Модул: Телекомуникациони саобраћај и мреже

БЕЗБЕДНОСТ ИНФОРМАЦИЈА

Наставник: Андреја Самчовић (andrej@sf.bg.ac.rs)

Мастер академске студије

Наставни програм:

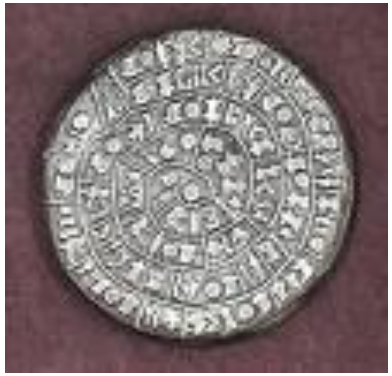
Недеља	Тема/активност
I	Увод
II	Основе криптологије
III	Симетрични криптосистеми
IV	Елементи Шенонове теорије заштите информација
V	Асиметрични криптосистеми
VI	Колоквијум 1
VII	Хеш функције

Мастер академске студије

Наставни програм:

Недеља	Тема/активност
VIII	PKI инфраструктура
IX	Ауторизација
X	Аутентификациони протоколи
XI	Колоквијум 2
XII	SSL, IPSEC, GSM и Kerberos протоколи
XIII	Безбедност софтвера
XIV	Безбедност оперативних система
XV	Безбедносне политике и евалуација безбедности

Садржај



- **Предавања:** 3 часа недељно
- **Вежбе:** 2 часа недељно
  - теоријске и лабораторијске

- **Циљ и задаци предмета:**
  - ✓Упознавање са основама безбедности информација, криптологијом као научном основом заштите информација, криптолошким механизмима заштите, сервисима безбедности: аутентификацијом, ауторизацијом, тајношћу, непорецивошћу и расположивошћу

- ✓Упознавање са PKI инфраструктуром, безбедносним протоколима, малициозним софтверима, безбедношћу оперативних система, као и основама безбедносних политика и евалуације система безбедности у информационим и комуникационим системима

- Безбедност информација – један од најважнијих проблема информационих технологија
- Повезивање и широка понуда нових сервиса
- Нове ИКТ у последњој деценији
- Напади на комуникационе системе, инфраструктуру и приватност корисника
- Аспекти безбедности од мрежног до апликационог слоја

- Безбедност рачунарских мрежа
- Провале у комуникационе системе
- Детекција и методе одбране
- Криптографија и криптотехнологије
- Безбедност веб апликација
- Биометрија
- Форензика

Појам криптографије

- Криптологија је термин који потиче од грчких речи kriptos (скривен, тајан) и logos (наука), и означава научну дисциплину која се бави сигурним (тајним) комуникацијама
- Две основне, тесно повезане гране криптологије су:
  - криптографија и
  - криптоанализа

- Предмет **криптоанализе** је разматрање метода којим се компромитују (“разбијају“ од стране неовлашћених корисника) поступци криптозаштите информација

Основни елементи криптографије

- **Шифровање** – поступак трансформације читљивог текста у облик нечитљив за онога коме тај текст није намењен
- **Дешифровање** – поступак враћања шифрованог текста у читљив облик
- **Кључ** – почетна вредност алгоритма којим се врши шифровање

- **Тајност** – обезбеђује да информациони садржај поруке буде доступан само овлашћеним корисницима
- **Интегритет** – обезбеђује откривање неовлашћене измене информационог садржаја поруке
- **Аутентичност** – омогућава проверу идентитета учесника у комуникацији
- **Непорецивост** – спречава могућност порицања реализације одређених активности учесника у комуникацији (као што су слање поруке, трансакција и др.)

- **Литература:**
  - Предавања, ppt презентације
  - Додатни pdf материјали
  - Тест питања

Литература

- Г. Грубор, М. Милосављевић, Основе заштите информација, Универзитет Сингидунум, 2010.
- М. Веиновић, С. Адамовић, Криптологија I, Универзитет Сингидунум, 2013.
- М. Милосављевић, Г. Грубор, Дигитална форензика рачунарског система, Универзитет Сингидунум, 2009.