NATIONAL INSTITUTE OF TECHNOLOGY
JAMSHEDPUR, JHARKHAND- 831014

Department of Computer Science & Engineering

SPRING SEMESTER 2019-2020

Course Handout

Date: 03-01-2020

Course No.	**:**	**CS4204**
Course Title	**:**	**Cryptography and Network Security**
Instructor-In-charge	**:**	**SANJAY KUMAR**

Course Description

Introduction: Basic objectives of cryptography, secret-key and public-key cryptography, one-way and trapdoor one-way functions, cryptanalysis, attack models, classical cryptography.

Block ciphers: Modes of operation, DES and its variants, RCS, IDEA, SAFER, FEAL, BlowFish, AES, linear and differential cryptanalysis.

Stream ciphers: Stream ciphers based on linear feedback shift registers, SEAL, unconditional security.
Message digest: Properties of hash functions, MD2, MD5 and SHA-1, keyed hash functions, attacks on hash functions.

Public-key parameters: Modular arithmetic, gcd, primality testing, Chinese remainder theorem, modular square roots, finite fields.

Intractable problems: Integer factorization problem, RSA problem, modular square root problem, discrete logarithm problem, Diffie-Hellman problem, known algorithms for solving the intractable problems.

Public-key encryption: RSA, Rabin and EIGamal schemes, side channel attacks. Key exchange: Diffie-Hellman and MQV.

Digital signatures: RSA, DSA and NR signature schemes, blind and undeniable signatures.

Entity authentication: Passwords, challenge-response algorithms, zero-knowledge protocols. Standards: IEEE, RSA and ISO standards.

Security issues: Terminology (Integrity, Availability, Confidentiality, Non-repudiation, Authentication, Authorization/Access Control, accounting, auditing, Passive and Active Attacker, Interruption, Interception, Modification, Fabrication, Social Engineering), Vulnerabilities and Counter Measures

(Viruses, worms, Trojan horses, backdoors, unused services, buffer overflows, RPC), Exploits (Buffer overflow, Port Scanning etc).

Network security: Certification, public-key infra-structure (PKI), secure socket layer (SSL), Kerberos, PGP, S/MIME, SSH, SET, IPsec, Kerberos, Firewalls, VPN etc, Secure (commerce) Transaction over a network, Network Anonymity.

Advanced topics: Elliptic and hyper-elliptic curve cryptography, number field sieve, lattices and their applications in cryptography, hidden monomial cryptosystems, cryptographically secure random number generators, Recent trends in cryptography.

Case studies: Installing Unix and common service daemons (Unix Security, Windows NT Security, Ping, traceroute, TCP Dump, sniffer etc.).

Text Books:

1. Behrouz A. Forouzan and D. Mukhopadhyay Cryptography and Network Security, Mc Graw Hill

2. Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone, Handbook of Applied Cryptography, CRC Press.

3. William Stallings, Cryptography and Network Security: Principles and Practice, Prentice Hall of India.

Reference Books:

1. Neal Koblitz, A course in number theory and cryptography, Springer.

2. Johannes A. Buchmann, Introduction to Cryptography, Undergraduate Text in Mathematics, Springer.
3. B. Schneier, Applied Cryptography, 2nd Ed, John Wiley & Sons, Inc., 1996.

4. C. Kauffman, R. Perham and M. Speciner, Network Security: Private Communication in a Public World, Prentice-Hall, 1994.

5. H. C. A. van Tilborg, Fundamentals of Cryptology, Kluwer Academic Publishers, 2000.

6. P. Garrett, Making and Breaking Codes: An Introduction to Cryptology, Prentice-Hall, 2001.

7. W. Cheswick, S. Bellovin and A. Rubin, Firewalls and Internet Security. Repellingthe Hacker, 2ndEd. Addison–Wesley, 2003.

Course Plan

Lecture No.	Topics to be covered	Refer to Chapter of (Text Book 1)
1	Introduction	Chap 1 (pg 1-13)
2-6	Symmetric- key cryptography: Substitution, Transpostion, Stream and Block ciphers	Chap 2, chap 4 and chap 5
7-8	DES, AES	Chap 6and 7
9-12	Asymmetric key cryptography: RSA, Rabin, EIGama,Elliptic curve cryptosystem	Chap 10
13-15	Message Integrity and message authentication	Chap 11
16-19	Cryptographic Hash functions: Description of MD hash family, whirlpool, SHA-512	Chap 12
20-22	Digital Signature	Chap 13
23-25	Entity authentication	Chap 14
26-28	Key management: kerberose, symmetric key distribution and agreement, public key distribution, hijacking	Chap 15
29-32	Network security: security at application layer (PGP and S/ MIME), security at transport layer (SSL and TLS), security at network layer (IPSec)	Chap 16,17and 18
33-37	System security	Chap 19
38-40	Advance Topics	Notes provided
41-44	Case Studies	

Evaluation Scheme

S.No.	Evaluation Component	Duration	Weightage	Date & Time	Nature of Component
1	Mid Term examination	2 Hrs.	30%		Closed Book
2	End Sem examination	3 Hrs.	50%		Closed Book
3	Assignment/Seminar/ Tutorial/Project		20%		Take Home/Lab

Chamber consultation hour: Monday [from (5-6 PM)]

Notices: *All notices regarding the course will be displayed only on the department of Computer Science & Engineering notice board.*

Instructor -In -charge