Namal University Mianwali
Faculty of Computer Science

COURSE OUTLINE – Fall 2023

1. Course Details	
Title	Cyber Security
Code	CS-380
Credit(s)	3 credit hours
Pre-Requisite(s)	Information Security/Cryptography/Network Security
Co-Requisite(s)	None

2. Instructor Details	
Name	Dr. Arshad Farhad
Lecture Timing	Tuesday 10:30-1:00 Wednesday 3:30-5:00
Office	CS department
Office Telephone	0459-236995, Ext. 187
Email	arshad.farhad@namal.edu.pk

3. COURSE RELEVANT DETAILS

Course Aim:
To understand mechanisms to ensure confidentiality, integrity and availability of information in Communication Networks, along with security protocols and tools used to circumvent network security threats.

Course Learning Outcomes (CLOs)

On successful completion of this course, the student will be able to:

Course Learning Outcome	CLO Statement	Taxonomy Level
CLO-1	**Understand** the basic concepts of cyber security, network security, information security.	C2 (Cognitive)
CLO-2	**Understand** the concepts and cryptography/encryption techniques	C4 (Cognitive)
CLO-3	**Understand** network security attacks and how to mitigate them.	C4 (Cognitive)
CLO-4	**Understand** the use and importance of Artificial Intelligence. AI algorithms, data collection, feature engineering, and implementation.	P5 (Psychomotor)

Week#	Topics Covered in Class	Reference in Book/ Course Material
Week 1	**Overview of Cyber Security** Computer Security Network Security Internet Security Information Security Cyber Security CIA triad Threats and Attacks	Chapter-1 [1]
Week 2	**Overview of Security Attacks** Attacks (active and passive) Security Service Security mechanisms Network Security model Statistics of security attacks Real-world examples of Cyber-attacks (Use cases)	Chapter-1 [1]
Week 3	**Classical Encryption Techniques** Basic terminologies related to encryption and decryption. Ciphers Block ciphers Stream ciphers Asymmetric ciphers Cryptography	Chapter-3 [1]

Week 4	**Classical Encryption Techniques** Brute-force and non-brute-force attacks Substitution cipher Mono-alphabetic cipher Ceaser Cipher Cryptanalysis Homophonic ciphers Polyalphabetic ciphers	Chapter-3 [1] Quiz # 1 Assignment #1
Week 5	**Classical Encryption Techniques** Vigenère cipher Autokey cipher Vernam cipher Polygram cipher Playfair cipher Rail Fence Columnar Transposition Grille cipher Polybius square ADFGVX cipher Bifid Cipher	Chapter-3 [1]

Week 6	**Block Ciphers and the Data Encryption Standard** Modern block ciphers Block vs stream ciphers Shannonn's guide to good ciphers Diffusion and Confusion Block cipher principles Fiestel Cipher structure DES history DES algorithm	Chapter-4 [1]
Week 7	**Advanced Encryption Standard** Introduction Criteria Rounds Transformation Structure Substitution Permutation Mixing Key adding	Chapter-6 [1] Quiz # 2 Assignment #2
Week 8	**The Use of AI in Cyber Security** Example of anomaly detection using AI Datasets available Feature engineering Use of appropriate model Offline vs Online AI models	Research Based
Week 9	**Mid-Term Exam**	

Week 10	**Pseudorandom Number Generation and Stream Ciphers** Random number generators Usage of random numbers Properties of random numbers Streams ciphers	Chapter-7 [1] Project proposal submission. Assignment # 3
Week 11	**Public-Key Cryptography** Principles of Public-Key Cryptography The RSA algorithm Deffie-Hellman	Chapter-9 [1]
Week 12	**IDS, IPS, and SIEM** Intrusion detection system Intrusion prevention system Security Information and Event Management Honeypots	Research Quiz # 3
Week 13	**Sandbox Technology** Purpose Implementation Benefits Types of sandboxes	Research
Week 14	**Malware Analysis Techniques** Static Analysis Dynamic Analysis Benefits Available sandboxes Malware analysis using Cuckoo Sandboxing Sandbox Evasion Techniques Limitations of sandboxing	Research Quiz # 4
Week 15	**Cyber Laws** Cyber crimes Cyber laws Cyber laws in the World Cyber laws in Pakistan	Research Assignment #4 (Project deliverables)
Week 16	**Project Presentations**	Activity
Week 17	**Project Presentations**	Activity
Week 18	**Final-Term Exam**	

4. TEACHING METHODOLOGY

Mixture of White board and PPT based teaching

Activities based learning

The students have to be drawn into the participative process of learning and creating

5. TEACHING MATERIAL

Textbooks and Reading Material

[1] Cryptography and Network Security, 7th Edition, William Stallings, Pearsor Publishing Education, 2017

[2]. Principles of Information Security, 6th Edition, Michael E. Whitman & Herbert J. Mattord, Cengage Learning, 2017

6. COURSE ASSESSMENT and EVALUATION

No.	Assessment Instruments	Weight
1	Assignments	10%
2	Project	15%
3	Quizzes	15%
4	Mid Term Exam	20%
5	Final Term Exam	40%

8. UNIVERSITY POLICIES

The students are required to fully understand and observe the following policies of the university.

Eighty percent (80%) attendance is mandatory for the lectures/laboratory work delivered in the course.

For further details, please refer to university policies mentioned in the student handbook and undergraduate academic regulations of Namal University Mianwali.

9. VERIFICATION

(i) I verify that the content of this document are correct and up-to-date.	
Dr. Arshad Farhad _____ **Instructor's Name and Signature**	**02-10-2023** **Date**
(ii) I have reviewed course-outline and state that it complies with Namal Institute policies and guidelines.	
_____ **Name and Signature of Head of Department**	_____ **Date**