Syllabus for network Security

Unit 1: Introduction to Network Security

Key security requirements-confidentiality, integrity, availability. Security architecture for OSI. Types of security threats and attacks with examples in different categories. Fundamental security design principles. Attack surfaces and attack trees. Organizations involved in Cryptography standards. Classical encryption techniques

Unit-2: Cryptography

Introduction, overview of Symmetric Cryptography, Cryptanalysis, general structure of DES, working steps of DES algorithm, functionality of DES, overview of AES, AES Structure, Symmetric Cipher, overview of stream ciphers.  Mathematics of Asymmetric Key Cryptography, RSA algorithm, Key management- Diffie-Hellman Key exchange, Man in the middle attack using Diffie-Hellman Key exchange.

Unit-3: Network Security Application

Introduction, approaches to message authentication, SHA, MAC, Digital Signature, Public key distribution, Key Distribution, types of key distribution, public key distribution technique, Digital Certificate, digital signature versus digital certificate introduction to X.509 certificate, X.509 certificate format, X.509 certificate revocation list fields**,** Symmetric key distribution centre (KDC), introduction to Kerberos, steps taken to authenticate in Kerberos, issues on use of asymmetric encryption and distributed symmetric keys. Overview of public-key infrastructure. Understand the need of federated identity management system.

Unit 4: System Security

Introduction, three broad mechanisms malware uses to propagate. Basic operation of viruses, worms and trojans. Four broad categories of malware payloads. Threats posed by bots, spyware and rootkits. Malware counter-measure elements. Malware detection mechanisms. Firewalls.