St. Xavier's College (Autonomous), Ahmedabad

Syllabus of Semester – VI of the following departments under Faculty of Computer Science based on Undergraduate Curriculum Framework to be implemented from the Academic Year 2024-25.

DEPARTMENT OF COMPUTER SCIENCE

BCA (Hons.) Category – IV

Minor Course - 1 Information Security

CREDIT DISTRIBUTION, ELIGIBILITY AND PRE-REQUISITES OF THE COURSE

Course Title & Code	Credit Distribution of The Course			Eligibility Criteria	Pre-requisite(s) of the Course (if any)
	Lecture	Tutorial	Practical / Practice		
Information Security BCAMN661C	4	0	0	10 + 2 from a recognized board in any stream	Nil

Course Objectives:

The objective of the course is to understand the fundamentals of cryptography, various encryption mechanisms, different key distribution techniques and deployment of encryption schemes to secure data across data networks

Course Outcome:

After the completion of the course students will be able to :
COBF6403.01: Describe the fundamentals of Cryptography
COBF6403.02: Describe standard algorithms used to provide confidentiality, integrity and authenticity.
COBF6403.03: Explain the various key distribution and management schemes.
COBF6403.04:Explain how to deploy encryption techniques to secure data in transit across data networks
COBF6403.05: Design security applications in the field of Information technology.

Unit	Unit Details
I	**INTRODUCTION** ● Computer security concepts ● The OSI security architecture ● Security attacks ● security services ● security mechanisms ● A model for network security **CRYPTOGRAPHY** ● Symmetric encryption principles o Cryptography o Cryptanalysis o Fiestel Cipher structure ● Symmetric block encryption algorithms o Data encryption standard o Triple DES o Advanced Encryption standard
II	**CRYPTOGRAPHY CONTD…** ● Stream Cipher structure ● Cipher block modes of operations o Electronic code book o cipher block chaining mode o cipher feedback mode o counter mode **PUBLIC KEY CRYPTOGRAPHY AND MESSAGE AUTHENTICATION** ● Approaches to Message Authentication o Authentication using convention encryption o Message Authentication without message encryption ● Secure Hash Functions