Syllabus Break up : Information System Security(7CS2)

Class: VII Sem.CSE

Faculty Name:-Gagandeep Kaur

Lecture No.	Topic	Month in which the topic will be covered	Actual date of covering	Reason for not covering the topic in due time	E-contents provided
	Unit 1				
1	Introduction to security attacks, services and mechanism	July-2015	20/07/2015	-	tutorialpoint.com
2	Classical Encryption techniques- substitution ciphers and transposition Ciphers	July-2015	21/07/2015	-	tutorialpoint.com
3	Cryptanalysis,Stream and block ciphers	July-2015	22/07/2015	-	tutorialpoint.com
4	Modern Block Ciphers: Block ciphers principals	July-2015	27/07/2015	-	tutorialpoint.com
5	Shannon's theory of confusion and diffusion,	July-2015	28/07/2015	-	tutorialpoint.com
6	Fiestal structure,Data Encryption Standard(DES)	July-2015	29/07/2015	-	tutorialpoint.com
7	Differential and linear cryptanalysis of DES	August-2015	03/08/2015	-	tutorialpoint.com
8	Block cipher modes of operations	August-2015	04/08/2015	-	tutorialpoint.com
9	Triple DES	August-2015	05/08/2015	-	tutorialpoint.com
	Unit II				
10	AES	August-2015	10/08/2015	-	NPTEL.ac.in
11	RC6	August-2015	11/08/2015	-	NPTEL.ac.in
12	Random number generation.	August-2015	12/08/2015	-	NPTEL.ac.in

13	S-box theory: Boolean Function	August-2015	17/08/2015	-	NPTEL.ac.in
14	S-box design criteria,Bent functions	August-2015	18/08/2015	-	NPTEL.ac.in
15	Propagation and nonlinearity	August-2015	19/08/2015	-	NPTEL.ac.in
16	Construction of balanced functions, S-box design.	August-2015	24/08/2015	-	NPTEL.ac.in
	Unit III				
17	Public Key Cryptosystems: Principles of Public Key Cryptosystems	August-2015	25/08/2015	-	tutorialpoint.com
18	RSA Algorithm, security analysis of RSA	August-2015	26/08/2015	-	tutorialpoint.com
19	Exponentiation in Modular Arithmetic	September-2015	02/09/2015	-	tutorialpoint.com
20	Key Management in Public Key Cryptosystems: Distribution of Public Keys	September-2015	07/09/2015	-	tutorialpoint.com
21	Distribution of Secret keys using Public Key Cryptosystems. X.509	September-2015	08/09/2015	-	tutorialpoint.com
22	Discrete Logarithms,Diffie-Hellman Key Exchange	September-2015	14/09/2015	-	tutorialpoint.com
	Unit IV				
23	Message Authentication and Hash Function: Authentication Requirements	September-2015	15/09/2015	-	NPTEL.ac.in
24	Authentication functions	September-2015	16/09/2015	-	NPTEL.ac.in
25	Message authentication code,Hash functions	September-2015	21/09/2015	-	NPTEL.ac.in
26	Birthday attacks,	September-2015	22/09/2015	-	NPTEL.ac.in
27	Security of hash functions and MAC	September-2015	28/09/2015	-	NPTEL.ac.in
28	MD5 message digest algorithm	September-2015	29/09/2015	-	NPTEL.ac.in
29	Secure hash algorithm(SHA)	September-2015	30/09/2015	-	NPTEL.ac.in

30	Digital Signatures: Digital Signatures	October-2015	05/10/2015	Strike	NPTEL.ac.in
31	Authentication protocols	October-2015	06/10/2015	-	NPTEL.ac.in
32	Digital signature standards (DSS),	October-2015	07/10/2015	-	NPTEL.ac.in
33	Proof of digital signature algorithm	October-2015	12/10/2015	-	NPTEL.ac.in
34	Remote user Authentication using symmetric and Asymmetric Authentication	October-2015	14/10/2015	-	NPTEL.ac.in
	Unit V				
35	Pretty Good Privacy	October-2015	19/10/2015	-	NPTEL.ac.in
36	IP Security: Overview, IP Security Architecture	October-2015	20/10/2015	-	NPTEL.ac.in
37	Authentication Header	October-2015	26/10/2015	-	NPTEL.ac.in
38	Encapsulation Security Payload in Transport and Tunnel mode with multiple security associations	October-2015	27/10/2015	-	NPTEL.ac.in
39	Strong Password Protocols: Lamport's Hash	October-2015	28/10/2015	Strike	NPTEL.ac.in
40	Encrypted Key Exchange.	November-2015	09/11/2015	-	NPTEL.ac.in