UE18CS314 : Applied Cryptography 4:0:0:0:4

# of Credits: 4 **# of Hours: 56**

Class #	Chapter Title / Reference Literature	Topics to be Covered	% of Portion covered	
			% of syllabus	Cumulative %
1	**Unit#1 Classical Ciphers (Chapter 1,2)**	Introduction to cryptography, cryptanalysis, and cryptology		
2		Overview of cryptography		
3		Basic Cryptographic primitives		
4		Classical ciphers: substitution cipher – Caesar, Playfair and Hill cipher	**21.43**	**21.43**
5		Transposition cipher – Rail fence, Columnar and Double columnar		
6		Cryptanalysis of classical ciphers		
7		Introduction to probability, Conditional probability, Law of Total probability		
8		Shannon's theorem		
9		One-time-pad encryption		
10		Limitations of One-Time-Pad		
11		**Lab1**		
12				
13	**Unit#2**	Introduction to symmetric key cryptography		
14	**Symmetric Key Cryptography (chapter- 3,6)**	Pseudo Random Numbers		
15		Feistel Cipher		
16		S-box and E-box		
17		Initial and Final permutations		
18		Data Encryption Standard (DES)	**21.41**	**42.84**
19		Cryptanalysis and avalanche effect		
20		Advanced Encryption Standard (AES)		
21		AES key scheduling		
22		Block and Stream ciphers		
23		**Lab2**		
24				

25	**Unit #3** **Public Key Cryptography (chapter-8,11)**	Introduction to Public key cryptography	**21.43**	**64.27**
26		Modes of operation		
27		Prime number, Primitive root		
28		Modular arithmetic		
29		Polynomials		
30		Diffie Hellman Protocol		
31		Elgamal crypto systems		
32		Prime Factorization		
33		Rivest–Shamir–Adleman cryptosystem (RSA)		
34		Applications.		
35		**Lab3**		
36				
37	**Unit#4** **Key management Hashing Techniques** **(chapter 10,6,7)**	Key management and distribution (KDC)	**17.85**	**82.12**
38				
39		Birthday attack		
40		Zero knowledge protocols		
41		MD5, One-way function, Collision resistant hash function (CRHF)		
42				
43		Secure Hash Algorithm (SHA), Applications		
44				
45		**Lab4**		
46				
47	**Unit #5** **Authentication using Cryptography** **Chapter-4,12,8.3**	Identification protocols	**17.88**	**100**
48		Digital Signature (DS)		
49		Elliptic Curve cryptography-based signature (ECDSA)		
50		RSA based signature		
51		Message Authentication Code (MAC)		
52		Cipher Block Chain MAC (CBC MAC)		
53		Different areas where cryptography needs to be applied		
54				
55		**Lab5**		
56				

Lab:

Lab 1	**Pseudo Random Number Generation.**
Lab 2	**Secret-Key Encryption.**
Lab 3	**RSA Encryption and Signature.**

Lab 4	**Hash Length Extension Attack.**
Lab 5	**MD5 Collision Attack.**

Literature

Book Type	Code	Title & Author	Publication Information		
			Edition	Publisher	Year
Textbook	T1	"Introduction to Modern Cryptography", Jonathan Katz, Yehuda Lindell	2	CRC Press	2015