Computer Security	Code & No:	CS 442
	Credits:	3 (3,0,1)
	Pre-requisite:	IT 341
	Co-requisite:	None
	Level:	9

Course Description:

This course will cover computer security including cryptography, network security, application security, and web security. Traditional topics such as buffer overflows, intrusion detection, packet analysis, and malware will be discussed. Topics also include privacy, incident handling, forensics and anti-forensics, legal issues, politics, and security in emerging technologies.

- Basic cryptography
- Authentication
- Secure network protocols (Kerberos, SSL)
- Program security
- Bug exploits
- Malicious code: viruses, worms, Trojan horses, and more
- Attacks and defenses on computer systems
- Firewalls
- Intrusion detection
- Counter measures
- Trusted operating systems
- Societal issues in computer security: legal, ethical, governmental

Course Aims:

1. Learning the different threats on computer systems.
2. Learning different approaches for protecting computer resources.
3. Acquiring the ability to construct and implement security policy.
4. Presenting developments in Information and computer security.

Student Outcomes (SOs):

☐(a) An ability to apply knowledge of computing and mathematics appropriate to the program's student outcomes and to the discipline

☒(b) An ability to analyze a problem, and identify and define the computing requirements appropriate to its solution

☐(c) An ability to design, implement, and evaluate a computer-based system, process, component, or program to meet desired needs

☐(d) An ability to function effectively on teams to accomplish a common goal

☒(e) An understanding of professional, ethical, legal, security and social issues and responsibilities

☐(f) An ability to communicate effectively with a range of audiences

☒(g) An ability to analyze the local and global impact of computing on individuals, organizations, and society

☐(h) Recognition of the need for and an ability to engage in continuing professional development

☐(i) An ability to use current techniques, skills, and tools necessary for computing practice.

☒(j) An ability to apply mathematical foundations, algorithmic principles, and computer science theory in the modeling and design of computer-based systems in a way that demonstrates comprehension of the tradeoffs involved in design choices. [CS]

☐(k) An ability to apply design and development principles in the construction of software systems of varying complexity. [CS]

☐(j) An ability to use and apply current technical concepts and practices in the core information technologies of human computer interaction, information management, programming, networking, and web systems and technologies. [IT]

☐(k) An ability to identify and analyze user needs and take them into account in the selection, creation, evaluation, and administration of computer-based systems. [IT]

☐(l) An ability to effectively integrate IT-based solutions into the user environment. [IT]

☐(m) An understanding of best practices and standards and their application. [IT]

☐(n) An ability to assist in the creation of an effective project plan. [IT]

Course Learning Outcomes (CLOs):

1. Understand the concept of public-key cryptography and infrastructure.
2. Understand and implement the techniques used for ensuring data integrity.
3. Learn the current state of the art techniques that are employed for defeating secure systems.
4. Get experience in secure system design and analysis.
5. Become familiar with the current technical, economical and ethical issues that concern computing professionals with respect to security.

SOs and CLOs Mapping:

CLO/SO	a	b	c	d	e	f	g	h	i	j	k	l	m	n
CLO1		√								√				

CLO2		√								√				
CLO3														
CLO4														
CLO5					√									
CLO6		√												
CLO7		√												

No.	Topics	Weeks	Teaching hours
1	Cryptography Introduction	1	3
2	Classical Encryption Techniques	2	6
	Block Ciphers and the Data Encryption Standard, Block Cipher Operation		
	Basic Concepts in Number Theory and Finite Fields		
3	Principles of Public-Key Cryptosystems, RSA Algorithm Diffie-Hellman Key Exchange Elliptic Curve Cryptography	2	6
4	Applications of Cryptographic Hash Functions, Secure Hash Algorithm (SHA)	3	9
	Message Authentication Codes, MACs Based on Hash Functions: HMAC		
	Digital Signatures Digital Signature Standard (DSS)		
	Key Management and Distribution X.509 Certificates		
5	Secure network protocols (Kerberos, SSL) Remote User Authentication Kerberos Web Security Issues Secure Sockets Layer (SSL) Transport Layer Security (TLS) HTTPS Secure Shell (SSH)	2	6
6	Electronic Mail Security Pretty Good Privacy (PGP)	2	6
	IP Security		
7	SYSTEM SECURITY	2	6

		Malicious code: viruses, worms, trojan horses, and more(Malicious Software		
		Attacks and defenses on computer systems		
		Intrusion detection, Counter measures & Trusted operating systems		
		Societal issues in computer security: legal, ethical, governmental (Legal and Ethical Issues)		
		Total	14	42

Textbook:

- Cryptography and Network Security: Principles and Practice (6th Edition), William Stallings, Prentice Hall, 2013 .

Essential references:

- Computer Security 3rd Edition Dieter Gollmann, Wiley; 3 edition (February 28, 2011), ISBN-10: 0470741155 and ISBN-13: 978-0470741153
- Security in Computing, 5th Edition, C. P. Pfleeger and S.L. P fleeger, Prentice Hall ,2015, ISBN-10: 0134085043, ISBN-13: 978-0134085043