Course: Cryptography and Network Security

Course Code: noc21-cs16

Session: 2020-21

Duration: 12 Weeks

Assessment procedures: Weekly Assignment (25%) + proctored certification Exam (75%)

Curriculum of the Course:

Week 1:

- Introduction to cryptography
- Classical Cryptosystem
- Block Cipher.

Week 2:

- Data Encryption Standard (DES)
- Triple DES, Modes of Operation
- Stream Cipher. Free and Forced Response

Week 3 :

- LFSR based Stream Cipher
- Mathematical background
- Abstract algebra
- Number Theory

Week 4 :

- Modular Inverse
- Extended Euclid Algorithm
- Fermats Little Theorem
- Euler Phi-Function
- Eulers theorem.

Week 5 :

- Advanced Encryption Standard (AES)
- Introduction to Public Key Cryptosystem
- Diffie-Hellman Key Exchange

Week 6 :

- Primarily Testing,
- ElGamal Cryptosystem,
- Elliptic Curve over the Reals,

- Elliptic curve Modulo a Prime.

Week 7 :

- Generalized ElGamal Public Key Cryptosystem
- Rabin Cryptosystem

Week 8 :

- Message Authentication
- Digital Signature
- Key Management
- Key Exchange
- Hash Function..

Week9 :

- Cryptographic Hash Function
- Secure Hash Algorithm (SHA)
- Digital Signature Standard (DSS).

Week 10 :

- Cryptanalysis
- Time-Memory Trade-off Attack
- Differential and Linear Cryptanalysis .

Week 11 :

- Cryptanalysis on Stream Cipher
- Modern Stream Ciphers,
- Shamirs secret sharing and BE
- Identity-based Encryption (IBE)

Week 12 :

- Side-channel attack
- The Secure Sockets Layer (SSL)
- Pretty Good Privacy (PGP)
- Introduction to Quantum Cryptography

List of students enrolled

S. No	**Name of Student**
1	VED SHARMA
2	Aryan Saini

3	Ashokjat
4	EKLAVYA JOSHI
5	Kashish Sharma
6	khushi punia
7	Abhinav Mishra
8	Mukul Palol
9	Keshav Pareek
10	Pranav Parashar
11	Prateek Goyal
12	Lakshya Purohit
13	Purvi Harpalani
14	RAHUL KHATIK
15	Rudraksh Agarwal
16	Shubham Udsaria
17	Kashish Sharma
18	Utkarsh Dattatrey
19	Divyansh Sharma