

KOMISIJI ZA STUDIJE II STEPENA ELEKTROTEHNIČKOG FAKULTETA U BEOGRADU

Komisija za studije II stepena, Elektrotehničkog fakulteta u Beogradu, na svojoj sednici održanoj 12.07.2012. godine imenovala nas je u Komisiju za pregled i ocenu master rada kandidatkinje Jovane Stolović pod naslovom „Analiza i računarska primena algoritma kodiranja pomoću knjige“. Nakon pregleda materijala Komisija podnosi sledeći

IZVEŠTAJ

1. Biografski podaci kandidata

Jovana Stolović je rođena 07.11.1986. godine u Kraljevu. Osnovnu školu „Braća Vilotijević“ završila je 2001. godine, kada je upisala Kraljevačku Gimnaziju. Elektrotehnički fakultet u Beogradu je upisala 2005. godine, a diplomirala septembra 2011 godine. Oktobra 2011. godine se upisala na master studije na Elektrotehničkom fakultetu, na modulu Računarska tehnika i informatika.

2. Opis master rada

Master rad kandidatkinje Jovane Stolović sadrži 57 stranica teksta sa slikama, tabelama i delovima programskog koda. Rad je podeljen u šest poglavlja.

U prvom poglavlju, uvodu, opisan je razvoj kriptografije uz primere korišćenih algoritama u istoriji razvoja ove nauke. Hronološki su prikazani razvojni putevi različitih algoritama kriptografije iz prošlosti. Navedeni su i glavni principi koje današnja kriptografija koristi i razvija. Drugo poglavlje predstavlja objašnjenje funkcionisanja Book Cipher algoritma. Obrazložene su sve njegove karakteristike, kao i osnove na kojima se zasniva njegova sigurnost, sama primena algoritma i mogućnost njegovog dekodovanja. U ovom poglavlju dat je uvod u probleme koji utiču na efikasnost i performanse algoritma.

Treće poglavlje prikazuje sve analize koje su urađene, gde je glavni parametar koji se menjao bio jezik kodne knjige. Izabrana su četiri svetska jezika (engleski, francuski, holandski i finski), i više različitih formata fajlova koji su eksperimentalno iskodirani korišćenjem algoritma. Parametar koji se menjao i uticao na analizu, jeste vrednost offset-a. Uzimajući sve parametre u obzir, formirane su tabele i grafikoni koji prikazuju rezultate analize.

Četvrto poglavlje predstavlja novi set urađenih analiza. U ovim analizama korišćen je umesto kodne knjige kodni fajl. Objašnjeno je formiranje originalno osmišljene „veštačke reči“ u kodnom fajlu koji predstavlja reč po kojoj se traži šifra. Za analizu je uzeto sedam datoteka različitih formata, koje su predstavljale kodni fajl, a fajlovi za koje je pokušano kodiranje su isti kao u prethodnom poglavlju. Svi rezultati analize su prikazani kroz tabele.

Peto poglavlje predstavlja zaključak rada, gde su sažete sve prednosti dobijene ovakvim načinom korišćenja Book Cipher algoritma, kao i smernice za neka sledeća istraživanja.

3. Analiza rada sa ključnim rezultatima

Master rad dipl. inž. Jovane Stolović se bavi analizom i računarskom primenom algoritma kodiranja pomoću knjige. Urađene analize ukazuju na neke nove načine korišćenja ovog


algoritma i mogućnosti prelaska sa teksta na fajlove različitih formata, što povoljno utiče na upotrebljivost Book Cipher algoritma, kao i na mogućnost poboljšanja njegovih performansi.

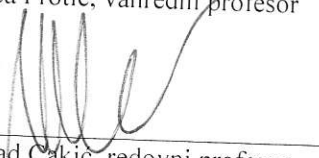
4. Zaključak i predlog

Kandidatkinja Jovana Stolović je u svom master radu uspešno rešila problem računarske primene algoritma kodiranja pomoću knjige i detaljne analize različitih varijanti ovog algoritma za različite jezike i formate. Na osnovu gore navedenog, Komisija predlaže Nastavno-naučnom veću Elektrotehničkog fakulteta u Beogradu da prihvati rad „ Analiza i računarska primena algoritma kodiranja pomoću knjige “ dipl. inž. Jovane Stolović kao master rad i odobri javnu usmenu odbranu.

U Beogradu, 06.9.2014.

Članovi Komisije


dr Jelica Protić, vanredni profesor


dr Nenad Čakić, redovni profesor