

<b>Име на предметот</b>	<b>Криптоанализа</b>		
<b>Наставник</b>	Проф. д-р Смиле Марковски ас. м-р Весна Димитрова		
<b>Статус</b>	Изборен	<b>Кредити</b>	8
<b>Семестар</b>	9 или 10	<b>Неделен фонд</b>	2+2
<b>Условеност</b>			
<b>Начин на реализација</b>	Предавања, вежби, домашни задачи, семинарски		
<b>Цели</b>	Изучување на основните алатки за криптоанализа		
<b>Содржини</b>	Видови на напади со груба сила, статистички напади, диференцијална и линеарна криптоанализа, претставувања на крипто системи како булови функции и испитувања на својствата за линеарност, специјални видови напади за посебни крипто продукти (хаш функции, блок шифривуаци, со јавни клучеви, протоколи)		
<b>Основна литература</b>	<ol style="list-style-type: none"> <li>1) N. Smart: Introduction to cryptography, McGraw-Hill 2003</li> <li>2) S. Vaudenay: A classical introduction to cryptography – Applications for communications security, Springer, 2006</li> </ol>		