THIRD-YEAR OF BACHELOR OF COMPUTER SCIENCE REVISED SYLLABUS ACCORDING TO CBCS

COURSE TITLE: INFORMATION AND NETWORK SECURITY

SEMESTER-V, W.E.F. 2021-2022

Recommended by the Board of Studies in Computer Science
And
Approved by the Academic Council

Devrukh Shikshan Prasarak Mandal's
Nya. Tatyasaheb Athalye Arts, Ved. S. R. Sapre Commerce, and
Vid. Dadasaheb Pitre Science College (Autonomous), Devrukh.
Tal. Sangameshwar, Dist. Ratnagiri-415804, Maharashtra,
India

Academic Council Item No: ______________

Name of the Implementing Institute	:	Nya. Tatyasaheb Athalye Arts, Ved. S. R. Sapre Commerce, and Vid. Dadasaheb Pitre Science College (Autonomous), Devrukh. Tal. Sangameshwar, Dist. Ratnagiri-415804,
Name of the Parent University	:	University of Mumbai
Name of the Programme	:	Bachelor of Science
Name of the Department	:	Computer Science
Name of the Class	:	Third Year
Semester	:	Five
No. of Credits	:	03
Title of the Course	:	Information and Network Security
Course Code	:	USCST54
Name of the Vertical	:	Elective II
Eligibility for Admission	:	Any 12th Pass seeking Admission to Degree Programme in adherence to Rules and Regulations of the University of Mumbai and Government of Maharashtra
Passing Marks	:	40%
Mode of Assessment	:	Formative and Summative
Level	:	UG
Pattern of Marks Distribution for TE and CIA	:	70:30
Status	:	CBCS
To be implemented from Academic Year	:	2021-2022
Ordinances /Regulations (if any)		

Syllabus for Third Year of Bachelor of Science in Computer Science

(With effect from the academic year 2021-2022)

SEMESTER-V	**Paper No.– 4**
Course Title: Information and Network Security	**No. of Credits - 03**
Type of Vertical: Elective II	**COURSE CODE: USCST54**

Learning Outcomes Based on BLOOM's Taxonomy:

After completing the course, the learner will be able to…

Course Learning Outcome No.	Blooms Taxonomy	Course Learning Outcome
CO-01	Understand	Understand the principles and practices of cryptographic techniques.
CO-02	Understand	Understand a variety of generic security threats and vulnerabilities, and identify & analyze particular security problems for a given application.
CO-03	Understand	Understand various protocols for network security to protect against the threats in a network.

Syllabus for Third Year of Bachelor of Science in Computer Science

(With effect from the academic year 2021-2022)

SEMESTER-V **Paper No.– 4**

Course Title: Information and Network Security **No. of Credits - 03**

Type of Vertical: Elective II **COURSE CODE: USCST54**

COURSE CONTENT			
Unit No.	**Content**	**Credits**	**No. of Lectures**
I	Introduction: Security Trends, The OSI Security Architecture, Security Attacks, Security Services, Security Mechanisms Classical Encryption Techniques: Symmetric Cipher Model, Substitution Techniques, Transposition Techniques, Steganography, Block Cipher Principles, The Data Encryption Standard, The Strength of DES, AES (round details not expected), Multiple Encryption and Triple DES, Block Cipher Modes of Operation, Stream Ciphers Public-Key Cryptography and RSA: Principles of Public-Key Cryptosystems, The RSA Algorithm	**01**	**15**
II	Key Management: Public-Key Cryptosystems, Key Management, Diffie-Hellman Key Exchange Message Authentication and Hash Functions: Authentication Requirements, Authentication Functions, Message Authentication Codes, Hash Functions, Security of Hash Functions and Macs, Secure Hash Algorithm, HMAC Digital Signatures and Authentication: Digital Signatures, Authentication Protocols, Digital Signature Standard Authentication Applications: Kerberos, X.509 Authentication, Public-Key Infrastructure.	**01**	**15**

III	Electronic Mail Security: Pretty Good Privacy, S/MIME IP Security: Overview, Architecture, Authentication Header, Encapsulating Security Payload, Combining Security Associations, Key Management Web Security: Web Security Considerations, Secure Socket Layer and Transport Layer Security, Secure Electronic Transaction Intrusion: Intruders, Intrusion Techniques, Intrusion Detection Malicious Software: Viruses and Related Threats, Virus Countermeasures, DDOS Firewalls: Firewall Design Principles, Types of Firewalls	**01**	**15**
	Total	03	45

Required Previous Knowledge

Students should know basic concepts related to computer and computer handling

Access to the Course

The course is available for all the students admitted for Bachelor of Science (Computer Science).

Forms of Assessment

The assessment of the course will be of Diagnostic, Formative and Summative type. At the beginning of the course diagnostic assessment will be carried out. The formative assessment will be used for the Continuous Internal Evaluation whereas the summative assessment will be conducted at the end of the term. The weightage for formative and summative assessment will be 60:40. The detailed pattern is as given below.

Semester End Evaluation (60 Marks)
Question Paper Pattern
Time: 2 hours

Question No.	Unit/s	Question Pattern	Marks
Q.1	I ,II &III	MCQ/Fill in the blanks/One line sentence	10
Q.2	I	Descriptive Questions	20
Q.3	II	Descriptive Questions	20
Q4.	III	Descriptive Questions	20
	Total		**70**

Internal evaluation (30 Marks)

Sr. No.	Description	Marks
1	Classroom Tests	10
2	Project/ Viva/ Presentations/ Assignments	10
3	Attendance	10
	Total	**30**

Grading Scale

10 points grading scale will be used. The grading scale used is O to F. Grade O is the highest passing grade on the grading scale, and grade F is a fail. The Board of Examinations of the college reserves the right to change the grading scale.

Reference book:

□ Cryptography and Network Security: Principles and Practice 5th Edition, William Stallings, Pearson,2010

□ **Text book:**

- Techmax publication book

Additional References:

- Cryptography and Network Security, Atul Kahate, Tata McGraw-Hill, 2013.
- Cryptography and Network, Behrouz A Fourouzan, Debdeep Mukhopadhyay, 2nd Edition,TMH,2011

Course: USCSP59	**Practical of USCST54 (Credits : 1, Lectures/Week: 3)**
USCSP59	1.Write programs to implement the following Substitution Cipher Techniques: - Caesar Cipher - Monoalphabetic Cipher 2 Write programs to implement the following Substitution Cipher Techniques: - Vernam Cipher - Playfair Cipher 3 Write programs to implement the following Transposition Cipher Techniques: - Rail Fence Cipher - Simple Columnar Technique 4 Write program to encrypt and decrypt strings using - DES Algorithm - AES Algorithm 5 Write a program to implement RSA algorithm to perform encryption / decryption of a given string. 6 Write a program to implement the Diffie-Hellman Key Agreement algorithm to generate symmetric keys. 7 Write a program to implement the MD5 algorithm compute the message digests. 8 Write a program to calculate HMAC-SHA1 Signature 9 Write a program to implement SSL. 10 Configure Windows Firewall to block: - A port - An Program - A website