|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **NAME OF DEPARTMENT:** | | | | | | | | | | | | | | | | | | | School of Computing | | | | | | | | | | | | | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | | | | | |  | | | | | | | | | | | | | | | | | | | | | | | | | | |
| **Course Name:** | | | | | | | | | Bachelor of Computer Applications (BCA) | | | | | | | | | | | | | | | | | | | | | | | | |  | | | | | | | | |  | | |
|  | | | | | | | | |  | | | | | | | | | | | | | | | | | | | | | | | | |  | | | | | | | | |  | | |
| **Subject Name:** | | | | | | | | | Cryptography | | | | | | | | | | | | | | | | | | | | | | | | | **Subject Code:** | | | | | | | | | TBC 503 | | |
|  | | | | | | | | |  | | | | | | | | | | | | | | | | | | | | | | |  | | | | | | | | |  | | | | |
| **1** | **Contact Hours:** | | | | | | | | | | 48 | | | | |  | | | | | | | | | | | | | | | | | | | **L** | | 3 | | | **T** | | 1 | | **P** | 0 | |
|  |  | | | | | | | | | |  | | | | |  | | | | | | | | | | | | | | | | | | |  | |  | | |  | |  | |  |  | |
| **2** | **Examination Duration(Hrs):** | | | | | | | | | | | | | | | | | | | | |  | **Theory** | | | | | 0 | 3 |  | **Practical** | | | | | 0 | | 0 | |  | | | | | |
|  |  | | | | | | | | | | | | | | | | | | | | |  |  | | | | |  |  |  |  | | | | |  | |  | |  | | | | | |
| **3** | **Relative Weightage:** | | | | | | | | | | | | |  | | | | | **CWE:** | | | | | | | 25 | | **MTE:** | | | 25 | | **ETE:** | | | | 50 | | | |  | | | | |
|  |  | | | | | | | | | | | | |  | | | | |  | | | | | |  | | |  | | |  | |  | | | |  | | | |  | | | | |
| **4** | **Credits:** | | | | | | 0 | | | 4 |  | | | | | | | | | | | | | |  | | |  | | |  | |  | | | |  | | | |  | | | | |
|  |  | | | | | |  | | |  |  | | | | | | | | | | | | | |  | | |  | | |  | |  | | | |  | | | |  | | | | |
| **5** | **Semester:** | | | | | | | \* | | |  | | | |  | | |  | | |  | | |  | | | | | | | | | | | | | | | | | | | | | |
|  |  | | | | | **Autumn** | | | | | | **Spring** | | | | | | | | **Both** | | | | | | |  | | | | | | | | | | | | | | | | | | |
|  |  | | | | |  | | | | | |  | | | | | | | |  | | | | | | |  | | | | | | | | | | | | | | | | | | |
| **6** | **Pre-Requisite:** | | | | | | | | | | | | Basics of the Networking | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|  |  | | | | | | | | | | | |  | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| **7** | **Subject Area:** | | | | | | | | | | | | Cryptography and Security | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|  |  | | | | | | | | | | | |  | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| **8** | **Objective:** | | | | | | | | | | | | To familiarize students with the Security algorithms regarding the networking issue | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|  |  | | | | | | | | | | | |  | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| **9** | **Course Outcome:** | | | | | | | | | | | | A student who successfully fulfills the course requirements will be able to- | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|  | **a.** | | | | Identify some of the factors driving the need for security and cryptography. | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|  | **b.** | | | | Identify and classify particular examples of attacks. | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|  | **c.** | | | | Understand the basics of symmetric key cryptography. | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|  | **d.** | | | | Understand the basics of Asymmetric key cryptography. | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|  | **e.** | | | | Understand the concept of Hash functions and their use. | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|  | **f.** | | | | Understand the basics Digital Signatures. | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|  |  | | | |  | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| **10** | | **Details of the Course:** | | | | | | | | | | | | | | |  | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| **Unit No.** | | | | **CONTENT** | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | **CONTACT HOURS** | | | | | | |
| **1** | | | | **Introduction to Cryptography:** Introduction to Cryptography, Security Goals, Cryptographic Attacks. Mathematics of Cryptography: Modular Arithmetic, Congruence and Matrices. Conventional Encryption Model, Symmetric Key Ciphers, Categories of Symmetric Key Ciphers. Stream and Block Ciphers, | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | 8 | | | | | | |
| **2** | | | | Modern Block Ciphers: Components of Modern Block Ciphers, Thoughts of Feistel Design, Block Cipher Principles, Product Ciphers. Simplified DES, DES Structure, DES Standard, DES Strength, Differential & Linear Cryptanalysis, Block Cipher Design Principles, Block Cipher Modes of Operation.  Multiple DES: Double DES, Triples DES. Introduction to AES. | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | 10 | | | | | | |
| **3** | | | | **Advanced Encryption Algorithms:** Blowfish Algorithm, International Data Encryption Algorithm, RC-5, Symmetric Key Distribution, Random Number Generators, Placement of Encryption Function. | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | 10 | | | | | | |
| **4** | | | | **Public Key Encryption:** Difference between Symmetric and Asymmetric key Cryptosystems, Public-Key Cryptography: Principles of Public-Key Cryptosystems, RSA Algorithm, Rabin Cryptosystem, ElGamal Cryptosystem, Key Management, Public Key Distribution, Fermat’s & Euler’s Theorem. | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | 10 | | | | | | |
| **5** | | | | **Hash Functions:** Message Authentication & Hash Functions: Authentication Requirements, Authentication Functions, Message Authentication Codes, Hash Functions, Security Of Hash Function & MACS, MD-5 Message Digest Algorithm, Secure Hash Algorithm (SHA-512), Digital Signatures: Digital Signature Standard, Authentication Protocol, Digital Signature Algorithm (DSA). | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | 10 | | | | | | |
|  | | | | **TOTAL** | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | **48** | | | | | | |
|  | | | |  | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |  | | | | | | |
|  | | | |  | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |  | | | | | | |
| **11** | | **Suggested Books:** | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |  | | | | | | |
| **Sl. NO.** | | | **NAME OF AUTHORS/BOOKS/PUBLISHERS** | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | **YEAR OF PUBLICATION** | | | | | |
| **1** | | | William Stallings, “Cryptography and Network Security: Principles and Practice”, Prentice Hall, New Jersey. | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | 2002 | | | | | |
| **2** | | | Johannes A. Buchmann, “Introduction to cryptography”, Springer- Verlag. | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | 2004 | | | | | |
| **3** | | | Atul Kahate, “Cryptography and Network Security”, TMH | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | 2008 | | | | | |
| **4** | | | Behrouz A Forouzan, “Cryptography and Network Security”, McGraw Hill, 3rd ED. | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | 2016 | | | | | |