**Shyama Prasad Mukherji College**

**Teaching Plan**

**Course and Year: B.Sc. (Hons.) Mathematics, III Year (July-Nov, 2022)**

**Semester: V**

**Taught Individually or Shared: Individually**

**Paper: DSE-2(iii) Cryptography and Network Security**

**Faculty: Dr. Pooja Arora**

**No. of Classes (per week): 5 Lectures, 1 Tutorial (per week)**

**Total Marks:** 100 (Theory: 75 + Internal Assessment: 25)

**Duration:** 14 Weeks (70 Hrs.) **Examination:** 3 Hrs.

**Course Objectives:** This course helps the students to develop skills and knowledge of standard concepts in cryptography and demonstrates how cryptography plays an important role in the present digital world by knowing encryption and decryption techniques and secure data in transit across data networks.

**Course Learning Outcomes: After the course, the student will be able to:**

1. Understand the fundamentals of cryptography and computer security attacks.
2. Learn about various ciphers and data encryption standard.
3. Review basic concepts of number theory and finite fields.
4. Learn about advanced encryption standard.
5. Understand the fundamentals of RSA and elliptic curve cryptography.
6. Encrypt and decrypt messages using block ciphers, sign and verify messages using well known signature generation and verification algorithms.

**Teaching Plan (DSE-2 (iii): Cryptography and Network Security):**

**Weeks 1 and 2**: Overview of Cryptography, Computer security concepts, Security attacks, Symmetric cipher model, Cryptanalysis and brute-force attack, Substitution techniques, Caesar cipher, Monoalphabetic ciphers, Playfair cipher, Hill cipher, Polyalphabetic ciphers, One-time pad.

[2] Chapter 1.

[1] Chapter 1 (Sections 1.1 and 1.3) and Chapter 3 (Sections 3.1 and 3.2).

**Weeks 3 and 4:** Transposition techniques, Binary and ASCII, Pseudo-random bit generation, Stream ciphers and Block ciphers, Feistal cipher, Data Encryption Standard (DES), DES example.

1. Chapter 3 (Section 3.3) and Chapter 4 (Sections 4.1 to 4.3).
2. Chapter 2 (Sections 2.8 and 2.10).

**Weeks 5 and 6:** Review of basic concepts in Number theory and Finite Fields: divisibility, polynomial and modular arithmetic, Statements of Fermat’s and Euler’s theorems, Chinese remainder theorem, Discrete logarithm, Finite fields of the form GF(p) and GF(2n)

[1] Chapter 1 (Sections 2.1 to 2.3, 2.5, 2.7, and 2.8) and Chapter S (Sections 5.4 to 5.6).

**Weeks** 7 **and 8:** Advanced encryption standard (AES), AES transformation functions, AES key expansion, AES example.

[1] Chapter 6 [Sections 6.1 to 6.5 (up to Page 195)].

**Weeks 9 and 10:** Principles of public-key cryptosystems, RSA algorithm and security of RSA, Elliptic curve arithmetic, Elliptic curve cryptography.

[1] Chapter 9 (Sections 9.1 and 9.2), and Chapter 10 (Sections 10.3 and 10.4).

**Week 11:** Cryptographic Hash functions, Secure Hash algorithm.

[1] Sections 11.1 and 11.5.

**Weeks 12 and 13:** Digital signatures, Elgamal and Sehnorr digital signature schemes, Digital signature algorithm, Wireless network and mobile device security.

[l] Chapter 13 (Sections 13.1 to 13.4) and Chapter 18 (Sections 18.1 and 18.2).

**Week 14:** Email architecture, threats and security, Secure/Multipurpose Internet Mail Extension (S/MIME) and Pretty Good Privacy (PGP).

[1] Chapter 19 [Sections 19.1 to 19.5 (Confidentiality excluded)].

**References:**

* 1. Stallings, William (2017). *Cryptography and Network Security, Principles and Practice* (7th ed.). Pearson Education Limited. England.
  2. Trappe, Wade & Washington, Lawrence C. (2006). *Introduction to Cryptography with Coding Theory* (2nd ed.). Pearson Education International.

**Additional Reading:**

1. Stinson, Douglas R. (2005). *Cryptography Theory and Practice* (3rd ed.). CRC Press.
2. Delfs, H., Knebi, H. (2007). Introduction to Cryptography: Principles and Applications (2nd Edition). Springer-Verlag.
3. [Smart](http://en.wikipedia.org/wiki/Nigel_Smart_%28cryptographer%29) N. (2013). Cryptography: An Introduction, 3rd Edition. Mcgraw-Hill College.
4. Paar C., Pelzl J. (2009). Understanding Cryptography, A Textbook for Students and Practitioners, Foreword by Bart Preneel. Springer-Verlag.
5. Boneh D., Shoup V. (2020). A Graduate Course in Applied Cryptography. Stanford University (Version 0.5, Jan. 2020).

**e-references:**

1. [www.vssut.ac.in/lecture\_notes/lecture1428550736.pdf](http://www.vssut.ac.in/lecture_notes/lecture1428550736.pdf)
2. Online video lectures

|  |  |
| --- | --- |
| **No of classes required (approx.):**  Weeks 1 and 2: 9-10  Weeks 3 and 4: 10-12  Weeks 5 and 6: 12-14  Weeks 7 and 8: 8-10  Weeks 9 and 10: 10-12  Week 11: 4-5  Weeks 12 and13: 8-10  Week 14: 5-6 |  |

**Sub topics to be covered and their order along with the respective time frames (if any):**

Basic concept of Groups, Rings and Fields. Properties of Fields. Representation of a digit in Bits and Hexadecimal notation.

**Resources and Methodology of Teaching:**

1. Using online available resources.
2. Guide, how to read and write research articles and elaboration of research papers.
3. Mentor students to present research paper.
4. Encourage students to participate in the academic activities of the college and department as well as in other colleges.

**Assessment plan:**

* Tentative dates of Assessment and Assignment:
* Test 1 in the end of September,
* Test 2 in the mid of November
* Assignment 1 in the mid of September
* Test 3 and Assignment 2 in the end of October

**Criteria of Assessment:**

Written Test/ Assignment/ Presentations/Performance in Inter-College Academic Activities.