University of Asia Pacific (UAP)

Department of Computer Science and Engineering (CSE)

BSc in CSE Program

Course Outline – Computer and Cyber Security

Part A – Introduction

1. **Course No. / Course Code** : CSE 317
2. **Course Title** : Computer and Cyber Security
3. **Course Type** : Core
4. **Level/Term and Section** : 3rd Year 2nd semester
5. **Academic Session** : Spring 2025
6. **Course Instructor** : **Dr. Md Towfiqur Rahman,**
   Dr. Subhra Prosun Paul
   Email : towfiq@uap-bd.edu
   subhra@uap-bd.edu
   Consultation Hours : Monday (9:30 to 11:00 and 2:00 to 3:20)
7. **Pre-requisite (If any)** : N/A
8. **Credit Value** : 3.0
9. **Contact Hours** : 3.0
10. **Total Marks** : 100
11. **Course Objectives and Course Summary:**
    Rationale of the Course: Required course in the CSE program. This course builds on the fundamental concepts of cryptography, computer security, and cyber security. Standard methodologies and tools for the evaluation and application of organizational security policies related to confidentiality, integrity, and availability will also be covered.

12. Course Learning Outcomes: At the end of the course, student will be able to-

CLO No.	CO Statements: Upon successful completion of the course, students should be able to:	Corresponding PLOs (Appendix-1)	Bloom's taxonomy domain/level (Appendix-2)	Delivery methods and activities	Assessment Tools
CLO1	**Explain** the basic concepts related to computer security, ethical hacking and identify the security vulnerabilities of networked systems and Digital Forensics.	1	Understand	Lecture, Classwork, Assignments	Quiz, Written exam
CLO2	**Apply** cryptographic algorithms for authentication, cryptanalysis, and steganography.	2	Apply	Lecture, Designing Flowcharts	Quiz, Written exam
CLO3	**Analyze** authentication keys, digital signatures and the security threats on networked systems, assess the existing	4	Analyze	Lecture, Q&A	Assignment, Written exam, Quiz

	state of security, and deduce realistic security policies.				
CO4	**Design** realistic prevention of intrusion and disaster recovery solutions; thus, able to write policy and action reports.	3	Development	Problem Solving, Practice sessions	Online Contest, Assignment, Written exam, Quiz

13. Mapping/ Alignment of CLOs to Program Learning Outcomes (PLOs):

	PLO 1	PLO 2	PLO3	PLO 4	PLO 5	PLO 6	PLO 7	PLO 8	PLO 9	PLO10	PLO11	PLO 12
CLO1	√											
CLO2		√										
CLO3				√								
CLO4			√									

Part B – Content of the Course

14. Course Content:

Introduction to the Fundamental Concepts of Computer Security; Well-known attack types and vulnerabilities; Social engineering attacks; Cryptography and classical cryptosystems; Authentication protocols and public key infrastructure; IPSec, VPNs, E-commerce issues; Attack classification and vulnerability analysis; Security models and policy issues; Security evaluation and auditing of networked systems; intrusion detection, prevention, response, containment (Digital Forensic Evidence) and disaster recovery; Network defense tools: Firewalls, VPNs, intrusion detection, and filters. Cyber-attack, data incident handling, new approaches to management of cybersecurity and new threats, vulnerabilities and controls.

Prerequisite: ~~Computer Networks~~

15. Alignment of the topics with CLOs

16. Class Schedule/Lesson Plan/Weekly plan:

Weeks	Topics / Content	CLO	Delivery methods	Materials
1	Topics of Discussion Basic computer and network security requirements for maintaining a system. Needs of computer security in the private and public networks,	CLO1	Lecture, Multimedia	Slides PDF
2	Application of network security in real life, case study (Equifax, Colonial Pipeline, Bangladesh Bank Reserve Heist, cyber warfare)			
3	CIA triad (confidentiality, integrity, availability).	CLO1	Lecture, Multimedia	Slides PDF
4	Types of attack in cybersecurity (Mechanism and Mitigation techniques). Vulnerability analysis and prevention.			Slides
5	CT +1	CLO2	Lecture, Multimedia	Slides PDF
6	Cryptography and Classifications Distribution of the keys. Justify public and private keys, Basics of Modular Arithmetic (Modular Exponentiation, Modular inverse)			
7	Fundamentals of cipher (substitution, shift), stream cipher, monolithic and block cipher (Vigenere and rail) [Math]	CLO2	Lecture, Multimedia	Slides PDF
8	**Cryptographic algorithms** and corresponding attacks.(Explain the hierarchy of cryptography , one-time pad, DES, AES)	CLO2	Lecture, Multimedia	Slides PDF
9	Diffie-Hellman Key Exchange,			
10	RSA encryption-decryption, Homomorphic Cryptosystem) [Math]			
11	CT2 +	CLO3	Lecture, Multimedia	Slides PDF
12	**Cryptographic Hash Function**, Hashing & Message Authentication Code (MAC), Message Authentication Methods, Handshake Protocols			

13	Combinations of Basic Techniques (symmetric + asymmetric),	CLO3	Lecture, Multimedia	Slides PDF
14	Digital Signature and Digital Certificate Public Key Infrastructure (PKI)	CLO3	Lecture, Multimedia	Slides PDF
MID-SEMESTER EXAMINATION				
15	Network security issues, Authentication algorithm (Zero-knowledge proof, CKKS, consensus mechanism)	CLO4	Lecture, Multimedia	Slides PDF
16	Research on Cybersecurity Assignment			
17	Research on Cybersecurity Assignment submission			
18	Firewall design Designs of firewalls in public and private networks for stopping intrusion? + discussion class			
19	Ethical Hacking, Digital Rights, and Privacy Laws. Cyber Security Act 2023, ICT 2006 Digital Signature.	CLO1	Lecture, Multimedia	Slides PDF
20	Steganography tools and techniques (Hide information inside image, audio), Extract information from image and audio, OSINT			
21	Analysis of VPN protocols. Classifications of VPNs, how to build and operate a network.	CLO3	Lecture, Multimedia	Slides PDF
22	Basics of Blockchain			
23	Data acquisition. Disk forensic, Image forensic Memory forensics, Network forensics	CLO3	Lecture, Multimedia; Written Exam	Slides PDF
24	CT3+ Digital forensic	CLO3	Lecture, Multimedia	Slides PDF
25	VAPT			
26	Final Review	CLO1	Lecture, Multimedia	Slides PDF

17. Teaching-Learning Strategies:

18. Assessment Techniques of each topic of the course:

Mapping of Course Learning Outcomes (CLOs) with the Teaching-Learning & Assessment Strategy:

CLOs	Teaching-Learning Strategy	Assessment Strategy
CLO1	Lecture, Multimedia	Quiz, Written Examination
CLO2	Lecture, Multimedia	Written Examination
CLO3	Lecture, Problem Solving	Quiz, Written Examination
CLO4	Lecture, Group Discussion	Quiz, Assignment, Written Examination

Part C – Assessment and Evaluation

19. Assessment Strategy

Class Tests: Altogether, 4 class tests may be taken during the semester, 2 class tests will be taken for the midterm, and 2 class tests will be taken for the final term. Out of these 2 class tests for each term best class tests will be counted. No makeup class tests will be taken. Students are strongly recommended not to miss any class tests.

Assignment: The students will have to form a group of a maximum of 4 members. The topic or case studies will be given as assignments in groups during the class, which they have to prepare at home and will submit on or before the due date. No late submission of assignments will be accepted. Students will have to do the presentation on the given topic as an assignment.

20. Evaluation Policy

Assessment Type	**% Weight**	**CO1**	**CO2**	**CO3**	**CO4**
Final Examination:	**50%**	15	10	15	10
Mid-Semester Examination:	**20%**	10	10		
Continuous Evaluation: Class performance, Short Quizzes, Problem-Solving Sessions	**30%**	10	10	10	
Total	**100%**	35	30	25	10

UAP Grading Policy

Numeric Grade	Letter Grade	Grade Point
80% and above	A+	4.00
75% to less than 80%	A	3.75
70% to less than 75%	A-	3.50
65% to less than 70%	B+	3.25
60% to less than 65%	B	3.00
55% to less than 60%	B-	2.75

50% to less than 55%	C+	2.50
45% to less than 50%	C	2.25
40% to less than 45%	D	2.00
Less than 40%	F	0.00

Part D – Learning Resources

21. Text Book:

1. Cybersecurity: Public Sector Threats and Responses, Author(s): Kim J. Andersson, Series: Public Administration and Public Policy, Publisher: CRC Press

2. Cyber-Security and Information Warfare, Nicholas J. Daras

3. Cybercrime and Digital Forensics: An Introduction, By Thomas J. Holt, Adam M. Bossler, 2022, published by Routledge

4. Sanjib Sinha, Sanjib Sinha, and Karkal. Beginning Ethical Hacking with Kali Linux. Apress, 2018.

Reference Books:

1. Charles P. Pfleeger, Security in Computing, 5th Edition, Prentice Hall, 2015, ISBN-10: 0134085043,