Department of Artificial Intelligence and Machine Learning

Academic Year	:	2026-2027	Course Name	:	Data Security and Privacy
Semester	:	VII	Course Code	:	**BAD703**
Scheme	:	2022	L: T: P: S(Credits)	:	4:0:0:3(4-Credits)
Total Contact hours	:	50	CIE Marks	:	50
Course Plan Author	:	Mr. Asghar Pasha	SEE Marks	:	50
Date	:	27.6.2026	Total Marks	:	100

Self-Study Hours: 70 hrs

- Directed study: 45 hrs (e-notes + book chapters)
- Tools Learning 5 hrs (**Wireshark, Steghide**)
- Assignments: 5 hrs (Quizes(3) + Implementation and Demo)
- Assessment prep: 10 hrs (IA+SEE)
- University Question paper solving: 5 hrs

Course Prerequisites:

- Basics of OS,Computer Network and Security

Learning Objectives:

1.Understand the basics of, Security, its principle and Cryptography
2.To study varios symmetric and asymmetric cryptographic Algorithm
3. Apply the knowlwdge of Cryptography to various fields
4. Study the key management system
5. Understand the necessity of data security

Course Outcomes:

CO		*At the end of the course, student should be able to . . .*	**Blooms' Level**
CO1	:	Explain the basic concepts of Security and Cryptography	L3
CO2	:	Use various Cryptographic Algorithms	L3
CO3	:	Describe various key management scenarios.	L2
CO4	:	Explain about IP security and Web security.	L2
CO5	:	Apply the Data security concepts for Text and images.	L3

Blooms' Taxonomy:

L1	L2	L3	L4	L5	L6
Remembering	Understanding	Applying	Analyzing	Evaluating	Creating

Program Outcomes:

PO1	:	Engineering knowledge	**PO7**	:	Environment and sustainability
PO2	:	Problem analysis	**PO8**	:	Ethics
PO3	:	Design/development of solutions	**PO9**	:	Individual and team work
PO4	:	Conduct investigations of complex problems	**PO10**	:	Communication
PO5	:	Modern tool usage	**PO11**	:	Project management and finance
PO6	:	The engineer and society	**PO12**	:	Life-long learning

Program Specific Outcomes:

PSO1:	Graduates will have the ability to adapt, contribute and innovate ideas in the field of Artificial Intelligence and Machine Learning
PSO2:	To provide a concrete foundation and enrich their abilities to qualify for Employment, Higher studies and Research in various domains of Artificial Intelligence and Machine Learning such as Data Science, Computer Vision, Natural Language Processing with Ethical Values.
PSO3:	Graduates will acquire the practical proficiency with niche technologies and open-source platforms and to become Entrepreneur in the domain Artificial Intelligence and Machine Learning.

CO-PO-PSO Mapping:

CO	Program Outcomes														
	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO11	PO 12	PSO 1	PSO 2	PSO 3
CO1	3	2	-	_	_	-	-	-	_	_	_	1	1	2	1
CO2	3	3	2	_	_	-	-	-	_	_	_	1	2	2	1
CO3	3	2	2	_	_	-	-	-	_	_	_	1	2	2	1
CO4	3	2	-	_	_	-	-	-	_	_	_	1	1	2	1
CO5	3	3	3	_	2	-	-	-	_	_	_	1	3	3	3

CO	PO / PSO	Wt.age	Justification
CO1	PO1	3	Explaining the network security model, symmetric cipher model, and classical encryption techniques requires strong foundational knowledge of mathematics, computer science principles, and algorithmic logic.
	PO2	2	Understanding the rationale behind cryptographic primitives involves identifying security threats and vulnerabilities, requiring basic problem analysis skills.
	PO12	1	The rapidly evolving nature of security threats necessitates continuous learning of new cryptographic concepts, though at the introductory level this is minimal.
	PSO1	1	Basic cryptographic concepts provide foundational knowledge, but direct innovation in AI/ML from this introductory level is limited.
	PSO2	2	A strong understanding of cryptography fundamentals is essential for pursuing higher studies and research in secure AI/ML domains.
	PSO3	1	While foundational, this knowledge is a prerequisite for practical proficiency in secure system development.

CO	PO / PSO	Wt.age	Justification
CO2	PO1	3	Analyzing algorithms like DES, RSA, Diffie-Hellman, and ECC requires deep mathematical understanding of number theory, modular arithmetic, finite fields, and computational complexity.
	PO2	3	Analyzing cryptographic algorithms involves breaking down their structure, identifying strengths and weaknesses, comparing computational efficiency, and evaluating security vulnerabilities.
	PO3	2	Understanding design principles of block ciphers (confusion/diffusion) and public-key systems enables students to make informed design choices when developing secure systems.
	PO12	1	New cryptographic attacks emerge regularly, requiring ongoing learning to stay current with algorithm vulnerabilities and improvements.

CO	PO / PSO	Wt.age	Justification
	PSO1	2	Analyzing cryptography enables innovation in privacy-preserving AI/ML techniques, such as homomorphic encryption and secure multi-party computation.
	PSO2	2	Advanced algorithm analysis is critical for research in secure AI/ML domains, including developing novel encryption methods for data protection.
	PSO3	1	Understanding algorithm internals contributes to proficiency in implementing secure solutions, though direct entrepreneurial application is limited.

CO	PO / PSO	Wt.age	Justification
CO 3	PO1	3	Key management involves understanding cryptographic protocols, key generation algorithms (LCG, BBS), storage mechanisms, and lifecycle processes—all rooted in engineering principles.
	PO2	2	Describing key management scenarios involves understanding security challenges like key distribution, storage security, and lifecycle management, requiring problem analysis skills.
	PO3	2	Understanding key management fundamentals enables students to design secure key handling procedures in system development.
	PO12	1	Key management standards and best practices evolve with new threats and technologies, requiring ongoing professional development.
	PSO1	2	Key management is crucial for secure AI/ML systems, including model encryption, secure parameter storage, and privacy-preserving data sharing.
	PSO2	2	Deep understanding of key management is essential for advanced research in secure AI/ML architectures and data protection strategies.

CO	PO / PSO	Wt.age	Justification
	PSO3	1	Implementing key management securely is a practical skill needed for developing secure AI products, though entrepreneurial application is indirect.

CO	PO / PSO	Wt.age	Justification
CO 4	PO1	3	IP Security (IPSec, ESP, IKE) and Web Security (TLS) involve complex networking protocols, cryptographic algorithms, and security architectures—demanding strong engineering knowledge.
	PO2	2	Understanding security policies, combining security associations, and Transport Layer Security involves analyzing network vulnerabilities and identifying appropriate countermeasures.
	PO12	1	Web and IP security protocols continuously evolve with emerging threats, requiring lifelong learning to maintain currency in security practices.
	PSO1	1	Understanding network security provides foundational knowledge for AI/ML deployment security (model APIs, data in transit), but direct innovation impact is limited.
	PSO2	2	Network security knowledge is critical for research in secure distributed AI/ML systems, federated learning, and edge computing applications.
	PSO3	1	Practical implementation of secure web and IP services is a valuable skill for AI product development, though entrepreneurial application is indirect.

CO	PO / PSO	Wt.age	Justification
CO 5	PO1	3	Applying data hiding techniques like LSB encoding, BPCS Steganography, and watermarking involves fundamental knowledge of digital signal processing, image processing, and information theory.
	PO2	3	Applying data security concepts requires analyzing text and image properties to select appropriate hiding mechanisms, evaluating capacity vs. robustness trade-offs, and solving real-world security problems.
	PO3	3	Implementing data security solutions for text and images involves designing embedding schemes, developing watermarking strategies, and creating robust data protection mechanisms.
	PO5	2	Practical application of LSB encoding, BPCS, and lossless data hiding requires familiarity with programming tools, image processing libraries, and simulation environments.
	PO12	1	New data hiding techniques and attack methods emerge continuously, necessitating ongoing learning to maintain effective data protection strategies.
	PSO1	3	Data security in text and images is directly applicable to AI/ML data pipelines—protecting training data, watermarking AI-generated content, and innovating privacy-preserving data sharing methods.
	PSO2	3	Data hiding and watermarking are critical research areas in AI/ML, including copyright protection for generative AI and robust training data management.
	PSO3	3	Hands-on implementation of steganography and watermarking provides practical proficiency with niche technologies, enabling entrepreneurial ventures in secure AI products.

Course Content (Syllabus)

Module 1	**CH**
A model for Network Security, Classical encryption techniques: Symmetric cipher model, Substitution ciphers-Caesar Cipher, Monoalphabetic Cipher, Playfair Cipher, Hill Cipher, Polyalphabetic Ciphers, One time pad, Steganography Block Ciphers and Data Encryption Standards: Traditional Block Cipher structures, data Encryption Standard (DES), A DES Example, The strength of DES, Block cipher design principles Text book 1:Chapter 1: 1.8 Chapter 3: 3.1, 3.2, 3.5 Chapter 4: 4.1, 4.2, 4.3, 4.4, 4.5	**10**
Module 2	
Pseudorandom number Generators: Linear Congruential Generators, Blum Blum Shub Generator Public key cryptography and RSA: Principles of public key cryptosystems-Public key cryptosystems, Applications for public key cryptosystems, Requirements for public key cryptography, Public key Cryptanalysis, The RSA algorithm: Description of the Algorithm, Computational aspects, The Security of RSA Diffie-Hellman key exchange: The Algorithm, Key exchange Protocols, Man-in-the-middle Attack, Elliptic Curve Cryptography: Analog of Diffie-Hellman key Exchange, Elliptic Curve Encryption/Decryption, Security of Elliptic Curve Cryptography Text book 1: Chapter 8: 8.2 Chapter 9: 9.1, 9.2 Chapter 10: 10.1, 10.4	**10**
Module 3	
Key management fundamentals, Key lengths and lifetimes, Key generation, Key establishment, Key storage, Key usage, Governing key management. Public-Key Management: Certification of public keys, The certificate lifecycle, Public-key management models, Alternative approaches. Text book 2: Chapter 10, Chapter 11	**10**
Module 4	
Web security consideration, Transport layer security. IP Security: IP Security overview, IP Security Policy, Encapsulating Security Payload, Combining security associations, Internet key exchange. Text book1:Chapter 17: 17.1, 17.2 Chapter 20: 20.1, 20.2, 20.3 20.4, 20.5	**10**
Module 5	
Data Security: Data hiding in Text-Basic features, Applications of data hiding, Watermarking, Intuitive Methods, Simple Digital methods, Data hiding in Text, Innocuous Text, Mimic Functions. Data hiding in Images: LSB encoding, BPCS Steganography, Lossless data hiding Textbook 3:Chapter 10: 10.1, 10.2, 10.3, 10.4, 10.5, 10.6, 10.7, 10.8 Chapter 11: 11.1, 11.2, 11.3	**10**

Schedule of Instruction:

Class No.	Topic	Date	RBT	CO	Mode
Module-1: Classical Encryption & DES (CO1, CO2)					
1	Introduction to the Course, CO's, PO's, Assignment Date, etc	20/7/2026	L2	1	Lecture
2	A model for Network Security, Classical encryption techniques: Symmetric cipher model	21/7/2026	L2	1	Interactive Lecture +PPT
3	Substitution ciphers – Caesar Cipher	22/7/2026	L2	1	
4	Monoalphabetic Cipher	23/7/2026	L2	1	Interactive Lecture
5	Hill Cipher	27/7/2026	L2	1	Interactive Lecture
6	Polyalphabetic Ciphers (Vigenère)	28/7/2026	L2	1	Interactive Lecture
7	One Time Pad, Steganography	29/7/2026	L2	1	Interactive Lecture
8	Block Ciphers and Data Encryption Standards: Traditional Block Cipher structures	30/7/2026	L2	1	Interactive Lecture

Class No.	Topic	Date	RBT	CO	Mode
9	Data Encryption Standard (DES), A DES Example, The strength of DES	3/8/2026	L3	2	Interactive Lecture
10	Data Encryption Standard (DES), A DES Example, The strength of DES(continued)	4/8/2026	L3	2	Interactive Lecture
Module-2: Public Key Cryptography & RSA (CO1, CO2)					
11	Pseudorandom Number Generators: Linear Congruential Generators, Blum Blum Shub Generator	5/8/2026	L2	2	Interactive Lecture + PPT
12	Public key cryptography and RSA: Principles of public key cryptosystems	6/8/2026	L2	2	Interactive Lecture
13	Applications for public key cryptosystems, Requirements for public key cryptography, Public key Cryptanalysis	10/8/2026	L3	2	Interactive Lecture
14	The RSA algorithm: Description of the Algorithm, Computational aspects, The Security of RSA	11/8/2026	L4	2	Interactive Lecture
15	Diffie-Hellman key exchange: The Algorithm, Key exchange Protocols	12/8/2026	L2	2	Interactive Lecture
16	Diffie-Hellman key exchange: The Algorithm, Key exchange Protocols(continued)	13/8/2026	L2	2	Interactive Lecture

Class No.	Topic	Date	RBT	CO	Mode
17	Man-in-the-Middle Attack	17/8/2026	L2	2	Interactive Lecture + Demo
18	Elliptic Curve Cryptography: Analog of Diffie-Hellman key Exchange	18/8/2026	L2	2	Interactive Lecture +PPT
19	Elliptic Curve Encryption/Decryption	19/8/2026	L3	2	PPT + Interactive Lecture
20	Security of Elliptic Curve Cryptography	20/8/2026	L2	2	Interactive Lecture +PPT
Module-3: Key Management (CO3)					
21	Key management fundamentals	24/8/2026	L2	3	Interactive Lecture +PPT
22	Key lengths and lifetimes	25/8/2026	L2	3	Interactive Lecture +PPT
23	Key generation	27/8/2026	L2	3	Interactive Lecture +PPT
24	Key establishment	31/8/2026	L2	3	Interactive Lecture +PPT
25	Key storage, Key usage	1/9/2026	L2	3	Interactive Lecture +PPT
26	Scheme & solution Discusion	2/9/2026	-	1,2,3	-

Class No.	Topic	Date	RBT	CO	Mode
27	Governing key management	3/9/2026	L2	3	Interactive Lecture +PPT
28	Public-Key Management: Certification of public keys	7/9/2026	L2	3	Interactive Lecture +PPT
29	The certificate lifecycle	8/9/2026	L2	3	Interactive Lecture +PPT
30	Public-key management models	9/9/2026	L2	3	Chalk & Board
31	Alternative approaches	14/9/2026	L2	3	Interactive Lecture +PPT
Module-4: IP Security & Web Security (CO4)					
32	Web security considerations	16/9/2026	L2	4	Interactive Lecture +PPT
33	Transport Layer Security (TLS)	17/9/2026	L2	4	Chalk & Board
34	Transport Layer Security (continued)	21/9/2026	L2	4	Interactive Lecture +PPT
35	IP Security: IP Security overview	22/9/2026	L2	4	Interactive Lecture +PPT
36	IP Security Policy	23/9/2026	L2	4	Interactive Lecture +PPT

Class No.	Topic	Date	RBT	CO	Mode
37	IP Security Policy (continued)	24/9/2026	L2	4	Interactive Lecture +PPT
38	Encapsulating Security Payload (ESP)	28/9/2026	L2	4	Interactive Lecture +PPT
39	Combining Security Associations	29/9/2026	L2	4	Interactive Lecture +PPT
40	Internet Key Exchange (IKE)	30/9/2026	L2	4	Interactive Lecture +PPT
41	Internet Key Exchange (IKE) (continued)	1/10/2026	L2	4	Interactive Lecture +PPT
Module-5: Data Security (Text & Images) (CO5)					
42	Data Security: Data hiding in Text - Basic features	5/10/2026	L2	5	Interactive Lecture +PPT
43	Applications of data hiding	6/10/2026	L3	5	Interactive Lecture +PPT
44	Watermarking	7/10/2026	L3	5	Interactive Lecture +PPT
45	Intuitive Methods	8/10/2026	L3	5	Interactive Lecture +PPT

Class No.	Topic	Date	RBT	CO	Mode
46	Simple Digital methods	12/10/2026	L3	5	Interactive Lecture +PPT
47	Data hiding in Text	13/10/2026	L3	5	Interactive Lecture +PPT
48	Innocuous Text, Mimic Functions	14/10/2026	L3	5	Interactive Lecture +PPT
49	Data hiding in Images: LSB encoding	15/10/2026	L3	5	Interactive Lecture +PPT + Demo
50	BPCS Steganography, Textstego and Styleuxx tool	22/10/2026	L3	5	Interactive Lecture +PPT + Demo
51	Lossless data hiding	29/10/2026	L3	5	Interactive Lecture +PPT
52	Revision	2/11/2026	-	1-5	Interactive Lecture +PPT

Textbooks:

T1	Cryptography and Network Security", William Stallings, Pearson Publication, Seventh Edition.
T2	Everyday Cryptography: Fundamental Principles and Applications Keith M. Martin Oxford Scholarship Online: December 2013.
T3	Data Privacy and Security, Salomon, David, Springer, 2003.

Reference books:

R1	Cryptography and Network Security, Behrouz A Forouzan, Dedeep Mukhopadhyay,

	TMH, 2nd edition, 2013
R2	Information Security: Principles and practice, Mark Stamp, Wiley Inter Science, 2011

Web links and Video Lectures (e-Resources):

1.	https://sites.google.com/view/easgwebsite/home
2.	https://www.youtube.com/watch?v=R9eerqP78PE - **RSA Algorithm**- Create public and private key for secure communication
3.	https://www.youtube.com/watch?v=J1RmZZEkN0k - **AES Encryption/Decryption** (1) : Creating Secret Keys to encrypt a message
4.	https://www.youtube.com/watch?v=wgGvSwrRHV8 - **DES algorithm** implementation

Assessment Schedule:

S.N.	Assessment Type	Content	CO	Duration	Marks	Date
1.	IA-1	Module 1, 2 & 3(first half)	CO1,CO2, CO3	1:30 hr	50	
2.	IA-2	Module 3(second half),4 &5	CO3,CO4, CO5	1:30 hr		
				IA Scaled down to	25	
				IA Theory component	25	
3.	Quiz-1 Quiz-2 Quiz-3	Module-1 Module-2 Module-4&5	CO1,2,4, CO5	30 MCQ's per Quiz	15	
4.	Implementation of **RSA or DES** using any programming language and simulation	Module-3	CO3	-	10	

	using a suitable tool					
				Assessment Total	25	
				Total (IA + Assessment)	50	
5.	Semester End Examination	Module 1-5	CO1-5	3: 0 hrs	100	
				SEE Scaled down to	50	
				Total (IA+ SEE)	100	

Faculty In charge **Course Coordinator** **HoD**