

Chapter/Student Branch Name: CMR Technical Campus

Region: V

Event Date: 22-12-2016

Event Title: Guest Lecture on “**Information and Network Security**”

Speakers: Mr. Raghu, Technical Assistant, Zoom Technologies, Hyderabad

Gist of the Event:

Speaker delivered Concepts on “**Information and Network Security**” and covered following Concepts:

- Overview on Modern Cryptography
- Introduction to Number Theory
- Probability and Information Theory
- Classical Cryptosystems
- Cryptanalysis of Classical Ciphers
- Shannons Theory
- Symmetric Key Ciphers
- Block Cipher Standards (DES, AES)
- Linear Cryptanalysis
- Differential Cryptanalysis
- Overview on S-Box Design Principles
- Cryptographic Hash Functions
- The RSA Cryptosystem
- Discrete Logarithm Problem (DLP)
- The Diffie-Hellman Problem and Security of ElGamal Systems
- Application of Elliptic Curves to Cryptography
- Secret Sharing Schemes
- Firewalls and Intrusion Detection Systems



Guest delivering the lecture to the Students