testno napravo, ki je bila priključena na en kabel, ponavadi na tistega, ki predstavlja črko, ki se v cribu najpogosteje pojavlja. Ko je bila na tem kablu živa ena ali 25 žic, se je bomba ustavila. Tako smo dobili možno rešitev, ki jo je seveda operater moral potem še preveriti na prejetih zašifriranih sporočilih. Najdena orientacija bobnov se je seveda nanašala na ključ sporočila, iz katerega smo poiskali crib. Da pridemo do dnevnega ključa, postopamo isto kot je to naredil Rejewski.
Zelo redko se je zgodilo, da je bila v testni napravi živa več kot ena in manj kot 25 žic. Tudi v teh primerih se je bomba ustavila. Če je bilo živih npr. 24 žic, je operater v eno mrtvo žico spustil tok. Če je potem tudi druga postala živa, je to pomenilo, da ta orientacija ni pravilna. Če pa je oživela le ena žica v vsakem

kablu, nam to da dve možni rešitvi: za zanko pravkar oživljenih žic in za zanko iz mrtvih žic. Tudi v primeru na zgornji sliki sta v kablu F mrtvi dve žici. To torej ne pomeni, da predpostavka ni pravilna. Žica f je mrtva zaradi tega, ker črka f v cribu ne nastopa in zato ta žica ni povezana z nobeno drugo žico.
Da bi bilo nepravilnih zaustavitev bombe čimmanj, je bil potreben dober crib, torej dovolj dolg in s čimveč zankami. Ko so angleški kriptoanalisti našli pravilen crib, so mu mogli najti še pravo mesto v sporočilu. Pri tem so si pomagali z dejstvom, da se zaradi zgradbe Enigme, natančneje zaradi reflektorja, nobena črka ne zašifrira v samo sebe. Ko so torej podpisali domneven čistopis pod tajnopis, so preverili, če se je katera črka zašifrirala v samo sebe. Če se je, so čistopis premikali tako dolgo levo in desno, da se to ni več zgodilo.
Če je bil crib zelo dolg, so angleški kriptoanalisti naleteli še na en problem. Če ima crib recimo 23 črk, je $\frac{23}{26} \approx 88\%$ možnosti, da se je med tem šifriranjem obrnil tudi sredinski boben. Ker seveda ne vemo, kdaj se je to zgodilo, ne znamo ustrezno nastaviti bobne. Da se temu izognemo, lahko crib razdelimo na dva dela. Tako se je sredinski boben obrnil le v enem izmed njih, torej so v enem delu bobni sigurno prav nastavljeni. Seveda pa je vprašanje, če potem dobimo zadosti dober crib.
Razbijanje Enigminih sporočil torej kljub bombi še zdaleč ni bilo enostavno. V Bletchley Parku so se spoprijemali tudi z drugimi težavami, npr: kako predvideti frekvenco, po kateri bodo Nemci pošiljali sporočilo in slab tok zaradi velike oddaljenosti sprejemne postaje.
Angleži so tako vse do konca vojne razbijali Enigmina sporočila. Ker Nemci seveda tega niso smeli izvedeti, so to zelo skrivali pred javnostjo. Celo najbližji sorodniki kriptoanalistov v Bletchley Parku niso vedeli, s čim se dejansko ukvarjajo. Tako je javnost šele v zgodnjih sedemdesetih izvedela za njihovo pomembno delo.

6 Zaključek

Enigma je najznamenitejša šifrirna naprava na osnovi vrtljivih diskov. Kar nekaj ohranjenih naprav je danes shranjenih v muzejih po vsem svetu, recimo v *Deutsches Museum* v Münchnu in v *National Security Agency Museum* v zvezni državi Maryland v ZDA. Nekatere naprave lahko obiskovalci tudi sami preizkusijo. Tudi na medmrežju ([6] in [7]) so simulacije Enigme, pa tudi drugih podobnih šifrirnih naprav. Tako lahko sami izberete začetne nastavitve Enigme in zašifrirate svoje sporočilo.

Enigma je imela tudi pomembno vlogo pri nadaljnem razvoju vrtljivih šifrirnih naprav. V zgodnjih tridesetih je japonska vojska komercialno verzijo Enigme posodobila in jo začela uporabljati v svoje namene. Naprava se je imenovala Red. Najpomembnejša razlika med Enigmo in Redom je bila v tem, da se posamezni disk ni premaknil vsakič le za en položaj, pač pa do položaja, ki ga je operater določil pred začetkom šifriranja. Red so uporabljali za šifriranje najpomembnejših sporočil med Japonsko in njihovimi zavezniki po vsem svetu. Leta 1936 je American Army Signal Intelligence Servis (SIS) z uporabo statistično - analitične tehnike, ki jo je izdelal Wiliam Friedman, razbil Red. V začetku leta 1939 so Japonci začeli uporabljati novo šifrirno napravo, imenovano Purple. Ta je imel namesto diskov stopničasta stikala, ki so bila nekoliko nenavadno razporejena. Stikala so se po vsaki zašifrirani črki, podobno kot pri Redu, premaknila za vsakič drugačno število položajev. Z razbitjem Purpla se je prav tako ukvarjal Wiliam Friedman. Njegova ekipa je jeseni leta 1940 imela že nekaj replik Purpla in začela razbijati sporočila.
V času druge svetovone vojne so različni narodi uporabljali še druge šifrirne naprave, saj je pošiljanje zašifriranih sporočil bilo takrat nepogrešljivo. Po drugi strani pa je tudi branje sovražnikovih razbitih sporočil imelo ogromen pomen, saj so na ta način lahko izvedeli za marsikateri sovražnikov namen in se nanj ustrezno pripravili. Šifrirne naprave so tako odločilno vplivale na razplet 2. svetovne vojne.

Literatura:

[1] Simon Singh: *The Code Book, the science of secrecy from Ancient Egypt to quantum cryptography*; New York, Anchor, 2000

[2] http://www.ellsbury.com/enigmabombe.htm

[3] http://www.codesandciphers.org.uk/enigma

[4] http://ovid.cs.depaul.edu/classes/cs233-W04/Papers/PurpleMagic.pdf

[5] David Kahn: *The Codebreakers; The story of Secret Writing*; New York, Scribner, 1996

[6] http://frode.home.cern.ch/frode/crypto/simula

[7] http://members.aon.at/cipherclerk