Enigma

Artur Šerbijus je koristeći znanje stečeno na studijama elektrotehnike u Hanoveru i Minhenu, razvio jedan od najpoznatijih šifarskih sistema krećući od osnove Albertijevog „šifarskog diska“ (korišćen za šifrovanje u Američkom gradjanskom ratu). Razvio je „**Enigmu**“.

Šifarski disk je izum iz petnaestog veka a izumeo ga je italijanski arhitekta Leon Alberti. Uredjaj se sastojao od dva bakarna diska, jednog većeg i jednog manjeg, na čijim krajevima je izgravirana abeceda. Oba diska su spojena iglom u sredini i mogla su se slobodno rotirati oko svoje ose. Ovakav način šifrovanja je samo olakšana upotreba Cezarove šifre (supstitucija „slovo za slovo“) ali je kasniji rad Albertija doprineo razvoju novog sistema šifrovanja za koji je najviše zasluga pokupio Blez de Vižner, francuski diplomata koji ju je konačno uobličio.

Razvijeni sistem „**Enigma**“ se sastojao od 5 bitnijih komponenti (mada ih ima više, ove su dovoljne za razumevanje rada).

Tastatura služi za unos početnog teksta, bilo radi šifrovanja, bilo radi dešifrovanja.

Ploča s lampama predstavlja izlazni uredjaj za prikazivanje šifrovanog odnosno dešifrovanog teksta. Vrlo rana verzija monitora (o LCD ekranima nema ni govora)

Skrembler je najbitniji deo ove mašine. Predstavljen je u obliku diska na kome je bilo 26 rupa kroz koje su prolazile žice. Žice su povezivale tastaturu na jednom kraju i ploču s lampama na drugom kraju (nakon niza preplitanja naravno). Da cela stvar ne predstavlja samo fensi varijantu Vižnerove šifre (Cezarova šifra sa više alfabeta) pobrinuo se mehanizam za **rotiranje diska**. Nakon svakog otkucaja na tastaturi disk se rotira za 1/26 kruga. To znači da, ako teorijski **26** puta zaredom otkucate slovo „a“, 25 puta će ono biti kodirano drugačije od prethodnog puta a samo jednom kao slovo „a“. Kako je ponavljanje simptom slabe šifre, ovaj problem je delimično otklonjen dodavanjem još dva diska. Čisto računice radi ako pomnožite 26*26*26 i u kombinaciju dodate 6 mogućih rasporeda tri diska, dobijate broj od **105456** kombinacija. Dovoljno jako?

Četvrti deo je bila **ploča s kablovima**. Operater Enigme je kod sebe imao 6 kablova kojim je mogao da direktno „prespoji“ slova na tastaturi (tako da kad recimo kucate slovo „b“ šifrovanje ide putanjom namenjenom slovu „t“). Broj načina na koji mogu da se ukrste 6 parova od ukupno 26 slova je **100391791500.** To ukratko znači da je broj ključeva koje treba isprobati da bi se došlo do „šablona“ veći od **10 000 000 000 000 000**. A to je tek početak.

Regularna mašina dostupna Nemcima imala je na raspolaganju 5 diskova od kojih su birana 3 a operateri mornaričke enigme imali su na raspolaganju 8 diskova. Pred početak rata je i broj kablova sa 6 povećan na 10. Računati broj ključeva nije potrebno jer kada na sve to dodate i proceduru da je ključ svakog dana menjan, jasno je da tada nije bilo moguće razbiti šifru Enigme, tada nije postojao odgovarajući tehnički odgovor kripnoanalize na ovu prednost kriptografije. Ili možda jeste?

Da bi se obezbedilo dešifrovanje poruka, mašina je posedovala deo nazvan **„reflektor“**. Taj deo je vraćao struju nazad kroz skremblere pa je za dešifrovanje poruke bilo potrebno samo posedovati „Enigmu“ i imati knjigu šifara u kojima je pravilan početni raspored skremblera za taj dan.

Bez obzira na jačinu šifre, koja je bila glavni adut, Šejbijus nije najbolje prošao kada je „Enigmu“ izneo na poslovno i vojno tržište. Cena jednog primerka je iznosila oko 20 000 funti u današnjem novcu. Visoka cena je bila dovoljan razlog za nerazmišljanje o ovom rešenju. Nemačka vojska je i dalje bila samouverena po pitanju trenutne sigurnosti njihovih komunikacija i tek je 1923. godine, nakon objavljivanja „zvanične istorije Prvog svetskog rata“ britanske kraljevske mornarice, shvatila da su njihove komunikacije već dugo, dugo, dugo kompromitovane.

Već 1925. „Enigma“ je ušla u masovnu proizvodnju kao izabrano najbolje rešenje a 1926. je vojska počela da je koristi nakon čega su usledile sve važnije institucije, vlada, železnica... Samo vojska je kupila 10 000 primeraka ali Šejbijus nije dočekao da vidi kako njegovo delo donosi prevagu u ratu koji sledi. Umro je od unutrašnjeg krvarenja nastalog udarcem u zid 1929. nakon što je izgubio kontrolu nad kočijama.

Alan Tjuring

Mančester, **godina 1952**. Jedan čovek je pokraden i nedugo potom, u izjavi policajcima naivno otkriva da je u vezi sa mladjim čovekom iz istog grada. Po tadašnjem zakonu, nije im ostavljena druga mogućnost do privodjenja i podizanja optužnice za „veliku nepristojnost suprotnu Sekciji 11 Amandmana 1885 Krivičnog zakona“. Čekalo ga je sudjenje...

26 godina ranije

Dorset, **škola Šerborn**, **godina 1926**. Četrnaestogodišnji mladić, nakon puta dugog 100 km, biciklom stiže na početak prvog polugodja. Podvig su propratile lokalne novine a taj entuzijazam će se kasnije pretvoriti u veliku ljubav prema nauci i eksperimentima i pratiće ga kroz čitav život i u svemu što radi. Jedini drug koji je sa njim delio istu viziju a koji je po njegovim i tvrdnjama drugih bio darovitiji, Kristofer Morkom umire 1930. godine od tuberkuloze. To je dogadjaj koji je najverovatnije odredio njegov dalji put, darujući svetu genija - jednog od najzaslužnijih za razvoj računarstva. Kako je Morkom , kao izuzetno nadaren, već dobio stipendiju za Kembridž, **Alan Tjuring** odlučuje da konkuriše za taj koledž.

Kembridž, Specijalna i Univerzalna mašina

1931. godine Tjuring je primljen na Kembridž gde je imao prilike da se nadje u okruženju velikih umova poput Bertranda Rasela (Nobelova nagrada za književnost 1950.), Alfreda Norta Vajtheda (*Principia Mathematica*), Ludvig Vitgenštajn (*Tractatus Logico-Philosophicus*, *Philosophical Investigations*)... Taj period je karakterističan po jednoj debati o prirodi matematike i logike. Matematika je bila u krizi jer je logicar Kurt Gedel pokazao da postoji odredjen broj problema koji se logički ne mogu rešiti. Time je srušen čitav jedan aksiom da je moguće odgovoriti na sva matematička pitanja. U nadi da će tako „spasti matematiku“, matematičari su pokušali da identifikuju sva „neodlučiva pitanja“. Cela polemika inspirisala je Tjuringa da napiše svoj najuticajniji rad iz oblasti matematike – **„O izračunljivim brojevima“**.

U tom delu govori se o apstraktnoj mašini koja bi trebala pomoći da se otkriju sva „neodlučiva pitanja“. Ta mašina izvršavala bi unapred odredjen algoritam (niz koraka). Jedna mašina bi npr. izvršavala jednu matematičku operaciju, gde bi se potrbni parametri unosili preko jedne papirne trake a rezultat bi se ispisivao na drugu papirnu traku. Kako je važilo „jedna mašina – jedan algoritam“, taj apstraktni model je nazvan **„Specijalna Tjuringova mašina“**.

Kako je već bio zamislio čitav niz specijalnih mašina, sledeći korak je bio „stvaranje“ (sve je teorijski) jedne fleksibilne mašine koja bi bila (sada je tako možemo nazvati) programabilna i sposobna da izvrši bilo koju funkciju. Izbor

funkcija bi se takodje vršio ubacivanjem odabranih traka. **„Univerzalna Tjuringova mašina“**, kako ju je nazvao, u teoriji je trebala dati odgovor **na svako** pitanje koje je imalo logičan odgovor. Iako se pokazalo da ne može da identifikuje sva „neodlučiva pitanja“, ovaj apstraktni model predstavlja prvi moderni programabilni računar, iako je te **1937**. godine postojao samo u teoriji. A i to će se ubrzo promeniti.

Možda jednako bitna stvar njegovim dostignućima u nauci, bilo je okruženje u kojima su ona postizana. Tjuring je u jednoj izuzetno tolerantnoj sredini imao veliku podršku. Čak je i homoseksualnost na univerzitetu bila široko prihvaćena pa je bio lišen brige o tome da li će neko saznati za njegovu orjentaciju i šta će na to reći.

Razbijanje Enigme, Blečli Park

Godina je 1926. Britanija, Francuska, Amerika, svet... Uhvaćene nemačke poruke su stizale do kriptoanalitičara i ostavljale ih kompletno – zbunjene. Početni pokušaji da se odgonetnu poruke bili su apsolutno bezuspešni, vrlo brzo se odustalo od samog pokušaja razbijanja „Enigme“ a Nemci su praktično preko noći dobili najsigurniju komunikaciju na svetu.

Ime koje treba pomenuti je **Marjan Rejevski**, poljski kriptoanalitičar koji je uz pomoć tri elementa pronašao prve slabosti „Enigme“ – straha, matematike i špijunaže.

Poljska je bila jedina država koja ni jednog trenutka nije smela da se opušta i odustaje od pokušaja da dešifruje poruke. Sa jedne strane se graničila sa Rusijom koja je želela da proširi komunizam a sa druge sa Nemačkom koja je želela da povrati teritoriju izgubljenu u Prvom svetskom ratu.

Element matematike bi morao biti jasan jer za razumevanje rada kao i za dešifrovanje „Enigme“ bio je potreban izuzetan mentalni napor. Špijunaža je pak doprinela konstrukciji modela vojne „Enigme“ i mašine nazvane „bomba“ koja je praktično predstavljala „bruteforce atack“ mašinu (isprobavala je sve kombinacije i kada bi pronašla pravu, lampice bi se upalile).

Godina je 1939. Blečli Park. Iskusni britanski kriptoanalitičari iz **„Sobe 40“** su odabrali pogodno mesto za Vladinu školu za šifre i kodove. 4. Septembra Alan Tjuring se odaziva na poziv i seli se u Šenli Bruk End, udaljen 5 kilometara od Blečlija.

Iako je Blečli u početku nizao uspehe, oni su se uglavnom zasnivali na radovima Rejevskog i činjenici da su operateri „Enigme“ svaki ključ poruke šifrovali dva puta (ako je ključ bio **ABC**, operater bi kucao **ABCABC**). Tjuring je odmah pretpostavio da će ubrzo Nemci shvatiti da je to slabost šifre i preći na drugi

sistem, pa je stoga počeo sa traganjem alternativnog načina „razbijanja Enigme“.

Ubrzo je analizom dešifrovanih poruka shvatio da se sadržaj nekih može znati samo na osnovu vremena i mesta odakle je poslata. Na primer, Nemci su u 6 ujutru slali izveštaj o vremenu, i to na vojnički rigidan način (kratko i jasno) tako da je poruka uhvaćena u to vreme sigurno sadržala reč **wetter**. Ako bi dešifrant pred sobom imao tekst **ETJWPX** i znao da on predstavlja reč **wetter** ostalo bi samo da proveri koja postavka odgovara ovakvom šifrovanju.Kada bi našli pravu postavku, na osnovu samo te jedne poruke znao se dnevni ključ i sve ostale poruke koje stignu tokom dana su sa lakoćom „otvarane“. Ali da li je to bilo zaista tako lako?

Kriptoanalitičaru bi i dalje ostalo da proveri 159 000 000 000 000 000 000 mogućih kombinacija, pa je Tjuring pribegao „rastavljanju postavki“. Najveći uspeh je bio poništavanje efekta kablova za ukrštanje. Konstruišući električno kolo koje je vršilo tu funkciju broj kombinacija za proveru sada je iznosio 1 054 560 što je fenomenalan napredak. Osmislivši sistem od 60 grupa bombi (broj kombinacija skremblera „3 od 5“), gde bi svaka grupa trebalo da proveri 17 576 kombinacija, brzinom jedna kombinacija po sekundi – dnevni ključ bi uz pomoć puškice bio dostupan za samo 5 sati. Sve ovo je bilo samo teorija a Blečli je uspeo da izdejstvuje 100 000 funti kako bi ideju pretvorili u funkcionalni uredjaj.

14. Marta 1940. svetlost dana je ugledala **Victory**, prvi prototip Tjuringove „bombe“ ali je nakon stavljanja u pogon pokazala da se razlikuje od mašine u teoriji. Umesto 5 sati, za dobijanje jednog ključa bilo je potrebno 5 dana. Usledili su veliki napori da se poboljša efikasnost. **1. Maja 1940.** Nemci, prestaju sa ponavljanjem ključa poruke i time znatno poboljšavaju sigurnost svojih komunikacija do **8. Avgusta 1940.** kada je u Blečli stigla nova „bomba“ **Agnus Dei** (skraćeno Agnes). Ona je bila u stanju da do ključa dodje u roku od sat vremena (ako je sve išlo kako treba).

Blečli je nastavio da redja uspehe. Da pokaže da to zaista ceni, tadašnji predsednik Vlade Vinston Čerčil odlazi u posetu. Zvao ih je „zlatnim guskama koje ležu jaja i nikada ne gaču“. I možda to jeste prava slika koja govori o Blečli parku. Svi zajedno su obavljali izuzetno bitan rad koji je saveznicima pružao neophodne informacije a čak ni najbliži nisu smeli da znaju čime se ovi kriptoanalitičari bave. Zanimljivo je to što je Tjurin jednom prilikom pomenuo majci da je uključen u neku vrstu vojnog istraživanja a ona je bila razočarana što ga to nije nateralo da sredi razbarušenu frizuru. Činjenica da je bio jedan od vrhunskih kriptoanalitičara na svetu je bila strogo čuvana vojna tajna.

12 godina kasnije

Alan Tjuring u svedočenju policajcima povodom kradje naivno otkriva da je u vezi sa mladjim čovekom iz istog grada. Po tadašnjem zakonu, nije im ostavljena druga mogućnost do privodjenja i podizanja optužnice za „veliku nepristojnost suprotnu Sekciji 11 Amandmana 1885 Krivičnog zakona“.

Izveštavanje medija sa sudjenja i javno objavljivanje presude je doprinelo javnom poniženju. Tjuringu je pružena prilika da bira izmedju zatvorske kazne i jednogodišnje hormonske terapije estrogenom. Bira terapiju, koja je po mišljenu suda trebalo da obuzda njegov libido.

Britanska vlada mu ubrzo oduzima dozvolu za rad na poverljivim projektima i zabranjuje mu da radi na istraživačkim projektima iz oblasti razvoja računara. Terapija ga je učinila gojaznim i impotentnim. Vojna tajna je i dalje bila na snazi.

8. Juna 1954. čistačica je pronašla Tjuringa zavaljenog u fotelji. Na stočiću kraj nje je bila polupojedena jabuka u koju je porethodno ubrizgan cijanid. Zaključak patologa bio je – samoubistvo!

Slavko Ilić
www.itkutak.com