Студијски програм:	Информационе технологије и системи
Назив предмета:	САВРЕМЕНИ КРИПТОГРАФСКИ СИСТЕМИ
Наставник:	**Музафер Сарачевић**
Статус предмета:	Изборни предмет
Број ЕСПБ:	6
Услов:	Нема

Циљ предмета:
Упознавање са основним криптографским концептима и технологијама. Стицање знања о принципима безбедности информација и основним техникама и алгоритмима који се користе у криптографији. Разумевање комуникација у криптографском систему.

Исход предмета:
Оспособљеност студената за примену криптографских техника којима се обезбеђују разни видови сигурности информација. Имплементација савремених криптографских система за заштиту и пренос података уз разумевање и примену актуелних стандарда и добре праксе у области криптографије.

Садржај предмета:

Теоријска настава

Историја криптографије; Концепти криптографије; Циљеви криптографије; Алгоритми и имплементација алгоритама за шифровање; Кључеви, Vernam-ове шифре (one-time pad), енкрипционе шеме, математичке основе криптографије, бијекције, пермутације, једносмерне и једносмерне trapdoor функције, цели бројеви, тестови простости, методе факторизације, блок шифре, супституцијске и транспозицијске шифре, композиција шифри, проточне шифре, криптосистеми са тајним (симетричним) кључем, DES, криптосистеми са јавним кључем, RSA криптосистем, криптоанализа, аутентификација, дистрибуција кључева, дигитални потписи, стеганографске методе.

Практична настава: Вежбе, Израда задатака за примену метода шифровања, Семинарски рад.

Литература:

1. Veinović, M., & Adamović, S. (2013). Kriptologija 1. Beograd: Univerzitet Singidunum.
2. Milosavljević, M., & Adamović, S. (2014). Kriptologija 2. Univerzitet Singidunum, Beograd.
3. Menezes, A. J., Van Oorschot, P. C., & Vanstone, S. A. (2018). Handbook of applied cryptography. CRC press.
4. Delfs, H., Knebl, H., & Knebl, H. (2002). Introduction to cryptography (Vol. 2). Heidelberg: Springer.
5. Banoth, R., & Regar, R. (2023). Classical and Modern Cryptography for Beginners. Springer Nature.
6. Vidick, T., & Wehner, S. (2023). Introduction to Quantum Cryptography. Cambridge University Press.

Број часова активне наставе: 75	**Теоријске наставе**: 30	**Практичне наставе**: 30	**Студијски истраживачки рад**: 15

Методе извођења наставе:
Предавања, семинари, презентација и дискусија о радовима студената, појединачне и групне консултације.

Оцена знања (максималан број поена 100)

Предиспитне обавезе	Поени	**Завршни испит**	Поени
Активност у току предавања	10	Усмени испит	30
Презентација на часу/дискусија	15		
Колоквијуми	20		
Семинарски рад	25		