SEMINARSKI RAD IZ PREDMETA
INFORMATIKA I INFORMATIČKE TEHNOLOGIJE

Naslov rada:
Kriptografija- šifriranje dokumenata

http://www.MATURSKIRADOVI.NET/

Sadržaj:

1. Povijest kriptografije

Kroz cijelu povijest čovječanstva postojala je potreba za sigurnom razmjenom informacija. Problemom sigurne komunikacije bavili su se već Egipćani i Indijci prije više od 3000 godina i od tada do danas osnovna ideja se nije promijenila – prenijeti neku poruku s jednog mjesta na drugo što je sigurnije moguće, tj. napraviti algoritam koji bi omogućio skrivanje originalne poruke tako da bude potpuno (u idealnom slučaju) nerazumljiva osobama koje bi neovlašteno došle u njen posjed. Prve korištene metode nisu bili složeni matematički algoritmi nego se počelo korištenjem alternativnih jezika koji su bili poznati samo malom broju ljudi. Razvoj složenijih metoda sigurne komunikacije počeo je tek razvojem pisma, što je omogućilo da se bilo koja informacija prikaže određenim brojem znakova koji bi, nakon upotrebe određenog ključa, formirali ponovno početnu poruku. S vremenom se javila i ideja prikaza slova drugim simbolima. Primjeri koji su i danas u upotrebi su: *Morseov kod*, *Braille-ovo pismo* i *ASCII kod*.

Slika 1. EnIgma

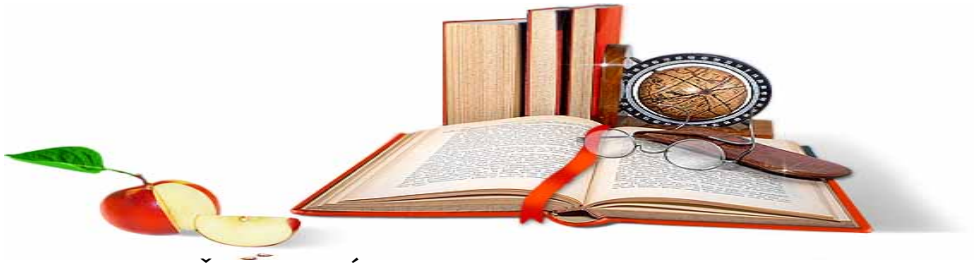
Slika 2.. Sigaba

Nikad nije točno utvrđen početak kriptografije, ali se smatra da je počela više od 2000 godina pr. Kr. jer iz tog vremena potječu prvi pronađeni tragovi šifriranja. Točnije, oko 1900. godine pr. Kr. u Egiptu nastao je natpis koji se danas smatra prvim dokumentiranim primjerom pisane kriptografije. U 6. stoljeću pr. Kr. u zapisu dijela Biblije, Knjige o Jeremiji, korištena je jednostavna šifra koja izvrće abecedu naopako. Šifra je poznata pod imenom ATBASH, a bila je jedna od hebrejskih šifri koje su u to vrijeme korištene. U 6. desetljeću pr. Kr. Julije Cezar je u državnim komunikacijama koristio jednostavnu supstituciju koja je kasnije njemu u čast dobila ime "caesar" šifriranje. Ideja je bila u pomicanju svih slova za tri mjesta naprijed. Takva šifra danas se smatra slabijom čak i od ATBASH šifre, ali je u to vrijeme bila dobra jer je mali broj ljudi znao čitati. U srednjem vijeku kriptografija je često korištena u službi Crkve, a jedan od primjera toga je nomenclator– kombinacija malog koda i supstitucijske abecede kojeg je na zahtjev pape Clementa VII stvorio Gabrieli di Lavinde. Ova šifra ostala je u upotrebi sljedećih 450 godina, iako su u međuvremenu stvorene i sigurnije šifre. Razlog tome je najvjerojatnije bio u njenoj jednostavnosti. 1518. Johannes Trithemius je napisao prvu tiskanu knjigu o kriptografiji. Oko 1790. Thomas Jefferson je uz pomoć matematičara Dr. Roberta Pattersona izumio šifrarnik s kotačem. On je kasnije ponovno izumljen u nekoliko

---- OSTATAK TEKSTA NIJE PRIKAZAN. CEO RAD MOŽETE PREUZETI NA SAJTU WWW.MATURSKI.NET ----

BESPLATNI GOTOVI SEMINARSKI, DIPLOMSKI I MATURSKI TEKST
RAZMENA LINKOVA - RAZMENA RADOVA
RADOVI IZ SVIH OBLASTI, POWERPOINT PREZENTACIJE I DRUGI EDUKATIVNI MATERIJALI.

WWW.SEMINARSKIRAD.ORG
WWW.MAGISTARSKI.COM
WWW.MATURSKIRADOVI.NET



NA NAŠIM SAJTOVIMA MOŽETE PRONAĆI SVE, BILO DA JE TO SEMINARSKI, DIPLOMSKI ILI MATURSKI RAD, POWERPOINT PREZENTACIJA I DRUGI EDUKATIVNI MATERIJAL. ZA RAZLIKU OD OSTALIH MI VAM PRUŽAMO DA POGLEDATE SVAKI RAD, NJEGOV SADRŽAJ I PRVE TRI STRANE TAKO DA MOŽETE TAČNO DA ODABERETE ONO ŠTO VAM U POTPUNOSTI ODGOVARA. U BAZI SE NALAZE GOTOVI SEMINARSKI, DIPLOMSKI I MATURSKI RADOVI KOJE MOŽETE SKINUTI I UZ NJIHOVU POMOĆ NAPRAVITI JEDINSTVEN I UNIKATAN RAD. AKO U BAZI NE NAĐETE RAD KOJI VAM JE POTREBAN, U SVAKOM MOMENTU MOŽETE NARUČITI DA VAM SE IZRADI NOVI, UNIKATAN SEMINARSKI ILI NEKI DRUGI RAD RAD NA LINKU IZRADA RADOVA. PITANJA I ODGOVORE MOŽETE DOBITI NA NAŠEM FORUMU ILI NA

maturskiradovi.net@gmail.com