Teaching Plan (2021-2022)

Name of the Faculty: Ms. Rashmeet Kaur

Name of the Course: B.Sc (Hons) Computer Science

Semester : VI

Title of the Paper : Information Security

Course Learning Outcomes

On successful completion of this course, a student will be able to,

1. Identify the major types of threats to information security
2. Describe the role of cryptography in security
3. Select appropriate error-detection and error-correction methods for an application
4. Discuss the strengths and weaknesses of private and public key crypto systems
5. Describe malwares and memory exploits
6. Discuss the need for security in Internet of Things.

Month	Topics Covered	References
January	Ch 1 Introduction (1.1, 1.2, 1.3, 1.4, 1.5) Ch 3 Substitution ciphers (3.1, 3.2)	[3]
February	Ch 3 Transposition ciphers, Steganography and Watermarking (3.3, 3.5) Ch 4 Stream and Block ciphers (4.1, 4.2, 4.3) Ch 9 Asymmetric encryption (9.1, 9.2) Ch 10 Diffie-Hellman Key Exchange (10.1) Practical: Q3, Q4, Q5, Q6, Q10 Assignment 1 (Last week of February)	[3] [3]
March	Ch 13 Digital Signature (13.1) Ch 3 Malicious software's (3.1, 3.2) Ch 13 Security in Internet-of-Things (13.1) Practical: Q7, Q8, Q9 Test 1 (First week of March)	[1] [1]

April	Assignment 2 - Presentations (Third week of March) Ch 3 Error Detecting/Correction (3.1 - 3.4) Ch 4 Hamming Codes (4.1) Revision Practical: Q1, Q2	[2]

Note : The tentative date of Assignment/test/Project may also be provided.

The schedule of Practicals may also be provided.

References:

[1] Pfleeger, C.P., Pfleeger,S.L., & Margulies, J. (2015). Security in Computing. 5th edition. Prentice Hall.

[2] Lin, S. & Costello, D. J. (2004). Error Control Coding: Fundamentals and applications. 2nd edition. Pearson Education

[3] Stallings, W. (2018). Cryptography and network security. 7th edition. Pearson Education.