

Назив предмета: Криптологија I		
Наставник или наставници: Миодраг Михаљевић		
Статус предмета:		
Број ЕСПБ:		
Услов:		
Циљ предмета Едукација из криптологије која је основа за остваривање информационе безбедности и приватности.		
Исход предмета Овладавање главним методама и техникама криптологије као полазиште за истраживачки рад у области криптологије и примена		
Садржај предмета <i>Теоријска настава</i> Увод и класична криптографија, Принципи модерне криптографије, Доказива сигурност и сигурност у реалном свету, Перфектна енкрипција (шифровање), Криптографија са приватним (симетричним) кључевима, Сигурност на бази сложености израчунавања, Напади на бази изабраног отвореног текста и СРА-сигурност, Напади на бази изабраног шифрата и ССА-сигурност, Секвенцијални шифарски поступци, Блок шифарски поступци, Кодови за аутентикацију порука, Аутентикована енкрипција, Хеш функције, Практичне конструкције криптографских примитива са симетричним кључевима, Теоријски приступи конструкцијама криптографских примитива са симетричним кључевима, Криптографија са асиметричним кључевима (јавним и тајним кључем), Теорија бројева и претпоставке о тешким проблемима, Алгоритми за факторизацију и израчунавање дискретних логаритама, Управљање криптографским кључевима, Енкрипција са јавним кључевима, Дигитално потписивање. <i>Практична настава</i> Решавање задатака из препоручене литературе		
Препоручена литература Jonathan Katz, Yehuda Lindell: <i>Introduction to Modern Cryptography</i> , 3rd Edition, ISBN 9780815354369, Published December, 2020 by Chapman and Hall/CRC, 648 Pages 50 B/W Illustrations		
Број часова наставе	активне Теоријска настава:	Практична настава:
Методе извођења наставе Консултације, семинарски радови, предавања, домаћи задатци, испит		
Оцена знања (максимални број поена 100) Предиспитне обавезе: активност у току предавања 10 поена, семинарски рад или одржани семинар 30 поена, Усмени испит 60 поена		
Начин провере знања могу бити различити : (писмени испити, усмени испт, презентација пројекта, семинари итд.....		
*максимална дужна 1 страница А4 формата		