**Format No. QSP/7.1/01.F01 (B) Issue No. 05, Rev. No. 5,Dated: Jan 1, 2017**

**UNIVERSITY OF PETROLEUM & ENERGY STUDIES**

**School of Computer Science**

**Dehradun**

**COURSE PLAN**

Programme : B. Tech CSE-All Branches

Course : Cryptography and network security LAB

Subject Code : CSEG428

No. of credits : 1

Semester : IV

Session : Jul 2019- Dec 2019

Batch : 2016-2020

Prepared by : Ms. Aradhana Kumari Singh

Email : aradhana.singh@ddn.upes.ac.in

**Approved By**

HOD/ Prog. Head

UPES Campus Tel : +91-135-2770137

“Energy Acres” Fax : +91 135- 27760904

P.O. Bidholi, , Dehradun

**COURSE PLAN**

1. **PREREQUISITE:**
   1. Computer Networks

1. **PROGRAM OUTCOMES (POs) and PROGRAM SPECIFIC OUTCOMES (PSOs) for :**

**B1. PROGRAM OUTCOMES (POs)**

1. Engineering knowledge: Apply the knowledge of mathematics, science, engineering fundamentals, and an engineering specialization to the solution of complex engineering problems.
2. 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.
3. 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.
4. 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.
5. 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.
6. 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.
7. 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.
8. Ethics: Apply ethical principles and commit to professional ethics and responsibilities and norms of the engineering practice.
9. Individual and team work: Function effectively as an individual, and as a member or leader in diverse teams, and in multidisciplinary settings.
10. 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.
11. 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.
12. 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.

**B2. Program Specific Outcomes (PSOs)**

1. Perform system and application programming using computer system concepts, concepts of Data Structures, algorithm development, problem solving and optimizing techniques,
2. Apply software development and project management methodologies using concepts of front-end and back-end development and emerging technologies and platforms.
3. Understand and apply Cloud Computing architecture for scalable, secure and dynamically provisioned business oriented environment with optimized performance tuning and data reliability.

**COURSE OUTCOMES for Cryptography and Network Security lab: At the end of this course student should be able to**

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

**Table: Correlation of POs and PSOs v/s COs**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| PO/CO | PO1 | PO2 | PO3 | PO4 | PO5 | PO6 | PO7 | PO  8 | PO9 | PO  10 | PO  11 | PO  12 | PSO  1 | PSO  2 | PSO  3 |
| CO1 | 1 |  |  |  |  |  |  |  |  |  |  |  | 2 |  |  |
| CO2 | 1 |  |  |  |  |  |  |  |  |  |  |  | 2 |  |  |
| CO3 | 1 |  |  |  | 2 |  |  |  |  |  |  |  | 2 |  |  |
| CO4 |  |  |  |  | 2 |  |  |  |  |  |  |  | 2 |  |  |

1: Slight (Low) 2: Moderate (Medium) 3: Substantial (High)

1. **PEDAGOGY**

**1. Power Point Presentation,**

**2. Experimental learning with continuous evaluation**

1. **COURSE COMPLETION PLAN**

|  |  |
| --- | --- |
| **Total Lab sessions** | 07 |
| **Total Viva** | 03 |

One Session =120 minutes

1. **EVALUATION & GRADING**

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

1. Performance & Record - 50%
2. Viva Voce - 50%

**F1. Performance & Record:** WEIGHTAGE - 50%

. The lists of activities performed under the experiments are detailed clearly in Section-F. F2F experiments have 100% weightage.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Experiment Evaluation (10 marks per experiment)** | |  |  |
|  | Algorithm Design | 3 Marks |  |  |
|  | Coding Syntax | 2 Marks |  |  |
|  | Execution / Bug Finding | 2 Marks |  |  |
|  | Records (submitted before the very next turn.) | 3 Marks |  |  |

**F2*.* Viva Voce:** WEIGHTAGE - 50%

The preparation of the students would be evaluated based on viva-voce or quiz examination in periodic schedules.

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.

**F3. 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. Students, who wish to re-appear in the practical subject, shall be required to pay the prescribed fee per subject as notified by the University. The student with Grade “F” only 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. There will be no capping of SGPA for the students re-appeared for Practical Subject. All Other rules and regulations such as requirement of passing, etc. will remain same as mentioned in rules & regulations.

1. **DETAILED SESSION 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 **Vigenère cipher.**

**EXPERIMENT NO-3: DES Encryption Techniques**   
**Objective: - To understand the concept of Block Ciphers**

1. Implement the Data Encryption Standards.

**EXPERIMENT NO-4: AES Encryption Techniques**   
**Objective: - To understand the concept of Block Ciphers**

1. Implement the Advanced Encryption Standards.

**EXPERIMENT-5: 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-6: 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 7: Hash Function**

**Objective: - To understand the concept of Integrity, Non-repudiation and message digest.**

1. Write a program to demonstrate the working of 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:
   1. Verify the author and the date and time of the signature.
   2. Authenticate the contents at the time of the signature.

1. **GUIDELINES:**

***Cell Phones and other Electronic Communication Devices*:** Cell phones and other electronic communication devices (such as Blackberries/Laptops) are not permitted in classes during Tests or the Mid/Final Examination. Such devices MUST be turned off in the class room.

***E-Mail and online learning tool:*** Each student in the class should have an e-mail id and a pass word to access the e-labs system regularly. Regularly, important information – Date of conducting class tests, guest lectures, via online learning tool. The best way to arrange meetings with us or ask specific questions is by email and prior appointment. All the assignments preferably should be uploaded on online learning tool. 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 each subject. Students with less than said percentage shall **NOT** be allowed to appear in the end semester examination.

***Passing criterion:*** Student has to secure minimum 40% marks of the “highest marks in the class scored by a student in that subject (in that class/group class)” individually in both the ‘End-Semester examination’ and ‘Total Marks’ in order to pass in that paper.

* Passing Criterion for B. Tech: minimum 40% of the highest marks in the class
* Passing Criterion for M. Tech: minimum 40% of the highest marks in the class

1. **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 quizzes, tests, assignment, Mid-term and/or End-term examinations. It is suggested that each examination 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.