FAKULTA APLIKOVANÝCH VĚD
ZÁPADOČESKÉ UNIVERZITY
V PLZNI

KATEDRA
KYBERNETIKY

Kryptos



Západočeská Univerzita V Plzni
Katedra Kybernetiky
Semestrální práce - HKUI

Sára Kokošková
1.semestr
3. února 2025

1 Úvod

Kryptos je skulptura amerického umělce Jima Sanborna v centrále CIA v Americe. Tato jedninečná instalace v sobě skrýva 4 zakódované zprávy, na což naráží i její jméno, slovo kryptos totiž v překladu znamená skryto.

2 Historie a struktura díla

Koncem 80.let proběhla generální oprava velitelství Ústřední spravodajské služby (CIA) v Americe. V rámci opravy bylo vytvořeno nové nádvoří a s ním myšlenka instalovat na něj umělecké dílo, které by nejen zpříjemnilo prostředí, ale i reprezentovalo práci CIA.

Služba tedy pověřila místního umělce Jima Sanborna, aby zkrášlil nový vnitroblok a západní vchod velitelství. Ten si k vytvoření svého díla přizval Edwarda Scheidta, bývalého předsedu kryptografického oddělení CIA.

Ke konci června roku 1990 bylo celé dílo, skádající se z více částí, instalováno.

První část tvoří tři deskové konstrukce z žuly a mědi, usazené u západního vchodu. Ve dvou z nich jsou vyryty zlomky Morseovy abecedy a ve třetím je zobrazena kompasová růžice, která ukazuje na přidělaný magnetovec.

Další částí je malé jezírko obklopené dvěma holými žulovými deskami.

Hlavní část instalace tvoří velký měděný plát podpíraný zkamenělým dřevem, do kterého je vyřezáno přes 1700 písmen.

3 Hlavní část

Jak již bylo zmíněno, hlavní částí celé instalace je měděný plát s vyřezanými písmeny, ta se dá rozdělit na dvě půlky - pravou a levou. Pravou část tvoří upravená Vigenèrova šifrovací tabulka/čtverec. Levou částí je šifrovaný text, který je tvořen přesně 865 písmeny a čtyřmi otazníky rozdělených do 28 řádků.

3.1 Vigenèrův čtverec

Vigenèrův šifrovací čtverec je tabulka 26x26 písmen anglické abecedy, který slouží pro rozkódování zprávy zakódované Vigenèrovou šifrou. První

řádek začíná písmenem A a pokračuje až do písmene Z. Od druhého řádku se písmena postupně poslouvají směrem vlevo a původní první písmeno jde na konec řádky. Tedy druhý řádek začína písmenem B a končí písmenem A a další řádek začíná písmenem C a končí B. Tento postup se opakuje dokud první sloupec tabulky netvoří anglickou abecedu.

Sanborn se Scheidtem ovšem použili upravený Vigenèrův čtverec. Jejich první řádek nezačínal písmenem A, protože před něj byly posunuty písmena „K R Y P T O S", původně zmíněný prncip posouvání se ovšem nezměnil.

Další modifikací bylo přidání indexových řádků a sloupce, které sestávaly ze seřazené anglické abecedy.

Poslední úpravou bylo zopakování prvních čtyř sloupců na konci tabulky a připsání písmene L do patnáctého řádku.

Pravá část tedy má 28 řádků a 31 sloupců.

3.2 Šifrovaný text

Pro zašifrování zprávy pomocí Vigenèrovy šifry je potřeba vymyslet klíč, slovo podle kterého se bude šifrovat. Pro dešifrování je tedy znalost klíče naprosto nezbytná.

Skutečnost, že polovinu sochy tvořil Vigenèrův čtverec, napovídala, že šifrovaný text je zakódovaný pomocí Vigenèrovy šifry.

V pár rozhovorech v letech 1990 a 1991 pan Sanborn prozradil, že kdokoli se znalostí Vigenèrova čtverce může rozšifrovat první polovinu zašifrovaného textu.

4 Řešitelé a jejich řešení

Od postavení sochy se mnoho jedinců snažilo Kryptos rozšifrovat, po dlouhých devět let se ale každý setkal s neúspěchem.

4.1 Jim Gillogly

Roku 1999 oznámil počítačový vědec Jim Gillogly, že byl v úspěšný v rozlomení Kryptosu. Tedy alepsoň částečně.

Zjistil, že Sanborn rozdělil šifrovaný text na čtyři části. Ty získali své pojmenování - K1, K2, K3 a K4.

Gillogly použil na míru vytořený program na svém počítači, který hrubou silou rozšifroval první tři části Kryptosu za čtyři dny. Poslední část textu zůstala tajemstvím.

Když svůj úspěch oznámil službě CIA, dozvěděl se smutnou zprávu. Jeden z jejich zaměstnaců ho v rozkódování předběhl.

4.2 David Stein

David Stein pracoval u CIA jako datový analytik. K rozšifrování Kryptosu využil sice pouze tužku a papír, to se ale odrazilo na investici času.

Stein nad Kryptosem strávil přes 400 hodin po dobu sedmi let. Za tuto dobu také přišel na skutečnost rozdělení šifrovaného textu do čtyř částí. Naneštěstí se setkal se stejnou překážkou jako pan Gillogly - K4. I přes velice nemalou oběť svého volného času se poslední úsek nehodlal zlomit.

Jeho úspěch byl zdokumentován v listopadu roku 1998, ale nikdo mu bohužel nevěnoval příliš pozornosti.

4.3 NSA

Po oznámení pana Gilloglyho vyšlo najevo, že ani Stein nebyl prvním úspěšným řešitelem. Národní bezpečnostní agentura (NSA) v Americe informovala veřejnost o tom, že skupina jejich zaměstanců Kryptos tajně rozšifrovala již v roce 1992. Této události předcházela oficiální výzva od CIA, kterou NSA přijala a ujali se ji čtyři zkušení kryptoanalytici.

Jejich prvním krokem bylo obrácení se na frekvenční analýzu, která zkoumá četnost jednotlivých znaků v textu.

V každém řádku šifrovaného textu spočítali četnost jednotlivých písmen (anglické abecedy) a díky tomu odhadli, že řádky 15 až 25 jsou nejspíše psané v angličtině a text je tedy zakódován pomocí transpoziční šifry. Ta spočívá na pouhém principu vzájemného prohození písmen textu.

Protože zbylé řádky měli jinou frekveni písmen než anglická jazyk, usoudili, že jsou zakódované pomocí substituční šifry. Její základní myšlenkou je nahrazení písmen textu jinými.

Šifrovaný text se jim tak rozdělil na tři úseky.

Byli přesvědčeni, že první část je zakódovaná pomocí Vigenèrovy šifry. Pomocí opakování shluků písmen v textu odhadli, že klíč k rozšifrování je slovo z osmi písmen. Pomocí dalšího užití frekvenční analýzy se postupně

prokopali až k čitelnému textu. Avšak ne celému. Zjistili, že první dva řádky jsou zašifrované pomocí jiného klíče.

Celý šifrovaný text se jim tedy rozdělil na 4 části a jako další se skupina vrhla na třetí (původně druhou). Všimla si, že v textu je napsané pouze jedno písmeno Q a to je v anglickém jazyce většinou následnováno písmenem U. Vzala tedy pár písmen před a po zmíněném Q a napsala je do sloupců. Poté udělala sloupce z okolních písmen U. Postupnými odhady a pokoušením kombinací sloupců se dostala k výsledku. Dokonce nakonec zjistila, že jejich teorie písmene Q předcházející písmenu U byla špatná a čtyři písmena na konci řádku 25 patří ke čtvrté části.

Posledním úspěchem bylo rozluštění první části, na kterou byla využita stejná metoda jako na druhou část.

Přes všechny snahy došel tým ostřilených kryptografů k závěru, že čtvrtou část nerozluští.

5 Jednotlivé vyřešené části

5.1 K1, K2, K3

Zpráva první části šifrovaného textu: „Between sublte shading and the absence of light lies the nuance of iqlusion."

K2 v sobě skrývá: „It was totally invisible. How's that possible? They used the Earth's magnetic field X the infromation was gathered and transmitted undergruund to an unknown location X Does Langley know about this? They should. It's buried out there somewhere. X Who knows the exact location? Only W.W. This was his last message X Thirty-eight degrees, fifty-seven minutes, six point five seconds, north. Seventy-seven degrees, eight minutes, forty-four seconds, west. Leyer two."

K3 zní: „Slowly, desparatly slowly, the remains of passage debris that encumbered the lower part of the doorway was removed with trembling hands. I made a tiny breach in the upper left-hand corner and then, widening the hole a little, I inserted the candle and peered in. The hot air escaping from the chamber caused the flame to flicker, but presently, details of the room within emerged from the mist X Can you see anything Q?"

V každé části je jedno slovo s pravopisnou chybou. Do dnes není jisté, zda přepisy slouží jako vodítko pro rozluštění poslední pasáže anebo jsou to pouze prostředky pro zmetení řešitele.

5.2 Další hádanka?

Jednotlivé zprávy, ikdyž odhalené, tak rozhodně nepůsobí. Pan Sanborn jednou v rozhovoru řekl: „They will be able to read what I wrote, but what I wrote is a mystery itself."

I přes neúplnou souvislost textu, jsou nějaké jeho části jednoznačné.

V druhé pasáži jsou jasně zmíněny souřadnice. Ty ukazují na místo pár metrů od sochy. Dříve zde byla zakopána geodetická značka. Jméno Langley má být alias pro službu CIA a W.W. má být odkazem na bývalého ředitele zmíněné služby.

Třetí segment je výtažek z knihy The Tomb of Tutankhamen. Poslední fráze textu z knihy není a je tak další záhadou.

6 Cesta ke správnému klíči

Důležitou zmínkou je, že nikdo z dotyčných řešitelů nerozlomil kódy tak, jak Sanborn a Scheidt plánovali. Jasná je skutečnost, že nikdo z řešitelů nepoužil k prolomení šifry klíč. Zpětným dosazením do se přislo na to, že klíčem je slovo abscissa. Nebylo však jasné jak se k němu dostat.

6.1 Morseova abeceda

Nadšenci naštěstí nezapomněli na ostatní části instalace a začali zkoumat kameny s Morseovým kódem. Ty nesou tuto zprávu: „E E VIRTUALLY E E E E E E E INVISIBLE DIGITAL E E E INTERPRETATIT E E SHADOW E E FORCES E E E E E LUCID E E E MEMORY E T IS YOUR POSITION E SOS RQ."

Od tohoto textu se ke slovu abscissa jde dostat. Avšak není úplně jasné, jak by to dělal jedinec, ketrý klíč předem nezná a tedy neví co hledá.

7 K4

Poslední část, o 97 písmenech, je přes dlouhých 24 let nerozlomená. Jim Sanborn i Edward Scheidt ovšem několikrát zmínili, že K4 jde vyřešit.

Sanborn dokonce přes tento dlouhý časový úsek nabídl pár vodítek. V roce 2006 zmínil, že první tři pasáže hrají roli v prolomení čtvrté. Od roku 2010 do roku 2020 čtyřikrát prozradil části dekódovaného textu.

Přes veškerou snahu mnoha jedniců s mnoha různými nápady zůstává Kryptos tajemstvím.

8 Zdroje

https://www.cia.gov/legacy/headquarters/kryptos-sculpture/
https://www.matweb.cz/vigenerova-sifra/
https://youtu.be/jVpsLMCIB0Y?si=93o-Xm7V0TppuDq0
https://www.matweb.cz/kryptografie/ https://jimsanborn.net/main.html