| MI006 | **Kriptografija** | P | V | S | ECTS |
|---|---|---|---|---|---|
| | | 2 | 2 | 0 | 6 |

**Cilj predmeta.** Upoznati studente s temeljnim pojmovima i metodama kriptografije i kriptoanalize različitih tipova kriptosustava. Predstavit će se osnovne ideje šifriranja i dešifriranja podataka kroz moderne simetrične i asimetrične kriptosustave. Kako su moderni kriptosustavi zasnovani na funkcijama iz teorije brojeva, svi nužni osnovni pojmovi uvest će se na mjestima gdje se za njima prvi put ukaže potreba. Na taj način omogućit će se jednostavnije proučavanje prednosti i nedostataka različitih tipova kriptosustava.

**Potrebna predznanja.** Preddiplomski studij matematičkog, računarskog ili srodnog smjera.

**Sadržaj predmeta.**

1. Osnovni pojmovi. Klasifikacija kriptosustava. Napadi na kriptosustave.
2. Supstitucijske šifre. Cezarova šifra. Afina šifra. Analiza frekvencije slova. Cezarova šifra s ključnom riječi. Vigenereova šifra. Playfairova šifra. Hillova šifra.
3. Transpozicijske šifre. Permutacijska šifra. Stupčana transpozicija.
4. Testovi prostosti i neke metode faktorizacije. Distribucija prostih brojeva. Pseudoprosti brojevi. Fermatova metoda faktorizacije. Pollardova metoda faktorizacije. Metoda verižnog razlomka.
5. Kriptografija javnog ključa. RSA kriptosustav i neke njegove modifikacije. Rabinov kriptosustav. ElGamalov kriptosustav.

**ISHODI UČENJA**

| R.b. | ISHODI UČENJA |
|---|---|
| 1. | Razlikovati osnovne tipove kriptosustava i napade na njih. |
| 2. | Primijeniti postupak šifriranja i dešifriranja podataka u prezentiranim kriptosustavima. |
| 3. | Obrazložiti ulogu osnovnih alata teorije brojeva u kriptografiji te prostih i pseudoprostih brojeva u konstrukciji kriptosustava. |
| 4. | Analizirati kriptosustav s javnim ključem. |
| 5. | Povezati različite dijelove kriptografije za samostalno rješavanje problemskih zadataka. |

**POVEZIVANJE ISHODA UČENJA, ORGANIZACIJE NASTAVNOG PROCESA I PROCJENA ISHODA UČENJA**

| ORGANIZACIJA NASTAVNOG PROCESA | ECTS | ISHOD UČENJA ** | AKTIVNOST STUDENATA* | METODA PROCJENE | BODOVI | |
|---|---|---|---|---|---|---|
| | | | | | min | max |
| Pohađanje predavanja i vježbi | 1 | 1-5 | Prisutnost na nastavi, rasprava, samostalan rad na zadacima | Potpisne liste, praćenje aktivnosti na nastavi | 0 | 4 |
| Domaće zadaće | 1 | 1-5 | Samostalno rješavanje predloženih zadataka | Provjera točnih rješenja (ocjenjivanje) | 0 | 4 |
| Provjera znanja (kolokvij) | 2 | 1-5 | Priprema za pismenu provjeru znanja | Provjera točnih odgovora (ocjenjivanje) | 25 | 46 |
| Završni ispit | 2 | 1-5 | Ponavljanje gradiva | Usmeni ispit | 25 | 46 |
| UKUPNO | 6 | | | | 50 | 100 |

**Izvođenje nastave i vrednovanje znanja.** Predavanja i vježbe su obvezni. Ispit se sastoji od pismenog i usmenog dijela, a polaže se nakon odslušanih predavanja. Prihvatljivi rezultati postignuti na kolokvijima, koje studenti pišu tijekom semestra, zamjenjuju pismeni dio ispita. Studenti mogu utjecati na ocjenu tako da tijekom semestra pišu domaće zadaće.

**Može li se predmet izvoditi na engleskom jeziku:** Da

## Osnovna literatura:


1. R. Mollin, An introduction to Cryptography, 2nd edition, Chapman and Hall/CRC Press, Boca Raton, 2007.
2. N. Koblitz, *A Course in number theory and cryptography*, Springer-Verlag, New York, 1994.
3. M. J. Hinek, Cryptanalysis of RSA and its variants, Chapman and Hall/CRC Press, Boca Raton, 2010.


## Dopunska literatura:


1. Dujella, M. Maretić, Kriptografija, Element, Zagreb, 2007.
2. S. C. Coutinho, The mathematics of ciphers; number theory and RSA cryptography, A. K. Peters, Natick, Massachusetts, 1999.
3. A. J. Menezes, P. C. Oorschot, S. A. Vanstone, Handbook of Applied Cryptography, CRC Press, Boca Raton, 1996.