Šifrirne naprave

Majić, Monika

Undergraduate thesis / Završni rad

2015

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **Josip Juraj Strossmayer University of Osijek, Department of Mathematics / Sveučilište Josipa Jurja Strossmayera u Osijeku, Odjel za matematiku**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:126:273927

Sveučilište J.J.Strossmayera u Osijeku
Odjel za matematiku
Preddiplomski studij matematike

Monika Majić

Šifrirne naprave

Završni rad

Osijek, 2015.

Sveučilište J.J.Strossmayera u Osijeku
Odjel za matematiku
Preddiplomski studij matematike

Monika Majić

Šifrirne naprave

Završni rad

Voditelj: doc.dr.sc. Ivan Matić

Osijek, 2015.

Sažetak: U ovom završnom radu navest ćemo nekoliko jednostavnih šifrirnih naprava, objasniti njihov princip šifriranja i njihovu primjenu. Spomenit ćemo i kratak razvoj kriptografije, od drevnih Egipćana do dvadesetog stoljeća i istaknuti Enigmu kao složeniji šifrirni stroj koji je imao utjecaj na ishod Drugog Svjetskog rata.

Ključne riječi: Kriptografija, Kriptoanaliza, Monoalfabetske šifre, Polialfabetske šifre, Steganografija, Skital, Albertijev disk, Šifrirna naprava Thomasa Jeffersona, Rešetka, Enigma

Abstract: This final project is about important and simple code machines. We are going to explain their principles of coding and decoding and their purpose.We are going to find out about developement of cryptography through history, from Ancient Egypt to 20th century where famous code machine is invented-Enigma.

Keywords: Cryptography, Cryptoanalysis, Monoalphabetic ciphre, Polyalphabetic ciphre, Steganography, The Scytale, The Alberti Disk, Thomas Jefferson's Wheel Cipher, Grilles, Enigma

Sadržaj

1 Uvod

U ovom završnom radu proučit ćemo jednostavne šifrirne naprave kao što su rešetka, trokut, disk zatim kodovi nastali pomoću pisaćih strojeva i telefona. Objasnit ćemo njihov princip rada te kako pomoću svake od njih razbiti složene šifre. Navest ćemo materijale od kojih mogu biti napravljeni i primjere radi lakšeg razumijevanja i glavne slabosti.
Prije svega definirat ćemo osnovne pojmove vezane za šifriranje i dešifriranje, zatim kroz povijest istaknuti koje zemlje su zaslužne za nastanak i razvoj kriptografije i kriptoanalize. Spomenut ćemo i Enigmu kao značajan šifrirni stroj dvadesetog stoljeća i konstrukciju i ideju rada tog stroja.

2 Klasična kriptografija

2.1 Osnovni pojmovi

Kriptografija je znanstvena disciplina koja se bavi proučavanjem metoda za slanje poruka u takvom obliku da ih samo onaj kome su namjenjene može pročitati. Riječ kriptografija dolazi od grčkih riječi *kryptós* što znači skriven i *graphein* što znači pisati i prevodi se kao tajnopis.

Osnovni zadatak kriptografije je omogućiti dvjema osobama, pošiljaocu i primaocu (u kriptografskoj literaturi su za njih rezervirana imena Alice i Bob) komuniciranje preko nesigurnog komunikacijskog kanala (telefonska linija, računalna mreža,...) na način da treća osoba (njihov protivnik- najčešće se koristi naziv Eva ili Oskar), koja može nadzirati komunikacijski kanal, ne može razumjeti njihove poruke.

Otvoreni tekst zvat ćemo poruka koju pošiljalac želi poslati primaocu. To može biti tekst na njihovom materinjem jeziku, numerički podatci ili bilo što drugo. Pošiljalac transformira otvoreni tekst koristeći unaprijed dogovoreni ključ. Taj postupak se zove šifriranje, a dobiveni rezultat je šifrat ili kriptogram. Nakon toga pošiljalac pošalje šifrat preko nekog komunikacijskog kanala. Protivnik prisluškujući može doznati sadržaj šifrata, ali ne može odrediti otvoreni tekst. Primalac, budući da zna ključ kojim je šifrirana poruka može dešifrirati šifrat i odrediti otvoreni tekst.

Kriptoanaliza ili dekriptiranje je znanstvena disciplina koja se bavi proučavanjem postupaka za čitanje skrivenih poruka bez prepoznavanja ključa. Kriptologija je grana znanosti koja obuhvaća kriptografiju i kriptoanalizu. Kriptografski algoritam ili $šifra$ je funkcija koja se koristi za šifriranje i dešifriranje. Radi se o dvije funkcije. Jedna funkcija služi za šifriranje, a druga za dešifriranje. Te funkcije preslikavaju osnovne elemente otvorenog teksta (najčešće su to slova, bitovi, grupe slova ili bitova) u osnovne elemente šifrata, i obratno. Funkcije se biraju iz određene familije funkcija u ovisnosti o ključu.

Prostor ključeva je skup svih mogućih vrijednosti ključeva. Kriptosustav se sastoji od kriptografskog algoritma, svih mogućih otvorenih tekstova, šifrata i ključeva.

Definicija 2.1. Kriptosustav je uređena petorka $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ za koju vrijedi:

(1) $\mathcal{P}$ je konačan skup svih mogućih osnovnih elemenata otvorenog teksta;

(2) $\mathcal{L}$ je konačan skup svih mogućih osnovnih elemenata šifrata;

(3) $\mathcal{K}$ je prostor ključeva, tj. konačan skup svih mogućih ključeva ;

(4) Za svaki $K \in \mathcal{K}$ postoji funkcija šifriranja $e_K \in \mathcal{E}$ i odgovarajuća funkcija dešifriranja $d_K \in \mathcal{D}$. Pritom su $e_K : \mathcal{P} \to \mathcal{C}$ funkcije sa svojstvom da je $d_K(e_K(x)) = x$ za svaki otvoreni tekst $x \in \mathcal{P}$.

Najvažnije svojstvo u definiciji je $d_K(e_K(x)) = x$. Iz toga slijedi da funkcije e_K moraju biti injekcije.

Ako bi vrijedilo $e_K(x_1) = e_K(x_2) = y$, za dva različita teksta x_1 i x_2 onda primalac ne bi mogao odrediti treba li y dešifrirati u x_1 ili u x_2.

Jedan kriterij za klasificiranje kriptosustava je prema tipu operacija koje se koriste pri šifriranju. Postoji podjela na supstitucijske šifre u kojima se svaki element otvorenog teksta (slovo, bit, grupa slova ili bitova) zamjenjuje s nekim drugim elementom, te transpozicijske šifre u kojima se elementi otvorenog teksta permutiraju (premještaju). Npr. ako riječ ALICE šifriramo u FQNHJ, načinili smo supstituciju, a ako je šifriramo u CIELA, načinili smo transpoziciju. Postoje kriptosustavi koji kombiniraju ove dvije metode.

2.2 Monoalfabetske šifre

Monoalfabetske šifre su supstitucijske šifre gdje svakom slovu otvorenog teksta odgovara jedinstveno slovo šifrata.
Poznati primjer supstitucijske šifre je Cezarova šifra. U toj šifri slova otvorenog teksta su se zamjenjivala slovima što su se nalazila tri mjesta dalje od njih u abecedi (A→ D, B→E itd). Pretpostavka je da se abeceda ciklički nastavlja tj, da nakon zadnjeg slova Z, ponovo dolaze A, B, C.
Ako bismo upotrijebili današnji engleski alfabet od 26 slova, otvoreni tekst VENI VIDI VICI bio bi šifriran kao YHQL YLGL YLFL. Danas se Cezarovom šifrom smatraju i šifre istog oblika s pomakom različitim od tri.

Da bi se precizno definirala Cezarova šifra, uvodi se relacija između slova abecede (A-Z) i cijelih brojeva (0-25). Skup 0, 1,. . . , 25 označit ćemo sa $\mathbb{Z}_{26}$, i pretpostaviti da su na njemu definirane operacije zbrajanja, oduzimanja i množenja na isti način kao i u skupu cijelih brojeva, ali tako da se rezultat (ako nije is skupa 0, 1,. . . , 25) na kraju zamjeni sa njegovim ostatkom pri djeljenju s 26.
Šifra je definirana nad $\mathbb{Z}_{26}$ budući da koristimo 26 slova. Ova relacija svakom slovu abecede daje njegov "numerički ekvivalent". Elementi otvorenog teksta su slova (odnosno njihovi numerički ekvivalenti). Ključ K određuje za koliko udesno ćemo pomicati slova pri šifriranju. Za $K = 3$ dobiva se originalna Cezarova šifra.

2.3 Polialfabetske šifre

Za primjer polialfabetske šifre uzet ćemo Vigenèreovu šifru. Kod nje se svako slovo otvorenog teksta može preslikati u jedno od m mogućih slova, u ovisnosti o svom položaju unutar otvorenog teksta. m predstavlja duljinu ključa.
U svojoj knjizi "Traicte de Chiffres" Blaise de Vigenère je opisao više originalnih polialfabetskih kriptosustava.
Vigenèreova šifra se definira na sljedeći način:

Definicija 2.2. Neka je m fiksan prirodan broj. Definiramo $\mathcal{P} = \mathcal{C} = \mathcal{K} = \mathbb{Z}_{26}^m$. Za ključ $K = (k_1, k_2, ..., k_m)$, definiramo

$$e_K(x_1, x_2, ..., x_m) = (x_1 +_{26} k_1, x_2 +_{26} k_2, ..., x_m +_{26} k_m)$$
$$d_K(y_1, y_2, ..., y_m) = (y_1 -_{26} k_1, y_2 -_{26} k_2, ..., y_m -_{26} k_m).$$

Dakle, slova otvorenog teksta pomičemo za $k_1, k_2...$, ili k_m mjesta, u ovisnosti o tome na kojem se mjestu nalaze u otvorenom tekstu.

Vigenèreova šifra je jedan od najpopularnijih kriptosustava u povijesti. Upotrebljavala se u Američkoj revoluciji, krajem 18. stoljeća. U časopisu "Scientific American" 1917. je objavljeno da je ovu šifru nemoguće za razbiti.

3 Povijest kriptografije

Neki od najranijih zapisa o tajnom pisanju potječu još od Herodota. U svojim *Historijama* on daje kroniku sukoba između Grčke i Perzije u petom stoljeću prije Krista i navodi da se već u tom razdoblju Grčka branila umijećem tajnog pisanja.

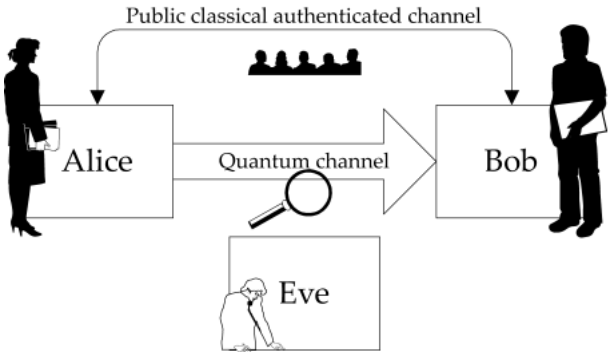
Demarat, izgnanik iz Grčke, uspio je upozoriti Grčku o perzijskom naoružavanju pomoću šifrirane poruke. Na pisaćim drvenim tablicama je napisao poruku, a zatim je prekrio rastaljenim voskom. Tako su pločice izgledale prazne, čime nije pobuđena sumnja stražara. Poruku je uspjela otkriti kći Kleomanta, koja se jedina dosjetila da bi vosak trebalo sastrugati sa drveta.

Demaratova strategija tajnog komuniciranja se svodila na skrivanje poruka. Još jedan slučaj zanimljivog prenošenja poruke jeste da se grčkom glasniku obrijala glava, na kojoj je zatim ispisana poruka. Glasnik je morao pričekati u njenom prenošenju dok mu kosa ne naraste a zatim je mogao nesmetano putovati.
Tajno komuniciranje pri kojem se skriva i samo postojanje poruke zove se *steganografija*. Ona dolazi od grčke riječi *steganos* što znači pokriven i *graphein*, što znači pisati. Za dvije tisuće godina od Herodota, steganografija se primjenjivala u različitim oblicima diljem svijeta. Tako su npr. stari Kinezi na tankoj svili pisali poruke. Zatim bi svilu zgužvali u kuglicu i natopili voskom, nakon čega ju je glasnik progutao.

Pisanje simpatetičkom tintom također spada u steganografiju. Nevidiljivu tintu moguće je dobiti iz mlijeka biljke mlječike. Takva tinta kad se osuši je nevidljiva, a pri laganom zagrijavanju posmeđi. Mana steganografije je u tome da ako glasnika pretraže i nađu poruku, njen sadržaj je razotkriven. Presretanje poruke razrješava tajnu.
Zbog toga se razvija i kriptografija usporedno sa steganografijom. Glavni cilj kriptografije nije samo zatajiti poruku, već i prikriti njeno značenje pomoću enkripcije. Prednost kriptografije je što neprijatelj ne može razabrati sadržaj čak ni uhvaćene poruke.

Pod šifrom smatramo svako kriptografsko rješenje kod kojeg je slovo otvorenog teksta zamijenjeno nekim drugim slovom ili simbolom. Svaku šifru možemo shvatiti kao da je nastala spajanjem opće enkripcijske metode ili algoritma i ključa koji točno određuje pravila po kojima se stvara neka šifra.
Primjer je Cezarova šifra kod koje ključ određuje koju šifrirnu abecedu treba uzeti za koju enkripciju. Neprijatelj koji je uhvatio takvu isprevrtanu poruku može naslutiti o kakvom je algoritmu riječ, ali neće moći odgonetnuti smisao jer ne zna ključ. Ako je šifrirna abeceda, tj. ključ informacija koju znaju samo pošiljalac i primalac, onda neprijatelj neće znati dešifrirati uhvaćenu poruku.

Ključ je najvažniji, što je Auguste Kerchoffs istaknio u svojoj knjizi. Njegovo pravilo glasi: "Sigurnost kriptosustava ne smije ovisiti o očuvanju tajnosti kriptoalgoritma. Sigurnost ovisi samo o čuvanju tajnosti ključeva."



Slika 1: Komunikacijski kanal

Međutim, nije dovoljno da sam ključ bude tajan već i da potencijalnih ključeva bude što više. Cezarova šifra zbog tog razloga je slabo enkriptirana jer postoji samo dvadest pet potencijalnih ključeva.
Arapsko zanimanje za kriptoanalizu započinje negdje oko 750. godine, nakon brojnih osvajanja. Enkripcija se razvijala u svrhu djelotvornog sustava upravljanja i zbog uspostave dobro organiziranog i imućnog društva. Državna uprava je ovisila o sigurnoj komunikaciji ostvarenoj pomoću enkripcije. Najviše su se kodirali dokumenti vezani za državne poslove i porezne knjige. Administracija se obično služila šifrirnom abecedom, koja je stvorena jednostavnim premještanjem slova otvorene abecede.

Arapski učenjaci se nisu samo služili šiframa, nego su ih znali i razbijati i upravo su oni razvili kriptoanalizu. Zadatak kriptografa je razvijanje metoda tajnog pisanja, a zadatak kriptoanalitičara jeste u njihovim metodama pronaći mane pomoću kojih će razbiti tajnu poruku. Baza za razvijanje kriptoanalize je matematika, lingvistika i statistika.

Između 800. i 1200. godine, dok se razvijala arapska kriptografija, u Europi su tek postojale osnove kriptografije. Redovnici su u tom razdoblju najviše proučavali tajno pisanje u potrazi za skrivenim značenjem Biblije. U 15. stoljeću kriptografija je uznapredovala.
Giovani Soro se smatra prvim velikim europskim kriptoanalitičarem. On je 1506. godine postavljen za šifrantskog tajnika. Kriptografi i dalje upotebljavaju monoalfabetske supstitucijske šifre, dok su ih kriptoanalitičari već razbili frekvencijskom analizom.

1918. godine njemački izumitelj Arthur Scherbius i Richard Ritter osnovali su trgovačko društvo, inovativnu strojarsku tvrtku. Jedna od Scherbiusovih ideja je bila zamijeniti neadekvatni kriptografski sustav primjenjen u Prvom Svjetskom ratu, tako da tradicionalne kodove i šifre zamjeni enkripcijom koja bi koristila tehnologiju dvadesetog stoljeća. Razvio je kriptografsku mašineriju koja je bila električna verzija Albertijeva diska. Taj stroj, Enigma, koristila je Njemačka u Drugom Svjetskom ratu. Enigma je također imala utjecaj na razvoj drugih šifrirnih strojeva.

Slika 2: Arthur Scherbius

Dešifriranje drevnih tekstova se možda čini kao nemoguć posao, no mnogi ljudi su se upustili u taj pothvat. Cilj je bio shvatiti spise predaka i više saznati i njihovom načinu života.
Dešifriranje starih tekstova ne spada u klasičnu kriptoanalizu i kriptografiju jer u njoj nema šifrotvoraca, tj. izvorni pisar nije namjerno pokušavao prikriti značenje teksta. Načela arheološkog dešifriranja su jednaka načelima konvencionalne vojne kriptoanalize.

Razbijanje tajne egipatskih hijeroglifa je najslavnije od svih arheoloških dešifriranja. Pomoću klasičnog slučaja razbijanja kodova, hijeroglifi su napokon bili dešifrirani te su tada arheolozi proširili svoja saznanja o kulturi i vjerovanjima starih Egipćana.
Zanimanje za hijeroglife počinje u sedamnaestom stoljeću kada je papa Siksto V. u Rimu napravio novu mrežu avenija i na svakom križanju podigao obelisk dopremljen iz Egipta. 1799. francuski vojnici su pronašli najslavniji kamen blok u povijesti arheologije, u gradu Rosetti, sred nilske delte. Na kamen bloku je isti tekst bio urezan tri puta: grčkim, demotskim i hijeroglifskim pismom. Kasnije je taj kamen prozvan kamenom iz Rosette. 1802. godine kamen

Slika 3: Kamen iz Rosette

dospjeva u engleski Portsmouth. Od te godine nalazi se u British Museumu, sve do danas.
Thomas Young je uspio većinu hijeroglifa povezati sa njihovim glasovnim vrijednostima. Međutim, kako je izgubio zanimanje za hijeroglife, svoj rad je prekinuo. Njegov rad prikupljao je francuz Jean-Francǫis Champollion, lingvist. Veliku je važnost pridavao pismu starih Egipćana i tome da postane prvi čovjek koji će to pismo moći pročitati.
1824. godine Champollion je objavio svoj rad u knjizi Uvod u hijeroglifski sustav. Time je omogućeno o povijesti faraona čitati u obliku u kojem su je zabilježili njihovi pisari.

4 Jednostavne naprave za kodiranje

Svaka tehnološki razvijenija zemlja danas koristi računala za kodiranje i dekodiranje. Iznad svega, računala se koriste za razbijanje šifrata protivnika, u diplomatske i vojne svrhe.Velike privatne korporacije sada ih također koriste za njihovo vlastito tajno komuniciranje između službenika iste firme. Postoji puno jednostavnih naprava za šifriranje koje se mogu napraviti te upotrebljavati za slanje tajnih poruka.

4.1 Kodovi pisaćih strojeva

Prosječni pisaći stroj može poslužiti kao osnova za puno jednostavnih zamjenskih šifri. Npr. umjesto utipkavanja određenog ključa za svako slovo, može se otkucati ključ direktno iznad njega i lijevo. Zavisno što se preferira, može se upotrijebiti ključ direktno desno, ili ključ gore i desno.
Ako odaberemo gore i lijevo KRIPTOSUSTAV biti će otkucan kao I48059W7W5QF.
Ako odaberemo desno O59 ’ 60E8E6WG.
Da bi se kod napravio težim za razbiti, mogu se prisvojiti strategije tako da se izmjenično upotrebljavaju upravo opisane metode krećući sa gore i lijevo 8 : 933 U9I.
Dekodirajuća tehnika je reverzna kodirajućoj proceduri. Ako kod koristi ključeve desno na pisaćem stroju tj. tipkovnici, prijevod šifriranog teksta bio bi utipkavanjem ključeva lijevo svakog simbola, i slično za ostale metode.

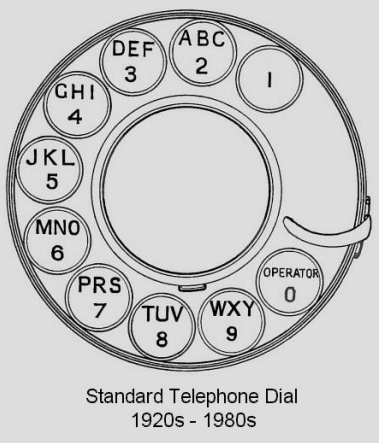
Slika 4: Pisaći stroj

4.2 Telefonski kôd

Ovaj kôd koristi uobičajene telefonske brojeve pomoću kojih je omogućen alfabet. Slova na pozivnim tipkama (brojevima) su grupirani u trojke, s tim da se svako slovo pojavljuje u jednoj trojci. Da bi se moglo kodirati u telefonskom kodu, potrebno je ispisati slova, a zatim napisati brojeve pored.

Ukoliko se slovo koje želimo odabrati u trojci nalazi najbliže početku abecede, to ćemo označiti crtom iznad broja, koja će biti nakrivljena ulijevo. Ukoliko se slovo u trojci nalazi najbliže kraju abecede, to ćemo označiti crtom nakrivljenom udesno iznad broja, a ukoliko se slovo nalazi u sredini, to označavamo vertikalnom crtom iznad broja.

Treba primjetiti da su Q i Z jedina slova koja se ne nalaze za biranje. Budući da znamenke 0 i 1 nemaju naznačena slova pokraj njih, obično se s 1 označava Q, a s 0 se označava Z.
SLOVO u obliku telefonskog kôda izgleda: $\acute{7}$ $\acute{5}$ $\acute{6}$ $\acute{8}$ $\acute{6}$.

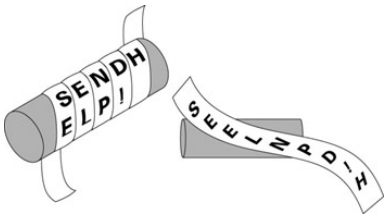


Slika 5: Telefonski kôd

4.3 Skital

Scytale je bio latinski naziv prvog poznatog stroja za kodiranje. Prvo su ga upotrebljavali Spartanci u 5. stoljeću prije Krista. Skital je imao oblik valjka te je bio napravljen od drveta ili nekog drugog materijala. Primalac mora imati valjak iste veličine. Moguće je upotrijebiti obične olovke, ali one su pretanke te zbog toga nisu prikladne. Zbog toga je najbolje nabaviti štap polumjera oko 2.5 cm. Kartonske tube unutar papirnih ručnika ili maramica su također prikladne za upotrebu. Da bi se poruka kodirala, treba uzeti dužu vrpcu (zavisno o dužini cilindra) i omotati oko cilindra. Na omotanu vrpcu se zatim okomito pisala poruka. Kada se vrpca razmota, slova su izmješana.

Dekodiranje je lako. Samo treba omotati vrpcu na isti način oko cilindra iste veličine koja je upotrebljena prilikom kodiranja.



Slika 6: Skital

4.4 Albertijev disk

Ova jednostavna šifrirna naprava-kotač brzo omogućuje šifriranje abecede i ima 26 ključeva. Čine ga dva koncentrična diska, pričvršćena pribadačom kroz središta diskova. Veći disk se naziva stacionarni a manji disk mobilni.

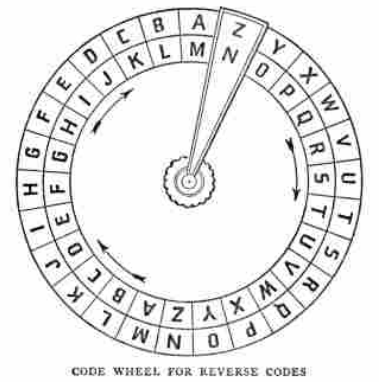
Uređaj se lako može napraviti tako da se od kartona odreže disk i postavi na novi karton i pričvrste se u središte diska. 26 slova na unutrašnjem disku su postavljena abecedno, ali na vanjskom disku slova su nasumično postavljena. Primalac naravno mora imati isti uređaj. Prije nego što se pošalje kodirana poruka, točak treba okreniti tako da bilo koje slovo koje želimo bude nasuprot slovu A na unutrašnjem disku. Prvo slovo na vanjskom disku je prvo slovo našeg šifrata. Od sada, kotač ostaje u istoj poziciji. Za svako slovo u poruci, treba pronaći slovo u abecedi na unutrašnjem disku i upotrijebiti slovo koje se pojavljuje nasuprot i u abecedi vanjskog diska. Primalac mora samo postaviti kotač na način kako ga je postavio pošiljalac, prema ključnom slovu na početku šifrata. Zatim se kotač može upotrijebiti za dekodiranje šifrata.

U ilustraciji, kotač je postavljen tako da se nasuprot A nalazi M u unutrašnjem disku. Nasuprot A moguće je postaviti 26 različitih slova, što znači da postoji 26 ključeva koji se mogu izabrati. Način kodiranja je moguće promijeniti svaki put prilikom slanja poruke.

Poruka GDJE JE ALICE kodirana na ovaj način glasi: GJDI DI MBEKI. Ovo je monoalfabetska šifra, i zbog toga ju je lako za razbiti.

Želimo li polialfabetsku šifru, koju je teže za razbiti, treba samo okreniti kotač nakon svakog slova. Jednostavan primjer ovoga postupka je pomjerati kotač za jedno slovo u smjeru kazaljke na satu (ili suprotno) nakon što se pojedino slovo kodira. Drugi primjer je da se kotač prvo pomjeri za jedno slovo, drugi put za dva, zatim za tri, onda opet za dva i jedan.
I sami možemo smisliti polialfabetske kodove. Ne bi trebali biti puno složeniji da bi se izbjegle moguće pogreške i zbog brzine kodiranja i dekodiranja.

Ovaj uređaj je prvi izumio Leon Battista Alberti, talijanski arhitekt iz 15. stoljeća. Zbog svojih pisanja kodova proglašen je ocem zapadne kriptografije. Albertijev disk je bio puno puta "ponovo izumljen" u kasnijim stoljećima.



Slika 7: Albertijev disk

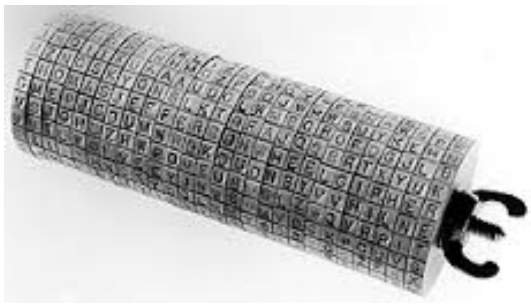
4.5 Šifrirna naprava Thomasa Jeffersona

Genijalnu metodu za konstrukciju polialfabetske šifre s dodatkom rotirajućih diskova izumio je Thomas Jefferson, 3. predsjednik SAD-a. Jeffersonova "kotač šifra" kako ju je nazvao, sastojala se od 36 drvenih kotača iste veličine, koji su bili namotani oko željeznog štapa. Svaki kotač je imao ispisan alfabet na svojoj vanjštini.

Da bi pošiljalac šifrirao otvoreni tekst, mora podijeliti tekst na blokove od po 26 slova. Blok se šifrira tako da se rotiranjem diska u jednom od 26 redaka dobije otvoreni tekst. Tada se za šifrat može odabrati bilo koji od preostalih 25 redova. Primalac treba namjestiti točak tako da odgovaraju šifratu, a zatim gleda red koji ima najviše smisla. U svim ostalim redovima slova će biti izmješana i neće tvoriti smislene riječi, tako da primalac neće napraviti grešku prilikom prepoznavanja poruke. Naravno, postoji mala šansa da druge linije imaju smislene riječi ili dio riječi. Pošiljalac i primalac moraju imati dva identična kotača.

Lako je napraviti jednostavniji oblik ovog uređaja tako da se šipka (koja može biti napravljena i od kartona) sastoji od 6 kotača koji su iste veličine i omotani oko kartona. Pričvršćivač za papir prolazi kroz centar diska i pričvršćuje kotače za karton i omogućava njihovu rotaciju. Rub svakog kotača ima 26 odjeljaka koji sadrže slova abecede, ali nisu poslagani po abecednom redu. Što se više kotača koristi, manja je vjerojatnost da druge linije imaju smisao i time je lakše prepoznati ispravni red. Kotač s šest diskova je jednostavnije napraviti nego s deset, ali kod kotača s deset diskova šifrat je teže za razbiti. Idući korak je kopirati proizvoljni red, sve osim otvorenog teksta. Procedura se ponavlja sve dok cijela poruka nije kodirana. U svakom koraku, za svaku grupu od 26 slova, (zavisno koliko imamo diskova)može se odabrati proizvoljan red.

Primalac podijeli šifrat u grupe od 26 slova i onda namješta diskove tako da su prvih šest slova šifrata u istom redu. On gleda redove sve dok ne prepozna onaj koja ima smisao. Ova procedura se ponavlja sve dok svaka grupa od 26 slova cijelog šifrata nije dekodirana. Jeffersonov kotač-šifrirnu napravu je gotovo nemoguće za razbiti. Osnovna ideja Jeffersonovog kotača je kreiranje poliafabetskog kriptosustava sa korištenjem diskova koji se rotiraju više ili manje nezavisno. Ova ideja je bila osnova kod mehaničkih i elektromehaničkih naprava izumljenih kasnije. 1922. Jeffersonova šifrirna naprava je usavršavana i prisvojila ju je američka vojska te se i danas koristi u američkoj mornarici.



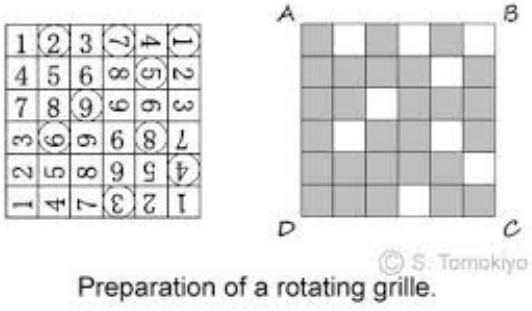
Slika 8: Jeffersonova kotač-šifrirna naprava

4.6 Rešetka

Rešetka (nekad zvana i koordinatna mreža) je kvadratni ili trokutasti dio kartona ili nekog drugog materijala koji ima otvore, tj. izrezan je na različitim mjestima.
Osnovna ideja korištenja rešetke je premještanje slova. Izumio ju je Girolomo Cardiano, talijanski matematičar 16. stoljeća. Cardiano je koristio rešetku u samo jednoj poziciji.

Slova ili riječi otvorenog teksta su bili ispisani kroz prozore-otvore. Nakon što je rešetka uklonjena, prostor između tih slova je bio popunjen sa beznačajnim slovima da bi se stvorila lažna poruka.
Kada se identična rešetka primaoca ponovo postavi na kodiranu poruku, beznačajna slova su pokrivena i "prava" slova se lako čitaju kroz prozore.
Kasnije su bile izumljene rešetke koje su se mogle rotirati tako da se svaka ćelija matrice sastojala od slova otvorenog teksta, ali u ispremiješanom redosljedu. Takve rotirajuće rešetke je upotrebljavala Njemačka u kratkom razdoblju na kraju Prvog Svjetskog rata.

Da bi se napravila 6×6 rešetka, pravilno se ucrtaju kvadrati, njih 36 na karton. Potrebno je numerirati ćelije kako je označeno na Slici 9. Najprije izrežemo bilo koju ćeliju s brojem 1, zatim bilo koju ćeliju označenu brojem 2, treću označenom s 3 itd. sve dok se na kartonu ne izreže devet ćelija. Rešetka može izgledati kao ona prikazana na Slici 9. Svaku ćeliju koja nedostaje zvat ćemo otvor ili prozor, iako se može dogoditi da su izrezani kvadratići jedan pored drugog, te formiraju jedan prozor. Zatim treba nacrtati kvadrat iste veličine na praz-



Slika 9: Rotirajuća rešetka

nom papiru. Staviti rešetku na papir u bilo kojoj poziciji i upisati prvih devet slova poruke u devet prozora. Može se upotrijebiti proizvoljna procedura. Npr. slova se mogu upisivati od dna prema vrhu, popunjavajući stupce od desno prema lijevo. Naravno, primalac mora znati redoslijed popunjavanja stupaca tj. proceduru kao i prvu poziciju rešetke.
Sada se rešetka rotira u smjeru kazaljke na satu, za 45° ili suprotno od smjera kazaljke na satu, što je proizvoljno i ispiše se idućih devet slova, slijedeći istu proceduru, kao i za prvih devet slova. Ponovo okretanje za 45° u istom smjeru omogućuje nam dodavanje devet novih slova itd. Nije bitno ukoliko je poruka kraća od 36 slova. Nije potrebno sve ispisati.

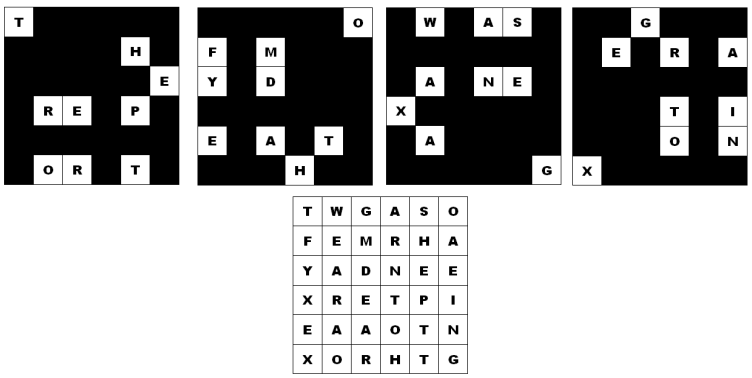
Ako je poruka duža od 36 slova, potrebno je koristiti novi papir i ponavljati iste operacije sve dok cijela poruka nije kodirana. Slika 10. pokazuje rešetku koja je rotirana u smjeru kazaljke na satu, omogućavajući četiri pozicije. Svaka pozicija smješta devet prozora, na različit skup ćelija kako bi se izbjeglo njihovo preklapanje.
Može se poslati i iscrtana matrica sa izmješanim slovima, ali to je opasno jer neprijatelj iz izgleda može pogoditi da je korištena rešetka kao kodirajući uređaj. Zato je najbolje kopirati slova na drugu stranicu papira. Može se koristiti proizvoljna procedura popunjavanja slova ali primalac mora znati taj postupak.

Pretpostavit ćemo da se ispisuju redovi od vrha na dolje, od lijevo na desno. Osoba koja prima kodiranu poruku prvo će nacrtati tablicu iste veličine. Zatim postavlja svoj duplikat rešetke na tablicu prema prvoj poziciji. Idući korak je kopirati slova u redove, od vrha na dolje i od lijevo na desno tj. slijedeći istu proceduru koja je bila dogovorena prilikom upisivanja slova u prozore.
Nakon što je primalac ispisao prvih devet slova, okreće rešetku u smjeru kazaljke na satu, u drugu poziciju, kopirajući idući skup od 9 slova. Nakon ukupno 4 okretaja ispisat će 36 slova izvorne poruke u točnom redoslijedu.

Ovo je složenija transpozicijska šifra. Rešetka je mehanički uređaj koji automatski izmješa slova za pošiljaoca i tako ih automatski razmješta za primaoca.
Mogu se napraviti kvadratne rešetke s bilo kojim kvadratnim brojem, ali ako je broj ćelija stranice neparan broj, npr. 5×5 rešetka, onda se središte rešetke ne može upotrijebiti. Razlog je tome ako se prozor nalazi u središtu, on ostaje na istom mjestu dok se ostatak rešetke rotira. U ovakvim slučajevima najbolje je ne napraviti prozor u središtu. Beznačajno slovo se može upisati u centralnu ćeliju, ili ćelija može ostati prazna.
Dobra ideja je označiti na neki način stranu rešetke koja bi trebala biti okrenuta prema gore. Jer, okretanjem rešetke dobit ćemo drugačiju rešetku. To je zrcalna slika prijašnje i stvara različit šifrat. Naravno, svaka rešetka se može upotrijebiti za dva različita šifrirna sustava.

Osim kvadratne, postoji i pravokutna rešetka sa pravokutnim otvorima, što nam omogućuje da ispisujemo riječi umjesto slova. Kao i kvadratna rešetka, ona također ima četiri pozicije. Jedan kut može biti izrezan, što čini lakšim da se rešetka smjesti pravilno. Ako je u prvoj poziciji izrezan kut smješten gore i lijevo, rotiranjem rešetke u smeru kazaljke na satu, taj kut će se nalaziti gore i desno. Možemo mijenjati pozicije tako da okrećemo izrezani kut suprotno od smjera kazaljke na satu, ili možemo uspostaviti vlastiti redoslijed za ove četiri pozicije.

Kao i sa slovima, nebitno je da li je poruka kraća zato što prazna mjesta neće utjecati na premještanje. Ako otvoreni tekst ima više od 26 riječi, rešetka se može pomjeriti na novu stranicu papira.
Svaki puta kada se rešetka koristi za šifriranje ili za dešifriranje, dobra je vježba prvo olovkom ucrtati rubove i time naznačiti oblik rešetke. Na ovaj način možemo biti sigurni da smo rešetku postavili ispravno u svakoj od četiri pozicije.
Ako je riječ dugačka pa ne stane u prozor, jedan dio treba zapisati u jedan prozor a drugi u drugi prozor. Dvije kratke riječi se mogu zajedno zapisati kao jedna riječ.



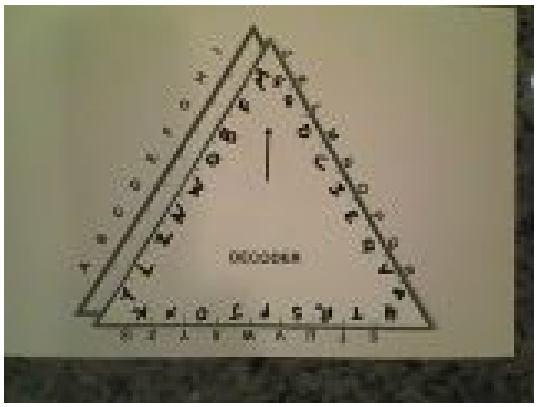
Slika 10: Rešetka

4.7 Trokut- šifrirna naprava

Da bismo napravili ovaj mali korisni uređaj za šifriranje, prvo trebamo nacrtati jednakostranični trokut na sredini stranice papira. Treba upisati slova po abecednom redu oko i izvan sve tri stranice trokuta. Slova moraju biti međusobno jednako udaljena. Zatim treba nacrtati identični trokut na kartonu. Abeceda treba biti napisana unutar i oko rubova sve tri stranice ali slučajnim redosljedom. Idući korak je ucrtavanje strelice koja je usmjerena prema jednom od vrhova trokuta. Izrezati kartonski trokut i smjestiti ga na papirni trokut. Strelica treba biti usmjerena prema gore.

Naprimjer, ako želimo kodirati slova A i B, treba prvo postaviti trokut u položaj gdje je strelica usmjerena prema gore, a zatim pronaći slovo A u abecedi papirnog trokuta i pogledati koje slovo mu odgovara u abecedi kartonskog trokuta. Slovo na abecedi kartonskog trokuta će biti prvo slovo šifrata. Zatim se trokut okrene u smjeru kazaljke na satu te se ponovno postavlja na drugi trokut tako da se preklapaju. Sada strelica treba biti usmjerena dolje i desno. Slovo koje odgovara slovu B će biti drugo slovo šifrata. Ponovno rotiranje u smjeru kazaljke na satu dat će treću poziciju. Sada strelica treba pokazivati dolje i lijevo. Iduće rotiranje vraća trokut u početnu poziciju.

Da bismo dešifrirali, potrebno je slijediti istu proceduru, tj. onu koja je dogovorena i korištena prilikom šifriranja. Svako slovo šifrata se iščita u abecedi kartonskog trokuta te mu se pridruži slovo abecede na papirnom trokutu. Svaki put trokut treba zarotirati u smjeru kazaljke na satu.



Slika 11: Trokut-šifrirna naprava

Slični uređaji za kodiranje oblika trokuta, peterokuta ili šesterokuta se mogu upotrijebiti za stvaranje složenijih polialfabetskih šifri. Ovi uređaji su specijalizirane vrste Porta šifre.
Porta šifru je razvio Giovanni Battista Della Porta u 16. stoljeću. Porta šifra je supstitucijska polialfabetska šifra. Ovisno o ključu, druga abeceda se upotrebljava za šifriranje otvorenog teksta.
Npr. uzmimo PORTA za otvoreni tekst i SIFRA za ključ. Ovisno o prvom ključu, a to je S, potražimo odgovarajuću supstitucijsku abecedu na Slici 12. Vidimo da prvom slovu otvorenog teksta P odgovara slovo L. To je prvo slovo šifrata. Drugi ključ je slovo I. Gledamo njegovu supstitucijsku abecedu. Slovu O odgovara slovo F. To je drugo slovo šifrata. Analogno ponavljamo postupak za preostala slova R T i A. Dobiveni šifrat je LFGBN.

Key	Substitution alphabet
A,B	A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
C,D	A B C D E F G H I J K L M Z N O P Q R S T U V W X Y
E,F	A B C D E F G H I J K L M Y Z N O P Q R S T U V W X
G,H	A B C D E F G H I J K L M X Y Z N O P Q R S T U V W
I,J	A B C D E F G H I J K L M W X Y Z N O P Q R S T U V
K,L	A B C D E F G H I J K L M V W X Y Z N O P Q R S T U
M,N	A B C D E F G H I J K L M U V W X Y Z N O P Q R S T
O,P	A B C D E F G H I J K L M T U V W X Y Z N O P Q R S
Q,R	A B C D E F G H I J K L M S T U V W X Y Z N O P Q R
S,T	A B C D E F G H I J K L M R S T U V W X Y Z N O P Q
U,V	A B C D E F G H I J K L M Q R S T U V W X Y Z N O P
W,X	A B C D E F G H I J K L M P Q R S T U V W X Y Z N O
Y,Z	A B C D E F G H I J K L M O P Q R S T U V W X Y Z N

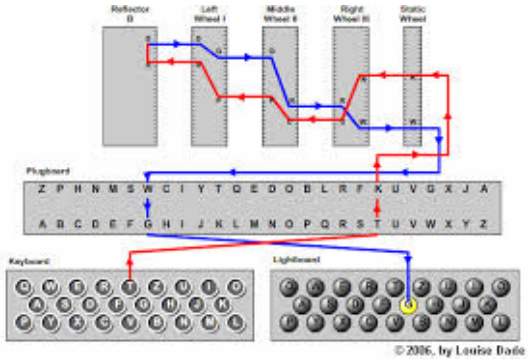
Slika 12: Ključevi Porta šifre i odgovarajuće supstitucijske abecede

5 Enigma

Enigma je danas naziv za seriju elektro-mehaničkih rotorskih uređaja za šifriranje. Razvila se i upotrebljavala u prvoj polovini dvadesetog stoljeća za komercijalne i vojne svrhe. Enigmu je izumio njemački inženjer Arthur Scherbius na kraju Prvog Svjetskog rata. Scherbiousov stroj Enigma se sastojao od velikog broja genijalno osmišljenih dijelova, koje je složio u vrlo složen šifrirni stroj. Sastojao se od tri osnovna elementa povezana žicama tipkovnice za unošenje otvorenog teksta, premetačke jedinice koja slova otvorenog teksta enkriptira u odgovarajuća slova šifrata i na kraju displeja koji je bio sastavljen od žaruljica koje prikazuju slova šifrata.
Da bi operater mogao enkriptirati otvoreni tekst, pritišće odgovarajuće otvoreno slovo na tipkovnici i time šalje električni impuls kroz središnju premetačku jedinicu. Zatim iz nje izlazi i osvjetljava odgovarajuće šifrirano slovo na displeju s lampicama.

Premetalo (scrambler ili pseudoslučajni koder) je najvažniji dio stroja. To je disk ispresplet ten žicama. Žice kreću od tipkovnice i na 26 mjesta ulaze u premetalo. U njemu se zakreću, da bi s druge strane izašle na 26 mjesta. Taj splet žica u premetalu određuje kako će se enkriptirati slova otvorenog teksta.
Svaki put kad se slovo utipka u tipkovnicu i enkriptira, premetalo se zakrene za jedno mjesto te se time mijenja potencijalna enkripcija svih slova.
Ako je premetalo postavljeno u osnovnom položaju, stroj može biti primjenjen za pisanje jednostavnom monoalfabetskom supstitucijskom šifrom.
Scherbiusova ideja je bila da se disk premetala automatski zakrene za jednu dvadesetšestinu kruga poslije enkripcije svakog slova.
Šifrirna se abeceda poslije svake enkripcije mijenja, pa se stalno mijenja i enkripcija pojedinog slova. Zahvaljujući toj rotaciji, premetalo zapravo definira 26 ključeva, pa stroj može poslužiti za pisanje poliafabetskom šifrom.

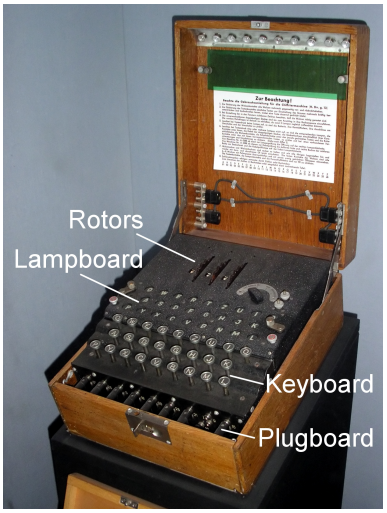
Jedna od najvažniijh karakteristika Scerbiusova stroja je bila rotacija. Međutim, slabosti ovog stroja su bile u tome, ako jedno slovo utipkamo 26 puta, premetalo će se vratiti u početni položaj. Koristimo li isto slovo uzastopno, obrazac enkripcije se ponavlja. Zato je glavni cilj izbjeći pravilnosti. To se može popraviti ugradnjom još jednog premetala. Stroj sada raspolaže



Slika 13: Struktura Enigme

sa $26 \cdot 26$ slova, to znači da se prilikom šifriranja mijenja 676 ključeva. Scherbiusov standardni stroj je imao i treće remetalo i reflektor.
Vjerovalo se da je njegov šifrirni stroj nemoguće za razbiti. 1925. godine započela je masovna proizvodnja Enigme, koju je prvenstveno koristila vojska, ali i u komercijalne svrhe. Nacistička Njemačka ju je prisvojila prije i tijekom Drugog Svjetskog rata.

Njemačke vojne poruke prvo je uspjela razbiti poljska vladina agencija koja se bavila kriptoanalizom 1932. godine. Ovaj uspjeh je bio rezultat truda tri poljska kriptoanalitičara Marian Rejewski, Jerzy Różycki i Henryk Zygalski, koji su radili za poljsku vojsku. Rejewski je dizajnirao reverzni uređaj, upotrebom teorijske matematike i pomoću materijala dobivenih od francuske vojske. Ova tri matematičara dizajnirali su mehanički uređaj za dekodiranje Enigminih šifrata.
Od 1938. pa nadalje, Enigma se usavršavala, čime je dekodiranje postalo složenije i zahtijevalo je više opreme i osoblja, što Poljska nije mogla omogućiti.
U srpnju 1939. godine u Varšavu, Poljaci su upoznali francusku i britansku vojsku sa svojim tehnikama za dekodiranje i obećali svakoj delegaciji poljsku rekonstruiranu Enigmu. Ova demonstracija je bila osnova za kasniji trud Britanaca. Tijekom rata, britanski kriptolozi uspjeli su dešifrirati ogroman broj poruka šifriranih Enigmom, što je bila znatna pomoć savezničkim ratnim naporima.



Slika 14: Enigma

Literatura

[1] A. Dujella, M. Maretić, Kriptografija, Element, Zagreb, 2007.

[2] M. Gardner, Codes, Ciphers and Secret Writing, Dover Publications, Inc. New York, 1984.

[3] S. Singh, Šifre: Kratka povijest kriptografije, Mozaik knjiga, Zagreb, 2003.