Име на предметот	**Криптоанализа**		
Наставник	Проф. д-р Смиле Марковски ас. м-р Весна Димитрова		
Статус	Изборен	**Кредити**	8
Семестар	9 или 10	**Неделен фонд**	2+2
Условеност			
Начин на реализација	Предавања, вежби, домашни задачи, семинарски		
Цели	Изучување на основните алатки за криптоанализа		
Содржини	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 клуцеви, протоколи)		
Основна литература	1) N. Smart: Introduction to cryptography, McGraw-Hill 2003 2) S. Vaudenay: A classical introduction to cryptography – Applications for comunications security, Springer, 2006		