KATALOG ZNANJA

1. IME PREDMETA

KRIPTOGRAFIJA

2. SPLOŠNI CILJI

Splošni cilji predmeta so:

- predstaviti zgodovinske zasnove kriptografije;
- predstaviti pomen zagotavljanja zaupne komunikacije, šifriranja sporočil;
- usposobiti za kritično mišljenje, učinkovito komunikacijo;
- razviti digitalno in računsko pismenost ter kreativnost;
- naučiti načrtovanja in določanja prioritet, samoupravljanja ter samorefleksije.

Specifično strokovno usmerjeni cilji so:

- obvladati funkcije kriptografije za potrjevanje identitete ter integritete informacij;
- uporabiti kriptografske sisteme, matematične algoritme pri kriptografiji ter kriptografski programski opremi;
- uporabiti simetrične in asimetrične metode šifriranja, razne šifre ter protokole šifriranje in njihovo uporabo v praktičnih scenarijih;
- poznati postopke šifriranja DES, 3DES ter AES;
- izvajati varnostne analize ter vrednotiti napredne protokole šifriranja;
- obvladati delovanje javnih in zasebnih ključev, infrastrukturo javnih ključev PKI, postopek testiranja praštevilskosti, diskretne algoritme ter šifriranje El Gamal.

3. PREDMETNO SPECIFIČNE KOMPETENCE

Pri predmetu študenti poleg generičnih pridobijo naslednje kompetence:

1. analiziranje algoritmov simetričnega šifriranja;
2. vrednotenje protokolov šifriranja javnih ključev in podpisov ter njihova uporaba pri izmenjavi sporočil in ključev;
3. ocenjevanje varnostnih pomislekov, povezanih z metodami simetričnega in asimetričnega šifriranja;
4. vrednotenje naprednih protokolov šifriranja ter njihove uporabe pri varni izmenjavi sporočil.

4. OPERATIVNI CILJI

INFORMATIVNI CILJI	FORMATIVNI CILJI
1. Analiziranje algoritmov simetričnega šifriranja	
● primerja razlike med delovanjem tokovnih in blokovnih šifer; ● opiše delovanje tokovne in blokovne šifre na vnaprej določenih primerih; ● analizira tokovne šifre, zgodovinski Lorenz SZ 40/42, sodobne tokovne šifre (npr. linearni registri, i. d.); ● definira blokovne šifre, Feistelovo šifro, blokovni algoritem DES – standard šifriranja podatkov, operacije 3DES ter Rijndaelovo šifro (AES); ● opiše zgodovinske šifre, Cezarjevo šifro, napravo Enigma in informacijsko teoretično varnost (verjetnost, entropija in lažne ključe), ter koncept edinstvenega ključa; ● razčleni distribucijo simetričnih ključev, funkcijo zgoščenih sporočil, kod potrjevanja sporočil ter upravljanja s ključi, varno distribucijo ključev, načrtovanje funkcij zgoščenih sporočil; ● analizira koncepte modularne aritmetike, eliptične krivilje, projektivne koordinate, grup, končnega polja in verjetnosti; ● ovrednoti matematične algoritme, ki so v rabi pri kriptografiji; ● oceni izboljšave, ki jih je vpeljala uveljavitev AES, v primerjavi s standardi šifriranja javnih in zasebnih ključev DES in 3DES	● izdela predstavitev izbranih težav pri distribuciji simetričnih ključev in postopek reševanja s funkcijami zgoščenih sporočil ter kodami za potrjevanje sporočil.
2. Vrednotenje protokolov šifriranja javnih ključev in podpisov ter njihova uporaba pri izmenjavi sporočil ter ključev	
● opiše postopek kriptografije javnih ključev; ● analizira algoritme za šifriranje javnih ključev, enosmerne funkcije, algoritem RSA ter šifriranje El Gamal; ● definira testiranje in faktorizacijo praštevilskosti, diskretne logaritme,	● izdela analizo implementacije izmenjave javnih ključev (npr. distribucija, protokoli šifriranja, podpisovanje, i. d.) na vnaprej določenih primerih.

faktorizacijo algoritmov, sodobne metode faktorizacije, algoritem PohligHellman, logaritmične metode končnih polj in metode za eliptične krivulje; ● definira pogoste metode šifriranja javnih ključev ter njihovo uporabo; ● ovrednoti izmenjavo ključev in podpisov, izmenjavo ključev po metodi Diffie-Hellman, digitalne podpise, ki uporabljajo funkcije zgoščenih sporočil ter algoritem za digitalne podpise (DSA); ● oceni javno infrastrukturo ključev PKI na vnaprej določenih primerih.	
3. Ocenjevanje varnostnih pomislekov, povezanih z metodami simetričnega in asimetričnega šifriranja	
● definira pogoste primere napadov na sisteme šifriranja javnih ključev (npr. Wienejev napad na RSA, Lattice napad na RSA, delna izpostavitev ključev, Meetin-the-Middle napad, napad surove sile ter analiza ranljivosti, i. d.); ● analizira pojem dokazljiva varnost ter definira naključne oraklje, varnost šifrirnih algoritmov in šifriranje z naključnimi oraklji ● ovrednoti varnost hibridnih šifer in izdelavo mehanizmov za inkapsulacijo ključev (KEM).	● predstavi delovanje javne infrastrukture ključev PKI na vnaprej določenih primerih in izpostavi izzive in varnostna vprašanja, povezana z metodami simetričnega in asimetričnega šifriranja.
4. Vrednotenje naprednih protokolov šifriranja ter njihove uporabe pri varni izmenjavi sporočil	
● opiše delovanje naprednih protokolov šifriranja in njihovo uporabo; ● definira izmenjavo skrivnih ključev; ● analizira implementacijo šifriranja javnih ključev pri sistemih za digitalno glasovanje; ● definira protokol Zero-Knowledge (v sistemih za digitalno glasovanje); ● ovrednoti varni skupinski izračun z dvema entitetama in več entitetami; ● oceni strukture dostopov za izmenjavo skrivnih ključev.	● uporabi deljeni podpis RSA za varno izmenjavo sporočil ter predstavi postopek implementacije; ● demonstrira izomorfizem grafov pri protokolih Zero-Knowledge in Sigma; ● izdela predstavitev o vrednotenju naprednih aplikacij kriptografskih pristopov v družbi (npr. kvantna kriptografija, digitalni denar, Bitcoin, i. d.).

5. OBVEZNOSTI ŠTUDENTOV IN POSEBNOSTI V IZVEDBI

Število kontaktnih ur: 70 ur (35 ur predavanj, 35 ur laboratorijskih vaj).
Število ur samostojnega dela študenta: 150 (študij literature, delo z besedilom, študij primerov, delo s programsko opremo in orodji kriptografije, priprava pisnih besedil in predstavitve …).