COURSE DESCRIPTION FORM INSTITUTION

National University of Computer & Emerging Sciences (FAST-NUCES) Karachi

PROGRAM (S) TO BE EVALUATED BS (Computer Science) / BS (Software Engineering)

A. Course Description

Course Code	**CS3002**
Course Title	Information Security (Fall 2023)
Credit Hours	3
Prerequisites by Course(s) and Topics	CS3001 Computer Networks
Assessment Instruments with Weights (homework, quizzes, midterms, final, programming assignments, lab work, etc.)	• Semester Assessments – 20% (2 Assignments 5% + 4 Quizzes 10% + Project 5%) • Mid-Term 1 Exam – 15% • Mid-Term 2 Exam – 15% • End-Term Exam – 50% • **Late submissions will only awarded a maximum of 20% weightage of the respective assessment.** • **Plagiarism punishment up to 20 weightage.** ❖ Project topics are limited to **IT Security Management and Risk Assessment Problems and their solutions including use of any tools covered in this course.** ❖ **Proposals based on programming are not entertained.** ❖ Marks distribution: 20% proposal , 60 Documentation and Execution, 20% Presentation
Course Coordinator	Dr. Nadeem Kafi Khan
URL (if any)	Individual URLs of Google classroom for each sections to be pasted here before posting the PDF version.
Current Course Description	Information security foundations, security design principles; security mechanisms, symmetric and asymmetric cryptography, encryption, hash functions, digital signatures, key management, authentication and access control; software security, vulnerabilities and protections, malware, database security; network security, firewalls, intrusion detection; security policies, policy formation and enforcement, risk assessment, cybercrime, law and ethics in information security, privacy and anonymity of data.
Textbook (or **Laboratory Manual** for Laboratory Courses)	1– Computer Security, Principles and Practice, William Stallings, 4th Edition, Pearson Publication, 2018 (Main Textbook for Theory) 2- Computer and Internet Security, A Hands-On Approach, Wenliang Du, 3rd Edition, Create Space Publications, 2022 (for labs)
Reference Material	1- Security in Computing, FIFTH EDITION by Charles P. Pfleeger, Shari Lawrence Pfleeger, Jonathan Margulies, 2015 2- Principles of Information Security, M. Whitman and H. Mattord, 7th Edition, CENGAGE Learning Inc., 2022
Course Goals	In this course, students learn basics of information security, in both management aspect and technical aspect. Students understand of various types of security incidents and attacks, and learn methods to prevent detect and react incidents and attacks. Students will also learn basics of application of cryptography, which are one of the key technologies to implement security functions. In the last session, teams of students will make presentation of their study project for a topic related to information security.

CLO	Course Learning Outcome (CLO)	Domain	Taxonomy Level	PLO			
01	**Explain** key concepts of information security such as design principles, cryptography, risk management, and ethics	Cognitive	C2 (Understanding)	1			
02	**Discuss** legal, ethical, and professional issues in information security.	Cognitive	C2 (Applying)	2			
03	**Apply** various security and risk management tools for achieving information security and privacy.	Cognitive	C3 (Applying)	5			
04	**Identify appropriate techniques to tackle** and solve problems in the discipline of information security.	Cognitive	C4 (Analyzing)	2			

Topics Covered in the Course, with Number of Lectures on Each Topic (assume 15-week instruction and three one-hour lectures per week)

Week #	Topic	Reference Text	CLO
1	**Information Security Foundations**: Definition of Computer Security with Examples, The Challenges of Computer Security, A Model for Computer Security, Threats, Attacks, and Assets, Functional Requirements, Security Design Principles, Attack Surfaces and Attack Trees, Security Policy, Security Implementation Assurance and Evaluation, Standards	Main Textbook, Chapter 1 Sections 1.1, 1.2, 1.4, 1,6, 1,7	1
2	**Cryptographic Tools**: Symmetric encryption, Feistel cipher structure. Structure and function of DES and AES, Compare and contrast stream encryption and block cipher encryption. Distinguish among the major block cipher modes of operation.	Textbook Chapter 2, Sections 2.1 and 2.2 + Slides provided for DES and AES	1,3,4
3	**Cryptographic Tools:** Message Authentication and Hash Functions, Authentication Using Symmetric Encryption, Message Authentication without Message Encryption, Secure Hash Functions, Public-Key Encryption, Public-Key Encryption Structure, Applications for Public-Key Cryptosystems **Quiz # 1**	Textbook Chapter 2, Section 2.3, 2.4	1,3,4
4	**Cryptographic Tools:** RSA (Asymmetric Encryption Algorithm), Digital Signature, Public-Key Certificates, Symmetric Key Exchange Using Public-Key Encryption Digital Envelopes	Textbook Chapter 2, Sections 1.1 and 1.2	1,3,4
5	**User Authentication:** Digital User Authentication Principles, Password based authentication, Token-based, and Biometric authentication and related security issues **ASSIGNMENT # 1 (18th Sep ← → 28th Sep)**	Textbook Chapter 3, Sections 3.1 to 3.6	1,3,4
	MIDTERM-I EXAM		

6	**Access Control**: Principles, Discretionary Access Control, Role-based Access Control and Attribute based Access Control	Textbook Chapter 4, Sections 4.1 to 4.7	**1,3,4**	
7	**Database Security:** Need, SQL Injection Attacks, Database Access Control and Database Encryption **Quiz # 2** **PROJECT PROPOSAL SUBMISSION**	Textbook Chapter 5, Sections 5.1 to 5.7	**1,3,4**	
8	**Malicious Software:** Types, Propagation, Payload, and Countermeasures	Textbook Chapter 6, Sections 6.1 to 6.10	**1,3,4**	
9	**Cloud Security and Approaches:** Service and Deployment models, Security Issues for Cloud Computing, Addressing Security Concerns, Data Protection, Security approaches in cloud Computing Assets **Quiz # 3 +** **ASSIGNMENT # 2 (16th Oct ← → 26th Oct)**	Textbook Chapter 13, Section 13.1, 13.2, 13.3	**1,3,4**	
MIDTERM-II EXAM				
10	**IT Security Management and Risk Assessment:** security policies, policy formation and enforcement, risk assessment	Textbook Chapter 14, Sections 14.1 to 14.3	**2**	
11	**Legal and Ethical Aspects:** Cybercrime, Intellectual Property, Privacy and Anonymity of Data and Ethical Issues.	Textbook Chapter 14, Sections 19.1 to 19.4	**2**	
12	**Intrusion Detection**: Basics, Types and Examples **PROJECT SUBMISSION**	Textbook Chapter 8, Sections 8.1 to 8.6	**1,3,4**	
13	**Firewalls and Intrusion Prevention**: Basics, Types, and Prevention Systems **Quiz # 4 (Latest by 17th Nov)**	Textbook Chapter 9, Sections 9.1 to 9.3 and 9.6	**1,3,4**	
14	**Software Security:** Software Vulnerabilities and Protection Mechanisms	Textbook Chapter 11, Sections 11.1 to 11.3	**1,3,4**	
15	**PROJECT PRESENTATIONS**			
FINAL EXAM				

Laboratory Projects/Experiments Done in the Course	Students will be given assignments related to the theory concepts they learn in classroom lectures. A project (research / development) discussing issues related to the state-of-the-art information security concepts will also be assigned.
Programming Assignments Done in the Course	A few programming labs are given to apply the key concepts of information security.

Class Time Spent on (in % credit hours)	**Theory**	**Problem Analysis**	**Solution Design**				**Social and Ethical Issues**
	40%	25%	25%				10%