Course Title: **Introduction to Cybersecurity**

A Program Elective Course (UG3)

Course Level: L1 L-T-P-C: 3 - 1 - 0 - 4

Pre-requisite: Data Structure, Basic Probability and Basics of Computer Network

1. Outline: An introductory course for cybersecurity which covers an overview of Computer Security, Cryptographic Tools, CIA triad, Authenticity, Access Control, Malicious Software, Firewall, IDS, etc.

2. Objectives: With emerging technologies, the internet across the globe is growing fast to fulfill our demands. On the other hand, the number of cybercrime activities has increased a lot nowadays. Cybersecurity is a systematic study to assess those cyber threats and tackle them by taking suitable countermeasures. The objective of this course is to provide a basic understanding (introductory level) of cybersecurity so that students can comfortably pursue further job/industry-oriented cybersecurity courses. This, in turn, helps the students to become a true leader and expert in the area of cybersecurity.

3. **Course Outline (Syllabus)**:
The following list of topics is tentative. Based on available time slots, some topics may be dropped or added or reordered.

1. **Overview:** Computer Security Concepts; Threats, Attacks, and Assets; Security Functional Requirements; Fundamental Security Design Principles; Attack Surfaces and Attack Trees; Computer Security Strategy

2. **Basics of networking:** An overview of TCS/IP, OSI model

3. **New direction in cryptography:** PKC vs SKC, Diffie-Hellman key-exchange, PKI

4. **Confidentiality:** Classical ciphers; One-time padding; PRNG: Stream Cipher-RC4; Random permutation; Feistel cipher, DES, SPN, AES; PKE- Elgamal; Mode of operations

5. **Authentication and Integrity:** Properties of hash function; Available candidates and their security; Birthday problem; Random oracle; Digital signature - RSA; MAC-HMAC;

6. **User Authentication:** password-based authentication, token-based authentication, biometric authentication, remote user authentication;

7. **Access control:** Access Control Principles; Subjects, Objects, and Access Rights;

Discretionary Access Control**;** Role-based access control, Attribute-based access control; Identity, Credential, and Access Management

8. **Protocols and popular standards:** Wired Equivalent Privacy (WEP); Wi-Fi protected access (WPA); SSL/TSL; VPN-IPSec

9. **Malicious software:** Virus, worms, spam e-mails, Trojans, spyware, Ransomware

10. **Denial-of-Service Attacks**

11. **Intrusion Detection System**

12. **Honeypots**

13. **Firewall**

14. **Quantum attack**: **A non-technical overview**

4. Books/References:

a) William Stallings and Lawrie Brown. Computer Security Principles and Practice (3rd Edition), Pearson, 2014
b) Douglas Robert Stinson and Maura Paterson. Cryptography Theory And Practice (4th Edition), CRC Press, 2018)
c) William Stallings. Cryptography and Network Security: Principle and Practice (6th Edition), Pearson, 2013

5. Grading Policy:

10% Mid-Exam-1
10% Mid-Exam-2
20% End-Exam
20% Term Project
20% Presentation/Assignment/Quiz

6. Industry Impact:

With the growing popularity of digitalization, cybercrime has been a constant threat to every individual/organization. Since data security has become the top priority in the 21st century, many big industries like Fortinet, Cisco, Microsoft, IBM have already started investing their revenue for cybersecurity solutions. Also, many startups have involved in the race of designing cybersecurity solutions.

7. List of Companies Working On Related Topics:

1. Fortinet
2. KnowBe4
3. Cisco
4. Splunk
5. Microsoft
6. IBM
7. Sophos
8. Palo Alto Networks
9. McAfee
10. Broadcom

8. Resources: The aformentioned books