

<b>Име на предметот</b>	<b>Безбедност и криптографија</b>	<b>Шифра</b>	<b>IBK420L4</b>
<b>Наставник</b>	Проф. Д-р Смиле Марковски		
<b>Статус</b>	Изборен	<b>Кредити</b>	<b>6</b>
<b>Препорачан Семестар</b>	Летен (VII)	<b>Неделен фонд</b>	2+1+2
<b>Цели</b>	Запознавање со основните криптографски принципи и методи; изучување на основните крипто-дизајни; практично користење на изучените крипто системи.		
<b>Содржина</b>	Потреба од безбедност на компјутерските системи, криптографија, криптологија; Историски примери; Симетрични крипто-системи; Крипто-системи со јавен клуч; Распределба на размена на клучеви; Хаш функции и генератори на случајни броеви; Дигитални потписи; Автентикација; Безбедносни протоколи; Несигурност на софтвер; Несигурност на оперативни системи; Безбедност на мрежи.		
<b>Условеност</b>	Дискретни структури 3		
<b>Литература</b>	<ol style="list-style-type: none"> <li>1. Nigel Smart: "Cryptography: An introduction", McGraw-Hill, 2003</li> <li>2. Mark Stamp: "Information security – principles and practice", John Willey and Sons, 2006</li> </ol>		
<b>Проверка на знаења и оценување</b>			
<b>Континуирана проверка</b>		<b>Комплетен испит</b>	
1. Колоквиуми	2	1. Писмен испит	
Писмено	не	Задачи	да
Усмено	не	Теорија	да
Задачи	Да	2. Практичен (лаб)	
Теорија	Да	3. Е-тест	не
Практичен (лаб)	Да	4. Усен испит	да
Е-тест	Не	5. Проект	да
2. Тестови	Да	<b>Забелешка:</b> Студентот ги задржува поените од писмените испити и домашните задачи добиени во текот на семестарот. Писмениот испит за делот за задачи се полага во лабораторија. Услов за добивање на задачите е студентот да ја открие шифрата што ќе му биде доделена.	
3. проекти	Да		
4. Активност и/или редовност	да		
5. Завршен испит	Да		
Е-тест			
<b>Услов за потпис и право на испит:</b> Решени сите задачи дадени за домашно во предвидените рокови			