	L	P	C
I Year I Semester			
Code: 17ES138	**4**	**0**	**3**

CYBER SECURITY
(Elective-II)

UNITI:

Introduction:

Security Attacks (Interruption, Interception, Modification and Fabrication), Security Services (Confidentiality, Authentication, Integrity, Non-repudiation, access Control and Availability) and Mechanisms, A model for Internetwork security, Internet Standards and RFCs, Buffer overflow & format string vulner abilities, TCP session hijacking, ARP attacks, route table modification, UDP hijacking, and man-in-the-middle attacks.

UNIT II:

Conventional Encryption:

Conventional Encryption Principles, Conventional encryption algorithms, cipher block modes of operation, location of encryption devices, key distribution Approaches of Message Authentication, Secure Hash Functions and HMAC

UNIT III:

Number Theory: Prime and Relatively Prime Numbers, Modular Arithmetic, Fermat's and Euler's Theorems, The Chinese Remainder theorem, Discrete Logarithms

Public key: Public key cryptography principles, public key cryptography algorithms, digital signatures, digital Certificates, Certificate Authority and key management Kerberos,X.509 Directory Authentication Service

UNIT IV:

IP Security: IP Security Overview, IP Security Architecture, Authentication Header, Encapsulating Security Payload, Combining Security Associations and Key Management

Transport Level Security: Web Security Requirements, Secure Socket Layer (SSL) and Transport Layer Security (TLS), Secure Electronic Transaction (SET)

Email Privacy: Pretty Good Privacy (PGP) and S/MIME.

UNIT V:

Intrusion Detection: Intruders, Intrusion Detection systems, Password Management.

Malicious Software: Viruses and related threats &Countermeasures.

Firewalls: Firewall Design principles, Trusted Systems.

TEXT BOOKS:

Network Security &Cryptography: Principles and Practices, William Stallings, PEA, Sixth edition.

HackProofingyour Network, Russell, Kaminsky, Forest Puppy, Wiley Dream tech

REFERENCE BOOKS:

Network Security & Cryptography, Bernard Menezes,Cengage,2010