03.10.2022

VI Semester

Cryptography

Course Code	**21EC642**	CIE Marks	50
Teaching Hours/Week (L:T:P:S)	2:2:0:0	SEE Marks	50
Total Hours of Pedagogy	40	Total Marks	100
Credits	3	Exam Hours	3

Course objectives:

This course will enable students to:

- Preparation: To prepare students with fundamental knowledge/ overview in the field of Information Security with knowledge of mathematical concepts required for cryptography.
- Core Competence: To equip students with a basic foundation of Cryptography by delivering the basics of symmetric key and public key cryptography and design of pseudo random sequence generation technique

Teaching-Learning Process (General Instructions)

The sample strategies, which the teacher can use to accelerate the attainment of the various course outcomes are listed in the following:

1. Lecture method (L) does not mean only the traditional lecture method, but a different type of teaching method may be adopted to develop the outcomes.
2. Show Video/animation films to explain the different Cryptographic Techniques / Algorithms
3. Encourage collaborative (Group) Learning in the class
4. Ask at least three HOTS (Higher order Thinking) questions in the class, which promotes critical thinking
5. Adopt Problem Based Learning (PBL), which fosters students' Analytical skills, develop thinking skills such as the ability to evaluate, generalize, and analyze information rather than simply recall it.
6. Topics will be introduced in a multiple representation.
7. Show the different ways to solve the same problem and encourage the students to come up with their own creative ways to solve them.
8. Discuss how every concept can be applied to the real world - and when that's possible, it helps improve the students' understanding.
9. Adopt Flipped class technique by sharing the materials / Sample Videos prior to the class and have discussions on the that topic in the succeeding classes
10. Give Programming Assignments

Module-1

Basic Concepts of Number Theory and Finite Fields: Divisibility and The Division Algorithm Euclidean algorithm, Modular arithmetic, Groups, Rings and Fields, Finite fields of the form GF(p), Polynomial Arithmetic, Finite Fields of the Form GF(2^m) (Text 1: Chapter 3)

Teaching-Learning Process	Chalk and Talk, YouTube videos, Flipped Class Technique Programming on implementation of Euclidean algorithm, multiplicative inverse, Finite fields of the form GF(p), construction of finite field over GF(2^m). **RBT Level:** L1, L2, L3

Module-2

Introduction: Computer Security Concepts, A Model for Network Security (Text 1: Chapter 1)
Classical Encryption Techniques: Symmetric cipher model, Substitution techniques, Transposition techniques (Text 1: Chapter 1)

Teaching-Learning Process	Chalk and Talk, YouTube videos, Flipped Class Technique and PPTs. Programming on Substitution and Transposition techniques. Self-study topics: Security Mechanisms, Services and Attacks. **RBT Level:** L1, L2, L3

Module-3

Block Ciphers: Traditional Block Cipher structure, Data encryption standard (DES) (Text 1: Chapter 2: Section1, 2) The AES Cipher. (Text 1: Chapter 4: Section 2, 3, 4)
More on Number Theory: Prime Numbers, Fermat's and Euler's theorem, discrete logarithm. (Text 1: Chapter 7: Section 1, 2, 5)

Teaching-Learning Process	Chalk and Talk, YouTube videos, Flipped Class Technique and PPTs. Implementation of SDES using programming languages like C++/Python/Java/Scilab. Self-study topics: DES S-Box- Linear and differential attacks **RBT Level:** L1, L2, L3

Module-4

ASYMMETRIC CIPHERS: Principles of Public-Key Cryptosystems, The RSA algorithm, Diffie - Hellman Key Exchange, Elliptic Curve Arithmetic, Elliptic Curve Cryptography (Text 1: Chapter 8, Chapter 9: Section 1, 3, 4)

Teaching-Learning Process	Chalk and Talk, YouTube videos, Flipped Class Technique and PPTs. Implementation of Asymmetric key algorithms using programming languages like C++/Python/Java/Scilab Numerical examples on Elliptic Curve Cryptography **RBT Level:** L1, L2, L3

Module-5

Pseudo-Random-Sequence Generators and Stream Ciphers:
Linear Congruential Generators, Linear Feedback Shift Registers, Design and analysis of stream ciphers, Stream ciphers using LFSRs, A5, Hughes XPD/KPD, Nanoteq, Rambutan, Additive generators, Gifford, Algorithm M, PKZIP (Text 2: Chapter 16)

Teaching-Learning Process	Chalk and Talk, YouTube videos, Flipped Class Technique and PPTs. Implementation of simple stream ciphers using programming languages like C++/Python/Java/Scilab. **RBT Level:** L1, L2, L3

Course outcomes (Course Skill Set)
At the end of the course the student will be able to:

1. Explain traditional cryptographic algorithms of encryption and decryption process.
2. Use symmetric and asymmetric cryptography algorithms to encrypt and decrypt the data.
3. Apply concepts of modern algebra in cryptography algorithms.
4. Design pseudo random sequence generation algorithms for stream cipher systems.

Assessment Details (both CIE and SEE)
The weightage of Continuous Internal Evaluation (CIE) is 50% and for Semester End Exam (SEE) is 50%. The minimum passing mark for the CIE is 40% of the maximum marks (20 marks out of 50). A student shall be deemed to have satisfied the academic requirements and earned the credits allotted to each subject/ course if the student secures not less than 35% (18 Marks out of 50) in the semester-end examination (SEE), and a minimum of 40% (40 marks out of 100) in the sum total of the CIE (Continuous Internal Evaluation) and SEE (Semester End Examination) taken together.

Continuous Internal Evaluation:
Three Unit Tests each of **20 Marks (duration 01 hour)**

1. First test at the end of 5th week of the semester
2. Second test at the end of the 10th week of the semester
3. Third test at the end of the 15th week of the semester

Two assignments each of **10 Marks**

4. First assignment at the end of 4th week of the semester
5. Second assignment at the end of 9th week of the semester

Group discussion/Seminar/quiz any one of three suitably planned to attain the COs and POs for **20 Marks (duration 01 hours)**

6. At the end of the 13th week of the semester

The sum of three tests, two assignments, and quiz/seminar/group discussion will be out of 100 marks and will be **scaled down to 50 marks**

(to have less stressed CIE, the portion of the syllabus should not be common /repeated for any of the methods of the CIE. Each method of CIE should have a different syllabus portion of the course).

CIE methods /question paper is designed to attain the different levels of Bloom's taxonomy as per the outcome defined for the course.

Semester End Examination:

Theory SEE will be conducted by University as per the scheduled timetable, with common question papers for the subject (**duration 03 hours)**

1. The question paper will have ten questions. Each question is set for 20 marks.
2. There will be 2 questions from each module. Each of the two questions under a module (with a maximum of 3 sub-questions), **should have a mix of topics** under that module.

The students have to answer 5 full questions, selecting one full question from each module. Marks scored out of 100 shall be reduced proportionally to 50 marks

Suggested Learning Resources:

Text Books:

1. William Stallings , "Cryptography and Network Security Principles and Practice", Pearson Education Inc., 6th Edition, 2014, ISBN: 978-93-325-1877-3
2. Bruce Schneier, "Applied Cryptography Protocols, Algorithms, and Source code in C", Wiley Publications, 2nd Edition, ISBN: 9971-51-348-X.

Reference Books:

1. Cryptography and Network Security, Behrouz A Forouzan, TMH, 2007.
2. Cryptography and Network Security, Atul Kahate, TMH, 2003.

Web links and Video Lectures (e-Resources)

- https://nptel.ac.in/courses/106105031

Activity Based Learning (Suggested Activities in Class)/ Practical Based learning

- Programming Assignments / Mini Projects can be given to improve programming skills

H. O. D.
Dept. Of Electronics & Communica
Alva's Institute of Engg. & Techno
Mijar, MOODBIDRI - 574 225