

Назив предмета: Криптологија II			
Наставник или наставници: Миодраг Михаљевић			
Статус предмета:			
Број ЕСПБ:			
Услов: положен испит Криптологија I			
Циљ предмета Додатна едукација из криптологије у областима криптологије са асиметричним криптографским кључевима (енкрипција са јавним криптографским кључевима) и квантне криптологије.			
Исход предмета Овладавање главним методама и техникама као полазиште за истраживачки рад у области криптологије са асиметричним криптографским кључевима и квантне криптологије			
Садржај предмета <i>Теоријска настава:</i> Системи са јавним кључевима (асиметрични криптографски кључеви): Степеновање, факторисање и дискретни логаритми: Основни алгоритми за дискретно логаритмовање, Алгоритми факторисање и дискретног логаритмовања применом псеудослучајног пута, Факторисање и дискретно логаритмовање у субекспоненцијалном времену; Решетке и алгоритми за решавање проблема најближег и најкраћег вектора; Криптографске технике на бази дискретног логаритмовања: Diffie–Hellman проблем и криптографске примене, Дигитални потписи засновани на дискретном логаритмовању, Енкрипција са јавним кључевима заснована на дискретном логаритмовању; Криптографске технике на бази интицеске факторизације: RSA и Rabin криптосистеми; Системи са јавним кључевима на бази елиптичких и хиперелиптичких кривих. Квантна криптографија: Елементи квантне теорије информација, Квантна дистрибуција кључева, Квантна конференцијска дистрибуција кључева, Примене квантне криптографије изван квантне дистрибуције кључева, Квантни секвенцијални шифарски системи. <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, Chapman and Hall/CRC, Dec. 2020. Steven D. Galbraith: <i>Mathematics of Public Key Cryptography</i> , Online ISBN: 9781139012843 DOI: https://doi.org/10.1017/CBO9781139012843 , Cambridge University Press, 2012. Federico Grasselli: <i>Quantum Cryptography</i> , ISBN: 978-3-030-64359-1, Springer, 2021.			
Број часова наставе	активне	Теоријска настава:	Практична настава:
Методe 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			