Playfairova šifra

Napravili Antonio Jadrejčić i Gregor Kostić

Youtube video: https://www.youtube.com/watch?v=G-eZ7mavbpc&ab_channel=LOREXANIMATIONS (https://www.youtube.com/watch?v=G-eZ7mavbpc&ab_channel=LOREXANIMATIONS)

U ovom projektu nam je bio cilj objasniti:

- povijest Playfairove šifre (tko ju je stvorio, gdje se i kad se koristila),
- kako ona funkcionira i kako se ona dekodira
- prikaz Playfairove šifre u programskom jeziku Pythoon.

Povijest

- Playfairovu šifru je izumio Charles Wheatstone.
- Ona je dobila ime po njegovom prijatelju Lord Lyon Playfairu koji ju je popularizirao.
- Prvi zabilježeni opis Playfair šifre nalazi se u dokumentu koji je potpisao Wheatstone 26. ožujka 1854.
- Koristila ga je britanska vojska u Drugom burskom ratu i Prvom svjetskom ratu u taktičke svrhe. Iz istog razloga su je koristili Britanci i Australci tijekom Drugog svjetskog rata. Jako je bila brza za korištenje, te nije zahtijevala nikakvu posebnu opremu. Tijekom Drugog svjetskog rata vlada Novog Zelanda ga je koristila za komunikaciju između Novog Zelanda, Chatamskih otoka i promatrača obale na pacifičkim otocima.
- Playfair više ne koriste vojne snage zbog pojave digitalnih uređaja za šifriranje. Ova šifra se sada smatra nesigurnom za bilo koju svrhu, jer bi je moderna računala mogla lako razbiti unutar nekoliko mikrosekundi.

Literatura

- Helen Fouche Gaines : Cryptanalysis a study of ciphers and their solution - https://archive.org/details/cryptanalysis00hele/mode/2up (https://archive.org/details/cryptanalysis00hele/mode/2up)
- https://www.simonsingh.net/The_Black_Chamber/playfair_cipher.html (https://www.simonsingh.net/The_Black_Chamber/playfair_cipher.html)
- https://web.math.pmf.unizg.hr/~duje/kript/playfair.html (https://web.math.pmf.unizg.hr/%7Eduje/kript/playfair.html)
- https://www.javatpoint.com/playfair-cipher-program-in-java (https://www.javatpoint.com/playfair-cipher-program-in-java)