Криптографија (Б и Ц)

Наставни план и информације

Основне информације

Предавач	Владимир Божовић
Предавања	Понедјељак, 17:15 - 18:00, сала 107-А
Предавања и вјежбе	Уторак, 18:15 - 20:00, сала 107-А
Веб сајт	www.vladimirbozovic.net/univerzitet
Консултације	По договору

Кратак садржај циљева курса

Циљ курса је да се у првом дијелу курса упознамо са основним темама класичне криптографије као што су *симетрични* криптографски системи, као и са основним *криптоаналитичким* техникама. У другом дијелу курса ћемо се углавном бавити асиметричним (public key) системима, техникама факторизације, елиптичном криптографијом, дигиталним потписом... Одређена поглавља из теорије бројева су укључена као саставни дио овог курса како би у потпуности разумјели поједине теоријске јединице.

Литература

Не постоји одређена књига које ћемо се држати у свим наставним јединицама овог курса. Ипак, највећи дио садржаја ће бити покривен у следећим књигама

1. ***An Introduction to Mathematical Cryptography***, Jeffrey Hoffstein, Jill Pipher, Joseph H. Silverman, 2008, ISBN: 978-0-387-77993-5.

2. ***A Course in Number Theory and Cryptography***, Neal Koblitz, 1994, ISBN: 0-387-94293-9.

Сви потребни садржаји, основни и додатни, ће бити обезбјеђени на веб страници овог курса.

Облици провјере знања и оцјењивање

Испитни елементи су

(а) Два теста која вриједе по 30 поена.

(б) Пројектни задатак (рад у групама) који вриједи 30 поена.

(в) Посебно залагање и труд током наставе, као и изузетна рјешења појединих задатака се вреднују до 10 поена.

Прелазна оцјена се добија ако је коначан збир освојених поена **строго већи** од 50 поена. У два испитна рока на крају семестра, студенти имају право да поправљају оба колоквијума и то:
- у првом року је поправак првог колоквијума;
- у другом поправак другог колоквијума.

Уколико студент није у прилици да приступи испиту у дефинисаним терминима, а нису озбиљни здравствени (поткријепљени документацијом) разлози, нема право на испит у посебном термину.

Ако студент излази на поправни колоквијум, онда ће се резултат који оствари на њему узимати као коначни за тај дио испита.

Студент који је на колоквијумима скупио мање од 20 поена нема право одбране пројектног задатка.

Присуство настави је пожељно али није обавезно.

Садржај курса и план рада

Слиједи преглед материјала и календар по којем ћемо радити. Предложени садржај и план рада се може у одређеној мјери промијенити у току извођења наставе.

I недјеља

Увод у криптографију; Историја криптографије; Једноставни супституциони системи. Увод у криптоанализу.

II недјеља

Дјељивост; Еуклидов алгоритам;

III недјеља

Прости бројеви и факторизација. Модуларна аритметика.

IV недјеља

Кинеска теорема о остацима. Диофантове једначине.

IV недјеља

Основне алгебарске структуре. Група, прстен, поље. Система остатака као прстен по датом модулу.

V недјеља

Аритметичке функције, Фермаова и Ојлерова теорема.

VI недјеља

Симетрична криптографија; Примјери симетричних крипто-система.

VII недјеља

Слободна недјеља.

VIII недјеља

Асиметрична криптографија; Проблем дискретног логаритма у коначном пољу; Дифи-Хелман алгоритам.

IX недјеља

Први тест; Ел-Гамал алгоритам; Комплексност проблема дискретног логаритма.

X недјеља

Baby step-Giant step алгоритам за тражење дискретног логаритма; Кинеска теорема о остацима; Скица Полиг-Хелман алгоритма.

XI недјеља

Факторизација у криптографији; Ојлерова формула и коријени модуло pq; Увод у RSA алгоритам.

XII недјеља

RSA имплементација; Сигурносна питања RSA алгоритма; Утицај RSA алгоритма на развој криптографије.

XIII недјеља

Тестови прималности. Полардови алгоритми за факторизацију. Факторизација помоћу разлике квадрата.

XIV недјеља

Абелова група елиптичне криве; Елиптична крива над коначним пољем; Дискретни логаритам на елиптичној кривој.

XV недјеља

Појам и имплементација дигиталног потписа; RSA дигитални потпис.

XVI недјеља

Други тест.

XVII-XXI недјеља

Овјера семестра и упис оцјена; Допунска настава и поправни испитни рок.

Академски интегритет

Сви испитни елементи морају бити рађени самостално уколико предметни наставник не дефинише другачије. Предаја домаћих задатака мора бити у оквиру термина који је дефинисан од стране предметног наставника или асистента. Кашњење предаје домаћег задака ће бити санкционисано одузимањем 2.5 поена. Уколико се на тесту или домаћем задатку утврди да је студент користио недозвољена средства, одузима се цјелокупан износ бодова који се односи на тај испитни елемент.