CE348: INFORMATION SECURITY

Credits and Hours:

Teaching Scheme	Theory	Practical	Tutorial	Total	Credit
Hours/week	4	2	-	6	**5**
Marks	100	50	-	150	

Pre-requisite courses:

- N/A

Outline of the Course:

Sr. No.	Title of the unit	Minimum number of hours
1.	Introduction	02
2.	Traditional Symmetric-Key Ciphers	05
3.	Introduction to Modern Symmetric-Key Ciphers	04
4.	Data Encryption Standard (DES)	04
5.	Advanced Encryption Standard (AES)	04
6.	Encipherment Using Modern Symmetric-Key Ciphers	04
7.	Asymmetric-Key Cryptography	05
8.	Message Integrity and Message Authentication	04
9.	Cryptographic Hash Functions	04
10.	Digital Signature	04
11.	Entity Authentication	04
12.	Key Management	04
13.	Security at the Application Layer: PGP and S/MIME	04
14.	Security at the Transport Layer: SSL and TLS	04
15.	Security at the Network Layer: IPSec	04
	Total hours (Theory) :	60
	Total hours (Lab) :	30
	Total hours :	90

Detailed Syllabus:

1.	**Introduction**	**02 Hours**	**06%**
	Security Goals, Attacks, Services and Mechanism and Techniques.		
2.	**Traditional Symmetric-Key Ciphers**	**05 Hours**	**10%**
	Introduction, Substitution Cipher, Transposition Cipher, Stream and Block Cipher		
3.	**Introduction to Modern Symmetric-Key Ciphers**	**04 Hours**	**06%**
	Modern Block Cipher, Modern Stream Cipher		
4.	**Data Encryption Standard (DES)**	**04 Hours**	**05%**
	Introduction, DES structure and Analysis, Multiple DES		
5.	**Advanced Encryption Standard (AES)**	**04 Hours**	**05%**
	Introduction, AES structure and Analysis		
6.	**Encipherment Using Modern Symmetric-Key Ciphers**	**04 Hours**	**06%**
	Use of Modern Block Ciphers, Use of Modern Stream Ciphers		
7.	**Asymmetric-Key Cryptography**	**05 Hours**	**10%**
	Introduction, RSA Cryptosystem, RABIN Cryptosystem, ELGAMAL Cryptosystem		
8.	**Message Integrity and Message Authentication**	**04 Hours**	**08%**
	Message Integrity, Message Authentication		
9.	**Cryptographic Hash Functions**	**04 Hours**	**08%**
	Introduction, SHA-512,MD5		
10.	**Digital Signature**	**04 Hours**	**06%**
	Services,RSA Digital Signature Scheme,ELGamal Digital Signature Scheme		
11.	**Entity Authentication**	**04 Hours**	**04%**
	Passwords, Challenge –Response,Zero –Knowledge		
12.	**Key Management**	**04 Hours**	**08%**

	Symmetric-Key Distribution,KERBEROS		
13.	**Security at the Application Layer: PGP and S/MIME**	**04 Hours**	**06%**
	E-Mail, PGP,S/MIME		
14.	**Security at the Transport Layer: SSL and TLS**	**04 Hours**	**06%**
	SSL Architecture,TLS cipher suite		
15.	**Security at the Network Layer: IPSec**	**04 Hours**	**06%**
	Introduction to IPSec		

Course Outcome (COs):

At the end of the course, the students will be able to

CO1	Define various security goal and understand the security policies such as the CIA triad of Confidentiality, Integrity and Availability.
CO2	Classify various forms of security attacks, where they arise, and appropriate tools or mechanism to quantify them.
CO3	Illustrate a basic understanding of cryptography, how it has evolved, and evaluate symmetric key encryption techniques used today.
CO4	Distinguish modern symmetric encryption standard, key distribution scenario and analyse effectiveness in todays’ environment.
CO5	Evaluate Asymmetric key encryption techniques, key distribution scenario and calculate public and private components of asymmetric key encryption techniques.
CO6	Develop message integrity and message authentication of message digest.

Course Articulation Matrix:

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2
CO1	1	2	-	-	3	1	-	2	1	-	-	-	-	-
CO2	2	3	3	2	3	1	-	-	-	-	-	-	1	-

CO3	2	2	3	2	3	2	-	-	2	1	-	-	2	-
CO4	2	2	3	2	3	-	2	-	2	1	-	-	3	1
CO5	3	2	3	2	1	-	2	1	1	-	-	-	3	1
CO6	2	2	3	1	-	-	2	2	1	-	2	-	2	2

Enter correlation levels 1, 2 or 3 as defined below:

1: Slight (Low) 2: Moderate (Medium) 3: Substantial (High)

If there is no correlation, put "-"

Recommended Study Material:

❖ **Text book:**

1. Cryptography and Network Security, Behrouz A. Forouzan, McGraw-Hill Companies.

❖ **Reference book:**

1. Cryptography And Network Principles And Practice, William Stallings, Prentice Hall, Pearson Education Asia.
2. Cryptography & Network Security, Atul Kahate, The McGraw-Hill Companies.
3. The DevOps Handbook: How to Create World-Class Agility, Reliability, and Security in Technology Organizations by Gene Kim, Jez Humble, Patrick Debois, and John Willis

❖ **Web material:**

1. http://people.csail.mit.edu/rivest/crypto-security.html.
2. http://www.cryptix.org/
3. http://www.cryptocd.org/
4. http://www.cryptopp.com/
5. http://www.freetechbooks.com/information-security-f52.html

❖ **Software:**

1. Nmap
2. Wireshark