VISOKO UČILIŠTE ALGEBRA

ZAGREB, REPUBLIKA HRVATSKA

Dominik Despot

Überenigma

ESEJ

Zagreb, prosinac 2022.

Sažetak

Ideja ovog rada je objasniti koncept Überenigme te primjenu istog u današnjem svijetu. Überenigma je koncept koji se nadovezuje na originalnu metodu mehaničke enkripcije Enigma stroja koji je bio razvijen početkom 20. st. za kriptiranje i dekriptiranje poruka visoke važnosti (poput vojnih naređenja, sastanaka i sl.). U današnje vrijeme rapidno razvijajućih informacijskih tehnologija gdje osobni podaci i povjerljive poruke internetom putuju po cijelom svijetu potreba za zaštitom istih postaje eksponencijalno važnija. Zlonamjerni napadači učestalo vrše napade na osobne podatke i serverske infrastrukture kako bi se domogli osobnih podataka običnih građani te ih prodavali raznim zlonamjernim kupcima u svrhu reklamiranja, krađe identiteta, napada na organizacije itd. Überenigma je nastavak kriptološkog procesa originalne enigme koji u potpunosti zaustavlja takve napade. Realizirane je dodatkom dodatnih komponenata te poboljšanjem funkcionalnosti i kompleksnosti istih. Überenigma također ostvaruje svoju neprobojnost radi iznimno visokog broja mogućih kombinacija. Naspram originalnih $1.5x10^{14}$ kombinacija Enigme, Überenigma sadrži $4.03x10^{10343}$ mogućih kombinacija što je čini praktički neprobojnom.

1. Uvod

Kriptiranje, dekriptiranje, samim time i čuvanje integriteta prenesenih informacija putem pouzdanosti kriptografske[1] opreme bila je dužnost kriptografa još od antičkih civilizacija. Situacija se nimalo nije promijenila u moderna doba gdje je, u svijetu informacijskih tehnologija, važnost sigurnosti informacija dosegla vrh. Pri rapidno razvijajućim komunikacijskim sposobnostima računala i ostalih pametnih uređaja mogućnosti za špijunažu i prisluškivanje su beskrajne.

Svijet je stoga u beskrajnim potragama za nove i inovativne metode zaštite osobnih podataka. Današnji favoriti su *end-to-end*[2] enkripcije s dugačkim ključevima kako bi se eliminirali potencijalni *brute-force*[3] napadi ali oni su vrlo neoriginalni te se mogu manipulirati raznim napadima radi svoje pretpostavljivosti i podložni backdoor[4] napadima, stoga su inovativni pristupi u modernoj kriptologiji[5] puno traženiji, a samim time i najbolje plaćeni. Iako su moderni pristupi enkripciji podataka često ranjivi, to ne znači da su beskorisni. Najjače enkripcije su *multi-layer* tipa što znači da se podaci kriptiraju s nekoliko različitih sustava enkripcije, pa se unutar koraka ubacuje moderna enkripcija dugačkog ključa kako bi se zaustavili *brute-force* napadi.

Enigma je u svoje vrijeme bila desetljeća ispred svoga vremena te je i u današnje vrijeme baza nekih modernih enkripcija. Štoviše, u svoje vrijeme Enigma je bila toliko napredna da ju je bilo nemoguće probiti samu po sebi. Moderne interpretacije dijele tu kvalitetu.

---

[1] Kriptografija – kako A. Dujella [1] navodi u poglavlju „Osnove kriptografije“: Kriptografija je znanstvena disciplina o metodama za slanje poruka (informacija) u obliku koji će biti razumljiv samo onima koji ih znaju pročitati, odnosno samo onima kojima su namijenjene.

[2] *End-to-end* enkripcije – vrsta enkripcije kod kojih se ključevi za kodiranje i dekodiranje nalaze isključivo kod pošiljatelja i primatelja.

[3] *Brute-force* – vrsta napada koja uključuje linearno isprobavanje svih mogućih kombinacija kako bi se došlo do ključa za dekodiranje, samim time i informacije

[4] *Backdoor* – “stražnji ulaz”, slabost u enkripciji ugrađena najčešće kako bi se mogla zaobići enkripcija radi potreba državnih službi.

[5] *Kriptologija* – znanost koja se bavi izučavanjem i definiranjem metoda za zaštitu informacija (šifriranjem) te izučavanjem i pronalaženjem metoda za otkrivanje šifriranih informacija (dešifriranjem).

2. Enigma

U ovom poglavlju objašnjene su komponente enigme te princip rada. Slika stroja vidljiva je na slici 1. Sve informacije prikupljene su unutar web-članka Wikipedija[3].

Slika 1: Enigma stroj

2.1. Komponente

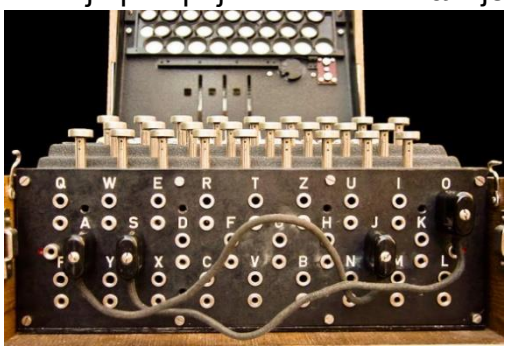
Enigma sadrži 5 glavnih komponenata: tipkovnicu, rasvjetnu ploču, priključnu ploču, rotore i reflektor. Ključevi za kodiranje su postavke reflektora, rotora i priključne ploče. Kada korisnik pritisne tipku na tipkovnici kodirani znak zasvijetli na rasvjetnoj ploči.

2.1.1. Tipkovnica

Tipkovnice na Enigma strojevima nisu bili standardnog poretka ali su bile najbliže QWERTZ poretku. Mehaničkog su dizajna te se pritiskom na tipku šalje električni signal u stroju dalje prema priključnoj ploči.

2.1.2. Priključna ploča

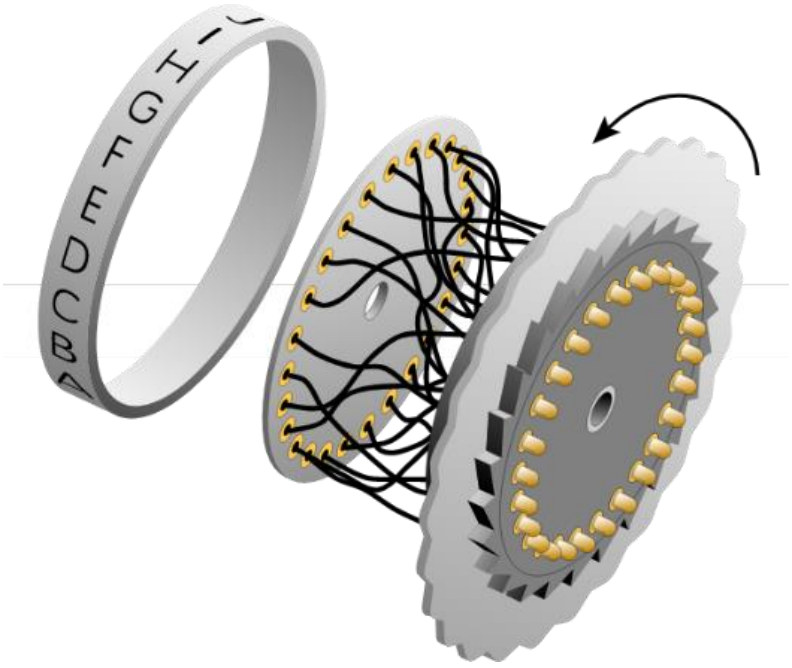
Priključna ploča (njem. *Steckerbrett*), vidljiva na slici 2, sadrži 26 električnih utičnica od kojih svaka predstavlja slovo u abecedi. Spojem utičnica prije i na kraju procesa kodiranja/dekodiranja prespojena slova će zamijeniti mjesta.



Slika 2: Priključna ploča

2.1.3. Rotor

Rotor je mehanička komponenta koja je i najgenijalnija i najinovativnija stvar enigme koja je promjenjivo kodirala informacije. Svaki rotor se sastoji od 26 elektroničkih kontakata poredanih u krug. Svaki kontakt je predstavljao slovo u abecedi. Kodni ključ je određivala, između ostalog, i pozicija rotora. Kako operater tipka po tipkovnici rotor se okreće i mijenja kod. Brzine rotore odnose se 1:26. Kako se rotor okreće mijenja se znak na izlazu, svaki put dajući drugu kombinaciju. Stoga se kod stalno mijenja pa se kodna riječ poput „aaa“ kodira u „grw“ ili sl. kombinaciju. Najčešće izvedbe enigme koriste 3 rotora. Grafika rotora vidljiva je na slici 3.



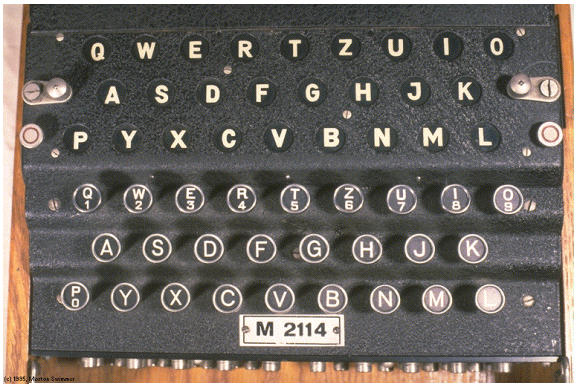
Slika 3: Rotor enigme

2.1.4. Reflektor

Reflektor je najbolje opisati kao statičan rotor. Njegova uloga jest vraćanje signala natrag kroz rotore, ali ne bez da se pri tome opet ne promijeni kodirani znak. Time se osigurava da se niti jedan znak nikada neće kodirati samo u sebe.

2.1.5. *Rasvjetna ploča*

Rasvjetna ploča izgleda slično kao tipkovnica samo umjesto tipki sadrži prozorčiće u obliku slova ispod kojih se nalazi lampica za prikaz kodiranog slova. Rasvjetna ploča vidljiva je na slici 4.

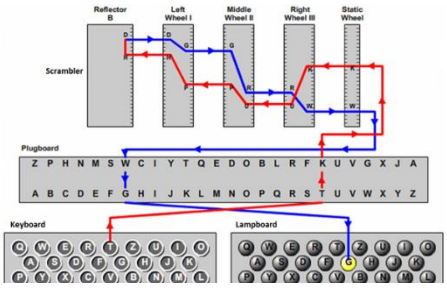


Slika 4: Tipkovnica i rasvjetna ploča

2.2. *Princip rada*

Na slici 5 je vidljiva vizualna reprezentacija principa rada.

1. Pritiskom na tipku tipkovnice električni signal putuje prema priključnoj ploči i okreće rotor/e.
2. Ovisno o postavkama priključne ploče znak se kodira u drugi znak te ide prema rotorima
3. Znak prolazi kroz rotore te se kodira n(broj rotora) puta
4. Reflektor šalje znak natrag kroz rotore te se ponavlja korak broj 3
5. Znak se vraća kroz priključnu ploču te ponovno kodira ovisno o postavkama ploče
6. Lampica na rasvjetnoj ploči zasvjetljuje u odgovarajućem znaku – kraj kodnog procesa.



Slika 5: Vizualna reprezentacija principa rada

3. Überenigma

Überenigma (njem. über- više, jače, preko) predstavlja koncept modernizacije originalnog Enigma stroja. U potpunosti je otporna na svaku današnju metodu probijanja. Radi svojih masivnih kombinacija ključeva smatra se, trenutno, apsolutno neprobojnom. Također sadrži podršku za 3000 znakova, naspram originalnih 26.

3.1. Komponente

Überenigma sadrži gotovo sve komponente kao i stroj na kojem je bazirana (osim tipkovnice i rasvjetne ploče). Sve komponente su, suprotno od originala, digitalne. Dodaci su: enkriptor, duplikator, refraktor i kompresor.

3.1.1. Enkriptor

Enkriptor je komponenta koja kriptira znak po modernom principu enkripcije DESC-K (koja sadrži ključ od 1024 bita – 2^{1024} mogućih kombinacija).

3.1.2. Duplikator

Zadaća duplikatora je dupliciranje pojedinih znakova ovisno o ključu enkripcije. Može se podesiti da duplicira svako n-to slovo (n = >10 & <100).

3.1.3. Refraktor

Refraktor vraća proces enkripcije na stadij natrag kroz rotore ali ga potom šalje natrag na nastavak procesa za svako n-to slovo (n = >1 & <1000).

3.1.4. Kompresor

Radi velike kompleksnosti principa rada, zadaća kompresora je pamtiti ponavljajuće nizove te ih zamijeniti poznatim nizom koji se ne ponavlja kako bi se suzila količina znakova.

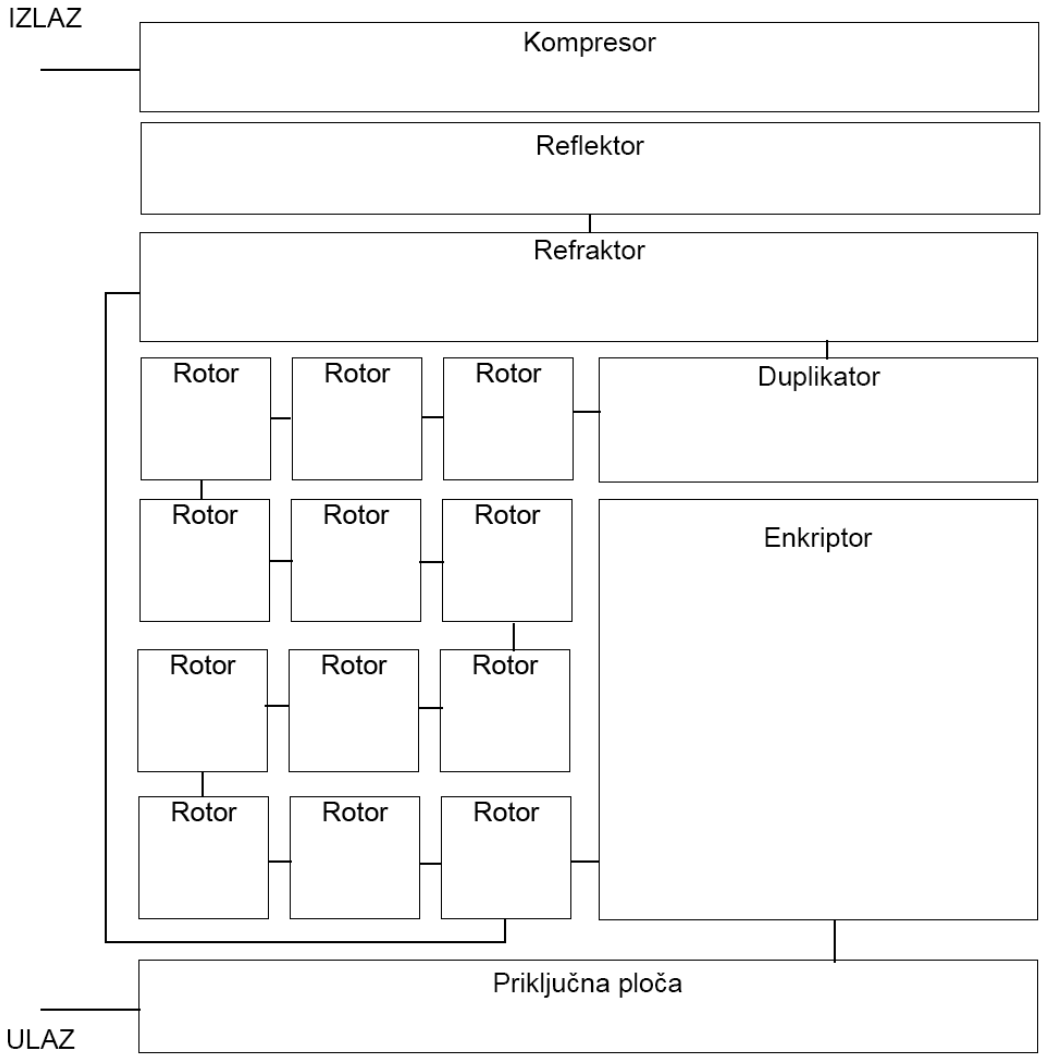
3.1.5. Rotori i reflektor

Rotori i reflektor su identični kao u originalnom stroju u svakom pogledu osim količini kombinacija (3000 umjesto 26). Faktor okreta je također drugačiji. Broj rotora je 12.

3.2. Princip rada

0. Stroj se podešava prema ključu(međuključevi su odvojeni znakom „:“, dok su ključevi odvojeni „::“, ključ se zapisuje u heksadekadskom sustavu):
    I. Ključevi rotora (12 x 3000 kombinacija)
    II. DESC-K ključ (2^{1024} kombinacija)
    III. Ključ duplikatora (88 kombinacija)
    IV. Ključ refraktora (997 kombinacija)
    V. Ključ reflektora (8.42 x 10^{5012} kombinacija)
    VI. Ključ priključne ploče (8.42 x 10^{5012} kombinacija)
1. Znak se unosi i proces započinje.
2. Znak ulazi u priključnu ploču te se ovisno o podešavanju mijenja za drugi znak.
3. Rotori se okreću sa startnih pozicija.
4. Enkriptor kodira znak po enkripciji (DESC-K).
    - Započinje petlja kodiranja svakog znaka jer DESC-K kodira jedan znak u više znakova.
5. Znak prolazi kroz sve rotore.
6. Duplikator ovisno o svom ključu duplicira znak.
7. Znak ulazi u refraktor te se ovisno o ključu vraća natrag kroz rotore ili nastavlja do reflektora.
8. Reflektor okreće proces natrag prema početku te ovisno o svom ključu mijenja znak te ga šalje natrag u izlaz.
9. Kompresor se aktivira samo pri kraju kodnog procesa kada su svi znakovi kodirani, tada obavlja svoju funkciju i proces je završen.

Princip rada je kroz shematski prikaz vidljiv na slici 7.



Slika 6: Blok shema rada

3.3. Otpornost na napade

Überenigma je otporna na svaku današnju poznatu metodu napada. Ne sadrži niti jedan *backdoor* te radi kompletno bez prisutnosti internetske veze. Ako se pretpostavlja da korisnik pravilno rukuje alatom jedina moguće metoda proboja zaštite jest *brute-force*.

3.3.1. Brute-force otpornost

Ukupan broj mogućih kombinacija Überenigme jest $4.03x10^{10343}$. Najefektivniji način obavljanja *brute-force* napada jest grafičkim karticama računala radi njenih rapidnih sposobnosti paralelnog obrađivanja podataka. Najmodernije grafičke kartice mogu isprobati oko 4 milijarde kombinacija u sekundi. Ako uzmemo u obzir da nas napada superračunalo ili skupina snažnih računala koji ukupno sadrže 2.5 milijuna grafičkih kartica[6] od kojih svaka isprobava 4 milijarde kombinacija po sekundi vrijeme koje bi potrajalo da se probije Überenigma jest $4.03x10^{10327}$ sekundi, odnosno $0.67x10^{10326}$ minuta odnosno $0.11x10^{10325}$ sati odnosno $0.46x10^{10323}$ dana odnosno $0.13x10^{10321}$ godina što predstavlja $0.13x10^{10318}$ tisućljeća. Iz navedenog se da zaključiti da Überenigma ne može biti probijena današnjim sredstvima te, ako se nastavi trenutni razvoj brzina računala, neće biti ni u bliskoj budućnosti.

[6] Broj baziran na trenutnoj estimaciji broja servera Google-a prema članku Data Center Knowledge-a [2].

4. Zaključak

Budući da je kroz cijelu povijest čovječanstva, a pogotovo u današnje vrijeme važnost sigurnost osobnih podataka dosegla je vrh. Stoga se učestalo javljaju potrebe za novim i inovativnim pristupima zaštite. Iz eseja se jasno da zaključiti da je Überenigma jedan od najsigurnijih načina zaštite osobnih podataka te slanja kriptiranih poruka.

Popis literature

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

[2] Data Center Knowledge, How many servers does Google have?, *Data Center Knowledge,* p. 1, 2017.

[3] Wikipedia: Enigma machine, 2022. Pristupljeno 8.12.2022. na mrežnim stranicama: https://en.wikipedia.org/wiki/Enigma_machine.