1.	Course title	**Computer security**		
2.	Course code	KK-Z-04		
3.	Study program	**Coding and Cryptography**		
4.	Unit offering the course	**FCSE**		
5.	Undergraduate/master/PhD	**Master**		
6.	Year/semester 1(2)/summer/compulsory	7. ECTS: **6**		
8.	Teacher(s)	Ass. Prof. Boro Jakimovski, Prof. Danilo Gligoroski		
9.	Course prerequisites	None		
10.	Goals (competences): Detailed and practical overview of current network and Internet security applications, protocols and standards. Concrete application of different cryptographycal primitives, covering algorithms and protocols that are base of network security applications such as: encryption, digital signature and key agreement. Upon completion of this course, students will be able to identify all security threats and corresponding techniques for their mitigation and removal. Students will know all details for every security protocol, and decisions that are made during its design, through which he will be able to detect possible problems and security threats.			
11.	Course content: - Security threats, services and mechanisms - Models for internet security - Internet security standards - Protocols for authentication and authorization - Email security - Transport level security - Web security - Network security management			
12.	Teaching methods: Lectures supported by slide presentations, interactive lectures, trainings (using lab equipment and software packages), team work, case studies, invited guests and lectures, individual practical assignments presentations, seminar paper, e-learning (forums, consultations).			
13.	Total available time	6 ECTS x 30 hours = 180 hours		
14.	Distribution of the available time	45 + 30 + 105 = 180 hours		
15.	Teaching activities	15.1.	Lectures	45 hours
		15.2.	Training (labs, problem solving), seminar and team work	30 hours
16.	Other activities	16.1.	Project work	60 hours
		16.2.	Self study	0 hours
		16.3.	Home work	45 hours
17.	Grading			
	17.1. Tests			40 points

	17.2.	Seminar work/project (written or oral presentation)		40 points
	17.3.	Active participation		20 points
18.	Grading criteria		to 50 points	5 (five) (F)
			from 51 to 60 points	6 (six) (E)
			from 61 to 70 points	7 (seven) (D)
			from 71 to 80 points	8 (eight) (C)
			from 81 to 90 points	9 (nine) (B)
			from 91 to 100 points	10 (ten) (A)
19.	Final exam prerequisites		Successfully completed activities 15.1 and 15.2	
20.	Course language		Macedonian and English	
21.	Quality assurance methods		Internal evaluation and student questionnaires	

22. Literature

22.1. Compulsory

No.	Authors	Title	Publisher	Year
1.	William Stallings	Network Security Essentials: Applications and Standards (4th ed.)	Prentice Hall	2010
2.	Gordon Fyodor Lyon	Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning	Nmap Project	2009
3.	Patrick Engebretson	The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy	Syngress	2011

22.2. Additional

No.	Authors	Title	Publisher	Year
1.	Chris Sanders	Practical Packet Analysis: Using Wireshark to Solve Real-World Network Problems	No Starch Press	2011
2.	Eric Cole	Network Security Bible	Wiley	2009
3.	Stuart McClure	Hacking Exposed: Network Security Secrets and Solutions	McGraw-Hill Osborne Media	2009