Šifra Zodiac

Blašković, Doris

SVEUČILIŠTE U ZAGREBU

PRIRODOSLOVNO–MATEMATIČKI FAKULTET

MATEMATIČKI ODSJEK

Doris Blašković

ŠIFRA ZODIAC

Diplomski rad

Voditelj rada:
prof. dr. sc. Andrej Dujella

Zagreb, veljača, 2025.

Ovaj diplomski rad obranjen je dana _____ pred ispitnim povjerenstvom u sastavu:

1. _____, predsjednik
2. _____, član
3. _____, član

Povjerenstvo je rad ocijenilo ocjenom _____.

Potpisi članova povjerenstva:

1. _____
2. _____
3. _____

Sve što poželiš, možeš!

Sadržaj

Uvod

U području kriminalistike, razumijevanje uma kriminalca predstavlja ključni izazov. Dok neki zločinci ne ostavljaju nikakve tragove svojih aktivnosti, drugi to čine namjerno kako bi izazvali istražitelje i širu javnost. Jedan od načina na koji to čine je kroz stvaranje šifri, poruka napisanih tajnim kodom. Takve šifre predstavljaju intelektualni izazov i često pružaju uvid u motive i psihološki profil počinitelja.

Jedan od najozloglašenijih primjera je serijski ubojica poznat kao Zodijak, koji je krajem 1960-ih i početkom 1970-ih slao šifrirana pisma lokalnim novinama u sjevernoj Kaliforniji. Prva tri pisma poslana su istovremeno na tri različite adrese novina, a svako je sadržavalo dio šifre poznate kao Z408. Uz ova pisma, Zodijak je priložio popratno pismo u kojem je tvrdio da je odgovoran za niz ubojstava te je zahtijevao da se šifre objave na naslovnicama novina, prijeteći novim zločinima ako njegov zahtjev ne bude ispunjen. Šifra Z408 je ubrzo dešifrirana od strane školskog učitelja i njegove supruge, što je pružilo uznemirujući uvid u um ubojice i njegove motive.

Međutim, Zodijak je kasnije poslao još nekoliko šifri koje su desetljećima ostale neriješene. Najpoznatija među njima je šifra poznata kao Z340, složena šifra sastavljena od 340 znakova, poslana San Francisco Chronicleu u studenom 1969. Unatoč brojnim pokušajima profesionalnih kriptografa, FBI-ja, CIA-e i bezbroj amaterskih entuzijasta, šifra je ostala neriješena više od pet desetljeća. Taj zagonetni kod postao je simbolom jedne od najtrajnijih misterija u povijesti kriminalistike, izazivajući pitanja o identitetu ubojice i njegovim motivima.

2020. godine, tijekom karantene usred pandemije virusa COVID-19, tim koji su sačinjavali programer David Oranchak, matematičar Sam Blake i amaterski kriptograf (inače skladišni radnik) Jarl Van Eycke konačno je uspio dešifrirati ovu zagonetnu poruku. Tako je dana 5. prosinca 2020. godine službeno potvrđeno dešifriranje šifre Z340. Ovaj monumentalni uspjeh nije bio rezultat jednog genija ili slučajne sreće, već kombinacija naprednih tehnoloških alata, interdisciplinarnog pristupa i upornosti. Korištenjem suvremenih računalnih metoda, uključujući strojno učenje i sofisticirane algoritme za pretraživanje, tim je uspio prodrijeti u složenu strukturu šifre.

Cilj ovog rada je detaljno istražiti proces dešifriranja Zodijakove šifre, naglašavajući znanstvene metode i tehnološke inovacije koje su omogućile ovaj proboj. Analizirat ćemo

povijesni kontekst Zodijakovih komunikacija, prirodu njegovih šifri i izazove s kojima su se suočili istraživači tijekom godina. Također ćemo ispitati utjecaj ovog otkrića na polje kriptografije i kriminalistike, kao i na javnu percepciju jednog od najzloglasnijih neriješenih slučajeva.

Rad se sastoji od pet poglavlja. U prvom poglavlju pod naslovom Klasična kriptografija definiraju se osnovni pojmovi iz kriptografije, opisuje se više vrsta supstitucijskih šifri te transpozicijska šifra, a sve je popraćeno primjerima za bolje shvaćanje teorijskog dijela. Glavni izvor bila je knjiga *Kriptografija* [4] Prvo je poglavlje iznimno bitno za razumijevanje ostalih poglavlja ovog rada, a osobito onim čitateljima koji nisu upoznati s teorijom kriptografije.

U drugom poglavlju pod nazivom Šifra Z408 predstavlja se prva Zodijakova šifra poslana 1969. godine, a u uvodu se mogu vidjeti i originalna pisma od kojih je šifra sastavljena, preuzeta sa stranice *Zodiac Killer* [12]. U nastavku se detaljno opisuju metode kojima su Donald i Bettye Harden dešifrirali šifru Z408 svega nekoliko dana nakon njezine objave, a na kraju se može pronaći otvoreni tekst.

Poglavlje pod nazivom Šifra Z340 strukturirano je vrlo slično kao prethodno poglavlje. Glavna je razlika u tome što je proces dešifriranja šifre Z340 trajao više od 50 godina, dok je šifra Z408 dešifrirana vrlo brzo. Samim tim dio poglavlja koji opisuje metode korištene u dešifriranju i zaključke koje su analitičari donosili puno je duži i kompleksniji. Glavni izvor za ovo poglavlje bio je rad *The Solution of the Zodiac Killer's 340-Character Cipher* [8] koji su napisala trojica zaslužna za konačno razbijanje ove šifre.

Četvrto i peto poglavlje ovog rada, Šifra Z13 i Šifra Z32, najkraća su, a glavni razlog tome je što su i same šifre o kojima govore poglavlja bile iznimno kratke zbog čega su do danas ostale nerješene. U zadnja se dva poglavlja kratko opisuju strukture obje šifre i daje se uvid u pokušaje dešifriranja te teorije i spekulacije koje stoje iza njih.

Diplomski rad napravljen je u sklopu aktivnosti Projekta PK.1.1.02.0004- Znanstveni centar izvrsnosti za kvantne i kompleksne sustave te reprezentacije Liejevih algebri.

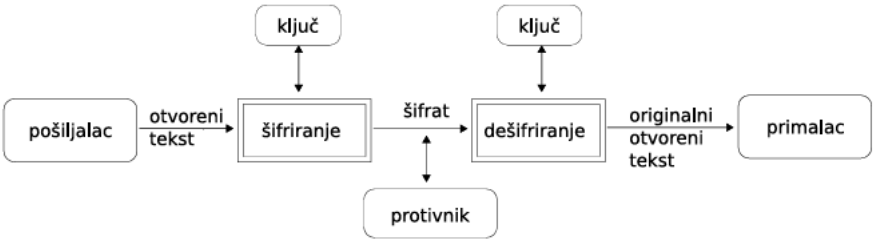
Poglavlje 1

Klasična kriptografija

Kriptografija je znanstvena disciplina koja se bavi proučavanjem metoda za slanje poruka u takvom obliku da ih samo onaj kome su namijenjene može pročitati.

Temeljni cilj kriptografije je omogućiti da dvije osobe, nazovimo ih *pošiljatelj* i *primalac*, sigurno komuniciraju tako da treća osoba koja nadzire komunikacijski kanal ne može razumjeti poruku koju razmjenjuju.

Poruka koju pošiljatelj želi prenijeti primatelju naziva se *otvoreni tekst* (engl. plaintext). Kako bi spriječio da prisluškivač otkrije sadržaj poruke, pošiljatelj primjenjuje postupak *šifriranja*, odnosno pretvara otvoreni tekst u *šifrat* (engl. ciphertext) ili *kriptogram* koristeći unaprijed dogovoreni *ključ* (engl. key). Ovaj šifrirani oblik poruke može se sigurno slati jer je bez tajnog ključa, koji služi kao osnova za šifriranje i dešifriranje, sadržaj nečitljiv. Legitiman primatelj, koristeći ključ, može dešifrirati šifrat i doći do izvornog sadržaja poruke, dok napadač, bez ključa, nema mogućnost razumijevanja šifriranog teksta.



Slika 1.1: Shema klasične kriptografije

Različite metode šifriranja tijekom povijesti uključivale su zamjenu elemenata poruke (supstituciju) ili njihov preustroj (transpoziciju). Danas se ove metode koriste u kombinaciji u modernim simetričnim šifriranim sustavima, dok asimetrični sustavi, uvedeni 70-tih

godina 20. stoljeća, koriste matematičke funkcije temeljene na jednosmjernim procesima za dodatnu sigurnost.

1.1 Supstitucijska šifra

Supstitucijska šifra je vrsta kriptografskog algoritma koji se temelji na zamjeni znakova iz otvorenog teksta drugim znakovima prema unaprijed definiranim pravilima. Ova metoda šifriranja jedna je od najstarijih i najjednostavnijih, a koristi se za zaštitu informacija tako da njihov sadržaj postane nečitljiv bez pristupa odgovarajućem ključu. U povijesti su supstitucijske šifre bile ključne za sigurno komuniciranje, osobito tijekom ratova i tajnih operacija, ali su i danas osnova mnogih modernih kriptografskih sustava.

Supstitucijska šifra funkcionira tako da svako slovo abecede iz otvorenog teksta zamijeni odgovarajućim slovom prema šifrirnom ključu. Ključ može biti jednostavna permutacija abecede ili složeniji skup pravila koji određuje kako se znakovi zamjenjuju. Jedan od najpoznatijih primjera jednostavne supstitucijske šifre je *Cezarova šifra*, gdje se slova pomiču za unaprijed definirani broj mjesta u abecedi.

Matematički zapis supstitucijske šifre može se izraziti kao:

$$C_i = E(P_i, K)$$

gdje je:

- C_i - šifrirani znak,
- P_i - znak otvorenog teksta,
- K - ključ šifriranja,
- E - funkcija šifriranja.

Supstitucijske šifre razlikuju se prema složenosti i otpornosti na napade, a neke od značajnijih su:

1. **Cezarova šifra**: Svako slovo zamjenjuje se slovom koje se nalazi nekoliko mjesta dalje u abecedi.
2. **Polialfabetska supstitucija**: U ovoj šifri koristi se više šifriranih abeceda koje se izmjenjuju prema određenom obrascu, primjerice u *Vigenèreovoj šifri*.
3. **Monoalfabetska šifra**: Svako slovo zamjenjuje se istim slovom ili simbolom tijekom cijelog procesa šifriranja.
4. **Homofonska supstitucija**: Svako slovo otvorenog teksta zamjenjuje se s jednim od više mogućih simbola.

Cezarova šifra

Cezarova šifra jedna je od najstarijih metoda šifriranja, nazvana po rimskom vojskovođi Juliju Cezaru. Temelji se na zamjeni svakog slova otvorenog teksta slovom koje se nalazi nekoliko mjesta dalje u abecedi, pri čemu se koristi unaprijed određeni broj mjesta, poznat kao ključ šifriranja. Ovaj jednostavan algoritam koristi ciklički princip, tako da se nakon posljednjeg slova abecede zamjena nastavlja od početka.

Matematički, šifriranje Cezarovom šifrom može se zapisati kao:

$$C_i = (P_i + K) \mod N$$

gdje su:

- C_i - šifrirano slovo (šifrat),
- P_i - slovo otvorenog teksta,
- K - ključ, tj. broj mjesta za pomak,
- N - broj slova u abecedi (za englesku abecedu $N = 26$).

Dešifriranje se provodi prema formuli:

$$P_i = (C_i - K) \mod N$$

Primjer 1.1.1. *Šifriranje riječi* `SIFRA ZODIAC`

Pretpostavimo da želimo šifrirati izraz `SIFRA ZODIAC` *koristeći ključ* $K = 5$. *Za ovaj primjer koristimo englesku abecedu gdje* $A = 0$, $B = 1$, ..., $Z = 25$.

1. *Zamijenimo slova brojčanim vrijednostima:*

$$S = 18, I = 8, F = 5, R = 17, A = 0, Z = 25, O = 14, D = 3, I = 8, A = 0, C = 2.$$

2. *Primijenimo formulu šifriranja* $C_i = (P_i + K) \mod 26$*:*

$$
\begin{aligned}
S &\to (18 + 5) \mod 26 = 23\,(X)\\
I &\to (8 + 5) \mod 26 = 13\,(N)\\
F &\to (5 + 5) \mod 26 = 10\,(K)\\
R &\to (17 + 5) \mod 26 = 22\,(W)\\
A &\to (0 + 5) \mod 26 = 5\,(F)\\
Z &\to (25 + 5) \mod 26 = 4\,(E)\\
O &\to (14 + 5) \mod 26 = 19\,(T)\\
D &\to (3 + 5) \mod 26 = 8\,(I)\\
I &\to (8 + 5) \mod 26 = 13\,(N)\\
A &\to (0 + 5) \mod 26 = 5\,(F)\\
C &\to (2 + 5) \mod 26 = 7\,(H).
\end{aligned}
$$

3. *Šifrirani tekst (šifrat) je:* `XNKWF ETINFH`*.*

Primjer 1.1.2. *Dekriptirati šifrat* `XQKPTHWZQNUI` *dobiven Cezarovom šifrom.*

Budući da prostor ključeva kod Cezarove šifre nije velik (ima ih 26), zadatak možemo riješiti grubom silom, tj. ispitivanjem svih mogućih ključeva dok ne dođemo do smislene poruke. Za različite vrijednosti ključa K*, dobivamo redom:*

$$
\begin{aligned}
K = 1 &\quad WPLJSGVYPTH\\
K = 2 &\quad VOKIRFUXOSE\\
K = 3 &\quad UNJHQETWNRD\\
K = 4 &\quad TMIGPDSVMQC\\
K = 5 &\quad SLHFOCRULPB\\
K = 6 &\quad RKGENDQTKOA
\end{aligned}
$$

Kada dođemo do ključa $K = 14$*, dobivamo smislenu poruku:* `OVO JE PORUKA`*. Dakle, ključ je* $K = 14$*, a otvoreni tekst je* `OVO JE PORUKA`*.*

Zaključak

Cezarova šifra jednostavna je metoda šifriranja koja pruža osnovnu razinu sigurnosti, ali je lako ranjiva na napade poput iscrpne pretrage ili frekvencijske analize. Ipak, ona je važna zbog povijesnog značaja i kao temelj za složenije kriptografske algoritme.

Vigenèreova šifra

Vigenèreova šifra jedna je od najpoznatijih *polialfabetskih šifri*, koja je značajno unaprijedila sigurnost šifriranja u odnosu na jednostavne monoalfabetske šifre poput Cezarove. Nazvana je po Blaiseu de Vigenèreu[1], iako su slične metode poznate i prije njegovog rada. Ova šifra koristi niz šifriranih abeceda koje se izmjenjuju prema unaprijed definiranom obrascu, čime otežava frekvencijsku analizu i povećava sigurnost poruke.

Glavna ideja Vigenèreove šifre je uporaba ključa u obliku riječi ili fraze koji određuje kojim redoslijedom se koriste šifrirane abecede. Svako slovo otvorenog teksta šifrira se prema odgovarajućem slovu ključa.

Matematički zapis Vigenèreove šifre je:

$$C_i = (P_i + K_j) \mod N$$

gdje su:

- C_i: šifrirani znak (šifrat),
- P_i: znak otvorenog teksta,
- K_j: znak ključa, koji se periodično ponavlja,
- N: broj znakova u abecedi (za englesku abecedu $N = 26$).

Dešifriranje se provodi prema obrnutom postupku:

$$P_i = (C_i - K_j) \mod N$$

Primjer 1.1.3. *Pretpostavimo da želimo šifrirati poruku* `KRIPTOGRAFIJA` *koristeći ključ* `KLJUC` *i englesku abecedu.*

1. *Ponavljamo ključ tako da odgovara duljini poruke:*

   `KRIPTOGRAFIJA  KLJUCKLJUCKLJ`

2. *Pretvaramo slova u njihove brojčane vrijednosti i prikazujemo ih u tablici:*

[1] Blaise de Vigenère (1523.–1596.) bio je francuski diplomat, kriptograf, prevoditelj i alkemičar.

Poruka	K	R	I	P	T	O	G	R	A	F	I	J	A
Vrijednost	10	17	8	15	19	14	6	17	0	5	8	9	0
Ključ	K	L	J	U	C	K	L	J	U	C	K	L	J
Vrijednost	10	11	9	20	2	10	11	9	20	2	10	11	9

Tablica 1.1: Pretvorba slova u brojčane vrijednosti

3. *Šifriramo pomoću formule* $C_i = (P_i + K_j) \mod 26$*:*

$$
\begin{aligned}
K + K &\rightarrow (10 + 10) \mod 26 = 20\,(U)\\
R + L &\rightarrow (17 + 11) \mod 26 = 2\,(C)\\
I + J &\rightarrow (8 + 9) \mod 26 = 17\,(R)\\
P + U &\rightarrow (15 + 20) \mod 26 = 9\,(J)\\
T + C &\rightarrow (19 + 2) \mod 26 = 21\,(V)\\
O + K &\rightarrow (14 + 10) \mod 26 = 24\,(Y)\\
G + L &\rightarrow (6 + 11) \mod 26 = 17\,(R)\\
R + J &\rightarrow (17 + 9) \mod 26 = 0\,(A)\\
A + U &\rightarrow (0 + 20) \mod 26 = 20\,(U)\\
F + C &\rightarrow (5 + 2) \mod 26 = 7\,(H)\\
I + K &\rightarrow (8 + 10) \mod 26 = 18\,(S)\\
J + L &\rightarrow (9 + 11) \mod 26 = 20\,(U)\\
A + J &\rightarrow (0 + 9) \mod 26 = 9\,(J)
\end{aligned}
$$

Šifrirani tekst (šifrat) je: `UCRJVYRAUHSUJ`*.*

Zaključak

Vigenèreova šifra pruža veću sigurnost od jednostavnih supstitucijskih šifri jer koristi više šifriranih abeceda, čineći frekvencijsku analizu znatno težom. Međutim, njezina otpornost ovisi o duljini i složenosti ključa – ako je ključ prekratak ili prejednostavan, šifra može biti ranjiva na analizu poput Kasiskijeve metode[2]. Usprkos tome, Vigenèreova šifra ima povijesni značaj i predstavlja temelj za daljnji razvoj kriptografskih metoda.

[2]Metoda se zove Kasiskijev test i uveo ju je Friedrich Kasiski 1863. godine. Zasniva na činjenici da će dva identična odsječka otvorenog teksta biti šifrirana na isti način ukoliko se njihove početne pozicije razlikuju za neki višekratnik od m. Obrnuto, ako uočimo dva identična odsječka u šifratu, duljine barem 3, tada je vrlo vjerojatno da oni odgovaraju identičnim odsječcima otvorenog teksta.

Za više detalja o kriptoanalizi Vigenèreove šifre i svim korištenim metodama pročitajte knjigu *Kriptografija* [4] ili pogledajte stranicu iz kolegija *Kriptografija i sigurnost mreža* [3] `https://web.math.pmf.unizg.hr/~duje/kript/vigener.html`

Homofonska supstitucijska šifra

Homofonska supstitucijska šifra poseban je oblik supstitucijske šifre u kojem se najfrekventnijim slovima otvorenog teksta pridružuje više različitih simbola šifriranog teksta. Ova tehnika pomaže u skrivanju frekvencijskih obrazaca slova u tekstu, što otežava kriptoanalizu.

Primjer 1.1.4. *Šifrirajmo poruku* `SIFRA ZODIAC`.

Prvo, izradimo tablicu homofonske supstitucije gdje svakom slovu abecede dodjeljujemo skup mogućih simbola:

Slovo	A	B	C	D	E	F
Simboli	12, 45, 78	34, 56	23, 67, 89	14, 58	11, 22, 33, 44	25, 68
Slovo	G	H	I	J	K	L
Simboli	19, 49	29, 59	13, 46, 79	35, 57	16, 69	24, 66
Slovo	M	N	O	P	Q	R
Simboli	18, 48	26, 77	15, 55, 85	21, 61	31, 71	17, 47, 87
Slovo	S	T	U	V	W	X
Simboli	27, 76	32, 72	36, 86	38, 88	39, 89	41, 91
Slovo	Y	Z				
Simboli	42, 92	43, 93				

Tablica 1.2: Tablica mogućih simbola za svako slovo

Sada, za svako slovo u poruci `SIFRA ZODIAC` *nasumično biramo jedan od dodijeljenih simbola:*

Slovo	S	I	F	R	A	Z	O	D	I	A	C
Odabrani simbol	27	46	68	87	12	93	55	14	79	45	67

Tablica 1.3: Odabrani simboli za svako slovo u poruci `SIFRA ZODIAC`

Šifrirani tekst bi bio niz odabranih simbola: `27 46 68 87 12 93 55 14 79 45 67`.

Zaključak

Prednost homofonske supstitucije je povećana otpornost na frekvencijsku analizu, jer ravnomjernija distribucija simbola otežava prepoznavanje uzoraka. Međutim, glavni nedosta-

tak je složenost u izradi i upravljanju velikim brojem simbola, što može povećati mogućnost pogrešaka i zahtijeva složenije ključeve.

Iako homofonska supstitucija pruža bolju sigurnost od jednostavnih supstitucijskih šifri, razvoj modernih kriptografskih tehnika i povećana računalna snaga učinili su ovu metodu manje praktičnom u suvremenoj primjeni.

1.2 Transpozicijska šifra

Transpozicijska šifra je metoda šifriranja u kojoj se znakovi otvorenog teksta preuređuju prema određenom sustavu, mijenjajući njihov redoslijed bez promjene samih znakova. Matematički gledano, transpozicija je bijektivna funkcija, što znači da svaki znak otvorenog teksta ima jedinstvenu poziciju u šifriranom tekstu i obrnuto.

Transpozicijska šifra s periodom 19 predstavlja specifičan slučaj *stupčane transpozicijske šifre*. U ovoj metodi šifriranja, otvoreni tekst organizira se u redove od po 19 znakova, nakon čega se znakovi preuređuju prema unaprijed određenom ključu kako bi se dobio šifrirani tekst.

Stupčane transpozicijske šifre temelje se na upisivanju otvorenog teksta u pravokutnu tablicu po redcima te kasnijem čitanju znakova prema unaprijed određenom rasporedu stupaca. U ovom slučaju, broj stupaca jednak je duljini perioda, odnosno 19, što znači da se poruka prvo ispisuje u redove širine 19 znakova prije nego što se stupci premjeste u novom poretku.

Ovakve šifre često se analiziraju koristeći tehnike poput prepoznavanja uzoraka u ponavljanjima slova i frekvencijske analize razmaka između istih simbola. Više informacija o stupčanoj transpozicijskoj šifri i njezinoj kriptoanalizi dostupno je u materijalima kolegija *Kriptografija i sigurnost mreža*[3] i na stranici `https://web.math.pmf.unizg.hr/~duje/kript/transp.html`.

Primjer 1.2.1 (Transpozicijska šifra s periodom 19)**.** *Razmotrimo otvoreni tekst:*
KRIPTOGRAFIJA JE ZANIMLJIVA DISCIPLINA
Prije svega, potrebno je ukloniti sve razmake i interpunkcijske znakove iz otvorenog teksta kako bismo dobili kontinuirani niz znakova:
KRIPTOGRAFIJAJEZANIMLJIVADISCIPLINA
Nakon toga, podijelimo niz znakova u redove, pri čemu svaki red sadrži točno 19 znakova (jer se radi o periodu 19). Ako posljednji red nema dovoljno znakova, dodamo proizvoljna slova (nule) koja ne mijenjaju sadržaj poruke.
KRIPTOGRAFIJAJEZANIML
JIVADISCIPLINAXXXXXXX
Za kraj, potrebno je promijeniti redoslijed stupaca prema unaprijed dogovorenom ključu.

Na primjer, ako je ključ permutacija stupaca [3, 1, 4, 2], to znači da će treći stupac postati prvi, prvi će postati drugi, četvrti će postati treći, a drugi će postati četvrti.

Originalni redoslijed stupaca:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
K	R	I	P	T	O	G	R	A	F	I	J	A	J	E	Z	A	N	I
J	I	V	A	D	I	S	C	I	P	L	I	N	A	X	X	X	X	X

Nakon permutacije stupaca prema ključu:

3	1	4	2	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
I	K	P	R	T	O	G	R	A	F	I	J	A	J	E	Z	A	N	I
V	J	A	I	D	I	S	C	I	P	L	I	N	A	X	X	X	X	X

Ovim postupkom dobivamo šifrirani tekst:
IVKJPAIRTOGRODICAFISPLIJANAXJEXZAXNIX

Zaključak

Transpozicijske šifre same po sebi ne pružaju visoku razinu sigurnosti jer ne mijenjaju sastav poruke, već samo redoslijed znakova. Međutim, njihova otpornost na analizu može se značajno povećati primjenom višestrukih iteracija (rundi) šifriranja. Ova tehnika omogućuje kompleksniju preraspodjelu znakova, čime se dodatno otežava analiza šifriranog teksta.

Zbog svoje jednostavne, ali učinkovite strukture, transpozicijske šifre se i danas koriste u modernim simetričnim kriptografskim sustavima. Najpoznatiji primjer je *Substitution–Permutation Network (SPN)*[3], gdje transpozicija igra ključnu ulogu u povećanju difuzije podataka, odnosno raspodjeli informacija unutar šifriranog teksta kako bi se smanjila predvidljivost ulaznih podataka.

Ova kombinacija supstitucije i transpozicije čini temelj mnogih suvremenih šifri, uključujući *Advanced Encryption Standard (AES)*[4], čija sigurnost dolazi upravo iz primjene višestrukih rundi permutacija i zamjena podataka. Stoga, iako su transpozicijske šifre same po sebi relativno slabe, njihova integracija u složenije kriptografske sustave i dalje igra ključnu ulogu u modernoj sigurnosti podataka.

[3] SPN je struktura koja kombinira supstitucijske i transpozicijske operacije kako bi se osigurala snažna enkripcija. Više informacija dostupno je na: `https://en.wikipedia.org/wiki/Substitution-permutation_network`.

[4] AES je jedan od najvažnijih modernih simetričnih kriptosustava koji se koristi širom svijeta za zaštitu podataka. Više informacija dostupno je na: `https://en.wikipedia.org/wiki/Advanced_Encryption_Standard`.

Poglavlje 2

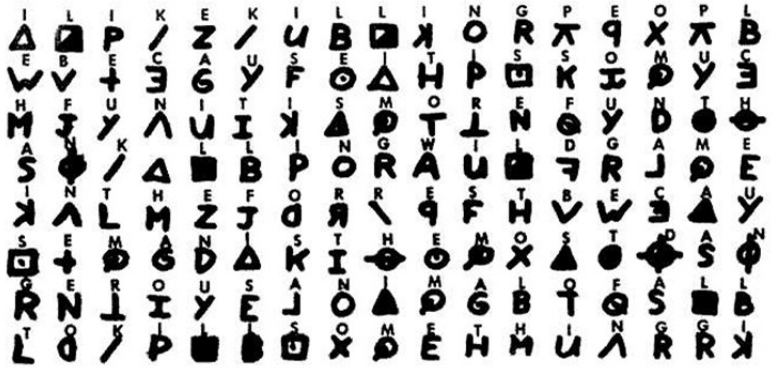
Šifra Z408

2.1 Uvod

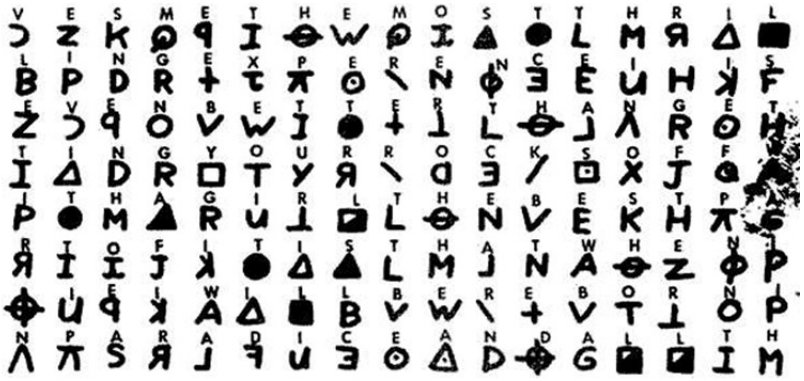
Šifra Z408 predstavlja prvu i jednu od najpoznatijih šifriranih poruka koje je Zodijak poslao tijekom svoje kriminalne aktivnosti, čime je započeo jedan od najintrigantnijih misterija u povijesti kriminalistike.

Dana 31. srpnja 1969., na adrese triju novinarskih redakcija u sjevernoj Kaliforniji– the Vallejo Times-Herald, San Francisco Examiner i the San Francisco Chronicle–stigla su gotovo identična pisma od osobe koja je tvrdila da je odgovorna za nedavna ubojstva u tom području.

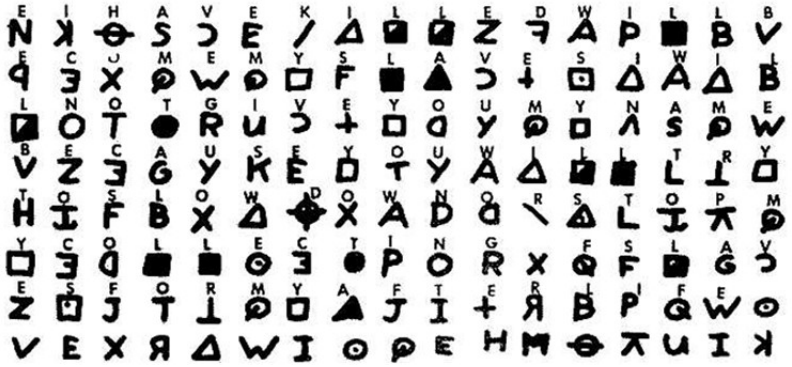
Svako od tih pisama sadržavalo je trećinu šifrirane poruke od 408 simbola, poznate kao Z408, uz zahtjev da se šifra objavi na naslovnici novina. U protivnom, Zodijak je prijetio nastavkom svojih zločina, što je dodatno povećalo pritisak na novinare i vlasti.



Slika 2.1: Prvi dio pisma, poslan novinama Vallejo Times-Herald 31.7.1969.
(izvor: www.ZodiacKiller.com[12])



Slika 2.2: Drugi dio pisma, poslan novinama San Francisco Chronicle 31.7.1969.
(izvor: www.ZodiacKiller.com[12])



Slika 2.3: Treći dio pisma, poslan novinama San Francisco Examiner 31.7.1969.
(izvor: www.ZodiacKiller.com[12])

Sve izdavačke kuće odlučile su objaviti svoje dijelove šifriranog teksta. Objavljivanjem šifre, mediji su ne samo ispunili Zodijakov zahtjev nego su i omogućili širem krugu ljudi da se uključe u njeno rješavanje. Ovaj potez označio je početak masovne suradnje između institucija i entuzijasta diljem svijeta.

Nakon objave šifre, lokalna policija zatražila je pomoć od američke mornarice, FBI-a i Kalifornijskog istražnog ureda. Osim službenih agencija, u rješavanje šifre bio je uključen i Donald C. B. Marsh, predsjednik Američkog udruženja kriptograma. Njegovo iskustvo i ugled u području kriptografije bili su ključni za koordinaciju i analizu šifriranog teksta. Ipak, unatoč uloženim resursima i stručnosti uključenih institucija, dešifriranje Z408 nije bilo jednostavno. Kombinacija inovativnih tehnika šifriranja i Zodijakovog specifičnog stila izražavanja dodatno je otežala rješavanje.

Proces rješavanja šifre postao je svojevrsna intelektualna utrka, uključujući profesi-

onalne kriptografe, amatere i znanstvenike iz različitih disciplina. Rješavanje Z408 zahtijevalo je ne samo tehničke vještine već i razumijevanje Zodijakovog načina razmišljanja, što je dodatno istaknulo kompleksnost ovog slučaja.

2.2 Metode dešifriranja

Dana 8. kolovoza 1969., osam dana nakon što je šifra poslana poštom, San Francisco Chronicle primio je rješenje od Donalda Hardena, školskog učitelja iz Salinasa, i njegove supruge Bettye, koji su riješili šifru nakon što su je vidjeli u novinama. Hardenovi su pokazali iznimnu intuiciju i upornost, koristeći jednostavne, ali efikasne metode, koje su na kraju dovele do razotkrivanja značenja šifre Z408. Ovaj uspjeh ih je učinio prvima koji su uspjeli razbiti Zodijakovu poruku, privlačeći pažnju medija i vlasti.

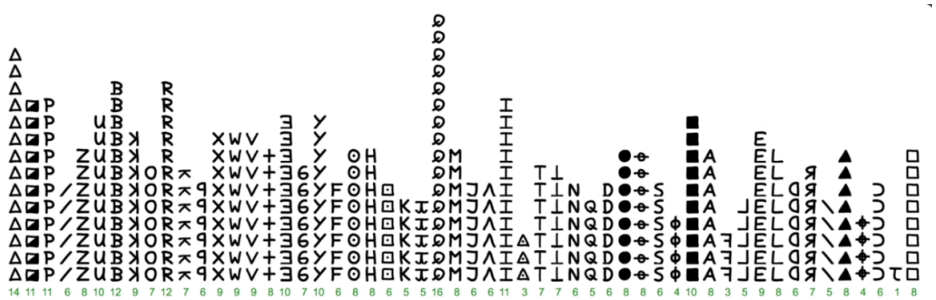
Šifra Z408 šifrirana je kao *supstitucijska homofona šifra*. Ova tehnika šifriranja uključuje zamjenu pojedinih slova ili riječi otvorenog teksta s više različitih simbola kako bi se otežala *frekvencijska analiza*, osnovna metoda za dešifriranje teksta. Zodijak je u ovom slučaju koristio 54 različita simbola za kodiranje poruke od 408 znakova, čime je uspješno prikrio uobičajene jezične uzorke.

Osnovna metoda za analizu šifriranog teksta temelji se na *frekvencijskoj analizi*. Ova metoda uključuje brojanje učestalosti svakog znaka unutar šifrata te usporedbu rezultata s poznatim statistikama raspodjele znakova u jeziku koji pretpostavljamo da je korišten u otvorenom tekstu. Uz analizu pojedinačnih znakova, korisne informacije mogu pružiti i podaci o najčešćim parovima slova (*bigramima*) ili nizovima od tri slova (*trigramima*).

Slovo	**Učestalost (%)**	**Slovo**	**Učestalost (%)**	**Slovo**	**Učestalost (%)**
E	12.70	T	9.06	A	8.17
O	7.51	I	6.97	N	6.75
S	6.33	H	6.09	R	5.99
D	4.25	L	4.03	C	2.78
U	2.76	M	2.41	W	2.36
F	2.23	G	2.02	Y	1.97
P	1.93	B	1.49	V	0.98
K	0.77	J	0.15	X	0.15
Q	0.10	Z	0.07		

Tablica 2.1: Najfrekventnija slova u engleskom jeziku i njihova učestalost.

U tablici 2.1 prikazana je učestalost pojedinih slova u engleskom jeziku. Najfrekventniji bigrami su TH (3.2%), HE (2.5%), AN, IN, ER, RE, ON, ES, TI, AT (1.2%), a trigrami THE (3.5%), ING (1.1%), AND (1.0%), ION,...



Slika 2.4: Frekvencijska analiza šifre Z408,
(izvor: www.youtube.com, David Oranchak)

Nakon frekvencijske analize sva tri pisma, prikazane na slici 2.4, analitičari uočavaju da ima 54 različita simbola, dok je slova u engleskoj abecedi samo 26, iz čega je jasno da se radi o *homofonskoj supstitucijskoj šifri* (eng. *simple-substitution cipher with suppression of frequencies, homophonic substitution, substitution with variance*).

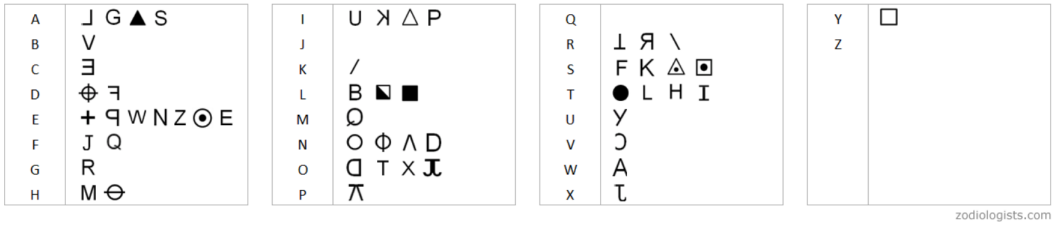
Sljedeći korak frekvencijske analize bio je uočavanje simbola koji se pojavljuju u parovima. Prema analizi u knjizi *The Secret and Urgent: The Story of Codes and Ciphers*[9], najfrekventniji parovi u engleskom su LL (1.9%), SS (1.5%), EE, OO, TT. S obzirom da je LL najčešći par istih slova, bilo je logično krenuti od pretpostavke da simboli ■ i ◪ predstavljaju slovo **L**.

Nakon što je slovo L uvršteno u šifrat, uočeni su uzorci ⁄ᑌᗷ**L**, ⁄Δ**L**ᗷ, ⁄ᑭ**L**ᗷ, ⁄Δ**LL** od četiri simbola. Uzimajući u obzir činjenicu da je pisma poslao serijski ubojica, bilo je za očekivati da će ista sadržavati riječ KILL (hrv. ubiti). Tako su Hardenovi zaključili da simboli ⁄ i Δ predstavljaju slovo **I**, ⁄ slovo **K** te da je ᗷ još jedan simbol za slovo **L**.

Slika 2.5: Prvi red šifre Z408 tokom dešifriranja,
(izvor: www.youtube.com, David Oranchak[7])

Ugledavši početak pisma prikazan na slici 2.5., Bettye Harden, vođena intuicijom, pretpostavila je da je Zodiac započeo svoje obraćanje svijetu sa ”I LIKE KILLING”.

Za nastavak nije bilo bolje metode od ”grube sile”, odnosno isprobavanjem svih mogućih varijanti dok se ne dobije nešto smisleno. To je vrlo dug i mukotrpan proces, a bračni par je dan i noć pokušavao. Na sreću, njihov se trud isplatio i 7. kolovoza kontaktirali su novine i policiju dostavivši svoje rješenje i *ključ* prikazan na slici 2.6



Slika 2.6: Ključ šifre Z408, (izvor: www.zodiologists.com[14])

U kriptografiji, *ključ* predstavlja tajni parametar koji se koristi u algoritmima za šifriranje i dešifriranje podataka. On određuje specifičan način na koji će se podaci transformirati iz čitljivog u nečitljiv oblik i obrnuto. Sigurnost kriptografskog sustava uvelike ovisi o tajnosti i kompleksnosti ključa.

Otvoreni tekst

Otvoreni tekst je tekstualni sadržaj poruke prije nego što je podvrgnut šifriranju. U kontekstu kriptografije, predstavlja čitljiv i razumljiv jezik koji se pretvara u šifrirani tekst pomoću šifre.

U nastavku slijedi otvoreni tekst Zodijakovih pisama koji je objavljen 9. kolovoza 1969. u novinama San Francisco Chronicle.

> ”I like killing people because it is so much fun it is more fun than killing wild game in the *forest* because man is the most *hongertue* animal of all to kill something *give eryetheyo a* thrilling experience it is even better than getting your rocks off with a girl the best part of it *ia thae* when I die I will be reborn in paradice and all the I have killed will become my slaves I will not give you my name because you will try to *sloi* down or *atop* my collecting of slaves for my afterlife *ebeorietemethhpiti*”

Zodijakov otvoreni tekst sadrži brojne pravopisne pogreške, poput ”forrest” umjesto ”forest”, ”ia thae” umjesto ”is that”ili ”sloi” umjesto ”slow”. Ove pogreške mogu biti namjerne kako bi zbunile istražitelje ili odraz pisčeve nepažnje i brzopletosti, kao i dokaz koliko je njegova šifra i njemu samom bila komplicirana i zamršena.

Osim glavnog dešifriranog dijela šifre, na kraju se nalazi nejasan dio s 18 znakova, čije značenje još uvijek nije utvrđeno. Prema jednoj teoriji, ovi simboli su jednostavno kopirani iz prethodnog dijela šifre kako bi se popunio prostor, čineći treći dio šifre jednakim po veličini s prva dva. Dok dio analitičara i obožavatelja vjeruje da ovaj dio samo zahtijeva dodatni proces dešifriranja kako bi se otkrilo njegovo pravo značenje te da je Zodijak možda otkrio svoje ime upravo u tom dijelu.

Poglavlje 3

Šifra Z340

Zodijakova druga šifra, poznata kao Z340, poslana je novinarskoj redakciji San Francisco Chronicle, 8. studenog 1969. godine. Za razliku od Z408, koja je uspješno dešifrirana relativno brzo zahvaljujući kombinaciji logičkog razmišljanja i osnovnih kriptografskih tehnika, Z340 je ostala neriješena 51 godinu, postavivši se kao jedna od najtrajnijih misterija u povijesti kriminalistike i kriptografije.

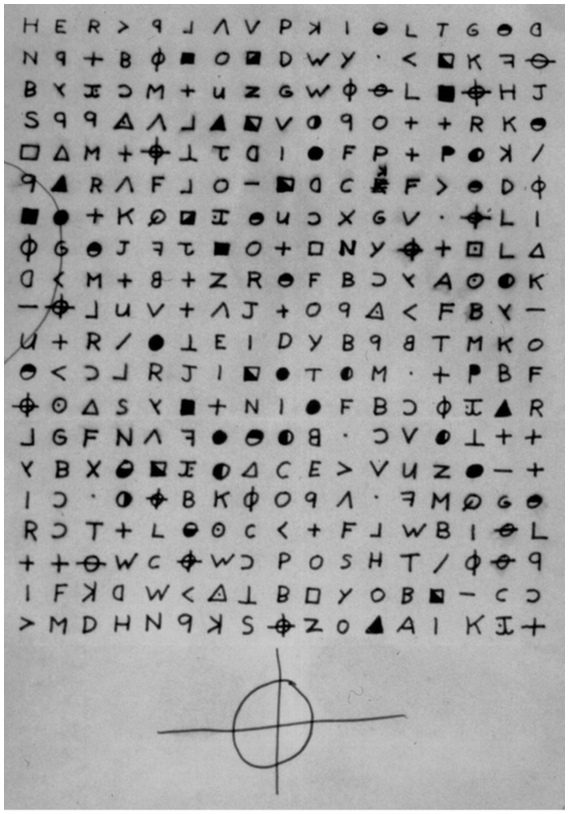
3.1 Zapažanja i analize

Godine 2012. David Oranchak pokrenuo je inicijativu za prikupljanje svih relevantnih činjenica i zapažanja o Zodijakovim šiframa, uključujući poznatu Z340 šifru. Cilj ove inicijative, realizirane putem web-stranice *zodiackillerciphers.com*[13], bio je stvoriti strukturiranu bazu podataka koja bi istraživačima omogućila lakše eksperimentiranje i otkrivanje potencijalnih rješenja. Nepoznati način šifriranja Z340 šifre otvarao je beskonačan broj mogućnosti, a prikupljena zapažanja trebala su poslužiti kao smjernice za usmjeravanje istraživanja.

Prema članku *The Solution of the Zodiac Killer's 340-Character Cipher*[8], od kud su preuzete i sve slike u ovom podpoglavlju, tijekom godina istaknulo se nekoliko ključnih zapažanja o šifri Z340 koja su imala značajan utjecaj na daljnje analize i pokušaje dešifriranja.

Cikličko korištenje homofona

Šifra Z408 pokazuje izrazito snažan obrazac cikličkog korištenja homofona. To znači da se za određeno slovo otvorenog teksta često koriste zamjenski simboli iz ponavljajuće sekvence šifriranih znakova. Primjer ovog cikličkog uzorka prikazan je na slici 3.2.



Slika 3.1: Pismo objavljeno u novinama San Francisco Examiner, 31.7.1969., (izvor: www.ZodiacKiller.com[12])

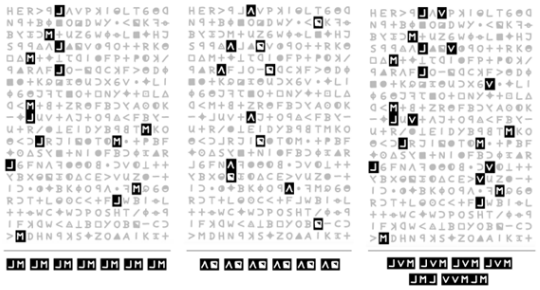
S druge strane, kao što je prikazano na slici 3.3, šifra Z340 pokazuje sličan, ali manje izražen obrazac cikličkog korištenja homofona. Pretpostavlja se da je ovaj obrazac mogao biti poremećen specifičnom metodom šifriranja korištenom u Z340, što dodatno otežava analizu i dešifriranje.

Novi simboli

Šifra Z340 sadrži dvadeset simbola koji nisu korišteni u šifri Z408, što čini gotovo četvrtinu cijelog Z340 šifriranog teksta. Dodavanje ovih simbola značajno povećava *prostor ključeva*, odnosno ukupan broj mogućih ključeva koji se mogu koristiti u šifriranju ili dešifriranju, za Z340, čineći ga 26^9 puta većim u usporedbi s prostorom ključeva za Z408.

Ovo povećanje složenosti čini Z340 znatno težom za analizu i dešifriranje u usporedbi sa Z408. Kraća duljina šifre Z340 dodatno smanjuje količinu dostupnih podataka za analizu, što predstavlja dodatni izazov za kriptografe.

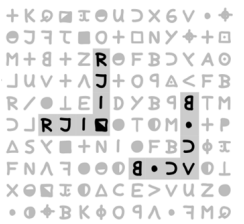
Slika 3.2: Cikličko korištenje homofona u šifri Z408



Slika 3.3: Cikličko korištenje homofona u šifri Z340

Neobični uzorci

Šifra Z340 pokazuje neobične uzorke, poput ponavljajućih ”obrnuto L” oblika sastavljenih od trigrama koji se ponavljaju vertikalno i horizontalno, povezani zajedničkim četvrtim simbolom. Ovi identično orijentirani oblici prvi su uočeni 2010. godine na internetskom forumu posvećenom Zodijaku. Njihova rijetkost u uobičajenim supstitucijskim šiframa i slučajnim permutacijama Z340 sugerira namjerni postupak šifriranja koji nadilazi homofonsku supstituciju. Dodatno, prisutnost ovih uzoraka ukazuje na mogućnost da je osnovni otvoreni tekst vrlo repetitivan, što može biti rezultat primjene transpozicijskih tehnika tijekom šifriranja.



Slika 3.4: Uzorak ”obrnuto L” u šifri Z340

3.2 Metode dešifriranja

Godine 2020., tijekom karantene usred pandemije virusa COVID-19, međunarodni tim koji su sačinjavali programer David Oranchak, matematičar Sam Blake i amaterski kriptograf (inače skladišni radnik) Jarl Van Eycke konačno je uspio zajedničkim snagama dešifrirati ovu zagonetnu poruku.

U videima na svom Youtube kanalu, David Oranchak iznosi ideju da je šifra Z340 i *homofonska supstitucijska* i *transpozicijska šifra*. David je iznio jednu posebnu transpoziciju, koju su 2015. godine neovisno otkrili Jarl Van Eycke i korisnik foruma o Zodijaku pod pseudonimom "daikon". Oni su primijetili povećanje broja bigrama pri periodu 19, što je ukazivalo na mogući obrazac transpozicije u šifri Z340.

Odgovarajuća transpozicija

U današnje vrijeme, za razliku od Zodijakovog vremena, postoje programi koji u vrlo kratkom vremenu mogu učinkovito dešifrirati supstitucijske šifre. Jedan od najboljih programa je *AZdecrypt*, koji može riješiti sve homofonske supstitucijske šifre iste duljine i distribucije simbola kao Z340.

Međutim, kada se pokrene na šifri Z340, program ne daje rezultate. Razlog tome je što Z340 nije obična homofonska supstitucijska šifra, već kombinira elemente transpozicije i supstitucije. Glavni izazov za kriptografe bio je pronalaženje odgovarajuće transpozicije (tj. permutacije znakova) koja bi omogućila primjenu *AZdecrypta* na šifru.

Kako je navedeno u članku *The Solution of the Zodiac Killer's 340-Character Cipher*[2], iz kojeg preuzimam i slike u ovom podpoglavlju, Sam Blake posvetio se istraživanju transpozicija nad šifrom Z340 kako bi pronašao onu pravu i time riješio misterij star više od 50 godina.

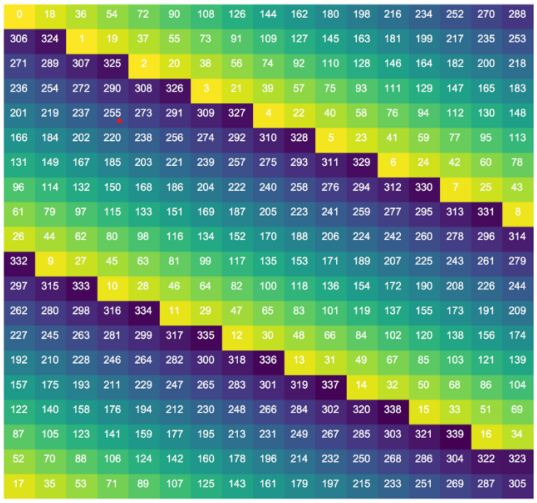
Za analizu je koristio program *Mathematica*, koji mu je omogućio vizualizaciju potencijalnih transpozicija. Njegov pristup obuhvaćao je sustavno ispitivanje različitih obrazaca transpozicije kako bi identificirao one s najvećim potencijalom za otkrivanje pravilnosti u šifri.

Blake je koristio Mathematica kod za vizualizaciju ove transpozicije s periodom 19 koju su predložili korisnik "daikon" i Jarl van Eycke (slika 3.5).

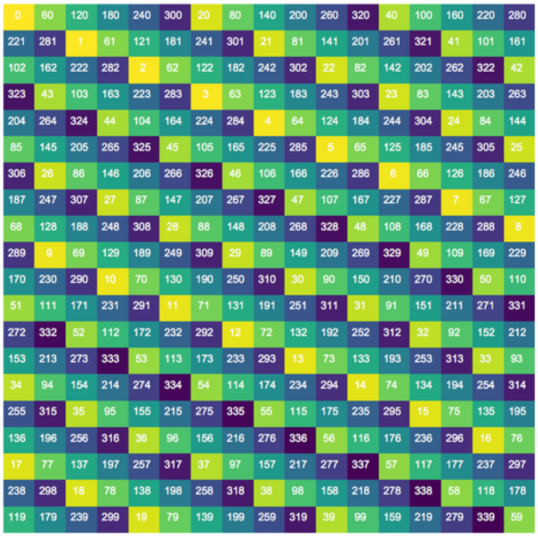
Za bolje razumijevanje, ukratko ću objasniti što je i zašto prikazano na slici 3.5. Na isti je način Blake prikazao i proučavao sve transpozicije kojima se bavio tijekom dešifriranja.

Slika prikazuje raspored indeksa (brojeva) u tablici, pri čemu su redci i stupci organizirani na način koji ilustrira transpozicijski postupak s periodom 18. Tablica ima fiksan broj redaka, u ovom slučaju 18, pa se pri popunjavanju teksta *cikličko pomicanje* ili *omatanje* (eng. wrap-around) događa nakon što se dostigne ta visina.

U kontekstu transpozicijske šifre, svaki broj predstavlja poziciju nekog znaka unutar šifriranog teksta (ukupno 340 brojeva koliko je dugačka šifra Z340), a različite nijanse boja (od zelene prema ljubičastoj) služe za vizualno razlikovanje i praćenje gdje se pojedine pozicije sele u tablici.



Slika 3.5: Transpozicija s periodom 19



Slika 3.6: 1,2-decimacijska transpozicija

Iako je transpozicija na slici 3.5 bila vizualno atraktivna, Blake je smatrao da to nije nešto što bi bilo prirodno napisati pomoću papira i olovke davne 1969. kada je šifra nastala.

Međutim, uočena je veza između transpozicije s periodom 19 te tzv. *1,2-decimacije* (metoda razrjeđivanja ili cikličkog pomaka 1 dolje i 2 desno) šifriranog teksta veličine 20x17. Naime, ako se krene od gornjeg lijevog kuta pa se pomiče tako da se prvo napravi jedan korak okomito, a zatim dva koraka vodoravno, uz istovremeno cikličko omatanje (eng. wrap-around) i u vodoravnom i u okomitom smjeru, kao da je šifra omotana oko torusa, tada ta transpozicija prati slične dijagonale kao i transpozicija s periodom 19.

Nažalost, pokretanje AZdecrypta nad dobivenim transpozicijama nije dalo rezultata iako se broj ponavljajućih bigrama povećao, što je istražiteljima dalo nade da su ipak na ispravnom putu. Isprobavali su razne transpozicije koje su smatrali izvedivima, pokretali su AZdecrypt i pomoću Mathematice brojali ponavljajuće bigrame, ali bez uspjeha.

3.3 Razdvajanje šifre

Nakon opsežne analize raznih transpozicija, djelomično opisanih u prethodnom odlomku, i niza neuspjeha, istražitelji su pretpostavili da bi trebalo još neke mogućnosti uzeti u obzir.

Zbog činjenice da je šifra Z408 poslana u 3 dijela, ustanovljena je mogućnost da je šifra Z340 konstruirana od više segmenata.

Kako Blake navodi u svom članku, razmatrali su podjelu šifre vodoravno na dva i tri segmenta, okomito na dva i tri segmenta te vodoravno i okomito na 2×2 i 3×3 segmente.

Upotrijebili su alat *Reduce* kako bi dobili sve moguće segmente, a budući da je 1,2-decimacijska transpozicija imala visoku učestalost bigrama, odlučili su krenuti s dvodimenzionalnim decimacijama, pri čemu je svaki segment imao istovjetnu (pojedinačnu) transpoziciju. Međutim, nisu dobili nove rezultate.

Nakon toga, uslijedilo je pretraživanje kompozicija (spajanja) višestrukih transpozicija i svih mogućih kombinacija transpozicija za sve segmente teksta.

Testirano je više od 650.000 transpozicija. Iako mnoge varijante nisu davale nikakve rezultate, jedna je postala zanimljiva jer je rezultirala izrazima u engleskom jeziku poput "HOPE YOU ARE" (hrv. "NADAM SE DA JESI"), "TRYING TO CATCH ME" (hrv. "POKUŠAVAŠ ME UHVATITI") i "THE GAS CHAMBER" (hrv. "PLINSKA KOMORA").

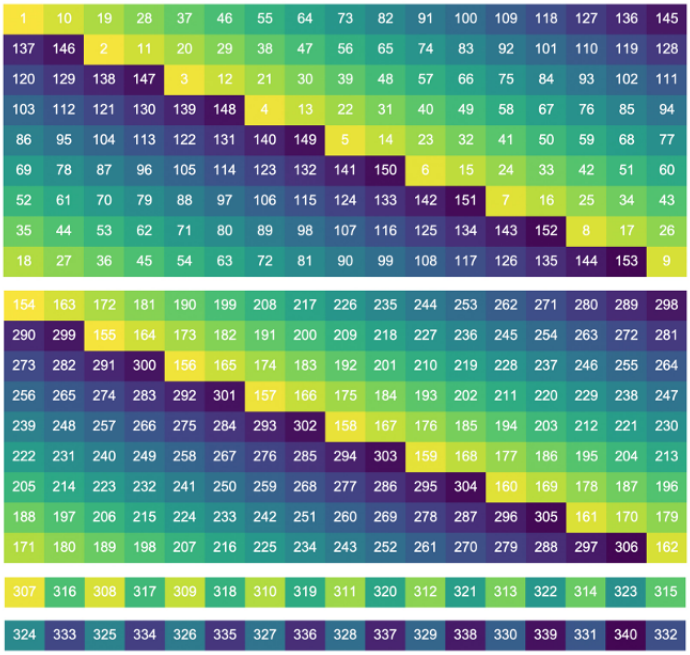
EHOPE YOU ARE HE SING IST TORRA ENN **TRYING**
TO CATCH ME TH AFTAINT MT ON THE TS SHOT WHICH
BRINGS UP ALS IN TABS IT ME NAME OF AR HEED
OR **THE GAS CHAMBER** BECA ATE IT WILD VENT
ME ROLER A DICE AI I THE VS SHEN BECAUSE
TOO WHA SEEN TIGHT DESERTS WORS ROS ME THERE
EVERYONEED HE HAS NOTHING THEN THEY HE ACH
PARADICT IS THEY ALREARE AND NORDER THER
AMEO EARRE AND BECAUITE IS YOT TV HAT MR
NEWE ITLE NEVER IND BAEYN NEIA AT A HOE CDR
PET

Slika 3.7: Rezultat jedne od transpozicija (izvor: https://blog.wolfram.com)

Autori su, umjesto da rade na svih 20 redaka Z340 odjednom, podijelili šifru na četiri segmenta prema redcima: prvih 9 redaka, sljedećih 9 redaka, redak broj 19, redak broj 20. Na svaku od tih sekcija primijenjena je *(1,2)-decimacijska* transpozicija kao što je prikazano na slici 3.8

Istražujući ovaj rezultat dalje, David Oranchak je pomoću programa AZdecrypt, zaključavši gore spomenute fraze na mjestu, pronašao sljedeće rješenje prvog segmenta:

I HOPE YOU ARE HAVING LOTS OF FUN IN TRYING TO CATCH ME THAT WASNT ME ON THE TV SHOW WHICH BRING OR PA POINT ABOUT ME I UM NOT AFRAID OF THE GAS CHAMBER BECUASE IT WILL SEND ME TO PAY UNCLE ALL THE



Slika 3.8: 1,2-decimacija primijenjena na sva četiri segmenta šifre Z340

Nakon ovog rezultata, značajan dio teksta poprimio je smislen oblik i poruka je u cjelini djelovala razumljivo. Dapače, tekst upućuje na konkretne događaje i izjave povezane sa Zodijakom. Primjerice, sedamnaest dana nakon što je poslano pismo i šifra Z340, tijekom jednoga televizijskog programa, nazvao je gledatelj koji se predstavio kao Zodijak i rekao:

> *"I need help. I'm sick. I don't want to go to the gas chamber."*
> (hrv. "Trebam pomoć. Bolestan sam. Ne želim ići u plinsku komoru.")

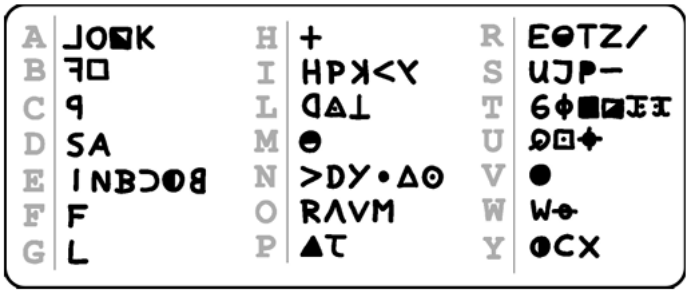
(*Izvor:* Duston Harvey, "'*Zodiac' Misses Appointment With Belli*". *The San Bernardino Sun*, 23. listopada 1969.)

Zbog svega navedenog, autori su vjerovali da su vrlo blizu točnog otvorenog teksta.

3.4 Završni koraci dešifriranja

Svi simboli Zodijakove abecede korištene u Z340 pojavljuju se u prvih devet redaka transponirane šifre. Na taj je način cjelokupni ključ (prikazan na slici 3.9 preuzetoj iz rada *The*

Solution of the Zodiac Killer's 340-Character Cipher [8]) bio određen već u ovoj fazi te se mogao primijeniti na preostale dijelove teksta.



Slika 3.9: Prijedlog ključa za šifru Z340

Primjenom ključa na cijelu šifru dobiven je otvoreni tekst od 340 znakova:

Odjeljak 1:
I HOPE YOU ARE HAVING LOTS OF
FUN IN TRYING TO CATCH ME THAT WASNT ME
ON THE TV SHOW WHICH BRING OR PA POINT
ABOUT ME I UM NOT AFRAID OF THE GAS
CHAMBER BECUASE IT WILL SEND ME TO PAY
UNLCE ALL THE

Odjeljak 2:
SOO HEN BE CURSEE OOW HAVE
ENSUGH SLAVER TO WOR V FOV ME WHERE
ESERYONE EL HEH US NOTHING WHEN THEY
REACH PAY UNICE SO TREY ALREU FAA I FI
OF NET TH IF AM NO EA FREA IF BNC ARISE
IV YO WT SHAT MR NEW

Odjeljak 3:
EIW LENESE FLIL BAAY

Odjeljak 4:
NNE I UADAHO I CFR PET

Budući da je tekst i dalje većim dijelom ostao nejasan, trojica autora ispitali su mogućnost da je Zodijak namjerno izmijenio strategiju za drugu polovicu pisma.

Pokazalo se da su u posljednja dva retka neke riječi bile *reverzibilno* zapisane (slika 3.10), što je potvrdilo da je doista riječ o drugačijem koraku transpozicije.

EFIL **WILL** EB NA **EASY** ENO NI
ECIDARAP **DEATH**

LIFE WILL BE AN EASY ONE IN
PARADICE DEATH

Slika 3.10: Zadnja dva redka šifre Z340

Osim toga, nakon primjene istoga ključa na cjelokupni (neprerađeni) Z340, pojavile su se nove smislene riječi, od kojih su posebno zanimljive bile:

- **DEATH**, smještenu na samome kraju zadnjega retka,
- **LIFE IS**, koja se vidjela u gornjem desnom dijelu drugoga segmenta.

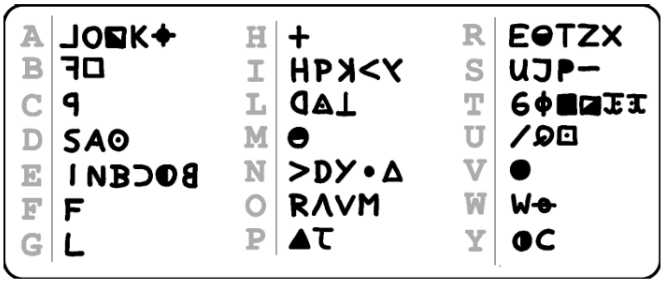
0	9	18	27	36	45	54	63	72	81	90	99	108	117	126	135	144
136	145	1	10	19	28	37	46	55	64	73	82	91	100	109	118	127
119	128	137	146	2	11	20	29	38	47	56	65	74	83	92	101	110
102	111	120	129	138	147	3	12	21	30	39	48	57	66	75	84	93
85	94	103	112	121	130	139	148	4	13	22	31	40	49	58	67	76
68	77	86	95	104	113	122	131	140	149	5	14	23	32	41	50	59
51	60	69	78	87	96	105	114	123	132	141	150	6	15	24	33	42
34	43	52	61	70	79	88	97	106	115	124	133	142	151	7	16	25
17	26	35	44	53	62	71	80	89	98	107	116	125	134	143	152	8

153	162	171	180	189	198	207	216	225	234	243	300	301	302	303	304	305
284	292	154	163	172	181	190	199	208	217	226	235	244	252	260	268	276
269	277	285	293	155	164	173	182	191	200	209	218	227	236	245	253	261
254	262	270	278	286	294	156	165	174	183	192	201	210	219	228	237	246
238	247	255	263	271	279	287	295	157	166	175	184	193	202	211	220	229
221	230	239	256	264	272	280	288	296	158	167	176	185	194	203	212	248
204	213	222	231	240	249	257	265	273	281	289	297	159	168	177	186	195
187	196	205	214	223	232	241	250	258	266	274	282	290	298	160	169	178
170	179	188	197	206	215	224	233	242	251	259	267	275	283	291	299	161

309	308	307	306	310	311	312	313	315	314	317	316	318	319	320	321	324
323	322	326	325	334	333	332	331	330	329	328	327	335	336	337	338	339

Slika 3.11: Transpozicija korištena u šifri Z340

Daljnjom provjerom utvrđeno je kako je na liniji 15 (šesti redak drugoga segmenta) Zodijak propustio jedan simbol, zbog čega je program pogrešno rasporedio veći dio preostalih slova. Ispravkom tog preskoka te privremenim ignoriranjem dijela teksta prilikom transpozicije, najveći se dio iskrivljenih riječi vratio se u normalan poredak. Time je, uz uočene reference na "DEATH" i "LIFE IS", drugo poglavlje teksta postalo daleko čitljivije i kontekstualno smisleno.
Nakon što su identificirani i ispravljeni propusti u transpoziciji (drugačiji raspored slova te reverzibilno zapisana mjesta u tekstu), istražitelji su došli do konačnog oblika transpozicijske sheme. Uz ove ispravke, transpozicija korištena za šifriranje Z340 prikazana je na slici 3.11.



Slika 3.12: Ključ šifru Z340

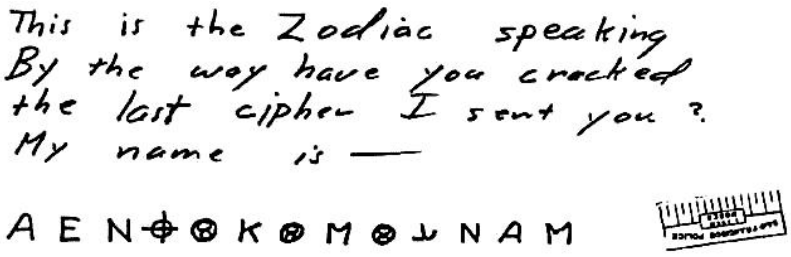
Uz tako dorađenu transpoziciju i novodobiveni, konačni ključ koji obuhvaća sve znakove korištene u Z340 (slika 3.12), dobiven je cjeloviti otvoreni tekst, uključujući nekoliko sporadičnih pogrešaka u pisanju (označenih uglastim zagradama):

I HOPE YOU ARE HAVING LOTS OF [FAN: FUN]
IN TRYING TO CATCH ME THAT WASN'T ME
ON THE TV SHOW WHICH [BRINGO: BRINGS]
UP A POINT ABOUT ME I AM NOT
AFRAID OF THE GAS CHAMBER [BECAASE: BECAUSE]
IT WILL SEND ME TO [PARADLCE: PARADISE]
ALL THE [SOOHER: SOONER] BECAUSE [E: I]
NOW HAVE ENOUGH SLAVES TO [WORV: WORK]
FOR ME WHERE EVERYONE ELSE HAS NOTHING
WHEN THEY REACH [PARADICE: PARADISE]
SO THEY ARE AFRAID OF DEATH I AM NOT AFRAID
BECAUSE I [VNOW: KNOW] THAT MY NEW LIFE WILL
BE AN EASY ONE IN [PARADICE: PARADISE]
LIFE IS DEATH

Poglavlje 4

Šifra Z13

Dana 20. travnja 1970. godine, Zodijak je poslao pismo redakciji San Francisco Chroniclea. U pismu je uključena kratka šifra od samo 13 simbola, poznata kao Z13, za koju se smatralo da bi mogla sadržavati njegovo ime. Ova šifra izazvala je veliku pažnju istražitelja i entuzijasta, ali zbog njezine kratkoće nijedna standardna metoda kriptografske analize nije dala pouzdano rješenje.



Slika 4.1: Izgled šifre Z13 (izvor: www.ZodiacKiller.com[12])

4.1 Struktura šifre Z13

Šifra Z13 je posebno intrigantna zbog svoje jednostavnosti i potencijalne važnosti. Njena kratkoća predstavlja značajan izazov za analizu, jer nedostatak podataka onemogućava primjenu mnogih uobičajenih tehnika, poput frekvencijske analize. Pojedinačni simboli u šifri nisu se podudarali s već poznatim uzorcima u drugim Zodijakovim šiframa, čime je dodatno otežano pronalaženje povezanosti s ostalim porukama.

4.2 Moguće metode dešifriranja

Unatoč izazovima, istraživači su tijekom godina predlagali nekoliko mogućih pristupa za rješavanje šifre Z13:

- **Homofonska supstitucija:** Pretpostavljalo se da je šifra možda kodirana jednostavnom zamjenom simbola za slova. Međutim, analiza nije dala pouzdane rezultate zbog malog broja simbola.
- **Anagrami:** Neki istraživači su pretpostavili da Zodijak koristi anagrame kako bi zamaskirao svoje ime. Ova hipoteza uključuje preuređivanje simbola kako bi se dobile različite kombinacije, ali nijedan rezultat nije bio uvjerljiv.
- **Povezivanje s drugim šiframa:** Postojala je teorija da Z13 sadrži ključ za razumijevanje ostalih šifri, poput Z340 ili Z32. Međutim, dosadašnja istraživanja nisu potvrdila ovu mogućnost.

4.3 Teorije i spekulacije

Zbog prirode šifre, mnogi vjeruju da Z13 možda uopće ne sadrži Zodijakovo ime, već služi kao sredstvo za izazivanje zbunjenosti i dodatne pažnje javnosti. Drugi smatraju da simboli mogu predstavljati inicijale, pseudonim ili šifriranu frazu koja zahtijeva dodatne informacije za dešifriranje.

Jedna od zanimljivijih hipoteza uključuje mogućnost da je šifra Z13 povezana s određenim događajem ili osobom iz Zodijakovog života, čime bi kontekst mogao pomoći u njenom rješavanju. Također se nagađa da bi Zodijakovo ime moglo biti skriveno u drugim njegovim pismima, a da Z13 pruža samo naznaku.

4.4 Zaključak

Šifra Z13 ostaje neriješen misterij i primjer ograničenja konvencionalnih kriptografskih metoda kada su suočene s nedostatkom podataka. Dok se njena važnost i dalje raspravlja, ona nesumnjivo doprinosi fascinaciji Zodijakovim šiframa te potiče istraživače i entuzijaste da nastave tražiti odgovore.

Poglavlje 5

Šifra Z32

Dana 26. lipnja 1970. godine, Zodijak je poslao pismo redakciji San Francisco Chroniclea koje je sadržavalo šifru poznatu kao Z32. Ova šifra, koja se sastoji od samo 32 simbola, bila je priložena uz prijetnju o postavljanju bombe na školskom autobusu. Zodijak je tvrdio da se pomoću šifre (slika 5.1) i karte (slika 5.2) može pronaći lokacija bombe prije nego što eksplodira. Šifra Z32 do danas ostaje neriješena, što dodatno pojačava fascinaciju i misterij oko Zodijakovih poruka.

Slika 5.1: Šifra Z32 (izvor: www.ZodiacKiller.com[12])

5.1 Struktura šifre Z32

Simboli korišteni u šifri ukazuju na moguću povezanost s matematičkim ili geometrijskim principima, osobito zbog referenci na radijane i inče duž radijana koje je Zodijak spomenuo u pismu. Kratkoća šifre čini konvencionalne kriptografske metode gotovo neprimjenjivima.

5.2 Moguće metode dešifriranja

Istraživači su tijekom godina pokušavali razne metode za dešifriranje šifre Z32:

- **Geometrijski pristup:** S obzirom na spominjanje radijana i inča, razmatrane su teorije da šifra sadrži geometrijske upute ili da je povezana s lokacijom na karti.

- **Homofonska supstitucija:** Pretpostavljeno je da šifra koristi jednostavnu zamjenu simbola za slova, no nedostatak podataka otežava ovu analizu.
- **Povezivanje s kartom:** Karta priložena uz šifru potaknula je istraživače na povezivanje simbola sa specifičnim koordinatama ili geografskim značajkama.

Slika 5.2: Karta priložena sa šifrom Z32 (izvor: www.ZodiacKiller.com [12])

5.3 Teorije i spekulacije

Postoje brojne teorije o namjeni i sadržaju šifre Z32. Neki istraživači vjeruju da šifra možda sadrži samo dezinformacije kako bi zbunila vlasti i skrenula pažnju sa stvarnih događaja. Drugi smatraju da bi šifra mogla sadržavati ključne informacije za identifikaciju Zodijaka ili lokaciju bombe, ali zahtijeva dodatne podatke koji nisu dostupni u trenutnoj dokumentaciji.

Jedna teorija sugerira da bi šifra Z32 mogla biti povezana s drugim Zodijakovim šiframa, poput Z340, te da se ove šifre trebaju dešifrirati zajedno kako bi se otkrilo njihovo pravo značenje. Također se razmatra mogućnost da šifra koristi više slojeva šifriranja, što dodatno otežava njen analitički pristup.

5.4 Zaključak

Šifra Z32 predstavlja intrigantan izazov za istraživače i entuzijaste kriptografije. Njena kratkoća i potencijalni kontekstualni značaj čine je jedinstvenim primjerom ograničenja tradicionalnih metoda dešifriranja. Iako je šifra do danas ostala neriješena, ona nastavlja nadahnjivati istraživače da traže nove pristupe i rješenja.

Šifra Z32 ostaje neriješena unatoč brojnim pokušajima dešifriranja i činjenici da su analitičari primijetili da šifra spominje ”radijane” i ”inče duž radijana”, što sugerira da bi kutne mjere mogle biti ključ za dešifriranje.

Bibliografija

[1] C. P. Bauer, *Unsolved! The History and Mystery of the World's Greatest Ciphers from Ancient Egypt to Online Secret Societies*, Princeton University Press, 2017.

[2] S. Blake, *The Solution of the Zodiac Killer's 340-Character Cipher*, Wolfram, 24. ožujka 2021., https://blog.wolfram.com/2021/03/24/the-solution-of-the-zodiac-killers-340-character-cipher/, pristupljeno: siječanj 2025.

[3] A. Dujella, *Kriptografija i sigurnost mreža*, https://web.math.pmf.unizg.hr/~duje/kriptsig.html, pristupljeno: siječanj 2025.

[4] A. Dujella i M. Maretić, *Kriptografija*, Element, Zagreb, 2007.

[5] T. Đao, *Analysis of the Zodiac 340-cipher*, Master Thesis, San Jose State University, 2008., https://core.ac.uk/download/pdf/145731734.pdf, pristupljeno: siječanj 2025.

[6] J. von zur Gathen, *Unicity distance of the Zodiac-340 cipher*, Cryptologia, Volume 47, Issue 5, 2023, pp. 474-488.,https://eprint.iacr.org/2021/1620.pdf, pristupljeno: siječanj 2025.

[7] D. Oranchak, Youtube kanal, https://www.youtube.com/@doranchak, pristupljeno: siječanj 2025.

[8] D. Oranchak, S. Blake i J. Van Eycke, *The Solution of the Zodiac Killer's 340-Character Cipher*, arXiv:2403.17350, 17.3.2024, https://arxiv.org/abs/2403.17350, pristupljeno: siječanj 2025.

[9] F. Pratt, *The Secret and Urgent: The Story of Codes and Ciphers*, Blue Ribbon Books, 1942.

[10] *The Zodiac Ciphers: What Cryptologists Know*, https://www.history.com/news/the-zodiac-ciphers-what-we-know, pristupljeno: siječanj 2025.

[11] *Zodiac Ciphers*, https://www.zodiacciphers.com/, pristupljeno: prosinac 2024.

[12] *Zodiac Killer*, https://zodiackiller.com/, pristupljeno: prosinac 2024.

[13] *Zodiac Killer Chiphers*, https://zodiackillerciphers.com, pristupljeno: prosinac 2024

[14] *Zodiologists.com*, https://www.zodiologists.com/, pristupljeno: siječanj 2025.

[15] https://bs.eitca.org/, pristupljeno: prosinac 2024.

[16] https://en.wikipedia.org/wiki/Substitution_cipher#Homophonic, pristupljeno: prosinac 2024.

Sažetak

U ovom radu prikazan je sadržaj i povijesni kontekst Zodijakovih šifri, Z408, Z340, Z13 i Z32, te je detaljno opisan postupak dešifriranja istih. Spomenute šifre svojom su složenošću desetljećima zbunjivale stručnjake iz područja kriptografije, forenzike i lingvistike. Iako je živio u doba kada tehnologija nije bila razvijena, Zodijak je uspio kreirati dovoljno složene šifre da ih čak niti moderne tehnologije nisu uspjele dešifrirati.

Šifra Z408 šifrirana je kao supstitucijska homofona šifra dok je šifra Z340 i homofonska supstitucijska i transpozicijska šifra. Zbog razumijevanja rada na početku je posebna pažnja posvećena definiranju supstitucijske i transpozicijske šifre.

Glavni dio rada opisuje ključne faze u dešifriranju spomenutih šifri i korištenu metodologiju, uključujući frekvencijsku analizu, prepoznavanje uzoraka i primjenu računalnih algoritama za automatizaciju procesa. Ovim dijelom daje se uvid u kompleksnost dešifriranja i specifične izazove poput nedosljednosti u šifriranju, mogućih grešaka pri pisanju na koje su nailazili kriptografi kroz više od 50 godina.

Summary

This thesis presents the content and historical context of the Zodiac ciphers, Z408, Z340, Z13, and Z32, and provides a detailed description of the decryption process. These ciphers, with their complexity, have puzzled experts in cryptography, forensics, and linguistics for decades. Despite living in an era where technology was not highly advanced, Zodiac managed to create ciphers complex enough that even modern technologies struggled to decrypt them.

The Z408 cipher was encrypted as a homophonic substitution cipher, while the Z340 cipher combined both homophonic substitution and transposition methods. To ensure a better understanding of the work, particular attention is given at the beginning to defining substitution and transposition ciphers.

The main part of the thesis describes the key phases in decrypting these ciphers and the methodologies used, including frequency analysis, pattern recognition, and the application of computational algorithms to automate the process. This section provides insight into the complexity of the decryption and the specific challenges, such as inconsistencies in encryption and possible writing errors, faced by cryptographers over more than 50 years.

Životopis

Rodena sam 17. listopada 1999. u Ogulinu. Osnovnoškolsko obrazovanje završila sam 2014. godine u Osnovnoj školi Ivane Brlić–Mažuranić u Ogulinu, nakon čega sam upisala opću gimnaziju, Gimnaziju Bernardina Frankopana u Ogulinu.

Godine 2018., nakon završene srednje škole, preselila sam se u Zagreb te upisala preddiplomski studij Matematika na Matematičkom odsjeku Prirodoslovno-matematičkog fakulteta u Zagrebu.

2022. godine, završetkom preddiplomskog studija stekla sam titulu sveučilišnog prvostupnika matematike i nastavila svoje školovanje na diplomskom sveučilišnom studiju Računarstvo i matematika na istom fakultetu.

Tokom diplomskog studija radila sam kao software developer što je dodatno obogatilo moje znanje, ali i poboljšalo organizacijske sposobnosti kako bih uspješno uskladila obrazovanje, posao i društveni život.