FACULTY OF COMPUTER APPLICATIONS
Bachelor of Computer Applications

- **Sem.**: 5
- **Subject Code**: 05BC3502
- **Subject**: Information Security
- **Course Objectives**:
    1. Understand basics of information security
    2. Learn fundamentals of cryptography and its application to network security.
    3. Acquire background on hash functions; authentication; digital signatures.
    4. Understand the program security, network security and security countermeasures.

Prerequisites :Basic knowledge of computers, Internet, operating system and Networking.

Unit No	Topics Covered	No of lectures required
1	**Introduction**: Computer Security Concepts (CIA), Threats, Attacks, and Assets, Security Fundamental Requirements, Fundamental Security Design Principles, Attack Surfaces and Attack Trees	**08**
2	**Symmetric and Asymmetric Cryptographic Techniques:** Introduction to Symmetric Cryptography, Data Encryption Standard (DES) Algorithm, Advanced Encryption Standard (AES) Algorithm. Introduction to Asymmetric Cryptography, Difference between symmetric and asymmetric cryptography, RSA Algorithm.	**10**
3	**Message Authentication and Digital Signatures:** Authentication Using Symmetric Encryption, Message Authentication without Message Encryption, Secure Hash Functions, Digital Signature, Public-Key Certificates, Symmetric Key Exchange Using Public-Key Encryption	**10**
4	**Program Security:** Non malicious Program errors – Buffer overflow, Incomplete Mediation, Time-of-Check to Time-of-Use, Malicious Code (Malware) – Viruses, Trojan Horses and Worms, Program Security Countermeasures for Users and Developers	**08**
5	**Network Security :**	**09**

	Internet Security Protocols – Secure E-Mail and S/MIME, SSL and TLS, HTTPS, IPv4 and IPv6 Security Internet Authentication Applications – Kerberos, X.509, Public Key Infrastructure Wireless Network Security – Wireless Security, Mobile Device Security, IEEE 802.11 Wireless LAN Overview	

Course Outcomes: On successful completion of course learner/student will be able to -

1. Understand the risks faced by computer systems and networks.
2. Analyze security problems in computer systems and networks.
3. Apply cryptography algorithms and protocols to achieve computer security.
4. Analyze security mechanisms to protect computer systems and networks.

Course Outcomes – Program Outcomes Mapping Table:

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PSO1	PSO2	PSO3
CO1				H		M	M	L	L	L	L
CO2				H		M	M	L	M	L	M
CO3	H	H	H	M		H	M	H	L	L	H
CO4	H	H	H	M		H	M	H	L	L	L

Text Book:

1. "Computer Security Principles and Practice", William Stallings, Lawrie Brown, Pearson, 3rd Edition
2. "Security in Computing", Charles P. Pfleeger, Shari Lawrence Pfleeger, Jonathan Margulies, Pearson Education, 5th Edition.

Reference Book:

1. "Cryptography And Network Security Principles And Practice", William Stallings, Pearson, 5th Edition.
2. "Modern Cryptography: Theory and Practice", Wenbo Mao, Prentice Hall.
3. "Network Security Essentials: Applications and Standards", William Stallings, Prentice Hall, 4th Edition.

Web References :

1. https://www.imperva.com/
2. https://www.tecmint.com/
3. https://www.cisco.com/c/en/us/products/security/what-is-information-security-infosec.html

App References :

1. Udemy
2. Coursera

Syllabus Coverage from Main reference:

Unit #	Chapter Numbers
1	Book 1 Chapter 1
2	Book 2 Chapter 12
3	Book 1 Chapter 2
4	Book 2 Chapter 3
5	Book 1Chapter 22, 23, 24