**DIT UNIVERSITY, DEHRADUN**

**Semester VII 2017 – 2018**

**Course Handout**

The following is the detailed course handout for the course mentioned below.

**Course No. : DA7210 (3 0 2)**

**Course Title : Cryptography and Network Security**

**Course Faculty : Mr. Anuj Kumar Yadav, Mr. Sandip Mandal, Mr. Chirag Joshi**

**Course Coordinator : Mr. Anuj Kumar Yadav**

**Scope and Objective of the Course:**

The course covers theory and practice of computer security, focusing in particular on the security aspects of the web and Internet. It surveys cryptographic tools used to provide security, such as shared key encryption (DES, 3DES, etc.); public key encryption, key exchange, and digital signature (Diffie-Hellmann, RSA, DSS, etc.). It then reviews how these tools are utilized in the internet protocols and applications such as SSL/TLS, IPSEC, Kerberos, PGP, S/MIME, SET, and others (including wireless). System security issues, such as viruses, intrusion, and firewalls, will also be covered.

**Text book [TB]:**

William Stallings, “Cryptography and Network Security: Principals and Practice”, 5th ed. Pearson Prentice Hall,2013.

**Reference books [RB]:**

1. [Behrouz A. Forouzan](http://www.amazon.in/s/ref=dp_byline_sr_book_1?ie=UTF8&field-author=Behrouz+A.+Forouzan&search-alias=stripbooks) , [Debdeep Mukhopadhyay](http://www.amazon.in/s/ref=dp_byline_sr_book_2?ie=UTF8&field-author=Debdeep+Mukhopadhyay&search-alias=stripbooks), “Cryptography and Network Security”, 2nd ed. Tata McGraw Hill Education Private Limited, 2012
2. Atul Kahate , “Cryptography and Network Security”, 3rd ed. Tata McGraw Hill Education Private Limited, 2012

**Course Plan / Schedule:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Sl.#** | **Learning objectives** | **Topics to be covered** | **Chapter No [TB]** |
| 1 | Basics of Cryptography | Introduction to security attacks, services and mechanism, introduction to cryptography. | TB 1.3,1.4,1.5 |
| 2 | Conventional Encryption Techniques | Conventional encryption model, classical encryption techniques-substitution ciphers and transposition ciphers, cryptanalysis, steganography, stream and block ciphers. | TB 2.1,2.2,2.3,2.5 |
| 3 | Modern Block Ciphers | Block ciphers principals, Shannon’s theory of confusion and diffusion, fiestal structure, data encryption standard(DES), strength of DES, differential and linear crypt analysis of DES, block cipher modes of operations, triple DES, confidentiality using conventional encryption, traffic confidentiality, key distribution | TB 3.1,3.2,3.3,6.1,6.2,7.2,7.3 |
| 4 | Public Key Cryptography | Introduction to prime and relative prime numbers, finite field of the form GF(p), modular arithmetic, Fermat’s and Euler’s theorem, primality testing, Euclid’s Algorithm, Chinese Remainder theorem, Principals of public key crypto systems, RSA algorithm, security of RSA, key management, Diffie-Hellman key exchange algorithm, introductory idea of Elliptic curve cryptography, Elgamel encryption. | TB 8.1,8.2,8.3,8.4,9.1,9.2,10.1,10.2,10.3,10.4  RB[i] 10.4 |
| 5 | Message Authentication and Hash Function | Authentication requirements, authentication functions, message authentication code, hash functions, birthday attacks, security of hash functions and MACS, MD5 message digest algorithm, Secure hash algorithm(SHA).Digital Signatures: Digital Signatures, authentication protocols, digital signature standards (DSS), proof of digital signature algorithm. | TB 11.1,11.2,11.3,11.4,11.5,12.1,13.1,13.2,13.3 |
| 6 | Authentication Applications | Kerberos and X.509, directory authentication service, electronic mail security-pretty good privacy (PGP), S/MIME. | TB 14.1,14.2,15.1,15.2 |
| 7 | IP Security & Web security | Architecture, Authentication header, Encapsulating security payloads, combining security associations, key management.  Secure socket layer and transport layer security, secure electronic transaction (SET). | TB 16.1,16.2,16.3,16.4,16.5,16.6,17.2,17.3 |
| 8 | System Security | Intruders, Viruses and related threads, firewall design principals, trusted systems. | TB 18.1,19.1,20.1,20.2 |
|  | | | |

**Evaluation scheme:**

|  |  |  |  |
| --- | --- | --- | --- |
| **EC N0** | **Evaluation Components** | **Duration** | **Total Weightage %** |
| 1 | Quizzes (2) | 10 Minutes each | 5 |
| 2 | Mid Term Exam | 2 Hours | 20 |
| 3 | Class Tests |  | 5 |
| 4 | Assignments | - | 5 |
| 5 | Practical Exam | 2 hours | 25 |
| 5 | End Term Exam | 3 Hours | 40 |
| TOTAL | | | 100 |

**General Instructions, Attendance etc***:*

*Please refer to Student Handbook*

**Notices:**

All notices will be displayed on the CSE/IT Department Notice Board.

**Mr. Anuj Kumar Yadav**

**Course Coordinator**

**Instructors’ Contact Details:**

**Mr. Anuj Kumar Yadav**, Assistant Professor, Room No.320 Vedanta, Contact Tel. No. +919997909115

E-mail: anuj.kumar@dituniversity.edu.in

**Mr. Sandip Mandal,** Assistant Professor, Room No.314 Vedanta, Contact Tel. No. +918449007365

E-mail: sandip.mandal@dituniversity.edu.in

**Mr. Chirag Joshi**, Assistant Professor, Room No.413 Vedanta, Contact Tel. No. +919827279630

E-mail: chirag.joshi@dituniversity.edu.in