UNIVERSITY OF PETROLEUM & ENERGY STUDIES

School of Computer Science

Dehradun

COURSE PLAN

Programme: B. Tech CSE+ All IBM Courses

Course: Cryptography and Network Security Lab

Subject Code: CSEG 4101

No. of credits: 1

Semester : VII

Session: Aug-Dec 2022

Batch : 2019-2023

Prepared by :

Email :

Approved by HOD

UPES Campus
"Energy Acres"
P.O. Bidholi, , Dehradun

Tel : +91-135-2770137
Fax : +91 135- 27760904

A. PRE-REQUISITES

- Computer Networks

B. PROGRAM OUTCOMES (POs) for B.Tech. in Computer Science and Engineering with Specialization in CSF

After completion of the program the student will be able to:

PO1: Engineering knowledge: Apply the knowledge of mathematics, science, engineering fundamentals, and an engineering specialization to the solution of complex engineering problems.

PO2: Problem analysis: Identify, formulate, review research literature, and analyze complex engineering problems reaching substantiated conclusions using first principles of mathematics, natural sciences, and engineering sciences.

PO3: Design/development of solutions: Design solutions for complex engineering problems and design system components or processes that meet the specified needs with appropriate consideration for the public health and safety, and the cultural, societal, and environmental considerations.

PO4: Conduct investigations of complex problems: Use research-based knowledge and research methods including design of experiments, analysis and interpretation of data, and synthesis of the information to provide valid conclusions.

PO5: Modern tool usage: Create, select, and apply appropriate techniques, resources, and modern engineering and IT tools including prediction and modeling to complex engineering activities with an understanding of the limitations.

PO6: The engineer and society: Apply reasoning informed by the contextual knowledge to assess societal, health, safety, legal and cultural issues and the consequent responsibilities relevant to the professional engineering practice.

PO7:Environment and sustainability: Understand the impact of the professional engineering solutions in societal and environmental contexts, and demonstrate the knowledge of, and need for sustainable development.

PO8: Ethics: Apply ethical principles and commit to professional ethics and responsibilities and norms of the engineering practice.

PO9: Individual and team work: Function effectively as an individual, and as a member or leader in diverse teams, and in multidisciplinary settings.

PO10: Communication: Communicate effectively on complex engineering activities with the engineering community and with society at large, such as, being able to comprehend and write effective reports and design documentation, make effective presentations, and give and receive clear instructions.

PO11: Project management and finance: Demonstrate knowledge and understanding of the engineering and management principles and apply these to one's own work, as a member and leader in a team, to manage projects and in multidisciplinary environments.

PO12:Life-long learning: Recognize the need for, and have the preparation and ability to engage in independent and life-long learning in the broadest context of technological change.

PROGRAM SPECIFIC OUTCOMES

PSO1: Perform system and application programming using computer system concepts, concepts of Data Structures, algorithm development, problem solving and optimizing techniques.

PSO2: Apply software development and project management methodologies using concepts of front-end and back-end development and emerging technologies and platforms.

PSO3:

1=weakly mapped
2= moderately mapped
3=strongly mapped

C. OBJECTIVES OF COURSE

- Students should be able to implement various cryptographic algorithms
- Students should be able to compute key generation and key management algorithms
- Students should be able to understand the implementation of security in computer networks

D. COURSE OUTCOMES (COs)

Upon completion of this course the learners will be able to:

CO1	Learn about various security services, possible attacks and traditional ciphers.
CO2	Apply knowledge of symmetric cryptography like data encryption standards and advanced encryption standards.
CO3	Compute asymmetric cryptographic algorithms and key management algorithms.
CO4	Understand implementation of various security controls in computer networks.

Table: Correlation of POs v/s COs

Course Outcome	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
CO1	2	2	1										2		
CO2	2	2	3										2		
CO3	2	2	3										2		
CO4	2	2	1										2		
Average	2	2	2										2		

1=weakly mapped
2= moderately mapped
3=strongly mapped

E. COURSE OUTLINE

Expt. No.	Big Ideas/ Topics	Modality
1	Classical Encryption Techniques	F2F
2	Shift Cipher Techniques	F2F
3	Polyalphabetic Cipher Techniques	F2F
4	Euclidean algorithms (Basic and Extended)	F2F
5	DES Encryption Techniques	F2F
6	AES Encryption Techniques	F2F
7	Public key Cryptography	F2F
8	Diffie Hellman Key Exchange Algorithm	F2F
9	Hash Function	F2F
10	Web Security	F2F

F. PEDAGOGY

- Synchronous Mode using BB Collaborate aided with power point presentations.
- Regular Communication for Tests/Quizzes/Vivas will be ensured by the faculty through email or Blackboard announcements/ email ids

In continuation to problem description, the solution to the given problem statement should be designed suitably using algorithm/flow-chart/pseudocode. After obtaining a successful design, the design is implemented using java language and tested with appropriate test cases (with an insight on Input/Output Data Constraints). Students are evaluated under two main categories (1) Performance (via efficient design and implementation) and record, and (2) Preparation of the student evaluated via viva-voce /quiz. The same is detailed in Section-E.

G. COURSE COMPLETION PLAN

No. of Experiments planned/taken		No. of Quizzes/ viva planned/ conducted	
10	-	3	-

One lab session = 120 min.

H. EVALUATION & GRADING

Students will be evaluated regularly/continuously throughout the course based on the following:

1) Performance & Record - 50%
2) Viva Voce or Quiz Examination - 50%

H.1 Performance & Record: *WEIGHTAGE - 50%*

12 lab Experiments are conducted in synchronous mode through BB Collaborate. The lists of activities performed under the experiments are detailed in Section-F. A sample template of the evaluation of lab activity is provided in the table below.

Evaluation of each Lab Activity	
Problem Description	10% marks
Algorithm Design	40% marks
Coding Syntax, Execution and Bug Fixing	30% marks
I/O Test cases & Data Constraints	10% marks
Records (submitted before the very next turn.)	10% marks

H.2 Viva Voce or Quiz Examination: *WEIGHTAGE - 50%*

The preparation of the students would be evaluated based on two viva-voce or quiz examinations in periodic schedules (each with 50% weightage).

It is mandatory for the students to attend the above said continuous evaluation. Students who do not attend will lose their marks. Continuous Internal Assessment Record Sheet will be displayed at the end of the semester.

H.3 GRADING:

The overall marks obtained at the end of the semester comprising the above two mentioned shall be converted to a grade.

Student(s), who have met the qualifying criteria of individual practical subject but not met qualifying criteria of SGPA, will not be allowed to re-appear for improvement. However those students with Grade “F” and those who wish to re-appear in the practical subject, shall be required to pay the prescribed fee per subject as notified by the University. These students will be eligible to *repeat continuous evaluation* of that respective practical subject(s) during summer vacation (June-July).

Grade shall be awarded on the performance of the student(s). The Grade will be capped as per the rules mentioned in student Bulletin. All Other rules and regulations such as requirement of passing, etc. will remain same as mentioned in rules & regulations.

I. DETAILED DELIVERY PLAN

EXPERIMENT NO – 1: Classical Encryption Techniques
Objective: - To understand the concept of passwords, Brute Force Techniques.

1. Develop a program to show the workings of substitution method.
2. Develop a login system, which will take two inputs username and password (4 digit pin). As an Adversary develop a program, which will generate passwords serially, and find the right password for the developed login system.

EXPERIMENT NO – 2: Shift Cipher Techniques
Objective: - To understand the concept of Shift Ciphers.

1. Implement a program to show the working of **Caesar cipher.**
2. Implement a program to show the working of the **Vigenère cipher.**

EXPERIMENT NO – 3: Polyalphabetic Cipher Techniques
Objective: - To understand the concept of Polyalphabetic Ciphers.

1. Implement the polyalphabetic cipher techniques.

EXPERIMENT NO – 4: Euclidean algorithms
Objective: - To understand the concept of Euclidean algorithms (Basic and Extended).

1. Implement the Euclidean algorithms.

EXPERIMENT NO-5: DES Encryption Techniques
Objective: - To understand the concept of Block Ciphers

1. Implement the Data Encryption Standards.

EXPERIMENT NO-6: AES Encryption Techniques
Objective: - To understand the concept of Block Ciphers

1. Implement the Advanced Encryption Standards.

EXPERIMENT-7: Public key Cryptography:
Objective: - To understand the concept of secret key, cipher and plain text.

1. Design a system, which will demonstrate the working of RSA public key cryptography.

EXPERIMENT-8: Diffie Hellman Key Exchange Algorithm:
Objective: - To understand the concept of exchanging keys through Diffie Hellman.

1. Design a system, which will demonstrate the working of Diffie Hellman.

Experiment No 9: Hash Function
Objective: - To understand the concept of Integrity, Non-repudiation and message digest.

1. Write a program to demonstrate the working of SHA 256/SHA-512.
2. Create a mail (treat it as a string) and attach the digital signature with your mail. show that the attached digital signature can be used to:
    a. Verify the author and the date and time of the signature.
    b. Authenticate the contents at the time of the signature.

Experiment No 10: Web Security
Objective: - To understand the concept of Web Security.

1. Design a system, which will demonstrate the working of Web Security.

J. SUGGESTED READINGS:

Text Books / Reference Books

Cryptography and Network Security, By William Stallings
Behrouz A. Forouzan (2016). Cryptography and Network Security. SIE Publication. ISBN: 978-0070702080

K. GUIDELINES

Cell Phones and other Electronic Communication Devices: Cell phones and other electronic communication devices MUST be turned off during the lab session.

E-Mail and online learning tool: Each student in the class should have UPES e-mail id and a password to access the Blackboard regularly. The best way to arrange meetings with faculty or is by email and prior appointment. Various research papers/reference material will be mailed/uploaded on online learning platform time to time.

Attendance: Students are required to have **minimum attendance of 75%** in the subject.

Passing criterion: Student has to secure minimum 35 marks for the subject in the total marks in order to pass in that paper.

L. COURSE OUTCOME ASSESSMENT

To assess the fulfilment of course outcomes two different approaches have been decided. Degree of fulfillment of course outcomes will be assessed in different ways through direct assessment and indirect assessment. In Direct Assessment, it is measured through Continuous assessments. Each assessment is designed in such a way that it can address one or two outcomes (depending upon the

course completion). Indirect assessment is done through the student survey which needs to be designed by the faculty (sample format is given below) and it shall be conducted towards the end of course completion. The evaluation of the achievement of the Course Outcomes shall be done by analyzing the inputs received through Direct and Indirect Assessments and then corrective actions suggested for further improvement.

Sample format for Indirect Assessment of Course outcomes

NAME:
ENROLLMENT NO:
SAP ID:
COURSE:
PROGRAM:

Please rate the following aspects of course outcomes of **Object Oriented Programming Lab**.
Use the scale 1-4* :

COs		1	2	3	4
CO1	Learn about various security services, possible attacks and traditional ciphers.				
CO2	Apply knowledge of symmetric cryptography like data encryption standards and advanced encryption standards.				
CO3	Compute asymmetric cryptographic algorithms and key management algorithms.				
CO4	Understand implementation of various security controls in computer networks.				

* 1 Below Average 3 Good

2 Average 4 Very Good

Signature