## NETWORK SECURITY AND CRYPTOGRAPHY

| II Semester: **ECE(ES)** | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Course Code** | **Category** | **Hours / Week** | | | **Credits** | **Maximum Marks** | | |
| **BESC20** | Elective | **L** | **T** | **P** | **C** | **CIA** | **SEE** | **Total** |
| | | 3 | 1 | 0 | 4 | 30 | 70 | 100 |
| Contact Classes: 45 | Tutorial Classes: 15 | Practical Classes: Nil | | | Total Classes:60 | | | |

### I. COURSE OVERVIEW:

This course provides a general overview of network security and cryptography. It gives a better understanding of cryptography and its types which are being leveraged to enhance security and privacy online. After completing this course, students will be able to analyze conventional block ciphers as well as public key cryptography.

### II. COURSE OBJECTIVES:

**The students will try to learn:**

I. Fundamental network security concepts and mechanisms.

II. The use of cryptography in achieving network security and understand how to design and build secure systems.

III. A wide variety of basic cryptographic primitives along with recent developments.

### III. COURSEOUTCOMES:

**After successful completion of the course, students should be able to:**

| | | |
|---|---|---|
| CO1 | **Understand** principles and practice of network security and cryptography by gaining knowledge in cryptographic algorithms; | Understand |
| CO2 | **Design** basic security architectures through selection and integration of relevant security components | Apply |
| CO3 | **Make use** of advanced cryptographic algorithms in network protocols and network applications. | Apply |
| CO4 | **Analyze and apply system security concept to recognize malicious code** | Analyze |
| CO5 | **Understand** Key management using smart cards for authentication requires the use of a PKI. | Understand |
| CO6 | **Illustrate** various Public key cryptographic techniques in encryption/ decryption. | Understand |

### IV. SYLLABUS:

**MODULE – I: SECURITY**

Need, security services, Attacks, OSI Security Architecture, one time passwords, Model for Network security, Classical Encryption Techniques like substitution ciphers, Transposition ciphers, Cryptanalysis of Classical Encryption Techniques.

**MODULE – II: NUMBER THEORY**

Number Theory: Introduction, Fermat's and Euler's Theorem, The Chinese Remainder Theorem, Euclidean Algorithm, Extended Euclidean Algorithm and Modular Arithmetic.

**MODULE – III: PRIVATE-KEY (SYMMETRIC) CRYPTOGRAPHY**

Block Ciphers, Stream Ciphers, RC4 Stream cipher, Data Encryption Standard (DES)

Advanced Encryption Standard (AES), Triple DES, RC5, IDEA, Linear and Differential Cryptanalysis.

**MODULE – IV: PUBLIC-KEY (ASYMMETRIC) CRYPTOGRAPHY**
RSA, Key Distribution and Management, Diffie Hellman Key Exchange, Elliptic Curve Cryptography, Message Authentication Code, hash functions, message digest algorithms:MD4MD5,Secure Hash algorithm,RIPEMD-160, HMAC.

**MODULE – V: AUTHENTICATION AND SYSTEM SECURITY:**
IP and Web Security Digital Signatures, Digital Signature Standards, Authentication Protocols, Kerberos, IP security Architecture, Encapsulating Security Payload, Key Management, Web Security Considerations, Secure Socket Layer, Secure Electronic Transaction Intruders, Intrusion Detection, Password Management, Worms, viruses, Trojans, Virus Counter measures, Firewalls, Trusted Systems

## TEXT BOOKS:

1. William Stallings, "Cryptography and Network Security, Principles and Practices", Pearson Education, 3rd Edition, 2007.
2. Charlie Kaufman, Radia Perlman and Mike Speciner, "Network Security, Private Communication in a PublicWorld", Prentice Hall, 2nd Edition, 2009.

## REFERENCE BOOKS:

1. Christopher M.King, Ertem Osmanoglu, Curtis Dalton,"Security Architecture, Design Deployment and Operations", RSA Press, 2nd Edition, 2009.
2. Stephen Northcutt, Leny Zeltser, Scott Winters, Karen Kent and RonaldW.Ritchey, "Inside Network Perimeter Security", Pearson Education, 2nd Edition, 2010.
3. Richard Bejtlich,"The Practice of Network Security Monitoring: Understanding Incident Detection and Response",William Pollock Publisher, 2013.

.

## WEB REFERENCES:

1. https://accessengineeringlibrary.com
2. http://www.radio-electronics.com
3. https://www.jntubook.com
4. http://www.iare.ac.in