**TEHNIČKO VELEUČILIŠTE U ZAGREBU**

**STRUČNI STUDIJ INFORMATIKE**

Ivan Regvar

Kryptos - analiza

ZAVRŠNI RAD br.

Zagreb, srpanj, 2025.

Table of Contents

[Uvod 3](#_Toc193894505)

[Kriptografija 4](#_Toc193894506)

[Osnovne informacije 4](#_Toc193894507)

[Pojmovi 4](#_Toc193894508)

[Primjene kriptografije 5](#_Toc193894509)

[Povijest kriptografije 6](#_Toc193894510)

[Kryptos 9](#_Toc193894511)

[Osnovne informacije 9](#_Toc193894512)

[Metode šifriranja korištene u Kryptosu 11](#_Toc193894513)

[Caesar šifra 11](#_Toc193894514)

[Vigenèreova šifra 14](#_Toc193894515)

[Frekvencijska analiza 20](#_Toc193894516)

[Početci analize 28](#_Toc193894517)

[K2 29](#_Toc193894518)

[K3 33](#_Toc193894519)

[K1 35](#_Toc193894520)

[K4 36](#_Toc193894521)

[Završetak 39](#_Toc193894522)

# 

# Uvod

“Kryptos” je skulptura smještena u sjedištu Centralne obavještajne agencije (CIA) u Langleyu, Virginia, a njezin autor je američki kipar Jim Sanborn. Dovršena 1990. godine, ova umjetnička instalacija postala je prepoznatljiva po svojem inovativnom spoju vizualne umjetnosti i kriptografije.

Skulptura se sastoji od četiri odvojena dijela, svaki sadržava vlastitu šifriranu poruku. Prva tri dijela uspješno su dešifrirana, dok četvrti dio, poznat kao “K4”, ostaje neriješen. Ova neriješena komponenta predstavlja središnji izazov za stručnjake i amatere širom svijeta, potičući kontinuirane napore u istraživanju i dešifriranju.

Kryptos nadilazi granice klasične umjetnosti: on simbolizira i estetsku i intelektualnu dimenziju šifriranja. Rješavanje šifri unutar ove skulpture postalo je kulturni fenomen te primjer dinamike između umjetničkog stvaralaštva i znanstvenog istraživanja.

Proučavanjem Kryptosa i njegovih enkripcijskih izazova, istražujemo načine na koje umjetnost i kriptografija mogu zajednički potaknuti ljudsku radoznalost i inovativnost, te otkriti načine interpretacije skrivenih značenja.

# 

# Kriptografija

## Osnovne informacije

Kriptografija je znanost i umjetnost skrivenog pisanja, koja se bavi tehnikama za osiguravanje sigurnosti komunikacija. Cilj kriptografije je zaštita informacija od neovlaštenog pristupa, omogućujući samo ovlaštenim osobama da ih pročitaju i razumiju.

### Pojmovi

* **Šifra**: Metoda ili algoritam koji se koristi za šifriranje i dešifriranje poruka.
* **Šifriranje**: Proces pretvaranja običnog teksta (čitljivog teksta) u šifrirani tekst (nečitljiv tekst) pomoću šifre.
* **Dešifriranje**: Proces pretvaranja šifriranog teksta natrag u običan tekst pomoću šifre.
* **Ključ**: Tajni podatak ili parametar koji se koristi u procesu šifriranja i dešifriranja.

### Primjene kriptografije

* **Sigurna komunikacija**: Osigurava privatnost i integritet informacija prilikom prijenosa podataka putem nesigurnih mreža, poput interneta.
* **Digitalni potpisi**: Omogućuju autentifikaciju izvora i integritet digitalnih dokumenata, osiguravajući da dokumenti nisu promijenjeni nakon potpisivanja.
* **Autentifikacija**: Potvrđuje identitet korisnika ili uređaja prije nego što im se omogući pristup osjetljivim informacijama ili sustavima.
* **Kriptovalute**: Koriste kriptografske tehnike za osiguranje i provjeru transakcija, kao što je to slučaj s Bitcoinom i drugim digitalnim valutama.

## 

## Povijest kriptografije

Kriptografija kao pojam jest relativno mlada znanost no korištena je već tisućama godina. Prvi primjeri korištenja tajno skrivenih poruka su oko 1900 BC u Egiptu u grobnici Khnumhotep II gdje su se koristili ne standardizirani oblici hijeroglifa. Ovaj kod je jedino bio poznat pisari koji koristili kod kako bi prenosili informacije kraljevima.

A close up of a hieroglyphic

Description automatically generated

Slika . Hijeroglifi stari 4000 godine

U vrijeme Rimskog doba, pojavljuje se prva poznata šifra, odnosno Caesar šifra. Ova šifra funkcionira tako da se svako slovo pretvori u drugo tako što se pomakne redni broj slova za određen broj.

Oko 800. godine, arapski matematičar Al-Kindi jest izumio jedan od najvažnijih alata koji se i danas koristi - frekvencijska analiza. Frekvencijska analiza koristi lingivističke podatke(učestalost slova ili parova slova, konstrukcije rečenice…) kako bi dekriptirali šifrirane podatke.

Poliaflabetska šifra, odnosno Vigenèreova šifra, jest otkrivana nekoliko puta no prvi primjer Polialfabetske šifre se može pronaći oko 1497. godine koju je otkrio Leon Battista Alberti, talijanski humanist, pjesnik, slikar arhitekt te kriptograf.

Alberti šifra koristi dva diska, jedan veći i jedan manji, koji su koncentrično postavljeni jedan na drugi. Diskovi se mogu rotirati nezavisno jedan od drugoga. Svaki disk ima niz slova ispisanih po rubu. Ovo je revolucioniralo kriptografiju jer je ovo prvi primjer šifre koja koristi 2 alfabeta.

Vigenèreova šifra je polialfabetska šifra koja koristi ključnu riječ za šifriranje i dešifriranje poruka. Koristeći Vigenèreov kvadrat, svako slovo otvorenog teksta se šifrira pomoću odgovarajućeg slova iz ključne riječi, što čini šifru otpornijom na frekvencijsku analizu. Ključna riječ se ponavlja onoliko puta koliko je potrebno da pokrije cijeli tekst.

Hebern rotor šifriranje je elektro-mehanički sustav za šifriranje koji je izumio Edward Hebern početkom 20. stoljeća. Ovaj sustav koristi rotirajuće diskove ili rotore s internim ožičenjem za stvaranje složenih zamjenskih šifri, a svaki pritisak tipke pomiče rotor, mijenjajući šifru za svako sljedeće slovo. Iako Hebernova mašina nije postigla široku primjenu, postavila je temelje za razvoj složenijih šifrirnih strojeva poput Enigme, koji su bili ključni tijekom Drugog svjetskog rata.

1975.istraživači koji su radili na blok šiframa u IBM-u razvili su Standard za enkripciju podataka (DES) - prvi kriptosustav koji je certificiran od strane Nacionalnog instituta za standarde i tehnologiju (tada poznat kao Nacionalni ured za standarde) za korištenje od strane američke vlade. Iako je DES bio dovoljno snažan da zaustavi čak i najjača računala 1970-ih, njegova kratka dužina ključa čini ga nesigurnim za moderne primjene, ali njegova arhitektura bila je i ostala izuzetno utjecajna u napretku kriptografije.

1976. istraživači Whitfield Hellman i Martin Diffie predstavili su metodu razmjene ključeva Diffie-Hellman za sigurno dijeljenje kriptografskih ključeva. To je omogućilo novi oblik šifriranja nazvan asimetrični algoritmi ključeva. Ti tipovi algoritama, također poznati kao kriptografija s javnim ključem, pružaju još višu razinu privatnosti jer više ne ovise o zajedničkom privatnom ključu.

U javnim kriptosustavima, svaki korisnik ima svoj vlastiti tajni privatni ključ koji djeluje u tandemu s zajedničkim javnim ključem za dodatnu sigurnost.

2001. odgovarajući na napredak računalne snage, DES je zamijenjen s robusnijim algoritmom za enkripciju Advanced Encryption Standard (AES). Slično DES-u, AES je također simetrični kriptosustav, međutim, koristi mnogo duži ključ za enkripciju koji nije moguće provaliti modernim hardverom.

# Kryptos

## Osnovne informacije

Kryptos je skulptura smještena unutar kompleksa središnje obavještajne agencije (CIA) u Sjedinjenim Američkim Državama, stvorena 1988. godine od strane umjetnika Jima Sanborna. Ova umjetnička instalacija sastoji se od četiri segmenta, od kojih svaki sadrži šifriranu poruku. Tri od četiri poruke već su dešifrirane, dok četvrti segment ostaje enigma koja nije razbijena već više od tri desetljeća. Tajna poruka i dalje predstavlja misterij, pružajući nepresušan izvor zanimanja i spekulacija. Kryptos je postao simbol misterije i intelektualnog izazova, inspirirajući istraživače da nastave svoj trud u pokušaju dešifriranja posljednjeg dijela ove zagonetke.

A metal screen with letters on it

AI-generated content may be incorrect.

Slika . Kryptos struktura ispred HNB zgrade u Langleyu, SAD

## James Sanborn

James Sanborn je umjetnik rođen u Washingtonu, D.C.-u, koji je diplomirao na Randolph-Macon koledžu s diplomom iz likovnih umjetnosti te stekao magisterij iz likovnih umjetnosti na Pratt Instituteu. Kako bi oblikovao "Kryptos", Sanborn je odabrao polirani crveni granit, kvarc, bakrovu ploču, magnetni kamen i okamenjeno drvo. Nakon temeljnog čitanja o temama obavještajne zajednice i kriptografije, gospodin Sanborn odlučio je interpretirati temu u smislu kako se informacije prikupljaju kroz povijest. U slučaju dvodijelnog kripta, informacije su simbolizirane kemijskim i fizičkim učincima koji su stvorili materijale, kao i na druge doslovnije načine. Da bi stvorio kod za "Kryptos", gospodin Sanborn je četiri mjeseca surađivao s umirovljenim kriptografom iz CIA-e kako bi osmislio kodove korištene u skulpturi.

## Metode šifriranja korištene u Kryptosu

### Caesar šifra

Prva metoda jest Caesar šifra. Bazira se na jednom alfabetu koji zapravo postaje kriptiran tako što se pomakne svako slovo za zadani broj. Alfabet se može sastajati od slova, brojeva ili znakova.

Primjer:

|  |
| --- |
| Tekst: '11&je&sati' |
| Alfabet: 'ABCČĆDĐEFGHIJKLMNOPRSŠTUVZŽ12345&'  Simbol '&': razmak  Svakom slovu alfabet pridružujemo slovo pomaknutog alfabeta.  Tablica 1. Caesar šifra sa pomakom 7   |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | A | B | C | Č | Ć | D | Đ | E | F | G | H | I | J | K | L | M | N | O | P | R | S | Š | T | U | V | Z | Ž | 1 | 2 | 3 | 4 | 5 | & | | Ž | 1 | 2 | 3 | 4 | 5 | & | A | B | C | Č | Ć | D | Đ | E | F | G | H | I | J | K | L | M | N | O | P | R | S | Š | T | U | V | Z | |
|  |

Enkriptirani tekst: sszdazkžmć

Za dekripciju, ukoliko je poznat pomak, potrebno je samo ispisati pomaknuti alfabet iznad običnog alfabeta te pridružiti slova.

Tablica . Dešifriranje Caesar šifra sa pomakom 9

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Ž | 1 | 2 | 3 | 4 | 5 | & | A | B | C | Č | Ć | D | Đ | E | F | G | H | I | J | K | L | M | N | O | P | R | S | Š | T | U | V | Z |
| A | B | C | Č | Ć | D | Đ | E | F | G | H | I | J | K | L | M | N | O | P | R | S | Š | T | U | V | Z | Ž | 1 | 2 | 3 | 4 | 5 | & |

Ovo je jednostavno enkripcija te zbog toga postoje nekoliko glavnih mana:

* Slovo 'a' će uvijek biti isti znak(ako je dodijeljeno slovu 'g', uvijek će postati to slovo)
* Ukoliko je alfebet koji se koristi poznat, vrlo je lako kroz brute force saznati rješenje
* Ukoliko je potrebno, može se koristiti i frekvencijska analiza slova u slučajevima višestruke Caesar šifre(na šifriranu poruku se ponovno vrši enkripciji)

### Vigenèreova šifra

Postoji više varijacija ove šifre te ovdje će biti objašnjena varijacija koja je korištena u Kryptosu.

Prvo započinjemo sa ispisivanjem alfabeta.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| A | B | C | Ć | Č | D | Đ | E | F | G | H | I | J | K | L | M | N | O | P | R | S | Š | T | U | V | Z | Ž |

Ključ = 'kripto'

Slova ključa se prebace na početak alfabeta.

Tablica . Vigenèreovo šifriranje – prvi korak

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| A | B | C | Č | Ć | D | Đ | E | F | G | H | I | J | K | L | M | N | O | P | R | S | Š | T | U | V | Z | Ž |
| K | R | I | P | T | O | A | B | C | Č | Ć | D | Đ | E | F | G | H | J | L | M | N | S | Š | U | V | Z | Ž |

Idući korak je pomaknuti donji alfabet ulijevo za 1 te ispisati ispod. Novi redak će započinjati sa slovom 'R' te završavati sa slovom 'K'. Na ovaj način se formira Vigenèreova tablica.

Tablica . Vigenèreova tablica

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | A | B | C | Č | Ć | D | Đ | E | F | G | H | I | J | K | L | M | N | O | P | R | S | Š | T | U | V | Z | Ž |
| A | K | R | I | P | T | O | A | B | C | Č | Ć | D | Đ | E | F | G | H | J | L | M | N | S | Š | U | V | Z | Ž |
| B | R | I | P | T | O | A | B | C | Č | Ć | D | Đ | E | F | G | H | J | L | M | N | S | Š | U | V | Z | Ž | K |
| C | I | C | T | O | A | B | C | Č | Ć | D | Đ | E | F | G | H | J | L | M | N | S | Š | U | V | Z | Ž | K | R |
| Č | P | T | O | A | B | C | Č | Ć | D | Đ | E | F | G | H | J | L | M | N | S | Š | U | V | Z | Ž | K | R | I |
| Ć | T | O | A | B | C | Č | Ć | D | Đ | E | F | G | H | J | L | M | N | S | Š | U | V | Z | Ž | K | R | I | P |
| D | O | A | B | C | Č | Ć | D | Đ | E | F | G | H | J | L | M | N | S | Š | U | V | Z | Ž | K | R | I | P | T |
| Đ | A | B | C | Č | Ć | D | Đ | E | F | G | H | J | L | M | N | S | Š | U | V | Z | Ž | K | R | I | P | T | O |
| E | B | C | Č | Ć | D | Đ | E | F | G | H | J | L | M | N | S | Š | U | V | Z | Ž | K | R | I | P | T | O | A |
| F | C | Č | Ć | D | Đ | E | F | G | H | J | L | M | N | S | Š | U | V | Z | Ž | K | R | I | P | T | O | A | B |
| G | Č | Ć | D | Đ | E | F | G | H | J | L | M | N | S | Š | U | V | Z | Ž | K | R | I | P | T | O | A | B | C |
| H | Ć | D | Đ | E | F | G | H | J | L | M | N | S | Š | U | V | Z | Ž | K | R | I | P | T | O | A | B | C | Č |
| I | D | Đ | E | F | G | H | J | L | M | N | S | Š | U | V | Z | Ž | K | R | I | P | T | O | A | B | C | Č | Ć |
| J | Đ | E | F | G | H | J | L | M | N | S | Š | U | V | Z | Ž | K | R | I | P | T | O | A | B | C | Č | Ć | D |
| K | E | F | G | H | J | L | M | N | S | Š | U | V | Z | Ž | K | R | I | P | T | O | A | B | C | Č | Ć | D | Đ |
| L | F | G | H | J | L | M | N | S | Š | U | V | Z | Ž | K | R | I | P | T | O | A | B | C | Č | Ć | D | Đ | E |
| M | G | H | J | L | M | N | S | Š | U | V | Z | Ž | K | R | I | P | T | O | A | B | C | Č | Ć | D | Đ | E | F |
| N | H | J | L | M | N | S | Š | U | V | Z | Ž | K | R | I | P | T | O | A | B | C | Č | Ć | D | Đ | E | F | G |
| O | J | L | M | N | S | Š | U | V | Z | Ž | K | R | I | P | T | O | A | B | C | Č | Ć | D | Đ | E | F | G | H |
| P | L | M | N | S | Š | U | V | Z | Ž | K | R | I | P | T | O | A | B | C | Č | Ć | D | Đ | E | F | G | H | J |
| R | M | N | S | Š | U | V | Z | Ž | K | R | I | P | T | O | A | B | C | Č | Ć | D | Đ | E | F | G | H | J | L |
| S | N | S | Š | U | V | Z | Ž | K | R | I | P | T | O | A | B | C | Č | Ć | D | Đ | E | F | G | H | J | L | M |
| Š | S | Š | U | V | Z | Ž | K | R | I | P | T | O | A | B | C | Č | Ć | D | Đ | E | F | G | H | J | L | M | N |
| T | Š | U | V | Z | Ž | K | R | I | P | T | O | A | B | C | Č | Ć | D | Đ | E | F | G | H | J | L | M | N | S |
| U | U | V | Z | Ž | K | R | I | P | T | O | A | B | C | Č | Ć | D | Đ | E | F | G | H | J | L | M | N | S | Š |
| V | V | Z | Ž | K | R | I | P | T | O | A | B | C | Č | Ć | D | Đ | E | F | G | H | J | L | M | N | S | Š | U |
| Z | Z | Ž | K | R | I | P | T | O | A | B | C | Č | Ć | D | Đ | E | F | G | H | J | L | M | N | S | Š | U | V |
| Ž | Ž | K | R | I | P | T | O | A | B | C | Č | Ć | D | Đ | E | F | G | H | J | L | M | N | S | Š | U | V | Z |

Sada kada imamo tablicu, možemo enkriptirati. Recimo da želimo enkriptirati tekst 'Tajna poruka'. Potrebna nam je još jedna riječ. Uzmimo riječ 'tvzsz'. Ova riječ će služiti kao lozinka. 'tvzsz' je kraći od 'Tajna poruka' pa ćemo samo ponoviti 'tvzsz' dok nije potrebne duljine.

Kada je tablica formirana, enkripcija može započeti.

Tekst: 'Tajna poruka'

Ključ: 'tvzsz'

Ukoliko je ključ kraći od poruke, ključ se ponavlja dok nije dovoljno.

Tablica . Vigenèreovo šifriranje – drugi korak

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| T | A | J | N | A | P | O | R | U | K | A |
| T | V | Z | S | Z | T | V | Z | S | Z | T |

Pronalazi se sjecište stupca koji počinje sa prvim slovom teksta('T') te redka koji počinje sa prvim slovom lozinke('T'). Sjecište ta dva slova je prvo slovo enkiptiranog teksta('C').

Ponavljajući ovaj proces, enkriptirani tekst je 'CPGFTBIŽJZĆ'.

Dekriptiranje:

Tablica . Dekripcija Vigenèreova šifriranja

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| T | V | Z | S | Z | T | V | Z | S | Z | T |
| C | P | G | F | K | B | I | Ž | J | Z | Ć |

Potrebno je pronaći redak koji počinje slovom 'T' te pratiti redak do slova 'C'. Prvo slovo stupca u kojem se slovo 'C' nalazi je rješenje('T').

Ponavljajući ovaj proces, dekriptirani tekst glasi 'tajnaporuka', odnosno 'tajna poruka'.

## Transpozicija

Poruka: transpozicija

Proizvoljno je odabran broj stupaca te je poruka ispisana po redovima.

Poruka sadrži 13 slova no tablica ima 15 mjesta pa se postavlja slovo 'X'.

Zatim iznad svakog stupca je potrebno upisati brojeve počinjajući sa 1.

Tablica . Enkriptiranje koristeći transpoziciju – prvi korak

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1 | 2 | 3 | 4 | 5 |
| T | R | A | N | S |
| P | O | Z | I | C |
| I | J | A | X | X |

Iduće, stvara se ključ tako što se proizvoljno izmješaju stupci. U ovom slučaju, redom 24513.

Tablica . Kriptiranje koristeći transpoziciju – drugi korak

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 2 | 4 | 5 | 1 | 3 |
| R | N | S | T | A |
| O | I | C | P | Z |
| J | X | X | I | A |

Kriptirana poruka po stupcima glasi: ROJNISCTPIAZA

Ova poruka se dekriptira koristeći brojeve redove i stupaca te korištenjem ključa.

Tablica . Dekripcija koristeći transpoziciju

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 2 | 4 | 5 | 1 | 3 |
| R | N | S | T | A |
| O | I | C | P | Z |
| J | X | X | I | A |

Koristeći poznate podatke, dobije se ova tablica. Sad je samo potrebno presložiti stupce kako bi se dobila poruka.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1 | 2 | 3 | 4 | 5 |
| T | R | A | N | S |
| P | O | Z | I | C |
| I | J | A | X | X |

Dekriptirani tekst: 'Transpozicija'

### Frekvencijska analiza

Ova analiza omogućuje razbijanje šifriranih tekstova koristeći lingvističku frekvencijsku analizu šifrirane poruke. Koristi frekvenciju određenih slova, bigrama i/ili trigrama u jeziku kako bi izvukli podatke. Ova analiza se najčešće koristi za razbijanje Caesar šifre te transpozicije no moguće je i za ostale.

Poruka:

„ovo je relativno jednostavan način dešifriranja no vrlo mukotrpan te postoji pogađanja i pretpostavljanja koristeći lingvističke podatke hrvatskog jezika“

Metoda enkripcije: Caesar šifra

Ključ: 6

Enkritirana poruka:

uču pk zksđbočtu pkitužbđčđt tđgot ikaolzozđtpđ tu čzsu šcrubzvđt bk vužbupo vumđjđtpđ o vzkbvužbđčspđtpđ ruzožbkho sotmčožbogrk vuiđbrk nzčđbžrum pkćorđ

A graph with blue and purple bars

Description automatically generated

Slika . Graf učestalosti slova u Hrvatskom jeziku

Najfrekventniji bigrami u Hrvatskom jeziku(u promilima) su:

JE(27) NA(15), RA(15), ST, AN, NI, KO, OS, TI, IJ, NO, EN, PR(10).

Najfrekventniji trigrami u Hrvatskom jeziku(u promilima) su:

IJE(6), STA, OST, JED, KOJ, OJE, JEN s frekvencijama izmedu 3 i 4.

A screenshot of a graph

Description automatically generated

Slika . Distrubucija slova u enkriptiranom tekstu

Uzimajući ove podatke u obzir, mogu se napraviti određene pretpostavke.

Za početak, usporedimo najčešća slova sa najčeščim slovima enkriptiranog teksta:

Tablica . Učestalost slova u enkriptiranom tekstu

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| A | I | O | E | N | S | R | J | T | D | V | K | L | M | P | Z | G | B | Š | C | H | Ž | Č | Ć | F | D |
| Đ | U | O | B | T | K | Z | P | Č | V | R | Ž | S | M | N | I | G | F | J | L | H | Č | C | A | E | Ć |
| 16 | 14 | 12 | 11 | 11 | 10 | 8 | 8 | 7 | 6 | 6 | 6 | 4 | 3 | 3 | 3 | 2 | 2 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 0 |

Kroz razne kompleksne kombinacije te jednostavno isprobavanjem te zaključivanjem koristeći lingvistiku, dođe se do idućih zaključka:

Đ → A - učestalost slova A

U → O – prva riječ „UČU“, pretpostavlja se da je riječ „OVO“

Č → V – prva riječ „UČU“, pretpostavlja se da je riječ „OVO“

K → E – dvije riječi(„pk“ i „bk“) završavaju na K te dvoslovne riječi najčešće završavaju na E

P → J – riječ „pk“ završava na slovo E te se prepostavlja da je to riječ „JE“

O → I – slovo O stoji samostalno te je to gotovo zasigurno veznik “I”

Napisat ćemo zamjene velikih slovima te ih boldati.

**OVO** J**E** z**E**s**A**b**IV**t**O** **JE**it**O**žb**AVA**t t**A**g**I**t i**E**a**I**lz**I**z**A**t**JA** t**O** **V**zs**O** šcr**O**bzv**A**t b**E** v**O**žb**OJI** v**O**m**A**j**A**t**JA** **I** vz**E**bv**O**žb**AV**s**JA**t**JA** r**O**z**I**žb**E**h**I** s**I**tm**VI**žb**I**gr**E** v**O**i**A**br**E** nz**VA**bžr**O**m **JE**ć**I**r**A**

Prelazimo na slovo 'B':

* Ne može biti slovo 'E' jer u trećoj riječi ide odmah poslije 'A'.
* Ne može biti slovo 'N' zbog 'vožbijo'. Ne postoji riječ koja završava na 'nijo'.
* Ne može biti slovo 'S' zbog 'vožbijo'. Ne postoji riječ koja završava na 'sijo'.
* Ne može biti slovo 'R' zbog 'be'. Ne postoji riječ 're'.
* Ne može biti slovo 'J' jer je ono već dekriptirano.
* Iduće slovo je slovo 'T'. Ne postoje neke očite zamjerke te vrijedi pokušaja.

B → T

**OVO** J**E** z**E**s**A**T**IV**t**O** **JE**it**O**žT**AVA**t t**A**g**I**t i**E**a**I**lz**I**z**A**t**JA** t**O** **V**zs**O** šcr**O**Bzv**A**t T**E** v**O**žT**OJI** v**O**m**A**j**A**t**JA** **I** vz**E**Tv**O**žT**AV**s**JA**t**JA** r**O**z**I**žT**E**h**I** s**I**tm**VI**žT**I**gr**E** v**O**i**A**Tr**E** nz**VA**Tžr**O**m **JE**ć**I**r**A**

Iduće slovo je slovo 'T':

T → N – na nekoliko mjesta riječi završavaju na „TJA“ te se može pretpostaviti zbog završetka riječi – bigram NJA

**OVO** J**E** z**E**s**A**T**IV**N**O** **JE**iN**O**žT**AVA**N N**A**g**I**N i**E**a**I**lz**I**z**A**T**JA** N**O** **V**zs**O** šcr**O**Bzv**A**N T**E** v**O**žT**OJI** v**O**m**A**j**A**N**JA** **I** vz**E**Tv**O**žT**AV**s**JA**N**JA** r**O**z**I**žT**E**h**I** s**I**Nm**VI**žT**I**gr**E** v**O**i**A**Tr**E** nz**VA**Tžr**O**m **JE**ć**I**r**A**

Neke riječi su postale očite te se dolazi do idućih zaključaka:

'zesativno' > relativno

'nagin' > način

Z → R

S → L

G → Č

**OVO** J**E** R**E**L**A**T**IV**N**O** **JE**iN**O**žT**AVA**N N**A**Č**I**N i**E**a**I**lR**I**R**A**T**JA** N**O** **V**RL**O** šcr**O**BRv**A**N T**E** v**O**žT**OJI** v**O**m**A**j**A**N**JA** **I** vR**E**Tv**O**žT**AV**L**JA**N**JA** r**O**R**I**žT**E**h**I** L**I**Nm**VI**žT**I**Čr**E** v**O**i**A**Tr**E** nR**VA**Tžr**O**m **JE**ć**I**r**A**

'jeinožtavan' → jednostavan

I → D

Ž → S

**OVO** J**E** R**E**L**A**T**IV**N**O** **JE**DN**O**ST**AVA**N N**A**Č**I**N D**E**a**I**lR**I**R**A**T**JA** N**O** **V**RL**O** šcr**O**BRv**A**N T**E** v**O**ST**OJI** v**O**m**A**j**A**N**JA** **I** vR**E**Tv**O**ST**AV**L**JA**N**JA** r**O**R**I**ST**E**h**I** L**I**Nm**VI**ST**I**Čr**E** v**O**D**A**Tr**E** nR**VA**TSr**O**m **JE**ć**I**r**A**

Uz nešto pogađanja po zvuku riječi, moguće je zaključiti iduće:

V → P – „vostoji“ → “postoji”

R → K – “roristehi” → “koristeći”

H → Ć – “roristehi” → “koristeći”

**OVO** J**E** R**E**L**A**T**IV**N**O** **JE**DN**O**ST**AVA**N N**A**Č**I**N D**E**a**I**lR**I**R**A**T**JA** N**O** **V**RL**O** šcK**O**BRP**A**N T**E** P**O**ST**OJI** P**O**m**A**j**A**N**JA** **I** PR**E**TP**O**ST**AV**L**JA**N**JA** K**O**R**I**ST**E***Ć***I** L**I**Nm**VI**ST**I**ČK**E** P**O**D**A**TK**E** nR**VA**TSK**O**m **JE**ć**I**K**A**

M → G – “linmvističke” → “lingvističke”

Š → M – “ščkotrpan” → “mukotrpan”

C → U – “ščtrpan” → “mukotrpan”

Ć → Z – “jećika” → “jezika”

**OVO** J**E** R**E**L**A**T**IV**N**O** **JE**DN**O**ST**AVA**N N**A**Č**I**N D**E**a**I**lR**I**R**A**T**JA** N**O** **V**RL**O** MUK**O**BRP**A**N T**E** P**O**ST**OJI** P**O**G**A**j**A**N**JA** **I** PR**E**TP**O**ST**AV**L**JA**N**JA** K**O**R**I**ST**E***Ć***I** L**I**NG**VI**ST**I**ČK**E** P**O**D**A**TK**E** nR**VA**TSK**O**G **JE**Z**I**K**A**

N → H – “nhrvatskog” → “hrvatskog”

J → Đ –“pogajanja” → “pogađanja”

**OVO** **JE** **RELATIVNO** **JEDNOSTAVAN** **NAČIN** **DE**a**I**l**RIRANJA** **NO** **VRLO** **MUKOTRPAN** **TE** **POSTOJI** **POGAĐANJA** **I** **PRETPOSTAVLJANJA** **KORISTEĆI** **LINGVISTIČKE** **PODATKE** **HRVATSKOG** **JEZIKA**

Jedina riječ koja nije dešifrirana jest „deailriranja“.

Ovdje postoje samo dvije opciju u standardnom Hrvatskom jeziku: dešifriranja ili deriviranja.

Iz konteksta je moguće zaključiti da je finalna riječ dešifriranja.

A → Š

L → F

**OVO** **JE** **RELATIVNO** **JEDNOSTAVAN** **NAČIN** **DEŠIFRIRANJA** **NO** **VRLO** **MUKOTRPAN** **TE** **POSTOJI** **POGAĐANJA** **I** **PRETPOSTAVLJANJA** **KORISTEĆI** **LINGVISTIČKE** **PODATKE** **HRVATSKOG** **JEZIKA**

ovo je relativno jednostavan način dešifriranja no vrlo mukotrpan te postoji pogađanja i pretpostavljanja koristeći lingvističke podatke hrvatskog jezika

## Početci analize Kryptosa

Na početku, smatralo se da je Kryptos jedna cjelina te da je enkriptirana tako. Kasnije, 1998., Jim Gillogly, bivši predsjednik Američke kriptografske zajednice, je uspio riješiti dio koda te je saznao da postoje 4 dijela. Mislio je da je on prvi riješio prva 3 dijela. Tada je saznao od strane CIA-a da je tehnički analist David Stein već riješio kod koristeći papir i olovku.

Cijeli kod je odvojen sa pet upitnika te se tada smatralo da je kod podijeljen na 5 dijelova. Za K3 su vjerovali da je kompletno nasumičan te da će brute force metoda biti potrebno. Za K4 su imali jednostavne riječi: „This part might be unbreakable."

1992. je bio formiran tim od četiri veteranskih kriptografa koji su odlučili ignorirati upitnike te su krenuli sa frekvencijskom analizom.

* Odluči su jednostavno prebrojati svako slovo u svatkom retku te su saznali da redovi 15. do 25. je imalo učestalost slova vrlo slično Engleskom jeziku
* Mnogo slova 'E', 'T' no nijedno 'Z' ni 'J'
* Ovdje su zaključili da je ovaj dio(kasnije nazvan K3) enkriptiran koristeći transpoziciju, a ostali vjerovatno koristeći substituciju
* Tada su vjerovali da je kod podijeljen na 3 dijela te su zaključili da je gornji dio(K1 i K2) enkriptiran koristeći Vigenere šifru

## K2

Tim je zaključio da je najbolji način za riješiti kod jest pokušati pronaći ključnu riječ. To je moguće analizom repeticija u kodu.  
A close up of a word search

Description automatically generated

Slika .Rješavanje K2 – prvi korak

Kada su našli repeticiju(TBJ) koja se desi u šifriranju, uzeli su razmak slova između repeticija koji je u ovom slučaju 8 što govori da je dužina ključa 1, 2, 4 ili 8. Tim je pretpostavio da je 8 jer bi ključ od samo 4 slova bio prelagan.

U teoriji je moguće kroz brute force metodu testirati svaku riječ od 8 slova jer postoji samo 42,150 riječi u jeziku no ključ ne mora biti smislena riječ. Može biti bilo koja kombinacija slova. Uzimajući u obzir 8 pozicija slova te da Engleski jezik ima 26 slova, dolazimo do broja 208,827,064,576 – nerealno za brute force metodu.

Kako bi započeli rješavanje, organizirali su slova te su podijelili stupce po broj osam – dužini ključa. Radi ovoga su mogli biti sigurni da svako 8. slovo šifrirane poruke je bilo šifrirano istim slovom ključa.

A black background with white letters

Description automatically generated

Slika .Rješavanje K2 – drugi korak

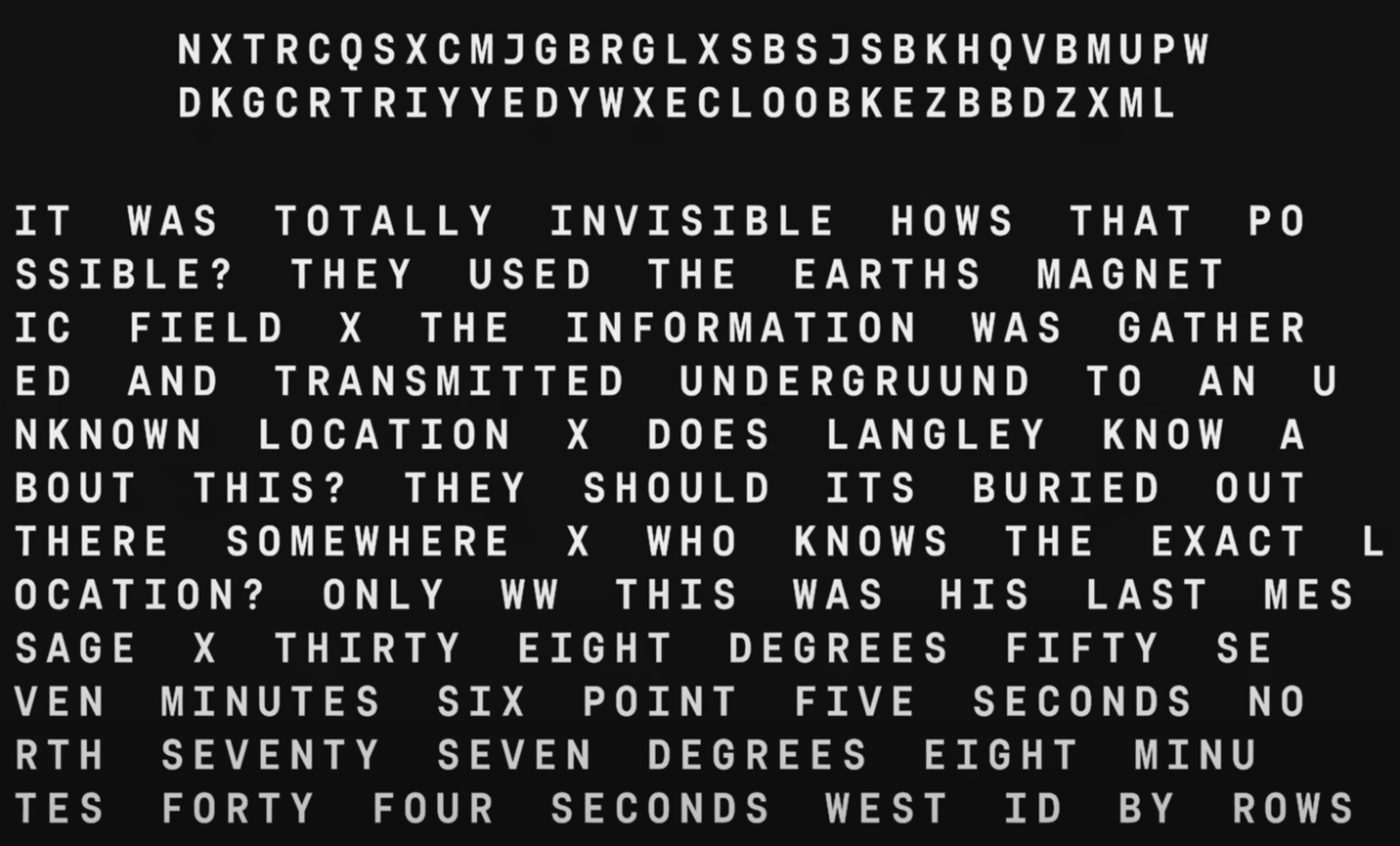
Koristeći ove podatke, zaključili su da slovo R predstavlja isto slovo jer je šifrirano sa istim slovom ključa. Ovo je ključna informacija jer je frekvencijskom analizom moguće dešifrirati šifrirani tekst. Slova koja se češće ponavljaju su vjerovatno 'E', 'T' dok manje učestala slova predstavljaju slova 'Q' ili 'Z'.

Tablica . Rješavanje K2 - treći korak

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

Nakon nekog vremena, uspjeli su doći do ovog dijela te su vidjeli kako se riječi krenu formirati: 'Six', 'Five' i 'Seven'.

Nakon nekog vremena su dobili iduće:



Slika . Rješenje K2

Postojala su 2 ključa: 'Abscissa'i 'Kryptos'.

Ovdje su saznali da dio koji su rješavali se zapravo sastoji od 2 dijela – K1 i K2. Uspjeli su riješiti K2.

## K3

Dalje, odlučeno je krenuti na K3 jer su već znali od prije da je vjerovatno enkriptiran koristeći transpoziciju. Postoji više načina transpozicije no većina se naslanja na neku vrstu matrice. Jednostavnost ovakve vrste enkripcije je najveća mana – može se pogađati rješenje te uz dovoljno strpljenja, sreće i znanja, upravo su to i napravili. K3 je riješen pogađenjem i pretpostavljanjem.

A close up of words

Description automatically generated

Slika . Rješavanje K3 - prvi korak

Prvo što su primijetili jest da postoji samo jedno slovo 'Q' u cijelom tekstu. U engleskom jeziku, riječi koje počinju na to slovo najčešće imaju za drugo slovo 'U'.

Nakon toga, uzeli su par slova prije slova 'Q' i par slova poslije te su formirali stupce. Zatim su uzeli isti broj slova kod slova 'U' te ih usporedivali.

Tablica . Rješavanje K3 - drugi korak

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Y | N |  | Y | T |  | Y | F |  | Y | T |  | Y | F |
| T | R |  | T | E |  | T | I |  | T | U |  | T | M |
| F | F |  | F | N |  | F | O |  | F | E |  | F | F |
| Y | Y |  | Y | E |  | Y | T |  | Y | T |  | Y | E |
| Q | U |  | Q | U |  | Q | U |  | Q | U |  | Q | U |
| H | L |  | H | D |  | H | E |  | H | A |  | H | H |
| E | D |  | E | R |  | E | T |  | E | E |  | E | E |
| E | S |  | E | E |  | E | U |  | E | O |  | E | E |
| N | L |  | N | T |  | N | A |  | N | T |  | N | C |

Bilo je određenih problema, kao što su dupli 'Y' te dupli 'H' no bilo je i pozitivnih strana kao što je kombinacije 'HE' što može biti riječ 'THE'; najčešća riječ u Engleskom jeziku.

Koristeći ovaj proces, uspjeli su riješiti cijeli kod.

A black text on a white background

Description automatically generated

Slika . Rješenje K3

Također, zaključili su da zadnja 4 slova šifriranog koda('OBKR') pripadaju K4, a ne K3.

Rješenje, odnos ključ, je bio '0362514' odnosno 'Kryptos'.

## K1

K1 je ostavljen za kraj upravo zato što je toliko kratak – samo 63 znakova. Ovo je razlog zašto su prvo riješavali K3, a ne K1.

K1 je bio samo još jedan Vigeneorova šifra. Sve što je bilo potrebno jest ponoviti korake s kojima su riješili K2 te su koristeći te metodu uspjeli riješiti čitav kod.

Tekst je bio enkriptiran koristeći 'Palimpsest' i 'Kryptos'.



Slika . Rješenje K1

Dekriptirani tekst glasi:

Between subtle shading and the absence of light lies the nuance of iqlusion.

## K4

Za kraj je ostao K4 – posljednji dio Kryptosa. Ovaj dio, do današnjeg dana, i dalje nije riješen.

2010. je stvorilac Kryptosa, Stanburn, objavio mali dio rješenja:

“NYPVTT” postaje “BERLIN”

2014. :

“MZFPK” postaje “CLOCK”

U siječnju 2020. :

“QQPRNGKSS” postaje “NORTHEAST”

U kolovozu 2020. :

“FLRV” postaje “EAST”

Postoje brojne teorije o prirodi K4 šifre. Neki vjeruju da bi K4 mogao biti šifriran novom tehnikom koja kombinira elemente iz prethodnih dijelova. Drugi smatraju da bi dešifriranje moglo zahtijevati fizičku interakciju s skulpturom ili primjenu specifičnih povijesnih konteksta.

Sam Sanburn daje vrlo zbunjujuće izjave u intervjuima kako bi dodao tajanstvenosti samog projekta.

„…I seem to like to manipulate the information coming out, in a sort of dissinformation fashion. Which seems appropriate for the project. And so, a lot of clues that I might give work in a sort of dissinformational way, and that's a good thing. I mean, that's clandestine ethos. „

-Jim Sanborn, 2005.

„It's not my intent to put out dissinformation. I'm a benelovent cryptographer.“

-Jim Sanborn, 2009.

Isto tako, ono što dodaje samoj težini Kryptosa, jest činjenica da Jim Sanburn nije kriptograf već umjetnik. Nije koristio tradicionalne načine kriptiranja te K4 je vjerovatno kriptiran koristeći neki proces koji nije uobičajan u području kriptografije.

Jedan od hipotetskih rješenja jest da je K4 kriptiran dvaput – prvi put koristeći Vigienere šifru kao što je korištena u K1 i K2 te zatim ponovno koristeći transpoziciju kao što je u K3.

K4 je kriptiran koristeći ideju skrivanja korištenja Engleskog jezika kako bi otežali korištenje frekvencijske analize.

K4 ostaje neriješen misterij i izazov za kriptografe diljem svijeta. Dok su tragovi koje je Sanborn pružio pomogli usmjeriti istraživanja, konačno rješenje K4 možda će zahtijevati potpuno novi pristup ili otkriće još jednog ključnog traga. Bez obzira na to, K4 dio Kryptosa nastavit će intrigirati i inspirirati kriptografe diljem svijeta.

# Završetak

Kryptos predstavlja jedinstveni spoj umjetnosti i kriptografije. Kroz analizu prvih triju dijelova šifrirane poruke (K1, K2 i K3), vidjeli smo kako različite metode šifriranja oblikuju složene i intelektualno izazovne zagonetke. Svaka dešifrirana poruka otkriva dio vizije i vještine Sanborna kao umjetnika i kriptografa. Međutim, četvrti dio (K4) ostaje neriješen, i dalje privlači pažnju i intrigira kriptografe i entuzijaste širom svijeta.

Kryptos nije samo umjetničko djelo već simbolizira dublje ljudske težnje za otkrivanjem tajni i razumijevanjem složenih sustava. Kroz neriješeni K4, Sanborn je uspio stvoriti trajnu misteriju koja nastavlja poticati intelektualnu znatiželju i okupljati zajednicu istraživača u zajedničkom naporu da dešifriraju njegovu tajnu. Tragovi koje je Sanborn pružio kroz godine dodatno naglašavaju složenost i dubinu izazova, potičući nove generacije kriptografa na kontinuirano istraživanje i inovaciju.

Ovaj završni rad istražio je povijest, strukturu i značaj Kryptosa, naglašavajući kako ova skulptura predstavlja ne samo umjetnički izazov, već i ključnu ulogu kriptografije u modernom svijetu. Kryptos nas podsjeća na važnost sigurnosti informacija, kreativnosti u šifriranju i moći umjetnosti da nadahne i izazove.

Bez obzira na to hoće li se tajna K4 ikada otkriti, Kryptos će ostati trajni simbol misterije i intelektualnog izazova. Njegova prisutnost odražava trajnu vezu između umjetnosti, znanosti i tehnologije, inspirirajući nas da uvijek tražimo dublja značenja i skrivene istine. Dok nastavljamo s naporima za dešifriranje posljednje poruke, Kryptos će nastaviti nadahnjivati buduće generacije kriptografa i ljubitelja enigmi, potičući nas da nikada ne prestanemo istraživati i otkrivati.