

ТЕОРИЈА БРОЈЕВА И КРИПТОГРАФИЈА

проф. др Бојана Боровићанин

ЗАШТО ОВАЈ ПРЕДМЕТ?

- Како безбедно послати поруку преко несигурне мреже?
- Зашто су велики прости бројеви важни за заштиту података?
- Како математика потврђује идентитет и аутентичност документа?

ОД ТЕОРИЈЕ ДО АЛГОРИТМА

- МОДУЛАРНА АРИТМЕТИКА → RSA
- КВАДРАТНИ ОСТАЦИ → ТЕСТОВИ ПРОСТОСТИ
- ДИСКРЕТНИ ЛОГАРИТАМ → DIFFIE–HELLMAN / ELGAMAL
- СИМЕТРИЧНЕ ШИФРЕ → AES

ШТА СТУДЕНТ ДОБИЈА?

- Разуме математичку основу савремене криптографије.
- Повезује теореме теорије бројева са конкретним алгоритмима.
- Анализира сигурност и ограничења криптосистема.
- Имплементира и испитује једноставне криптографске алгоритме.

КЉУЧНЕ ТЕМЕ КУРСА

ТЕОРИЈА БРОЈЕВА

НЗД и проширен Еуклидов алгоритам • конгруенције • Ојлерова и Фермаова теорема • Кинеска теорема о остацима

ПРОСТОСТ И АЛГОРИТМИ

квадратни остаци • Лежандров и Јакобијев симбол • квадратни реципроцитет • Solovay–Strassen • Miller–Rabin • факторизација

КРИПТОГРАФИЈА

симетрична и асиметрична криптографија • AES • RSA • Diffie–Hellman • ElGamal • хеш функције • дигитални потпис

НАЧИН ПОЛАГАЊА

Предиспитне обавезе **70 поена** | активност **10** • колоквијуми **20+20** • семинарски/пројектни рад **20**
Завршни испит **30 поена**