Sveučilište J.J. Strossmayera u Osijeku
Odjel za matematiku

Ana Antolović

Naprave za šifriranje

Diplomski rad

Osijek, 2015.

Sveučilište J.J. Strossmayera u Osijeku
Odjel za matematiku

Ana Antolović

Naprave za šifriranje

Diplomski rad

Mentor: doc.dr.sc. Ivan Matić

Osijek, 2015.

Sadržaj

1. Uvod

Od početka civilizacije i pojave pisma postoji želja da komunikacija među ljudima bude što sigurnija. Počevši od starih naroda Egipćana, Arapa, Grka, Rimljana, preko mnogih kraljeva, vojskovođa, a kasnije diplomata, moderne vojske i špijuna, svi su imali isti problem - kako poslati informaciju željenoj osobi, a da ju neprijatelj ne otkrije ili ne može razumjeti. Znali su što bi se dogodilo da važne poruke dospiju u krive ruke. Vođeni strahom od otkrivanja dragocjenih informacija, bili su prinuđeni naći načine kojima bi sigurno međusobno komunicirali. Prvo su se dosjetili raznih metoda skrivanja poruka. Takvo komuniciranje pri kojem se skriva samo postojanje poruke naziva se *steganografija*. Naziv dolazi od grčkih riječi *steganos*, što znači prikriven i *graphein*, što znači pisati. Ona je davala određenu sigurnost, ali imala je svoj nedostatak. Ako bi se poruka otkrila, tajne više ne bi bilo. Protivnik bi saznao njen cijeli sadržaj. Zato se razvila *kriptografija*, čije ime dolazi od grčke riječi *kryptos*, koja znači skriven. Cilj ove znanosti nije prikrivanje poruke, nego njenog sadržaja. U slučaju da protivnik presretne poruku, za njega ona ne bi imala nikakvog smisla, jer ju ne bi razumio. Proces prikrivanja poruke nazivamo *šifriranje*. Ono na temelju nekog dogovorenog pravila ispremješta slova *otvorenog teksta* (poruke), čime se dobiva *šifrat* - naizgled besmisleni niz slova. Primatelj zna to pravilo i pomoću njega vrati poruku u izvorno razumljivo stanje, a taj postupak naziva se *dešifriranje*. Kriptografija se dijeli na dvije grane, transpozicijsku i supstitucijsku. Transpozicijska samo premješta slova otvorenog teksta, pa je šifrat zapravo anagram početne poruke, dok supstitucijska mijenja svako slovo otvorenog teksta nekim drugim unaprijed zadanim slovom ili znakom.

Razvoj steganografije i kriptografije bio je uvjetovan razvojem naprava, koje su omogućavale brže i bolje prikrivanje otvorenog teksta.

Budući da su spomenute dvije znanstvene discipline usko povezane u svom cilju sigurne komunikacije, spomenut ćemo različita pomagala, male naprave i kompliciranije uređaje, koje vežemo uz jednu i drugu. Najprije ćemo spomenuti nekoliko zanimljivih metoda steganografije uz pomoć predmeta koji se mogu naći u kućanstvu, a potom malo opširnije o ozbiljnijim napravama za šifriranje u kriptografiji.

2. Jednostavne naprave i pomagala

2.1. Simpatetička tinta

Jedan od primjera prikrivanja poruke je pisanje pomoću tinte, koja je nevidljiva običnom promatraču. To je takozvana „nevidljiva" ili simpatetička tinta. Poruka postaje vidljiva tek kad se podvrgne određenom tretmanu. Korištenje nekog oblika takvih tinti bilo je prisutno od početka civilizacije, a najviše su ih koristili špijuni. Oni su rijetko kada posebnu tintu koristili na čistom bijelom papiru. U slučaju presretanja, to bi pobudilo veliku sumnju. Umjesto toga nevidljivom tintom bi pisali između redaka neke nevezane poruke ili na poleđini pisma ili fotografije. Često su se i označavala slova u knjizi ili časopisu. Tako da bi na prvi pogled knjiga izgledala sasvim obično, ali čitanjem slova označenih tintom prava poruka bi dobivala smisao. Nevidljivo pisanje može se kombinirati sa šifriranjem. Tada ako neželjeni promatrač uspije učiniti tintu vidljivom, sve što mu je dostupno je šifrat, kojeg ne zna dešifrirati.

Postoje stotine različitih vrsti tajnih tinti, a najbolje su one za čiji pripravak je potrebna rijetka kemikalija. Takvi spojevi su teško dostupni, pa samim time otežavaju otkrivanje poruke. Neki kemijski spojevi, prvobitno nevidljivi na papiru, postaju crveni ili plavi u doticaju s drugom tvari, koja se naziva reagens. Uloga reagensa je poticanje kemijske reakcije, koja će tintu učiniti vidljivom. Dosta spojeva, koji se mogu koristiti za ovakav način pisanja poruke, mogu biti opasni. Za njihovo rukovanje potrebne su velike mjere opreza. U daljnjem tekstu spominjat će se sigurne metode i tinte razvrstane u nekoliko skupina:

- tinte koje reagiraju na toplinu,
- tinte koje pocrvene,
- tinte koje svijetle pod crnim svjetlom,
- tinte vidljive nakon pudranja,
- tinte koje reagiraju na vodu,
- pismo vidljivo pod kosim svjetlom.

Sok skoro svih agruma (npr. limuna, grejpa, naranče), sok luka i „mlijeko" biljke mlječike može se koristiti kao tinta koja reagira na toplinu. Poruka se piše tankim kistom za slikanje, a ne kemijskom olovkom kako na papiru ne bi ostali tragovi pisanja, što bi moglo dovesti do lakšeg otkrivanja teksta. Treba se pisati na hrapavom, a ne glatkom papiru, da se tinta ne osuši na površini nego upije i tako ostane očuvana. Poruka se otkriva tako da se papir lagano zagrijava pomoću žarulje koja isijava toplinu ili nekog drugog slabog izvora topline. Vatra se ne upotrebljava jer bi se papir previše zagrijao, a možda i zapalio. Zbog organskog podrijetla tinte bogate ugljikom, dolazi do izlučivanja čađe, pa napisano posmeđi.

Primjer tvari koja pocrveni je bijeli kristalni prah fenolftalein. On je jedan od najpoznatijih kemijskih indikatora i poznati sastojak laksativa. U lužnatoj okolini mijenja boju u crvenu. Zato ga mađioničari često koriste za trik pretvaranja vode u vino. Postupak pisanja nevidljive poruke fenolftaleinom je sljedeći: pomiješati prah čiste tvari ili zdrobljenu tabletu laksativa sa 70-postotnim alkoholom. Prah mora biti posve otopljen da bi bio spreman za upotrebu. Nakon toga kistom ispisati željeni tekst. Poruka se otkriva tako da se krpica namoči lužnatim sredstvom (može poslužiti sredstvo za čišćenje s amonijakom) i njome pažljivo prijeđe po papiru.

Sljedeća skupina simpatetičkih tinti svijetli pod ultraljubičastim zračenjem, koje se naziva i crno svjetlo. One se koriste kao žigovi na zabavama, koncertima i zabavnim parkovima. Pomoću njih se identificira osoba koja je već platila ulaznicu, a želi ponovno ući. S druge strane koriste se i u bankama za potpise i identifikacijske kartice. Tako čine njihovo poslovanje sigurnijim. Najlakši način stvaranja ovakve tinte je otapanje u vodi bilo kojeg praška za pranje rublja koji izbjeljuje odjeću. Ultraljubičasto zračenje iz sunčevih zraka aktivira umjetne tvari koje potiču izbjeljivanje. Da bi se moglo komunicirati ovom metodom potrebno je pribaviti neku vrstu fluorescentne lampe koja zrači crno svjetlo. Pri korištenju lampe treba biti pažljiv i koristiti zaštitu za oči. Kako bi se postigla najbolja smjesa praška i vode, potrebno je eksperimentirati s omjerima. Previše praška može uzrokovati da je tinta odmah vidljiva na papiru, a previše vode smanjiti sjaj. I ovdje je važna vrsta papira. Najbolji je tamniji s grubom površinom, jer obični bijeli papir sam po sebi bliješti pod crnim svjetlom.

Slijede tinte vidljive nakon nanošenja pudera. Najbolji primjer je obično mlijeko. Nanese se kistom na deblji papir ili tanki karton te ostavi da se osuši. Napisano se razotkrije kada se utrlja puder bilo koje tamnije tvari. Može poslužiti pepeo, grafitna olovka ili drveni ugljen.

Nadalje, postoje mnoge kemijske formule, koje u doticaju s vodom postaju vidljive. Ovdje ćemo spomenuti slabo znanu metodu za isti efekt, ali koja ne koristi nikakvu tintu. Umjesto toga upotrebljava se vodeni žig. Primjenom pritiska mijenjaju se vlakna papira ostavljajući trag vidljiv samo kada je papir mokar. Potrebno je namočiti papir i staviti ga na ravnu tvrdu površinu. Na njega staviti novi suhi papir i tada napisati poruku olovkom ili kemijskom kako bi ostao trag od pritiska. Potom se uništi suhi papir, a napisano je vidljivo na mokrom papiru. Nakon sušenja napisano nestaje i ponovno se pojavljuje ako se uroni u vodu.

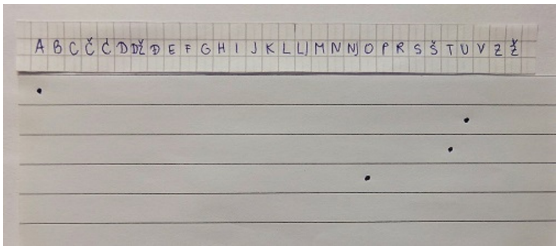
Posljednja metoda također koristi pritisak za promjenu vlakana papira. I ovdje se stavljaju dva papira jedan na drugi, ali oba moraju biti suha. Napiše se poruka i uništi gornji list. Pismo na drugom papiru može se vidjeti kada svjetlost pod određenim kutom pada na list ili u mračnoj sobi pomoću male svjetiljke. Snop svjetlosti otkriva bilo kakve nepravilnosti na površini. Često i u filmovima viđamo da se policija služi istim trikom. Zbog učinkovitosti lako rekonstruiraju što je pisalo na iskinutoj stranici neke bilježnice i bloka. Istu stvar moguće je napraviti pomoću pisaće mašine. Samo se umetnu dva lista, napiše

poruka i opet uništi ona stranica na kojoj je vidljiva tinta. Kako bi se dodatno zaštitili od presretanja poruke, moguće je napisati pogrešno pismo na list papira, a potom preko njega staviti novi papir i pisati između redaka prvog pisma pravu poruku. Nakon uništavanja gornjeg papira ostaje list na kojemu je nevidljiva poruka smještena između redova vidljive nevezane poruke.

2.2. Zanimljive metode slanja poruke

Kroz povijest se pojavljivao veliki niz različitih metoda slanja poruka. Neke od njih bile su doista domišljate, a neke čak i krajnje neobične. Primjerice, Grci su znali svojim glasnicima obrijati glave, poruku napisati na tjeme i čekati dok kosa naraste. Glasnik naizgled ne nosi ništa sporno i može lako proći pored protivnika. Kada bi stigao do odredišta, obrije glavu i pokaže primatelju poruku. Zabilježeno je i da su sa drvenih pločica za pisanje skidali vosak, na drvetu urezali poruku i ponovno pločicu prekrili voskom. Stražarima se sve činilo normalno i poruka bi se lako dopremila na cilj, gdje bi upućena osoba samo sastrugala vosak i pročitala sadržaj. Stari Kinezi bi pisali svoje poruke na tankoj svili, koju bi zgužvanu natopili voskom. Takva loptica davala bi se glasniku da je proguta. Još jedan primjer je pisanje mješavinom octa i aluminijeve soli po ljusci jajeta. Jaje se skuha i pošalje primatelju. Skidanjem ljuske otkriva se poruka na stjenkama kuhanog jajeta. U II. svjetskom ratu Nijemci su razvili fotografsku metodu prikrivanja poruka pomoću sitnih točkica. Cijelu stranicu papira bi fotografirali i sliku umanjili do veličine obične točke. To su samo neke od domišljatijih metoda, a one koje slijede su vrlo jednostavne i moguće ih je koristiti svakodnevno.

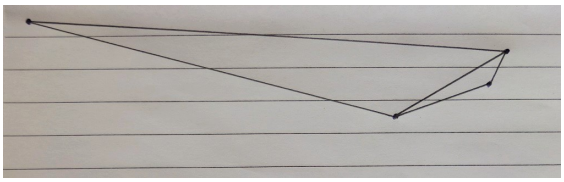
Prva je kôd pomoću točki. Za komuniciranje je potrebno imati dva komadića papira u obliku pruge. Svaka strana ima svoj primjerak, a oni su identični. Na papirić se zapišu slova abecede između kojih je jednak razmak. Mogu biti poredana u pravilnom poretku, ali ako su pomiješana, kôd je teže probiti. Za tajnu poruku koristi se papir s linijama. Šifriranje riječi AUTO izgleda ovako. Listić s abecedom stavi se ispod prve horizontalne linije na papiru i pritom se poravnaju lijevi rubovi. Iznad prvog slova riječi, u ovom slučaju A, označi se točkica. Pruga s abecedom se pomiče jedan redak ispod i točkica se stavlja iznad drugog slova – U. Postupak se ponavlja do kraja riječi ili poruke. Svaka točkica predstavlja jedno slovo.



Slika 1: Kôd pomoću točkica

Problem je što bilo tko može dešifrirati poruku ako ima isti papirić s abecedom. Kako bi se prikrila važnost točkica i zbunilo neprijatelja, moguće je točkice spojiti linijama. One

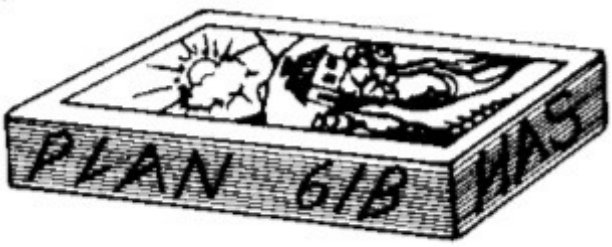
se ne smiju presijecati jer bi njihovo sjecište izgledalo kao još jedna točkica za slovo. Sada slika izgleda kao dijagram ili mapa (Slika 2). To ni na koji način ne utječe na dešifriranje. Umjesto točkica moguće je napraviti male rupice u papiru. Ako su dovoljno sitne, teško ih je primjetiti. Na isti list može se napisati poruka za zavaravanje, što će još više zbuniti promatrača.



Slika 2: Kod pomoću točkica i linija

Umjesto točkica nekad se upotrebljavaju čvorovi. Šifriranje i dešifriranje odvijaju se na isti način pomoću slova abecede. Ovdje je potrebno ostaviti veći razmak među slovima jer je potrebno više mjesta za pravljenje čvorova. Duž pruge sa slovima stavi se komad užeta ili neke druge niti tako da početak s lijeve strane odgovara početku papirića sa slovima. Na mjestu prvog slova željene riječi sveže se čvor. Zatim se uže pomakne ulijevo tako da je prvi čvor poravnat s početkom pomoćnog papirića. Naravno, isto se ponavlja do kraja poruke. Kada je postupak završen, rezultat je komad užeta s mnogo čvorova, koji su neupućenom promatraču smješteni nasumično.

Sljedeće pomagalo za prenošenje tajnih poruka je špil igračih karata. Bolje je koristiti karte za poker, kojih ima 52. Njihov poredak u špilu je unaprijed dogovoren na proizvoljan način. Kada se karte slože pravilnim redoslijedom, poruka se napiše s bočne strane po rubovima.



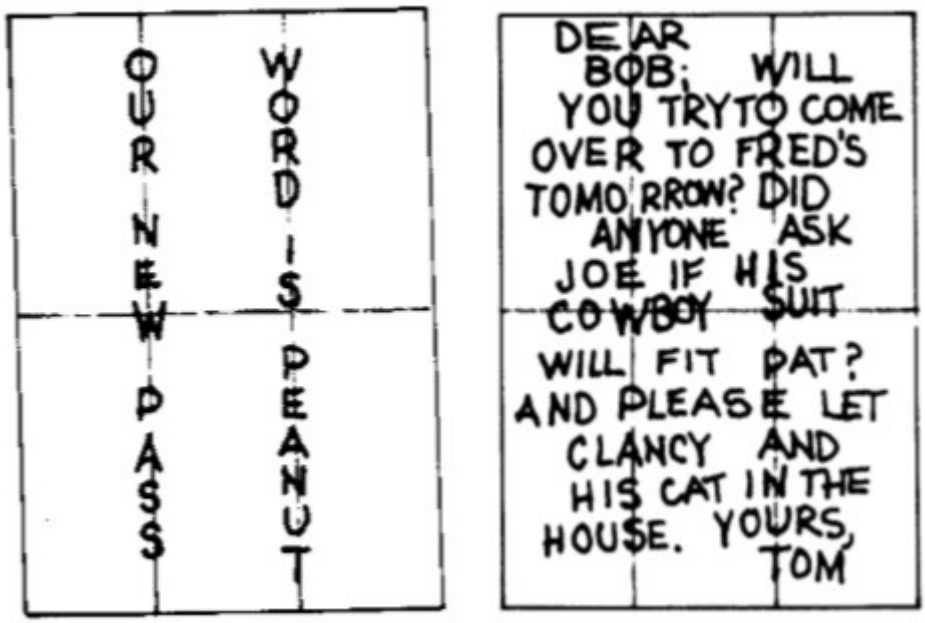
Slika 3: Šifriranje pomoću igračih karata

Karte se zatim promiješaju što više puta i poruka više nije vidljiva. Primatelj vrati karte u dogovoreni poredak i postupak dešifriranja je gotov. Ako je tekst pisan olovkom, isti špil se može koristiti više puta. Jednostavno se obriše prethodna poruka i napiše nova.

Crveni celofan za umotavanje poklona može se pronaći u mnogim trgovinama, a dobra je stvar za brzo šifriranje poruke. Prvo se piše lažna poruka ili nacrta bilo kakav crtež

korištenjem crvene kemijske olovke. Tajna poruka se potom nanosi plavom tankom kemijskom da se napisano slabo uočava. Po mogućnosti treba pisati točno na crvene tragove, a ne u bijele praznine. Kako bi se pročitala poruka, papir se prekrije crvenim celofanom. Sada nestaje napisano učinjeno crvenom kemijskom, a plave linije su jasne i čitke.

Postoji zanimljiva metoda tajnog komuniciranja za koju je potreban samo list papira i olovka. Papir se presavije tri ili više puta tako da ostanu vidljivi nabori. Ponovno se otvori i napiše poruka duž vertikalnih linija vidljivih od savijanja. Potom se ostatak ispuni različitim slovima ili se osmisli pismo, koje će zavarati protivnika kao što je prikazano na Slici 4. Čitanje poruke je lako. Samo se prate slova po naborima i pravi smisao je otkriven. Ako je u pitanju veći tekst, umjesto pisanja slova po naborima, mogu se na isti način pisati riječi. Opet se u praznine napišu riječi za zavaravanje i postupak je gotov.



Slika 4: Šifriranje presavijanjem papira

Plastični štapići za miješanje pića, koji se koriste u kafićima, zadnji su u nizu zanimljivih i neobičnih pomagala za šifriranje i skrivanje poruka, koje ćemo spominjati. Kroz takve štapiće moguće je gledati jer su prozirni. Imaju neobično svojstvo, ponašaju se kao cilindrične leće. Ako se kroz njih pokuša čitati tekst, to će biti težak posao, jer okreću sliku naopačke, tj. stvaraju zrcalnu sliku slova. Tajna poruka se piše korištenjem zamjenske abecede prikazane na Slici 5, pa je ovo jedna od supstitucijskih šifri.

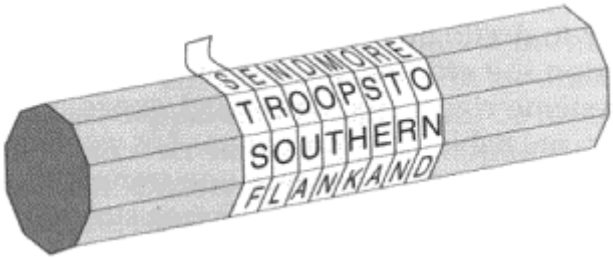
Slika 5: Zamjenska abeceda za šifriranje pomoću plastičnog štapića

Dešifriranje je gotovo istog trena kada se poruka pogleda kroz spomenuti štapić. U slučaju da primatelj pri ruci nema takav štapić, može se poslužiti sljedećim trikom. Okrenuti poruku naopačke i pogledati ju pomoću zrcala.

2.3. Skital

Skital ili *scitala* je prvi kriptografski uređaj u povijesti. Naziv je dobio po grčkoj riječi za palicu. Prvi puta je upotrijebljen u petom stoljeću prije Krista. Najviše su ga koristili Spartanci. Skital je **drveni štap** oko kojeg se omota **vrpca**. Prvobitno je vrpca bila od kože ili pergamenta, ali može se iskoristiti bilo koja tanka tkanina ili papir. Pošiljatelj na namotanoj traci napiše otvoreni tekst, a kada se odmota, izgleda kao da je na njoj napisan besmislen niz slova. Glasnici su nerijetko prenosili vrpcu tako da ju omotaju oko struka kao remen. Nimalo sumnjičavi poruku bi dostavili primatelju, koji mora imati štap istog promjera kao onaj kojeg je koristio pošiljatelj. Traku omota oko skitala i dešifriranje je gotovo. Ovo je primjer transpozicijske šifre.

Pretpostavlja se da je skital korišten u vojne svrhe, za komunikaciju tijekom bitke. Neki povjesničar smatraju da skital nije korišten za šifriranje. Razlog tomu je njegova jednostavnost. Protivnik samo treba pronaći štap iste debljine i saznaje tajnu poruku. Njihovo mišljenje je da je korišten kao sredstvo autentifikacije, kako neprijateljski špijuni ne bi mogli poslati lažne poruke i zavarati dvije strane koje komuniciraju skitalom.



Slika 6: Skital

2.4. Albertijev disk

Leon Battista Alberti rođen je 1404. godine i bio je firentinski slikar, skladatelj, pjesnik, arhitekt i filozof. Rođen u bogatoj trgovačkoj obitelji, imao je izvanredne intelektualne i atletske osobine. Bio je jedan od vodećih ličnosti renesanse. Napisao je prvu tiskanu knjigu o arhitekturi i utjecao na mnoge generacije iza njega.

Ali to nije sve što se tiče njegove svestranosti. Zbog svog doprinosa modernoj kriptografiji, zaradio je titulu „oca zapadne kriptografije“. On je bio prvi od grupe pisaca, koji su malo po malo razvili vrste šifriranja, koje su temelji moderne kriptografije. Alberti je zaslužan za razvoj *polialfabetske supstitucijske šifre*. Na razmišljanje o kriptografiji naveo ga je njegov prijatelj Leonardo Dato, tadašnji biskupski tajnik. Jednog dana tijekom šetnje Vatikanskim vrtovima, Dato je potaknuo temu šifriranja. Pitao je Albertija je li promišljao o novim mogućnostima u toj disciplini; na što je dobio obećanje da će pokušati nešto napraviti u vezi toga. I napravio je. U šezdesetdrugoj godini života napisao je esej o kriptoanalizi. Bio je to zapadnjački najstariji tekst o kriptoanalizi. Tek nakon toga što je objasnio kako se šifrati dešifriraju, počeo je razmišljati o načinima koji bi mogli otežati dešifriranje šifrata. Izmislio je šifru za koju je govorio da se ne može probiti. Zvao ju je „dostojnom kraljeva“. Naravno, to je šifrirajući disk, danas poznat kao *Albertijev disk*.

Disk se sastojao od **dva bakrena kruga**. Jedan je bio veći i zvao se statični, a drugi je bio manji i nazivao se pomični. Promjer statičkog kruga bio je za jednu devetinu veći od pomičnog kruga. Prednju stranu diskova podijelio je u 24 jednaka dijela, koje je nazvao poljima. U polja na velikom krugu upisao je velikim crvenim slovima slova abecede u pravilnom poretku, s time da je izostavio slova H, K i Y jer nisu bila potrebna za razumijevanje poruka. Tako je iskoristio 20 polja (latinska abeceda nije sadržavala slova J, U i W). U preostala četiri polja upisao je brojeve od 1 do 4 crnom bojom. 24 polja malog kruga ispunio je malim slovima abecede crnom bojom, ali ne u pravilnom poretku nego nasumično. Iako je koristio dvije različite boje, one nisu imale nikakvog značaja u šifriranju. Kada su sva slova ispisana na oba kruga, manji se postavi na veći i kroz sredinu se umetne igla, koja služi kao os oko koje se manji (pomični) krug može rotirati.

Sugovornici moraju imati identične diskove. Prije komuniciranja trebaju dogovoriti **in-**

Slika 7: Albertijev disk

deksno slovo u pomičnom krugu. Pošiljatelj poruke određuje poziciju unutarnjeg kruga, tj. s kojim će slovom velikog kruga upariti indeksno slovo. O toj odluci obavještava primatelja na početku šifrata. Sada svako slovo pomičnog kruga ima odgovarajuće slovo u statičnom krugu. Veliki krug sadrži slova koja predstavljaju otvoreni tekst, a mali krug šifrat. Revolucionarnost njegovog diska došla je do izražaja u naputku da se nakon tri, četiri riječi promijeni pozicija indeksnog slova. Prilikom promjene pozicije, pošiljatelj prije novog šifriranja u šifrat ubaci slovo koje sad predstavlja indeks na vanjskom krugu. Ta promjena znači da se u jednom dijelu poruke riječ DA šifrira u KD, a u drugom dijelu u MN i tako dalje. Svaka nova postavka Albertijevog diska donosi novu abecedu za šifriranje. Postoji onoliko različitih vrsta abeceda, koliko ima pozicija diska.

Alberti je dodao još nešto što disk čini posebnim: u jednoj tablici permutirao je znamenke od 1 do 4 tako da čine dvoznamenkaste, troznamenkaste i četveroznamenkaste brojeve (od 11 do 4444). Tablica je služila za dogovaranje kodova. Primjerice, 12 bi moglo značiti „Kreni u napad!“, a 434 „Povlačenje!“. Na isti način kao i slova, šifrirali bi se kodovi.

Tri sjajne prve stvari učinile su ovog svestranog intelektualca jednim od bitnijih ličnosti krptografije. To su prvo zapadnjačko proučavanje kriptoanalize, prvo korištenje polialfabetske supstitucije i prvo korištenje šifriranih kodova.

2.5. Jeffersonov kotač

Thomas Jefferson rođen je 1743. godine. Bio je glavi pisac Deklaracije nezavisnosti, prvi tajnik države, drugi podpredsjednik i treći predsjednik Sjedinjenih Američkih Država. Protivio se ropstvu i poticao demokraciju.

Prije nego što je postao državni tajnik (u kasnim 1780-ima), radio je kao ministar za Francusku, što bi se moglo usporediti s današnjim veleposlanikom. Na ministarskom mjestu

bio je zadužen za pregovore o komercijalnoj trgovini s Engleskom, Španjolskom i Francuskom. U to vrijeme spremala se velika revolucija, što je utjecalo na Thomasovu komunikaciju s SAD-om. Svaka pošta koja je dolazila ili odlazila bila bi otvarana i pregledavana od strane različitih redarstvenika. Kako bi informacije zadržao tajnima, Jefferson je osmislio napravu, kojom je uspješno šifrirao bilo koju poruku, a promatrači ju nisu mogli razumjeti. Iako nema potvrđenih informacija, smatra se da je ideju dobio od stare kineske naprave, preteče današnjeg lokota.

Za kotač je koristio **komad drveta valjkastog oblika** promjera oko 5 cm i dužine oko 20 cm. Kroz sredinu valjka probušio je rupu kako bi kroz nju provukao željeznu iglu, koja je služila kao os. Vanjski dio drveta (plašt) je podijelio na 26 jednakih dijelova (kasnije verzije često su imale manji broj). Olovkom je nacrtao paralelne linije duž cijelog drveta i zatim izrezao svaki od 26 dijelova. Režući bi označavao brojevima diskove koji nastaju. Na taj način ih je mogao poredati po želji. Na svakom disku ispisao je slova abecede, po jedno slovo između dvije paralelne linije. Slova nije pisao pravilnim poretkom nego je proizvoljno odabrao redoslijed. Nijedna dva diska pritom ne smiju imati isti poredak. Sada se spoje svi diskovi i pričvrste tako da tvore jednu cjelinu.

Slika 8: Jeffersonov kotač

Šifriranje otvorenog teksta odvija se tako da se na prvom disku kotača pronađe odgovarajuće slovo. Potom na drugom disku drugo slovo i postavi pored prvog. Postupak se nastavlja do zadnjeg slova. Na kraju se dobiju sva slova poruke poredana jedno do drugoga u jednom retku. Preostali retci predstavljaju moguće šifrate. Na pošiljatelju je da odabere jedan i pošalje ga primatelju. On na svojem primjerku kotača mora imati diskove nanizane istim poretkom. Slovo po slovo vrti diskove dok ne složi u jedan redak cijeli šifrat. Potom okreće kotač i pronalazi redak koji sadrži smislenu poruku, to je njegov otvoreni tekst. Preporučuje se mijenjanje redoslijeda diskova nakon svake poruke, jer će to otežati dešifriranje neželjenom promatraču.

Da je Jefferson potaknuo korištenje svoje naprave za njegova predsjedništva, gotovo sigurno bi mogao komunicirati bez straha da će itko probiti šifru. No, čini se da ju je bio

zaboravio, jer se nije spominjala do 1922. godine. Tada je otkrivena među njegovim starim spisima. Koliko je bio ispred svog vremena pokazuje činjenica da je iste godine američka vojska počela koristiti gotovo isti uređaj misleći da je tada otkriven. Dugi niz godina nakon toga Jeffersonov sistem se aktivno koristio u mornarici i drugim granama vlade. Zbog toga je danas poznat kao „otac američke kriptografije“.

3. Složene naprave

Krajem 19. i početkom 20. stoljeća pojavljuju se prvi radio odašiljači i prijemnici. Time započinje razvoj bežične tehnologije. Radio je donio lakoću komuniciranja, ali ubrzo je do izražaja došla i njegova slabost. Naime, poruke odaslane radio valovima bez problema su se mogle presresti i uhvatiti. Vojska je sada imala odlično sredstvo razmijene informacija, ali nije znala kako zajamčiti njihovu sigurnost.

U isto vrijeme javlja se želja za poboljšanjem nepraktičnih šifri, koje su se izvodile ručno i oduzimale dosta vremena. Također, više nije postojala nijedna sasvim sigurna metoda šifriranja. Sve su bile probijene i nesigurne za primjenu u važnim situacijama. Navedeni razlozi doprinijeli su izumu elektromehaničkih naprava, koje su zauvijek promijenile i unaprijedile kriptografiju. U sljedećoj tablici nabrojanje su najpoznatije naprave za šifriranje i države iz kojih potječu. Detaljnije ćemo obraditi neke od njih.

Naprava	Zemlja podrijetla
Discret	Njemačka
Enigma	Njemačka
Lorenz	Njemačka
Sigaba	SAD
Hagelin	Švedska
NEMA	Švicarska
Gretag	Švicarska
Fialka	Rusija
Race	Norveška
DUDEK	Poljska
Purple	Japan
Typex	Velika Britanija

Tablica 1: Najpoznatije naprave za šifriranje

3.1. Enigma

Najvažnija i najpoznatija naprava za šifriranje je *Enigma*. Njena povijest započinje izumom naprava za šifriranje temeljenih na pokretnim rotirajućim diskovima. Nekoliko izumitelja otprilike u isto vrijeme napravilo je svoju verziju takvog uređaja neovisno jedan o drugome. U Njemačkoj je to bio Arthur Scherbius. Prvu Enigmu sastavio je 1918., ali u javnost je puštena nakon nekih preinaka 1923. Tijekom godina javljale su se različite verzije, a ovdje ćemo spomeniti standardni model. Sastojao se od sljedećih dijelova spojenih električnim vodovima (žicama):

- **tipkovnice**,
- **premetačke jedinice**,
- **displeja**,

- **reflektora**,
- **razvodne ploče**.

Šifriranje počinje pritiskom tipke željenog slova na tipkovnici. Razvodna ploča mijenja utipkano slovo u neko drugo ovisno o njenim postavkama. Novo slovo dolazi do premetačke jedinice sastavljene od 3 premetala (rotora, rotirajuća diska), gdje se mijenja u neko drugo slovo. Premetala imaju 26 kontakata s jedne i druge strane za ulaz i izlaz električnih impulsa. Unutar svakog diska nalazi se splet žica kroz kojeg impulsi putuju. Upravo taj splet određuje kako će se koji znak šifrirati. Nakon premetala impuls dolazi do reflektora koji ga vraća natrag kroz premetala do razvodne ploče i konačno displeja sa žaruljicama na kojem se prikazuju slova šifrata. Za pravilno komuniciranje pošiljatelj i primatelj morali su znati dogovorene postavke svih premetala, reflektora i razvodne ploče.

Temelj za razbijanje Enigmine šifre postavili su Francuzi skupljanjem različitih podataka, koje nisu u potpunosti znali iskoristiti. Stoga su ih proslijedili saveznicima u Poljskoj. Zbog blizine Njemačke i prijetnje koju je predstavljala, oni su bili znatno više motivirani. Najveće napore u otkrivanju načina funkcioniranja naprave učinio je M. Rejewski. Nakon duge analize uspio je napraviti uređaje (*bombe*), koji su u roku od 2 sata rješavali šifrate. No, tada se stvari kompliciraju, jer Nijemci dodaju još dva premetala svom uređaju. Posao dešifriranja nastavljaju Englezi smješteni u Bletchley parku, britanskoj centralnoj ustanovi za kriptoanalizu, pod vodstvom A. Turinga, britanskog matematičara, kriptoanalitičara i znanstvenika. On je sastavio još bolje bombe, koje su provjeravale konfiguraciju premetala na temelju pretpostavljenog sadržaja poruke. Zahtjevan rad Rejewskog i Turinga pokazao se uvelike značajan za tijek rata i cijele povijesti.

Enigma je služila kao osnova razvoja mnogih drugih naprava. No, svaka je imala nešto po čemu je bila posebna i drugačija od ostalih. Bit će to vidljivo u nastavku rada, kada donosimo neke od njih.

3.2. Purple

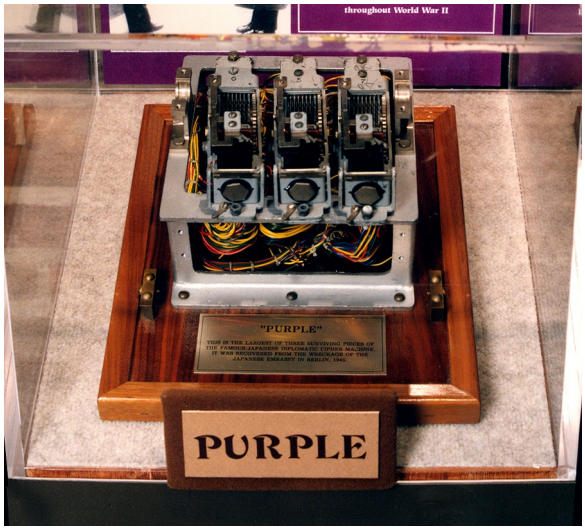
Japanski doprinos napravama za šifriranje započinje kupnjom jedne od verzija Enigme. Modificirali su ju kako bi dobili veću sigurnost, dodali određene specifikacije i nastala je naprava kodnog imena *Red*. Upotrebljavala se za šifriranje diplomatskih spisa najveće tajnosti u komunikaciji Japana sa svojim agencijama diljem svijeta i po tome je dobila ime, jer eng. *red* = crveno. 1936. godine probijen je njen princip rada zahvaljujući naporima američke vojske. Japan nije dozvolio otkrivanje svojih tajni, pa su već 1939. uveli novi, još sofisticiraniji uređaj za šifriranje – *Purple*. Ime su mu nadijenuli Amerikanci po boji omota za spise povezane s tom napravom.

Purple je bio zahtjevan u 1930-tima, ali je kompliciran tehnička naprava čak i za današnje pojmove. Sastojala se od tri važna dijela:

pisaće mašine - koja se koristila za unos podataka;

seta za šifriranje - čiji su sastavni dijelovi bili razvodna ploča, 4 električna premetala i niz žica i prekidača, koji su zajednički radili s ostatkom;

jedinice za ispis - pomoću koje se ispisivao šifrat upisane poruke.



Slika 9: Purple

Cijela naprava bila je jako teška, pa ju nije bilo lako upotrebljavati na bojištu. Pisaća mašina podržavala je tri različita pisma: latinicu, englesko pismo i romaji pismo, koje je sustav za prevođenje japanskog pisma na latinicu. Srce cijele naprave bila je premetačka jedinica. Ona, za razliku od Enigme, nije imala rotirajuće diskove kao premetala, nego posebnu vrstu zupčanika. Nalazili su se između pisaće jedinice i razvodne ploče. Tijekom tipkanja, svaki zupčanik bi konstantno mijenjao poziciju u odnosu na druge i time kompliciraо šifriranje slova otvorenog teksta. Značajno je bilo to što su zupčanici mijenjali položaj za varirajući broj koraka (ne svaki put za jedan korak). No, prije dolaska do premetala, slovo bi već jednom bilo promijenjeno. Uzrok tome je razvodna ploča. Njene postavke mijenjale su se od poruke do poruke na proizvoljan način, isto kao i postavke premetačkih zupčanika.

Postupak dešifriranja počinje pravilnim namještanjem razvodne ploče i zupčanika. Te ključne informacije su unaprijed dogovorene ili na neki način primljene od pošiljatelja. Kada je naprava spremna, sve što operater mora učiniti je utipkati šifrat i otvoreni tekst biva ispisan na papir.

Jedno ograničenje Purplea bilo je nemogućnost šifriranja brojeva i interpunkcijskih znakova. Svaki operater je imao knjigu kodova. Pošiljatelj bi u njoj morao potražiti potreban broj ili znak te utipkati odgovarajući kôd. Isti postupak ponavljao je primatelj. Drugo ograničenje je njena težina, koja je otežavala uporabu na bojištu i zbog toga je bila nepraktična.

Najvažniju ulogu u razbijanju Purpleove šifre imao je W. F. Friedman, američki kriptograf i član SIS-a (Signal Intelligence Service), odijeljenja za kriptoanalizu pri američkoj vojsci. Međutim, posao nije bio lak. Odjel je imao jedan od najtežih zadataka pred sobom. Bili su suočeni s mukotrpnim zadatkom pronalaženja obrazaca ponavljanja ili bilo kakve strukture u sakupljenim šifratima. Koliko je to bilo zahtjevno kazuje činjenica da je Friedman nakon 18 mjeseci rada doživio živčani slom.

Prvi korak u razbijanju šifre je skupljanje podataka. Japanci su koristili nekoliko naprava u svom komuniciranju. Purple je služio samo za najbitnije diplomatske informacije, a takvih poruka je bilo najmanje, pa je moralo proći dosta vremena da bi bili uspješni. Kada se skupilo dovoljno materijala, sljedeći korak bio je utvrđivanje kombinacije vodova unutar mašine. Zadatak nije bio trivijalan, ali imali su malu prednost – sustav šifriranja naprave Red bio je probijen nekoliko godina prije. Na temelju toga kriptoanalitičari su mogli pretpostaviti bar dio mehanizma nove naprave. Pomagalo im je i to što su došli u doticaj s kodnim knjigama japanske mornarice, pa su bili upoznati s time na koji način salutiraju i završavaju poruke. U periodu prelaska sa šifriranja pomoću Reda na šifriranje pomoću Purplea, neke poruke pisane su pomoću obje naprave. Japan nije shvatio da time pomažu šifrolomcima, jer su šifrate mogli analizirati uz pomoć već probijene šifre. Nespretnost je bila vidljiva i u slučaju pogreške operatera tijekom pisanja. Tada bi istu poruku poslali korištenjem drugog ključa.

Nakon napornog rada, Amerikanci su napokon uspjeli pronaći način na koji se otvoreni tekst transformira u šifrat. Do 1940. napravili su 8 replika Purplea, a bez da su ikada vidjeli pravu napravu. Sada su uz poznavanje ključa, kojim je poruka pisana, mogli odmah dešifrirati materijale prikupljene na terenu. Završni korak bio je otkrivanje obrazaca za stvaranje ključeva. Shvatili su da su ključevi za jedan mjesec podijeljeni u 3 grupe, tj. mjesec je podijeljen u grupe od po 10 dana. Nadalje, uočili su da je ključ za prvi dan jedne desetodnevne grupe povezan s ključevima preostalih 9 dana tako se ostalih dana na određeni način permutira početni ključ. U druge dvije desetodnevne grupe način promjene ključa u narednih 9 dana bio je isti kao u prvoj grupi. Stoga su poznavanjem ključa prvog dana mogli znati ključeve za idućih 9 dana. Bilo je to sve što je potrebno za konačno probijanje šifre.

Po Davidu Kahnu probijanje Purplea je najveći podvig kriptoanalitičara do tada, pa nije čudo da su dešifrirane Purpleove poruke dobile kodno ime *Magic* (eng. magic = magija, čarolija). Kako bi što duže zadržali prednost nad Japanom poznavajući njihove tajne poruke, samo mali broj osoba bio je upućen u postojanje Magica. Vodeći ljudi SAD-a nisu htjeli dozvoliti curenje informacija, koje bi dovelo do promjene u šifriranju japanskih poruka. Zbog strogog čuvanja tajne probijanja japanske šifre, pojedinci koji su trebali za nju znati, nikad nisu saznali.

Budući da Japanci više nisu imali način sigurne komunikacije, mnogi se pitaju zašto nije spriječen napad na Pearl Harbor. Iako nikad nije postojala poruka s direktnom uputom za

napad, danima prije javili su se znakovi za uzbunu. Proslijeđene su upute svim saveznicima da unište svoje naprave za šifriranje i važne dokumente. To je trebalo biti upozorenje da se nešto sprema. No, upozorenje nije imao tko uočiti. Naime, u SIS-u je nedostajalo ljudi za analiziranje velikog broja poruka, koje su stizale u njihov ured. Razlog tomu je nedostatak novaca. Tako je zbog bizarnih stvari potencijal Magic podataka ostao tek djelomično iskorišten.

3.3. Typex i Sigaba

Britanska kopija Enigme zvala se *Typex*. Bila je to elektromehanička naprava razvijena 1934. Njen izumitelj je zapovjednik O. G. W. Lywood, koji je imao pomoć od nekoliko poznanika iz RAF-a (Royal Air Force). Oni su se zbog vlastitog entuzijazma upustili u razvoj nove naprave, koju je kasnije RAF usvojio za potrebe svoje tajne komunikacije.

S lijeve strane mehanizma nalazio se **reflektor**, a s desne **ulazni disk**. Princip šifriranja temeljio se na **5 premetala** smještenih između reflektora i ulaznog diska, od kojih prva dva s desne strane ostaju statička (mogli su se proizvoljno namjestiti, ali nisu se kretali tijekom šifriranja). Imali su mogućnost promjene položaja za proizvoljan broj koraka. Typex je imao i **razvodnu ploču**, koja je omogućavala namještanje reflektora na bojištu. U Velikoj Britaniji ostala je u upotrebi do 1950-tih, kada je zamijenjena modernijim uređajima, a u nekim zemljama (npr. Kanadi) zadržala se i desetak godina duže. Očuvani primjerci mogu se pronaći u muzeju u Bletchley Parku.

Sigaba je američka naprava za šifriranje, koja se također temelji na principu elektromehaničkih rotora. Proizvedena je 1930-tih kao udruženi pothvat vojske i mornarice. Smatrali su ju superiornom što se kroz povijest i potvrdilo, jer njena šifra nikad nije bila probijena. U upotrebi je bila do 1950-tih.

Sličila je nezgrapnom pisaćem stroju s tipkovnicom s prednje strane. Imala je vlastiti **motor za napajanje** strujom i mogla je ispisivati tekst na traku papira. Imala je **tri grupe od po 5 rotirajućih diskova**. Svaka grupa se nalazila u malom spremniku, koji se lako mogao izvaditi i zamijeniti po volji. Glavna grupa, smještena sa stražnje strane, sadržavala je premetala, koja su bila glavni nositelji šifriranja. Druga grupa, u sredini naprave, služila je za kontroliranje položaja premetala. Treća grupa nalazila se s prednje strane i sastojala se od manjih diskova. Oni se nisu pomicali tijekom šifriranja i zajedno s drugom grupom bili su zaslužni za promjenu položaja premetala.

Pred kraj II. svjetskog rata pojavila se potreba za što sigurnijom komunikacijom između američke i britanske vojske. Obje strane su odlučile da će modificirati po jednu svoju napravu, kako bi postale kompatibilne i omogućile nesmetanu razmjenu informacija. Amerikanci su se odlučili za Sigabu, a Britanci za Typex. Zajedničku napravu nazvali su *CCM*

(Combined Cipher Machine). Iako su imale isti princip rada, američka i britanska verzija razlikovale su se po izgledu. Zanimljivo je da su Amerikanci bili upoznati s Typexom, ali Britancima nikad nisu dali na uvid svoju Sigabu. U godinama poslije rata, zajednički CCM koristio je i NATO.

3.4. NEMA

NEMA je bila elektromehanička naprava za šifriranje, koju je na tržište stavila tvrtka Zellweger AG iz Švicarske. Ime je dobila po početnim slovima njemačke riječi za novu napravu (**neue machine**), a službeni naziv bio je NEMA Modell 45. Tijekom II. svjetskog rata švicarska je vojska koristila jednu od verzija Enigme. Kada su saznali da se njihova komunikacija prati i od strane saveznika i Nijemaca, odlučili su promijeniti sredstvo šifriranja svojih poruka. Enigmu su poboljšali i napravili vlastitu novu napravu. Prototip je stvoren u ranim godinama 1940-tih, a konačna verzija bila je spremna 1947., prekasno za uporabu u ratu. Zato ju je švicarska vojska i diplomacija koristila najviše u poratnim godinama dok nije zamijenjena naprednijim napravama – Hagelinom i Gretagom.

Slika 10: NEMA

NEMA je imala mogućnost korištenja unutarnjeg izvora energije u obliku baterije ili vanjskog izvora pomoću transformatora struje, kako bi se mogla upotrijebiti bilo gdje u svijetu. Njena premetačka jedinica sadržavala je **10 kotačića**, od kojih je samo 5 bilo električki nabijeno. 4 od njih bila su premetala za šifriranje slova s 26 kontakata s obje strane. Peti električni kotačić bio je **reflektor** s mogućnošću pomicanja tijekom šifriranja (Enigmin reflektor nije to mogao). Preostalih 5 kotačića bili su rotirajući diskovi za promjenu položaja premetala. Taj mehanizam davao je premetalima nepravilan način promjene položaja, što napravu čini kompliciranijom, a ujedno i sigurnijom. Kotačić smješten na desnom kraju bio je crvene boje (drugi crne) i kroz njega je struja dolazila do ostalih; zvao se **ulazni kotač**. Na lijevom kraju nalazio se reflektor. Između reflektora i ulaznog kotača smješteni su preostali kotačići po parovima. Jedan par činio je jedno premetalo i jedan kotačić za promjenu

položaja premetala. To znači da je za promjenu položaja premetala zadužen samo onaj kotačić s kojim je uparen. Za postavljanje ključa na temelju kojeg će se izvršiti šifriranje, potrebno je znati unutrašnji i vanjski ključ. Unutrašnji određuje koji je kotačić uparen s kojim premetalom i na kojem se položaju nalaze, a vanjski specificira početni položaj svih diskova mehanizma prije pisanja poruke.

NEMA je imala **displej** s 26 lampica, koji je odgovarao tipkama na tipkovnici. Kako bi se omogućilo slanje poruka, koje će moći vidjeti samo operater, mogao se ugraditi vanjski displej s lampicama. Spojio bi se s napravom preko pomoćnog kabla, koji je zajedno s displejom bio smješten u poklopcu. Uz standardna slova tipkovnica je imala i nekoliko dodatnih tipki za prebacivanje slova i brojeva te ispis. Služila je za šifriranje i dešifriranje poruka.

Poznata su tri različita NEMA modela s nekim značajnim razlikama zbog kojih su međusobno nekompatibilni.

Naprava za trening - koristila se za uvježbavanje operatera. Zbog straha od prodaje mehanizma protivnicima, unutrašnjost je promijenjena u odnosu na naprave, koje su se koristile na bojištu. Ovakvih primjeraka je najviše očuvano, ali su većinom u lošem stanju zbog učestalog korištenja za vježbu.

Naprava za rat - čuvana u skladištu za korištenje prilikom potencijalnog izbijanja rata. Razlikovala se od drugih po dodatnom broju kotačića, drugačijim zupcima na diskovima za promjenu položaja i različitostima u operaciji šifriranja. Rijetko se može pronaći ova verzija.

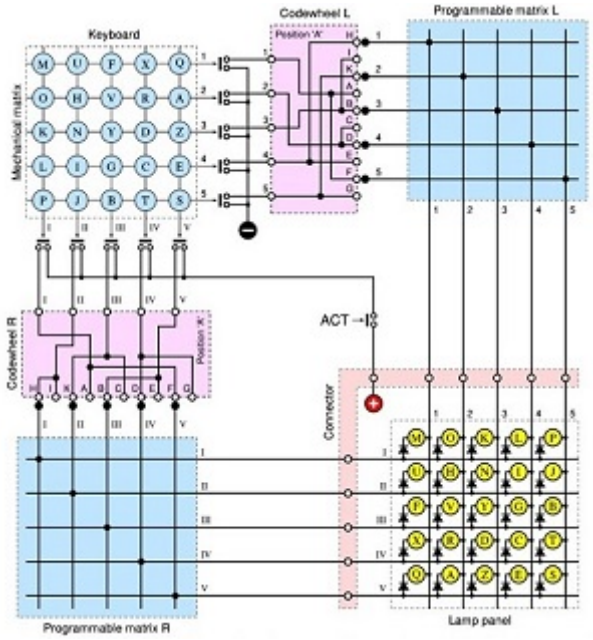
Diplomatska naprava - koja je služila samo za komunikaciju ureda vanjskih poslova. Do danas ova vrsta nije puštena u javnost, pa se ne mogu s preciznošću utvditi sve razlike s obzirom na ostale modele. No, neke su poznate - imala je promjenu u vodovima i u mehanizmu za promjenu položaja premetala.

3.5. Hagelin

Boris Caesar Wilhelm Hagelin bio je švedski izumitelj u povijesti poznat kao najkontroverzniji i najuspješniji proizvođač kripto naprava. U svijet proizvodnje naprava za šifriranje ušao je na nagovor oca K. W. Hagelina i Emanuela Nobela, nećaka poznatog Alfreda Nobela. Oni su odlučili investirati u AB Cryptography, tvrtku na čijem čelu je bio A. G. Damm, jedan od četiri izumitelja naprava temeljenih na rotirajućim diskovima, poznat po svojoj tvrdoglavosti. Kako bi bili sigurni u svoje ulaganje i imali nadzor nad poduzećem, postavili su Borisa Hagelina da prati situaciju. Nije prošlo dugo vremena i Damm je odstupio te je Hagelin preuzeo vodstvo.

Prvi doprinos tvrtki napravio je 1925. kada je za potrebe švedske vlade osmislio svoju napravu *B-21*. Ona kao i sve druge koje će uslijediti nazivane su zajedničkim imenom

Hagelin. Novi direktor dobio je informaciju da se vlada raspituje o Enigmi. Iako nije imao gotov proizvod, ponudio je svoje usluge i obećao da može napraviti još sigurniju napravu iste veličine i tako sklopio dogovor. Nakon dugog razmišljanja odlučio je za temelj šifriranja koristiti 5×5 **matricu**. Naprava je imala **tipkovnicu**, **2 premetala** (čijim pomicanjem su upravljala dva rotora s iglama) i **displej** s 25 električnih lampica za prikazivanje izlaznog pisma (šifrata ili otvorenog teksta). Zbog veličine mreže moralo se izbaciti jedno slovo abecede niske frekvencije ili koristiti jedan znak za dva slova. Najčešće se izbacivalo slovo W, jer se moglo pisati kao dva uzastopna V ili su se poistovjećivala slova I i J. Iako je Hagelin bio mišljenja da je neprobojna, njenu šifru uspjeli su razbiti za 24 sata.



Slika 11: B-21 mehanizam šifriranja pomoću 5×5 matrice

Tipkovnica je bila dizajnirana u obliku mehaničke matrice i spojena s dvije grupe od po 5 električnih **prekidača**. Pritisak tipke aktivira po jedan prekidač u svakoj grupi i uključuje struju. Signal svakog slova putuje preko **premetala** do **programirajuće matrice**. Izlazni podaci obiju matrica spajaju se i aktiviraju lampicu displeja odgovarajućeg slova. Shema za displej jednaka je mehaničkoj matrici tipkovnice. Ovim sustavom nije moguće vršiti dešifriranje. Za njega je potrebna prilagodba mehanizma upotrebom različitih kontakata i vodova.

Nakon Nobelove smrti 1932. prestao je dotok novca u AG Crptography i tvrtka se našla u lošoj financijskoj situaciji. No, spasilo je ih je zanimanje francuske vojske za B-21. Kako bi udovoljio kupcima, Hagelin je morao napraviti dvije preinake: dodati jedinicu za ispis i učiniti napravu mobilnom. Novu verziju nazvao je *B-211*. Poboljšanja su lako ispunjena uklanjanjem displeja s lampicama i ugrađivanjem motora za pokretanje. Francuzi su bili zadovoljni te se njihova ukupna narudžba sastojala od najmanje 600 primjeraka. Time započinje dugogodišnja suradnja između Hagelina i francuske vojske.

Nedugo nakon toga Hagelin dobiva zahtjev za razvijanjem naprave, koja bi mogla stati u džep vojne odore, a i dalje imati funkciju ispisa. Inženjer se hvata toga izazova dobivši inspiraciju u jednom njegovom starom patentu, koji nikad nije dospio u proizvodnju. Ideju za mehanizam dobio je od funkcije za računanje aparata za usitnjavanje novca. Kako bi uspješnije osmislio traženo, u džepu je nosio komad drveta veličine željene naprave. Trud se isplatio i nastaje još jedna Hagelinova naprava pod imenom *C-35*, prva u potpunosti mehanička naprava s mehanizmom *pin and lug*, tj. mehanizmom temeljenim na zupčanicima s iglama. Imala je **5 rotora s iglama**, a svaki je mogao činiti različiti broj koraka i imao je različiti broj igala. Korisnik ih je mogao namještati proizvoljno. Nakon 35-ice uslijedilo je još mašina iste serije (oznaka C), ali sve su bile veće.

Konačno je nastala najpoznatija Hagelinova naprava - *C-38*. Izrađena je za potrebe američke vojske, koja ju je koristila pod nazivom *M-209*. Proizvodila se u Americi pod Hagelinovom licencom, a distribuirana je u 140 tisuća primjeraka. Spretni izumitelj postaje milijunaš, jedan od rijetkih (ako ne i jedini) u grani kripto naprava. C-38 je bila malih dimenzija i lagane kilaže, idealna za upotrebu na bojištu. Najčešće se nosila u torbi kao na Slici 12. Bila je potpuno mehanička i nije imala potrebu za nikakvom vrstom napajanja. Imala je **6 kodnih diskova** vidljivih izvana i smještenih na prednjoj strani naprave. Nije imala tipkovnicu. Otvoreni tekst se unosio slovo po slovo tako da se **kotačić s abecedom** s lijeve strane okrenuo do željenog slova i potom povukla ručka s desne strane. Šifrirano slovo izlazilo je tiskano na papiru.

Slika 12: C-38

Iako je bila dosta dobra za svoje vrijeme, nije se pokazala kriptografski jakom. Njemački kriptolomci redovno su uspijevali probiti njen kôd za manje od 4 sata nakon primitka poruke. Iskoristili su neke njene slabosti kao činjenicu da su se brojevi morali unosti pomoću potpunih riječi. Zato su ju kasnije koristili samo za kraće taktičke poruke, koje nakon 4 sata više nemaju važnost.

Nakon II. svjetskog rata, Švedska je donijela zakon po kojemu su naprave za šifriranje proglašene vojnom opremom i nisu se više mogle izvoziti. Potaknut tom odlukom, Hagelin tvrtku seli u Švicarsku u grad Zug, gdje ubrzo osniva drugo poduzeće - Crypto AG. Proizvodi seriju novih naprava, od kojih su najpoznatije C-*52, CX-52* i *CD-57*. Ove mašine pokazale su se kasnije kao najunosnije u povijesti, jer su distribuirane u preko 120 zemalja diljem svijeta. Koristili su ih za povjerljive diplomatske, vojne i financijske poruke uz potpuno povjerenje prema švicarskoj tehnologiji. Ono što korisnici nisu znali bio je tajni dogovor između SAD-a i Hagelina. Sklopio ga je Friedman, kojeg je NSA 1957. pozvala iz mirovine samo za taj posao. Amerika je dobila uvid u tajnu komunikaciju svih kupaca Hagelinovih naprava. Nadzor njima bitnih država i diktatora trajao je godinama. Javnost je prvu informaciju o ilegalnim radnjama Crypto AG-a dobila tek 1992., kada je u Iranu uhićen jedan njihov zaposlenik H. Buehler pod sumnjom špijuniranja za SAD, zbog prodaje namještenih naprava. Zaposlenik nije ništa znao o tajnom dogovoru i bio je iznenađen optužbama. Nakon nekog vremena, poslodavac mu je platio jamčevinu od milijun dolara. Buehler se vraća samo da bi saznao da ga Crypto AG otpušta. Ljut i razočaran udružuje se s nekoliko bivših zaposlenika iste tvrtke i piše knjigu, gdje pokušava razjasniti cijelu istinu oko njihovog poslovanja. Naknadno je oslobođen svih optužbi, a Crypto AG počinje primjećivati posljedice lošeg javnog mišljenja u padu prodaje i smanjenju korisnika. Time i Amerika više nije imala koristi od uspostavljenog dogovora. Kasnije se saznalo za još jedan sumljiv dogovor, ovaj puta s izraelskim agentom i bogatim investitorom, koji je zbog uvida u tajne informacije ostvario značajan profit. Zanimljivo je da nisu sve zemlje prestale koristiti njihove naprave i usprkos svim informacijama koje su izašle na vidjelo.

3.6. Fialka

Odnos između Sjedinjenih Američkih Država i Sovjetskog Saveza tijekom Hladnog rada bio je napet i ozbiljan. Samo jedan napad mogao je dovesti do nuklearnog rata. U takvom iznimno osjetljivom razdoblju sigurnost je dobila još veću ulogu. Kako bi što bolje očuvali međusobnu komunikaciju, Sovjeti su izumili *Fialku*. Prvi put je prezentirana 1956. godine i uskoro postala najznačajnija naprava za šifriranje Varšavskog pakta. Ime je dobila po ljubičici, malom lijepom cvijetu. Ako želimo biti precizni, Fialka je zapravo naziv procesa šifriranja kojeg koristi naprava, čije je pravo ime *M-125*. Međutim, u govoru se ustalilo kodno ime Fialka za cijelu mašinu.

Funkcionirala je na principu sličnom Enigmi, zato ju nekad zovu ruskom Enigmom. Šifriranje se provodilo elektromehaničkim procesom preko niza rotora (**premetala**) spojenih električnim žicama, koji su premetali slova. Tekst se unosio pomoću tipkovnice. Nakon svakog pritiska tipke, premetala bi se postavljala u novu poziciju. To znači da se za svako slovo poruke koristi nova supstitucijska abeceda. Za razliku od Enigme, slova šifrata nisu se prikazivala na displeju s lampicama, nego su se ispisivala direktno na papir pomoću **jedinice za ispis**. Zbog toga ju je bilo lako koristiti. Dovoljna je bila jedna osoba za primanje i slanje poruka. Imala je i dodatni dio, koji je omogućavao odašiljanje ili dupliciranje poruke. Nije

Slika 13: Fialka

imala 3 nego 10 premetala, a susjedna dva su se mogla okretati u suprotnim smjerovima. Imala je **čitač kartica**, koji je dodavao još jedan sloj permutacije procesu šifriranja. On je imao ulogu nepomičnog premetala. Može ga se usporediti s Enigminom razvodnom pločom, od koje je bio superiorniji, jer se nije pojavljiva recipročnost u šifriranju slova (ako se A šifrira u B, to ne znači da se B šifrira u A). Permutacijska matrica se mijenjala promjenom bušene kartice s 30 rupica i bila je sastavni dio dnevnog ključa. Glava pisača imala je dodatnu mogućnost stvaranja bušenih kartica, što je uvelike olakšavalo promjenu ključa svaki dan. Uz sve to, Fialka je imala i **brojač slova**, koji je brojao skupine od pet simbola. Inače se šifrat slao tako da se raspodijeli na grupice po 5 znakova, pa je ovo svojstvo operateru pomagalo pri unošenju poruke.

Svaki primjerak Fialke imao je i razne dodatke. Prvi je popis dijelova koji dolaze s napravom. Izdavala ga je tvornica i svaki kupac bi dobio svoj primjerak. Zatim poklopac za zaštitu od prašine, vode itd., jer se uređaj često prenosio i imao je puno malih dijelova, koje je mogao uništiti utjecaj vanjskog svijeta. Imala je i spremnik za papir potreban za ispis, ručku kojom su se mogla okretati premetala u slučaju ispravka pogreške. Testni reflektor je služio kao pomagalo za otkrivanje kvarova. Rezervna premetala, set alata za popravak, bočica ulja za podmazivanje, svjetiljka i drugi rezervni dijelovi također su bili sastavni dio dodatne opreme.

Svaka članica Varšavskog saveza imala je verziju naprave prilagođenu njenom pismu. To je obuhvaćalo promjene u tipkovnici, glavi za ispis i sustavu električnih vodova kod diskova za premetanje. Gotovo sve verzije su podržavale latinicu i ćirilicu uz poneke specifičnosti kod svake države. Na svakoj tipki zelenom bojom bila su ispisana slova ruske ćirilice, a crvenom latinice.

Slika 14: Tipka ruske Fialke i Fialke s dva pisma

Za Fialku se saznalo tek 2005. godine. Do tada nije postojala nijedna informacija o njenom postojanju. Pad Berlinskog zida označio je sigurni raspad Sovjetskog Saveza, pri čemu je došlo do povlačenja ruskih snaga iz država pod Željeznom zavjesom. Odlazeći su redom uništavali sve primjerke koje su mogli naći. Tako su ovu napravu učinili tajnom dugi niz godina nakon njene upotrebe.

3.7. Lorenz

Lorenz je bila njemačka elektromehanička naprava za šifriranje korištena u II. svjetskom ratu za komunikaciju najveće važnosti. Bila je smještena između teleprintera i njegove linije. Teleprinter može slati i primati ispisane poruke s jednog mjesta na drugo ili više njih istovremeno. Britanci su poruke odaslane Lorenzom zvali *Tunny*.

Slika 15: Lorenz

Prilikom komuniciranja Lorenz bi automatski šifrirao signale koje je proizvodio teleprinter ili dešifrirao dolazeću poruku prije nego bi bila ispisana. Pošiljatelj bi na tipkovnici teleprintera upisivao otvoreni tekst, a na strani primatelja on bi se ispisivao pomoću drugog. Šifrat, koji bi bio poslan, nije bio vidljiv operaterima ni na jednoj strani. To je uporabu činilo jako lakom s obzirom na Enigmu: jedna osoba je unosila tekst, druga je bilježila šifrirana slova, koja su se još morala u obliku Morseovog kôda odašiljati radio vezom. Tunny nije

koristio Morseov kôd, nego bi se šifrirani teleprinterski kôd slao direktno u zrak. Postojao je internacionalni teleprinterski kôd, koji je svakom znaku dodjeljivao kombinaciju od 5 pulseva i pauza. Kada se poruka iz teleprintera ispiše na papir, svako slovo poprimi oblik određenog niza rupica na papirnatoj traci.

Svaka Lorenzova mobilna jedinica bila je raspoređena u dva spremnika. U jednom bi se prenosila radio oprema, a u drugom teleprinterska oprema s dvije Lorenzove naprave (jedna za primanje, a jedna za slanje poruka). Takav način transporta bio je sigurnosna zaštita za slučaj pokušaja krađe naprave, kako u ruke protivnika ne bi pao cijeli sustav za slanje poruka.

Proces šifriranja odvijao se dodavanjem po jednog slova svakom slovu otvorenog teksta. Unutarnji Lorenzov mehanizam je sam stvarao niz slova za dodavanje. Taj niz nazivao se **ključ**. Naprava je svako slovo bilježila kao određeni niz od 5 znakova: točkica i križića. Slova bi se dodavala tako da se zbrajaju točkice i križići koji ih reprezentiraju. Pravila za zbrajanje su bila sljedeća: točkica plus točkica je točkica, križić plus križić je točkica, točkica plus križić je križić i križić plus točkica je križić. Primjer je prikazan na sljedećoj slici.

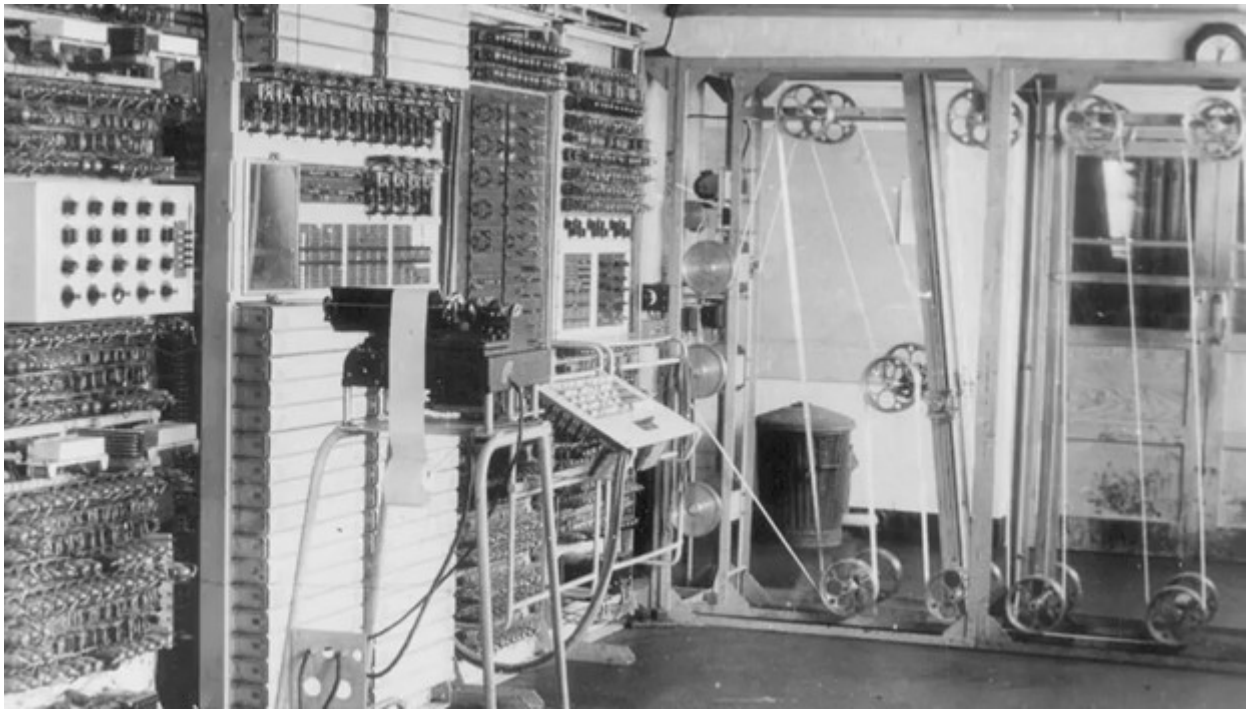
M		N		T
•	+	•	=	•
•	+	•	=	•
x	+	x	=	•
x	+	x	=	•
x	+	•	=	x

Slika 16: Primjer zbrajanja slova na temelju točkica i križića

Razlog zašto su inženjeri odabrali baš ovaj način zbrajanja je što dodavanjem jednog slova drugome i ponovnim dodavanjem tog slova nastalom slovu daje početno slovo: $(x+y)+y = x$. Tako je garantiran lak postupak dešifriranja. Isti niz slova, koji se dodao otvorenom tekstu, dodaje se šifratu i rezultat je dešifrirana poruka. Naprava proizvodi ključ kombiniranjem **dva niza slova**: ψ niz i χ niz. Oba niza proizvode **rotirajući diskovi**. Lorenz ih je imao 12, od čega 5 ψ, 5 χ i 2 monitor diska. Svaki od njih je imao različiti broj izbočina na svom vanjskom rubu, koje bi uzrokovale njihovo rotiranje. Pritisak tipke dovodi do usklađenog pomicanja svih 5 χ diskova, koji tada proizvedu jedno slovo. Isto rade i ψ diskovi, pa se dva dobivena slova zbrajaju i nastaje slovo ključa. Razlika u χ i ψ diskovima je ta da se χ pomjeraju za jednu poziciju, a ψ za neodređen broj koraka.

Kriptoanalitičari zaduženi za analiziranje Lorenza nisu imali mogućnost razbijanja šifre dok operateri nisu napravili ključnu pogrešku: dvije iste poruke poslali su koristeći iste početne postavke. To je bilo dovoljno da analitičari u Bletchley parku shvate princip rada naprave i osmisle njenu repliku. Nekoliko uređaja za pomoć pri dešifriranju prethodilo je onom najvažnijem stvorenom 1943., koji je dobio ime *Colossus*. Osmislio ga je matematičar Max Newman koristeći ideje Alana Turinga. No, svi su mislili da je takav stroj nemoguće

napraviti. Skepticizam je bio izražen dok se inženjer Tommy Flowers nije odlučio prihvatiti izazova. Nakon deset mjeseci rada uspio je završiti naprednu napravu. Bila je velikih dimenzija i proizvodila dosta topline, ali ujedno i do 5 puta brža od svoga prethodnika. Colossus je imao još jednu revolucionarnu mogućnost – mogao je biti programiran za različite zadatke. Tako je ušao u povijest kao prvo elektroničko računalo koje se može programirati. Iako je Eniac izumljen 1946. mnogi izvori i dalje tvrde da je on prvo elektroničko računalo, što kako vidimo nije točno.



Slika 17: Colossus

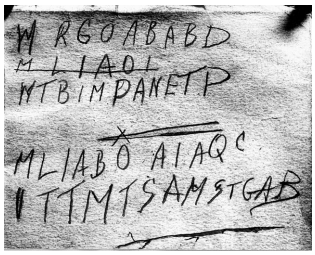
4. Neprobijeni šifrati

Kroz povijest kriptografije pojavljivale su se mnoge šifre. Neke su bile manje, a neke veće sigurnosti. Za većinu se u početku smatralo da su nerješive, ali tijekom vremena bi se pronašlo rješenje. Zato je teško povjerovati da još uvijek postoje šifre i kodovi za koje i dan danas ne postoji rješenje usprkos upotrebi raznih naprava. Ni sve poruke pisane Enigmom nisu probijene. Postoji primjer jedne, koja je uhvaćena u Atlantskom oceanu. Ona ni uz pomoć sustava zvanog enigma@home, koji koristi tisuće kućnih računala, nije poznata do danas. U nastavku ćemo spomenuti još nekoliko zanimljivih.

4.1. Čovjek iz Somertona

Prva zanimljivost dolazi iz Australije. Tamo je 1948. uz jedan od najmisterioznijih neriješenih policijskih slučajeva, pronađen kôd, koji još uvijek nije riješen. Priča započinje s lijepo odjevenim čovjekom, koji je viđen kako leži na plaži. Sutradan ujutro više nije bio živ, a nalazio se na istom mjestu kao i prethodni dan. Nitko nije poznavao tu osobu, a sa sobom nije imao nikakve identifikacijske dokumente. Analiza otisaka prstiju također nije bila uspješna. Zbog neuobičajene odjeće smatralo se da nije iz okolice. Neki su mislili da je ruski špijun, a neki da je napušteni ljubavnik. Teorija nije nedostajalo. Tako je nastala legenda o čovjeku iz Somertona.

6 mjeseci nakon incidenta, istražitelji su otkrili komad papira u skrivenom džepu njegovih hlača. Na papiru je pisalo samo „Tamam Shud“, što na perzijskom znači završeno. Kada je to izašlo u javnost, pojavio se novi trag. Naime, jedna osoba je našla u svom autu knjigu The Rubaiyat perzijskog pisca. Zadnjoj stranici knjige nedostajao je dio koji je odgovarao papiriću iz hlača čovjeka iz Somertona. Na pozadini knjige otkriven je kôd, napisan kroz nekoliko redaka. Svi napori policije za riješavanjem slučaja ostali su uzaludni. Nikad nije pronađeno objašnjenje što se zapravo dogodilo i što znači kôd na knjizi.



Slika 18: Kôd na pozadini knjige

Znanstvenici na Sveučilištu u Adelaide-u, pokušali su frekvencijskom analizom i drugim metodama doći do nekih zaključaka o šifratu. Sve što su uspjeli otkriti je postojanje određene strukture i utvrditi da poruka nije pisana jednom od 20 različitih šifri koje su uspoređivali. Iako je teško sa sigurnošću reći zbog dužine poruke, odbacili su mogućnost da je to zapravo

niz slova koji nema smisla. Do dan danas ne postoji veći napredak u otkrivanju značenja ovog kôda.

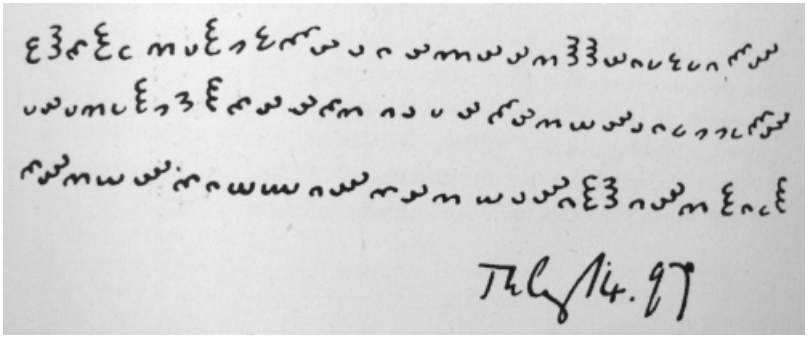
4.2. Bealeovo blago

1885. J. B. Ward objavio je The Beale Papers, neku vrstu letka s tri šifrirane poruke. Tvrdio je da rješenje triju poruka vodi do velikog blaga skrivenog u Virginiji. Po njemu je čovjek pod imenom Beale ostavio jednom gostioničaru malu zaključanu kutiju, koja je sadržavala šifrirane poruke. Gostioničar je poruke proslijedio prijatelju, koji je uspio riješiti jednu. U toj jednoj pisalo je da veliko bogatstvo očekuje onoga tko riješi preostala dva šifrata. Riješeni dio sastojao se od brojeva, koji su odgovarali početnim slovima riječi američke Deklaracije neovisnosti. Šifrat je bio niz brojeva, gdje je 12 primjerice označavao prvo slovo dvanaeste riječi spomenutog dokumenta.

1980. J. Gillogly, američki kriptograf i računalni znanstvenik, pokušao je dešifrirati jednu od preostale dvije poruke. Njegovo mišljenje bilo da je u pitanju prijevara. Tezu je temeljio na pronalasku niza brojeva, koji bi odgovarao pravilnom redoslijedu abecede. Vjerojatnost da se to dogodi je premala. Tajna još nije otkrivena, a dio znanstvenika smatra da je Gillogly došao do krivog zaključka jer je koristio drugačiju verziju Deklaracije nezavisnosti.

4.3. Kôd Dorabella

Engleski skladatelj Edward Elgar bio je oduševljen kriptografijom. 1897. napisao je šifrirano pismo svojoj prijateljici Dorabelli. Sadržavalo je 24 različita simbola napisana kroz tri linije. 40 godina poslije ona je pismo objavila u svojim memoarima uz napomenu da ga nikad nije riješila. Mnogi kriptoanalitičari zanimali su se za problem i pokušali na različite metode doći do izvorne poruke. Analiza je utvrdila da je moguće da simboli predstavljaju slova te da je to obična supstitucijska šifra. No, ni to nije pomoglo u otkrivanju poruke.



Slika 19: Kôd Dorabella

4.4. Kryptos

U sjedištu američke CIA-e postoji spomenik, koji oduševljava profesionalne i amaterske šifrolomce preko 20 godina. Napravljen 1990. Kryptos je bakrena skulptura s 1735 šifriranih slova. Napravio ju je američki umjetnik J. Sanborn, koji je kriptografiju naučio od jednog agenta zaduženog za šifriranje. Skulptura je podijeljena u 4 dijela. 3 su već riješena i upućuju na veću zagonetku završnog dijela. J. Gillogly je 1999. prvi objavio da je riješio prve tri poruke. Nedugo nakon toga javila se CIA s informacijom da je jedan njihov agent isto napravio godinu dana prije. No, posljednji dio ostao je netaknut. Sanborn je natuknuo da postoje tragovi u prethodnim dijelovima, koji će pomoći rješavanju cijelog problema.

Slika 20: Kryptos

Prva dva dijela šifrirana su Vigenèreovom šifrom. Koristeći frekvencijsku analizu i tragove koji su upisani na skulpturu, kriptoanalitičari su uspjeli pronaći dva ključa: KRYPTOS i PALIMPSEST. Pomoću njih su otkrili dio sadržaja, koji upućuje na skriveni objekt. Cijeli tekst sadrži namjerno napravljene pogreške u pisanju, kako bi zbunio analitičare. Za dešifriranje trećeg dijela prvo je bilo potrebno svaki četvrti stupac slova pomjeriti u lijevo i zatim presložiti redove. Taj dio spominje otvaranje Tutankhamonove grobnice. 2010. godine Sanborn je otkrio da 6 slova četvrtog dijela tvore riječ Berlin. Nakon toga desetci tisuća ljudi su se javljali s potencijalnim rješenjem, ali nitko ga nije imao.

5. Zaključak

Vođeni željom za stvaranjem neprobojne šifre, mnogi izumitelji i kriptografi obogatili su svijet tehnologije svojom vizijom najbolje naprave za šifriranje. Njima uz bok stajali su kriptoanalitičari, tj. šifrolomci, koji su imali još teži zadatak pronalaženja rješenja za inovativne i sve kompliciranije mehanizme šifriranja. Dvoboj šifrotvoraca i šifrolomaca dostigao je vrhunac razvojem modernog elektroničkog računala. Time su ljudi vezani za mehanizaciju tajnosti postavili ključni temelj funkcioniranju današnjice. Svaki čovjek ima pravo na vlastitu privatnost. Razvojem interneta i ubrzavanjem protoka informacija između običnih ljudi, privatnost je dobila drugi smisao. Kroz povijest tajno komuniciranje se većinom odnosilo na razmjenu poruka između vojskovođa, vladara i vodećih ljudi u politici. Sigurnost komuniciranja bila je vidljiva gotovo isključivo u ratnim vremenima i špijunskim poslovima. To se mijenja u 21. stoljeću. Svakodnevno je potrebna velika razina sigurnosti tajnih podataka. Banke, online trgovine i društvene mreže jedni su od primjera organizacija, koje redovito koriste kriptografiju i čije poslovanje ovisi baš o njoj. S. Singh slikovito objašnjava ovisnost informatičkog doba o uspješnosti zaštite informacija metaforom da šifriranje daje ključeve i brave informatičkog doba.

Računalo je zapravo najnaprednija naprava za šifriranje. Šifriranje poruka računalom razlikuje se od mehaničkog šifriranja samo u tri činjenice. Prva je da je mehanički stroj ograničen onim što je tehnički izvedivo, dok se računalo može ponašati kao hipotetski stroj. To mu omogućuje funkcioniranje na temelju velikog broja premetala, koji mogu mijenjati poziciju kako god se može zamisliti i okretati se u bilo kojem smjeru bilo kojom brzinom. Druga je neusporedivo veća brzina izvođenja šifriranja i dešifriranja. I treća je ta što klasične naprave rade sa slovima, a računalo koristi samo binarne brojeve. Zato je jasno da bez kriptografije i naprava, koje su bile alat za njezin razvoj, ne bi bilo današnjih računala ni stupnja tehnologije kojim smo okruženi.

Literatura

[1] M. Campbell: Killer codes, New Scientist, 210 (2011), 40 - 45

[2] M. Gardner: Codes, ciphers and secret writing, Dover Publications, New York, 1972.

[3] B. Hagelin: The Story of Hagelin-Cryptos, Crypto A.G., Zug, 1981.

[4] D. Kahn: The Codebreakers. The story of secret writing, Macmillan, New York, 1967.

[5] K. de Leeuw, J. Bergstra: The History of Information Security: A Comprehensive Handbook, Elsevier B.V., Amsterdam, 2007.

[6] S. Shane, T. Bowman: No Such Agency Part Four. Rigging the Game, The Baltimore Sun, 158 (1995), 9 - 11

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

[8] http://www.ciphermachines.com

[9] http://www.cryptomuseum.com/crypto/index.htm

[10] http://www.wondersandmarvels.com

Sažetak

Tijekom povijesti uvijek je postojala želja za tajnom komunikacijom. Prvo se pokušavalo prikriti postojanje važnih poruka, što nazivamo steganografija. Zbog njezinih nedostataka razvila se kriptografija, koja ne prikriva postojanje poruke nego njen sadržaj. Poruku koju šaljemo nazivamo otvoreni tekst. Otvoreni tekst šifriranjem postaje šifrat, kojeg u izvorno stanje vraćamo dešifriranjem. Jedan od primjera prikrivanja poruke je korištenje simpatetičke tinte. Poznate su i različite metode domišljatog slanja poruka, kao što su kôd pomoću točkica, kôd pomoću čvorova, šifriranje samo pomoću olovke i papira i mnogi drugi. Od jednostavnih naprava za šifriranje u radu su spomenuti i skital, Albertijev disk i Jeffersonov kotač. Razvoj radio tehnologije i potreba za sigurnijim šiframa potaknula je mnoge izumitelje na razvoj naprava za šifriranje temeljenih na rotirajućim diskovima, tkz. premetalima. Drugi dio rada bavi se ovakvim napravama. Najpoznatija takva je Enigma, a iza nje uslijedio je niz drugih: Purple, Typex, Sigaba, Hagelin, NEMA, Fialka, Lorenz, itd. Svaka naprava bila je po nečemu posebna i zanimljiva. No, postoje primjeri šifrata, koji nisu riješeni ni uz pomoć najsposobnijih stručnjaka i naprava: kôd vezan za čovjeka iz Somertona, Bealeovo blago, kôd Dorabella i Kryptos.

Ključne riječi: steganografija, kriptografija, otvoreni tekst, šifrat, šifriranje, dešifriranje, simpatetička tinta, skital, Albertijev disk, Jeffersonov kotač, premetalo, Enigma, Purple, Typex, Sigaba, Hagelin, NEMA, Fialka, Lorenz, Bealeovo blago, kôd Dorabella, Kryptos

Cipher machines

Summary

Throughout the history there's always been a need for secret communication. At first, people tried to hide the existence of important messages, which is called steganography. That method wasn't reliable and another method evolved named cryptography. It wasn't based on hiding the message but hiding its context. The message that wants to be send is called plaintext. Plaintext becomes ciphertext in the process of encryption. Decryption does the opposite shifting ciphertext back to plaintext. One example of steganography is the use of sympathetic ink. There are many different clever types of sending messages like the dot code, the knot code and encryption using just paper and pencil. In this paper there are also mentioned simple cipher machines: scytale, Alberti cipher disk and Jefferson wheel cipher. Radio technology and the need for safer ciphers induced the invention of rotor based cipher machines. The second part of this paper is about that type of machines. Fundamental piece of their mechanism were cipher wheels. The most important machine of that kind was Enigma, but there are known many others: Purple, Typex, Sigaba, Hagelin, NEMA, Fialka, Lorenz, etc. However, despite the effort of many cryptoanalysts and cipher machines there are still several ciphertexts which couldn't be broken: The Somerton man code, Beale's treasure, Dorabella code and Kryptos.

Key words: steganography, cryptography, plaintext, ciphertext, encryption, decryption, sympathetic ink, scytale, Alberti cipher disk, Jefferson wheel cipher, cipher wheel, Enigma, Purple, Typex, Sigaba, Hagelin, NEMA, Fialka, Lorenz, Beale's treasure, Dorabella code, Kryptos

Životopis

Rođena sam 11.12.1990. u Osijeku, a živim u Petrijevcima. Osnovnu školu pohađala sam u Petrijevcima. Obrazovanje nastavljam u I. gimnaziji u Osijeku, gdje sam maturirala 2009. godine kao najbolji maturant. Iste godine upisujem Preddiplomski sveučilišni studij matematike na Odjelu za matematiku u Osijeku. 2012. godine upisujem Diplomski studij matematike i odabirem smjer Financijska matematika i statistika. Posljednju godinu studija provodim radeći kao asistent u nastavi u OŠ Frana Krste Frankopana u Osijeku. Aktivni sam član DVD-a Petrijevci već niz godina i imam položen ispit za zvanje vatrogasca.