- Raspored nastave
- Literatura
- Formiranje ocene
- Opis predmeta
- Cilj predmeta
- Saveti za uspešan rad
- Osnovni pojmovi

Kriptologija 1

Raspored nastave

- Raspored nastave
- Literatura
- Formiranje ocene
- Opis predmeta
- Cilj predmeta
- Saveti za uspešan rad
- Osnovni pojmovi

Predavanja:

- Prof. Dr. Mladen Veinović
- mveinovic@singidunum.ac.rs
- Predavanja su utorkom od 11 do 14 č., Kumodraška – 015
- Konsultacije su utorkom od 14 do 15 č., Kumodraška – Zbornica 042

Vežbe

- Uroš Arnaut
- uarnaut@singidunum.ac.rs
- Vežbe su sredom od 09 do 11 časova, Kumodraška – E-117
- Konsultacije su:
- Utorkom od 11 do 12 časova, Kumodraška – Zbornica 042
- Petkom od 17 do 18 časova, Danijelova 32 – Zbornica II sprat

Literatura

- Raspored nastave
- Literatura
- Formiranje ocene
- Opis predmeta
- Cilj predmeta
- Saveti za uspešan rad
- Osnovni pojmovi

- M.Veinović, S.Adamović, Kriptologija 1, Univerzitet Singidunum, 2018
- Video materijale za predmet možete pronaći na linku.
- Materijali na stranici predmeta (predavanja i vežbe)

Formiranje ocene

- Raspored nastave
- Literatura
- Formiranje ocene
- Opis predmeta
- Cilj predmeta
- Saveti za uspešan rad
- Osnovni pojmovi

- Aktivnost na predavanjima: 5 poena
- Aktivnost na vežbama: 5 poena

- Prvi kolokvijum: 30 poena (20 zadatak + 10 teorija)
- Drugi kolokvijum: 30 poena (20 zadatak + 10 teorija)

- Ispit: 30 poena (30 teorija)

Formiranje ocene

- Ocena se formira na sledeći način:

1. Saberu se poeni sa oba kolokvijuma i sa ispita (PO1);
2. Ako je PO1 veće ili jednako 51, dodaju se poeni za aktivnost na predavanjima i vežbama (PO2);
3. Ocena se formira na osnovu broja poena PO2 i to:
   - [51 – 60] ocena 6
   - [61 – 70] ocena 7
   - [71 – 80] ocena 8
   - [81 – 90] ocena 9
   - [91 – 100] ocena 10

Opis predmeta

- Raspored nastave
- Literatura
- Formiranje ocene
- Opis predmeta
- Cilj predmeta
- Saveti za uspešan rad
- Osnovni pojmovi

- Na ovom predmetu studenti stiču neophodna znanja iz zaštite informacionih sistema uz primenu matematičkog aparata koji je potreban za analizu i sintezu savremenih šifarskih sistema.
- Savladavaju se osnovni servisi zaštite informacija: tajnost, integritet, autentifikacija i neporecivost. Definišu se apsolutno i praktično tajni šifarski sistemi.
- Detaljno se razmatraju svojstva simetričnih (sekvencijalni i blokovski) i asimetričnih šifarskih sistema.
- Prikazuju se savremeni algoritmi za šifrovanje i pravilna upotreba šifarskih ključeva (tajni, javni, privatni, sesijski, fabrički itd.). Praktičan deo vežbi se realizuje u Cryptool softverskom okruženju.

Cilj predmeta

- Studenti će biti osposobljeni da samostalno procenjuju kvalitet zadatog šifarskog sistema i razumeju njegovo mesto i ulogu u savremenom integrisanom računarskom okruženju.

Saveti za uspešan rad

- Raspored nastave
- Literatura
- Formiranje ocene
- Opis predmeta
- Cilj predmeta
- Saveti za uspešan rad
- Osnovni pojmovi

- Stalan rad tokom celog semestra (nedelja za nedeljom)
- Redovno praćenje nastave, ali, pre svega, samostalno praktično vežbanje na računaru u programu “Cryptool ”.
- Pitati o svemu što nije jasno na samim vežbama – ne čekati da se nejasnoće nagomilaju
- Ako se vidi da se zaostaje, ići na konsultacije

Osnovni pojmovi

- Kriptologija je nauka o zaštiti podataka nastala je od grčkih reči (*kryptós-skriven + logos-znanje)*
- Kriptografija je metoda koja se bavi očuvanjem tajnosti podataka
- Kriptoanaliza je proces razbijanja šifrarskih sistema.

Osnovni pojmovi

- Klasična kriptografija:
  - Šifre transpozicije
  - Šifre supstitucije
  - One-time pad
  - Kodne knjige

Osnovni pojmovi

- M- otvoreni tekst (poruka)
- C- šifrat = E(M,K)
- E- šifrovanje
- D – dešifrovanje- D(C,K) = M
- K – ključ

Univerzitet Singidunum

Hvala na pažnji !