Cryptography	Code & No:	CS 443
	Credits:	3 (3,0,1)
	Pre-requisite:	IT 341
	Co-requisite:	None
	Level:	9 or 10

Course Description:

The aim of this course is to facilitate understanding of the inherent strengths and limitations of cryptography, especially when used as a tool for information security. Armed with this knowledge, one should be able to make more informed decisions when building secure systems.

The course covers various aspects of symmetric and asymmetric cryptography. While some topics will be dealt with in more detail, the course will attempt to provide a broad coverage of possibly all the core areas of cryptography. The students will be expected to implement and analyze some simple cryptographic schemes and read various articles. To understand the principles of encryption algorithms; conventional and public key cryptography. To have a detailed knowledge about authentication, hash functions and application level security mechanisms.

Course Aims:

1) To discuss an introduction to information Security and Cryptographic protocols
2) To know the methods of conventional encryption.
3) To understand the concepts of public key encryption and number theory
4) To understand authentication and Hash functions.
5) To understand the system level security used

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. To discuss an introduction to information Security and Cryptographic protocols
2. To know the methods of conventional encryption.
3. To understand the concepts of public key encryption and number theory
4. To understand authentication and Hash functions.
5. To understand the system level security used

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					√				√	√				

No.	Topics	Weeks	Teaching hours
1	Introduction to OSI security Architecture	1	3
2	Classical Encryption Techniques	1	3
3	Block ciphers and data encryption model	1	3
4	Basic concepts in number theory and finite fields	2	6
5	Number Theory	1	3
6	Advanced Encryption Standard	1	3
7	Public-key cryptography and RSA	1	3
8	Other public-key cryptosystem	1	3
9	Cryptographic hash functions	1	3
10	Message authentication code, digital signatures	1	3
11	User authentication	1	3
12	Transport level security, IP security	2	6
	Total	**14**	**42**

Textbook:

- Cryptography And Network Security – Principles and Practices, William Stallings Prentice Hall,6th Edition, 2013.

Essential references:

- Network Security, Private Communication in a PublicWorld, by C. Kaufman, Radia Perlman, Mike Speciner. Second edition, Prentice Hall 2002
- Applied Cryptography, Bruce Schenier, John Wiley & Sons inc., 1996.