Mukesh Patel School of Technology Management and Engineering
Computer Engineering Department

Course Policy

<table>
<tr><td><b>Program/Branch/Semester</b></td><td><b>:</b></td><td colspan="2">B Tech/MBA Tech Artificial Intelligence, Computer Engineering, Electronics & Telecommunication Engineering), B Tech (AI and DS and CSBS), V/ VI/VII</td></tr>
<tr><td><b>Academic Year</b></td><td><b>:</b></td><td colspan="2">2023-24</td></tr>
<tr><td><b>Course Code &amp; Name</b></td><td><b>:</b></td><td colspan="2">Cryptography and Network Security (702AI0E007)</td></tr>
<tr><td><b>Credit Details</b></td><td><b>:</b></td><td colspan="2">L T P C
2 0 2 3</td></tr>
<tr><td><b>Course Anchor</b></td><td><b>:</b></td><td colspan="2">Dr. Upendra Verma</td></tr>
<tr><td><b>Contact No. &amp; Email</b></td><td><b>:</b></td><td colspan="2">+91 9096746437
upendra.verma@nmims.edu</td></tr>
<tr><td><b>Office</b></td><td><b>:</b></td><td colspan="2">MPSTME, B-Wing, Second Floor, Faculty Area-I, Shirpur Campus</td></tr>
<tr><td><b>Office Hours</b></td><td><b>:</b></td><td colspan="2">10:00 to 05:00 PM</td></tr>
<tr><td><b>Student Contact Hrs.</b></td><td><b>:</b></td><td colspan="2">9.00 to 10 AM (everyday)</td></tr>
<tr><td colspan="4"><b>Other Course Faculty members teaching this course:</b></td></tr>
<tr><td colspan="3"><b>Course Faculty:</b> Dr. Ami Munshi
<b>Contact No. & Email:</b> 9819859405/Ami.Munshi@nmims.edu
<b>Office:</b> Mumbai Campus
<b>Office Hours:</b> 10 to 6 PM
<b>Student Contact Hours:</b> Tues &amp; Fri- 02 to 03 PM</td><td><b>Course Faculty:</b> Prof. Ratnesh Chaturvedi
<b>Contact No. & Email:</b> 7977851980/ Ratnesh.Chaturvedi@nmims.edu
<b>Office:</b> Mumbai Campus
<b>Office Hours:</b> 10 to 06 PM</td></tr>
<tr><td colspan="3"><b>Course Faculty:</b> Dr. Atul Thakare
<b>Contact No. & Email:</b> 8767829219/atul.thakare@nmims.edu
<b>Office:</b> Navi Mumbai
<b>Office Hours:</b> 10 to 05 PM
<b>Student Contact Hours:</b> Wed &amp; Thur- 04 to 05 PM</td><td><b>Course Faculty:</b> Prof. Abhay Deep Seth
<b>Contact No. & Email:</b> 9981721822/abhaydeep.seth@nmims.edu
<b>Office:</b> Indore
<b>Office Hours:</b> 10 to 05 PM
<b>Student Contact Hours:</b> Fri &amp; Sat- 04 to 05 PM</td></tr>
<tr><td colspan="4"><b><i>Queries by Emails are encouraged.</i></b></td></tr>
<tr><td><b>Course link</b></td><td><b>:</b></td><td colspan="2">Portal Link
MS Teams Link:</td></tr>
</table>

1 Introduction to the Course

1.1 Importance of the course

Cryptography is an information security tactic used to protect enterprise information and communication from cyber threats through the use of codes. This practice refers to secure information and communication techniques derived from mathematical concepts and a set of rule-based calculations, called algorithms, to transform messages in ways that are hard to decipher. Cryptography achieves several information security-related objectives including confidentiality, integrity, and authentication, and non-repudiation. Individuals and organizations use cryptography on a daily basis to protect their privacy and keep their conversations and data confidential.

1.2 Objective of the Course

This course introduces concepts in cryptography and computer security and discusses both their theoretical foundations and practical applications. It also provides fundamental knowledge on various aspects of network and system Security

1.3 Pre-requisite

- Computer Networks

2 Course Outcomes (CO) and mapping with Program Outcomes (PO)

2.1 Course Outcomes

After successful completion of the course, a student will be able to-

CO1: Explain and analyze symmetric key encryption and decryption.

CO2: Use asymmetric key cryptography for data encryption.

CO3: Describe various techniques of network security.

CO4: Discuss various system security mechanisms.

2.2 Program Outcomes

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 modelling 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.

2.3 CO-PO Mapping

	PO1	**PO2**	**PO3**	**PO4**	**PO5**	**PO6**	**PO7**	**PO8**	**PO9**	**PO10**	**PO11**	**PO12**
CO1	1	3	2	1	2							
CO2	1	3	2	1	2							
CO3	2	2	2	1	1							
CO4	1	2	1		2			1				

1- Low, 2- Medium, 3-High

3. Syllabus, Pre-class activity and References

3.1 Teaching and evaluation scheme

Teaching Scheme				Evaluation Scheme	
Lecture Hours per week	**Practical Hours per week**	**Tutorial Hours per week**	**Credit**	**Internal Continuous Assessment (ICA) As per Institute Norms (50 Marks)**	**Theory (3 Hrs., 100 Marks)**
2	2	0	3	Marks Scaled to 50	Marks Scaled to 50

3.2 Syllabus

Unit	Description	Duration
1	**Introduction of Data Encryption** Need for Data encryption, Goal of Security: confidentiality, integrity, authentication, Security attacks: Active, Passive attacks, Cryptanalytic and non-cryptanalytic. Classical techniques: Substitution ciphers, Transposition ciphers, Symmetric and asymmetric encryption.	**02**
2	**Symmetric Key encryption** **Data Encryption Standard (DES)** Structure, Key generation, Encryption and Decryption, 2-DES, triple DES, confusion and Diffusion, Avalanche attack. **Advanced Encryption Standard (AES)** Algebraic structures, GF(2^8) fields, AES structure, round functions, key expansion, Encryption and Decryption, AES Security: Avalanche attack, confusion and Diffusion, Key management: Kerberos	**10**
3	**Asymmetric Key encryption** Number theory and Modular arithmetic: Primality testing Fermat's and Euler's theorems, Order of a number, Primitive roots, Euclidean and Extended Euclidean Algorithm, Principles of public key cryptosystems, RSA algorithm, Diffie-Hellman key exchange	**05**
4	**Message Integrity and message Authentication** Message authentication codes (MAC), Hash functions, SHA-512, digital signatures	**02**
5	**Network Security** Need for Security of Computer Networks, Transport layer security: Secure Socket Layer (SSL), IP Security: transport and tunnel modes, E-mail Security: PGP and S/MIME.	**05**
6	**System Security** Users, Trust and Trusted systems, Buffer overflow and malicious software, worms, viruses, denial of service attacks, Firewalls: construction and working principals, Intrusion detection systems, Introduction to SIEM (Security Information and Event Management) technology.	**06**

	Total hours	**30**

3.3 Pre-class activity

Outline for a preliminary study for each unit will be provided before the commencement of each unit. Preliminary study material (video links, presentation, notes, etc.) will be available on the student portal. Students are expected to go through this material before attending the upcoming session. It is expected that the students put in at least two hours of self-study for every one hour of classroom teaching. More emphasis will be given on in-depth topics, practical applications, and doubt solving during the lecture session.

3.4 References

Text Books

1. William Stallings, Cryptography and Network Security, 7th edition, Pearson Publication, 2017.
2. Behrouz A. Forouzan and Debdeep Mukhopadhyay, Cryptography and Network Security, 3rd edition, Mc Graw Hill, 2015.

Reference Books:

1. Wade Trappe and Lawrence C Washington, Introduction to Cryptography with Coding Theory, 3rd Edition, Pearson Education, 2020.
2. Wanbo Mao, Modern Cryptography: Theory and Practice, 4 th Edition, Pearson Education, 2011.

4 Laboratory details

4.1 Experiment List

Knowledge of C/ C++/ Java/ Python programming for laboratory exercise is a prerequisite. Students are expected to recall the fundamental theory concepts relevant to the exercise to be performed in the upcoming laboratory.

Sr. No.	Title	CO mapping
1	Implementation of Caesar cipher (Substitution technique) and Rail fence (Transposition technique).	CO-1
2	Demonstrate the use of DES and Implementation of DES encryption with two rounds.	CO-1
3	Demonstrate the use of AES and Implementation of AES encryption using the 128 bit-key size.	CO-1
4	Demonstrate the use of Asymmetric Key Encryption and Implementation of RSA cryptosystem	CO-2

5	Demonstrate the used of Diffie-Hellman Key Exchange algorithm and Implementation of Diffie-Hellman algorithm	CO-2
6	Show the difference between conventional and digital signature. Implementation of digital signature using RSA cryptosystem.	CO-2
7	Show the working of MAC and Implementation of Message Authentication Code (MAC).	CO-1
8	To install Wireshark tool (Network Protocol Analyzer) and Explore the various functionalities of Wireshark.	CO-3
9	To install network mapping tool (NMAP) and explore the various functionalities of NMAP.	CO-3
10	Demonstrate the use of Firewall and Intrusion Detection System.	CO-4

4.2 Deadlines for the Lab Work Submission

Experiment No. 1	**Submission Deadline**
Experiment No. 1	29 July 2023
Experiment No. 2	05 August 2023
Experiment No. 3	12 August 2023
Experiment No. 4	26 August 2023
Experiment No. 5	02 September 2023
Experiment No. 6	09 September 2023
Experiment No. 7	13 September 2023
Experiment No. 8	23 September 2023
Experiment No. 9	30 September 2023
Experiment No. 10	07 October 2023

5 Assessment Policy

5.1 Component wise Continuous Evaluation Internal Continuous Assessment (ICA) and Term End Examination (TEE)

Assessment Component					TEE (100 marks) (Marks scaled to 50)
	Lab Performance and Viva	**Demonstration of Security Tools or Research based Paper Presentation**	**MTT-1 and MTT-2**	**Quiz and Assignment**	
Weightage	20%	20%	40%	20%	100%
Marks	10	10	10+10	10	50
Time Line	Weekly	13-14th Week	MTT-1 (Week-6) and MTT-2 (Week-12)	Assignment (Before MTT1 and MTT2) and Quiz (After MTT1 and MTT2)	November

5.2 Assessment Policy for Internal Continuous Assessment (ICA)

Assessment of ICA comprises of the following components.

5.2.1 Class test 1 and 2 (10+10)

a. Two class tests will be conducted as per the academic calendar.
b. It will be conducted offline for 10 marks each

5.2.2 Lab performance evaluation and Viva (10 marks)

i. Continuous assessment for laboratory experiments will be conducted. There are 10 practicals', each carrying weightage of 10 marks. At the end of the course, average of total marks will be taken to obtain marks out of 10.

ii. Discussion of your work with your peers is allowed. However, each student is expected to submit his/her original work. Submissions which are very similar will be marked zero. Assessment of the lab works will be carried out based on parameters like timely completion of lab work file, understanding of the experiment performed, originality in the work, involvement of the student, regularity, discipline etc. during the session. There is a 30% penalty on late submission.

5.2.3 Demonstration of Open-Source Security Tool or Research based Paper Presentation Viva (10 marks):

Students need to make group of 2 or 3 members and can take an approved open source security tool. In group they can show demonstration to the class and answer Q/A by faculty. Demonstration carries 10 marks and Q/A carries 10 marks. OR Identify a journal/IEEE conference research paper based on the topic relevant to the course, Get the topic approval, Present the paper, d. Assessment will be based on the topic selection, understanding, content depth during presentation.

5.2.4 Quiz and Assignment (10 marks):

Every student will be asked to submit two assignments and two quizzes based on a topic from the course. This activity will be evaluated from 10 marks. There is a 30% penalty on late submission (If you submit with a delay of 2 days, afterwards 100% deduction).

5.3 Assessment Policy for Term End Examination (TEE)

A written examination of 100 marks for 3 Hours duration will be conducted for the course as per the academic calendar.

6. Lesson Plan

Session No.	Topics	Mapped CO	Reference
1	Introduction of Data Encryption (Unit1) Need for Data encryption, Goal of Security: confidentiality, integrity, authentication, Security attacks: Active, Passive attacks, Cryptanalytic and non-cryptanalytic.	CO1/2	TB1, TB2
2	Classical techniques: Substitution ciphers, Transposition ciphers, Symmetric and asymmetric encryption	CO1/2	TB1, TB2
3	Symmetric Key encryption (Unit2) Data Encryption Standard (DES)Structure Key generation	CO1	TB1, TB2
4	Data Encryption Standard (DES) Structure Key generation	CO1	TB1, TB2
5	Encryption and Decryption	CO1	TB1, TB2
6	2-DES, triple DES, confusion and Diffusion, Avalanche attack.	CO1	TB1, TB2
7	Advanced Encryption Standard (AES) Algebraic structures,	CO1	TB1, TB2
8	GF(28) fields, AES structure, round functions, key expansion,	CO1	TB1, TB2
9	Encryption and Decryption,	CO1	TB1, TB2
10	Midterm Test 1 [(21st -26th August)		
11	AES Security: Avalanche attack, confusion and Diffusion	CO1	TB1, TB2

12	Key management: Kerberos.	CO1	TB1, TB2
13	Asymmetric Key encryption (Unit3) Number theory and Modular arithmetic: Primality testing Fermat's and Euler's theorems	CO2	TB1, TB2
14	Order of a number, Primitive roots,	CO2	TB1, TB2
15	Euclidean and Extended Euclidean Algorithm	CO2	TB1, TB2
16	Principles of public key cryptosystems, RSA algorithm,	CO2	TB1, TB2
17	Diffie-Hellman key exchange	CO2	TB1, TB2
18	Message Integrity and message Authentication (Unit4) Message authentication codes (MAC),	CO2	TB1, TB2
19	Hash functions,	CO2	TB1, TB2
20	SHA-512, digital signatures	CO2	TB1, TB2
21	Network Security (Unit5) Need for Security of Computer Networks,	CO3	TB1, TB2
22	Midterm Test 2 (3rd-10th October)		
23	Transport layer security: Secure Socket Layer (SSL),	CO3	TB1, TB2
24	IP Security: transport and tunnel modes,	CO3	TB1, TB2
25	E-mail Security: PGP and S/MIME	CO3	TB1, TB2
26	System Security Users, Trust and Trusted systems,	CO4	TB1, TB2
27	Buffer overflow and malicious software, worms, viruses, denial of service attacks,	CO4	TB1, TB2
28	Firewalls: construction and working principals,	CO4	TB1, TB2
29	Intrusion detection systems	CO4	TB1, TB2
30	Introduction to SIEM (Security Information and Event Management) technology	CO4	TB1, TB2

7 Teaching-learning methodology

Faculty will make a group of 2-3 students for any group based activity such as demonstation of security tools, research paper based presentation etc. Lecture and laboratory session will be conducted as follows-

1. **Lectures:**
    - Outline for preliminary study to be done for each unit will be provided prior to commencement of each unit.

  - Deeper concepts and applications will be explained through Presentation and Video Lectures.

2. **Laboratory:**
    - Lab manual consisting of theory and algorithm to support the lab experiment will be uploaded on student portal.
    - Regular lab assessment and grading will be done. Students will be marked based on parameters like completion of lab assignment, originality, logic developed, interaction during the lab, submission, punctuality and discipline

8. Active learning techniques

Active learning is a method of learning in which students are actively or experientially involved in the learning process. Following active learning techniques will be adopted for the course.

1. **Muddiest topic:** Faculty will find out the least understood point/topic in the session. This topic is then further explained to ensure that it is understood well.
2. **The "One Minute Paper":** The faculty will ask students to take out a blank sheet of paper, pose a question (either specific or open-ended), and give them one (or perhaps two - but not many) minute(s) to respond.
3. **Blended Learning:** Students will be introduced to the topic at home while the in-depth topics, applications and numerical problems will be discussed by the faculty in the lecture session. Outline for preliminary study to be done for each unit will be provided prior to commencement of each unit. Preliminary study material (video links, presentation, notes etc) will be made available on the student portal.
4. **Frame a question: S**tudent will be asked to design and frame their own questions pertaining to the topic being taught. The idea is to stimulate students' curiosity, engage the students in collaborative teaching and learning, and motivating students to develop deeper understating of the topic.
    - Frame questions for each unit of the course: At the beginning of each using, the faculty will create a new page in *OneNote Class Notebook* in collaborative section where every student will post his/her question.
    - Frame a question in lab: As discussed in section 6.2, student will be asked to design one unique lab problem based on the course syllabus.
5. **Brainstorming: S**tudents will be asked to generate ideas on a certain topic, category or question while the faculty will facilitate and record the answers on the blackboard/whiteboard.

9. Course Material

Following course material is uploaded on the student portal: (give student portal link)

- Course Policy
- Lecture Notes

- Lecture Videos
- Lecture Presentations
- Books / Reference Books / NPTEL video lectures link
- Assignments
- Lab Manuals, Test images database link
- List of Program Outcomes

10. Course Outcome Attainment

Following means will be used to assess attainment of course learning outcomes.

- Use of formal evaluation components of continuous evaluation, assignments, laboratory work, semester end examination
- Informal feedback during course conduction

11. Academic Integrity Statement

Students are expected to carry out assigned work under Internal Continuous Assessment (ICA) independently. Copying in any form is not acceptable and will invite strict disciplinary action. Evaluation of corresponding component will be affected proportionately in such cases. Plagiarism detection software will be used to check plagiarism wherever applicable. Academic integrity is expected from students in all components of course assessment.