Lesson Plan

Name of Faculty : **Er. Arushi Bansal, Guest Faculty of CSE**
Discipline : **Computer Science and Engineering**
Semester : **5th (odd)**
Subject : **Cryptography and network security (PCC-CSE304-T)**

Week	**Theory**		**Topic Covered Date and Remarks**		
	Lecture Day	**Topic (Including Assignment/Test)**	**Date**	**HOD**	**Director-Principal**
1st	1	Overview of classical cryptosystem			
	2	Stream and block cipher			
	3	Cipher and cipher modes, Substitution cipher: monoalphabetic and polyalphabetic			
2nd	4	Transposition cipher: rail fence, scytale			
	5	Book cipher, vernam cipher			
	6	Vignere tabluae, hill cipher, Cryptanalysis of classical cryptosystem			
3rd	7	Revision of unit 1			
	8	Private/symmetric key cryptography:DES			
	9	AES, Feistel networks, modes of operation			
4th	10	RSA			
	11	Elliptic curve cryptography			
	12	Diffie hellman key exchange, Digital signature, knapsack algorithm			
5th	13	Public key infrastructure, Kerberos, secret sharing scheme			
	14	Digital certificates, X.509 certificates			
	15	Revision of unit 3			
6th	16	Attacks: types			
	17	Detection, mitigation			
	18	Network security foundations, Defence models			
7th	19	Access control: authentication and authorization			
	20	Network architecture, Network device security, wireless security			
	21	Firewalls, IDS			
8th	22	Email , PGP			
	23	PEM, S-MIME, Proxy servers			
	24	SSl, TLS, SET			
9th	25	SHTTP, IPSec			
	26	Virual private network security			
	27	Elementary number theory			
10th	28	Finite fields			
	29	Groups and subgroups			
	30	Matrix representation, Symmetric matrix and diagnolazation			
11th	31	Number theory: divisibility			
	32	Gcd, prime number, primality testing, Congruence			
	33	Chinese remainder theorem			
12th	34	Fermat theorem			
	35	Eulers theorem			
	36	Modular arithmetic and its properties, Modular exponential			
13th	37	Revision of unit 2			
	38	Revision of unit 3			
	39	Revision of unit 4			