COURSE DESCRIPTION FORM

INSTITUTION National University of Computer and Emerging Sciences

PROGRAM (S) TO BE EVALUATED Computer Science

A. Course Description

(Fill out the following table for each course in your computer science curriculum. A filled-out form should not be more than 2-3 pages.)

Course Code	CS3002
Course Title	Information Security
Credit Hours	3
Prerequisites by Course(s) and Topics	Computer Networks (CS3001), Operating Systems (CS2006)
Assessment Instruments with Weights (homework, quizzes, midterms, final, programming assignments, lab work, etc.)	Assessment with the weight.

Assessment Type	**Weight**
Assignments	10
Quiz	10
Mid-Term	25~30
Project	10
Final	40~45

Course Coordinator	Dr. Rana Asif Rehman
URL (if any)	
Current Catalog Description	Introduction to Information security, The CIA Triad: Confidentiality Integrity and Availability, Information security Models, Security compliance laws and regulations, Governance frameworks, Risk analysis, Security architectures, Malware classification. types of malware. Cryptography, Database & web security, Network security, Security policies,
Textbook (or **Laboratory Manual** for Laboratory Courses)	Cryptography Network Security: Principals and Practice, William Stallings Principle of Information Security, Whitman, Mattord Computer Security: Principals and Practice, William Stallings Hands-on Labs for Security Education, by SEED labs
Reference Material	Computer Security Fundamentals (second edition): Chuck Easttom

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

Timeline	Content Covered
Lecture 1	**Course Introduction** • Introducing syllabus, policies, and projects. • An overview of basic information security principles (with practical examples): confidentiality, integrity, availability, authentication, authorization and non-repudiation. • Component of an Information system
Lecture 2	**Security Design Principles** Discussion and evaluation of following primitives: Least-privilege, fail-safe defaults, complete mediation, separation of privilege, economy of mechanism, open design
Lecture 3	**Cryptography** Introduction to Cryptography: Symmetric cipher model, Substitution techniques (Caesar cipher, Monoalphabetic cipher)
Lecture 4	**Cryptography-II** Substitution techniques (Vigenere cipher, One-time pad) Transposition techniques (Rail fence cipher, Row transposition cipher)
Lecture 5	**Cryptography-II** Block cipher structure and design principle, Feistel cipher structure, the data encryption standard, DES (encryption, key generation)
Lecture 6	**Cryptography-III** AES structure, transformation, key expansion mechanism, AES example and implementation Stream ciphers introduction
Lecture 7	**Cryptography-IV** Introduction to Public Key cryptography RSA: principles, RSA algorithm Diffie-hellman key exchange algorithm with example, Man-in-the-middle attack in diffie-hellman
Lecture 8	**Cryptography-V** Hash functions, applications, Hash properties (preimage resistant, second preimage resistant, collision resistant) Message authentication code, requirements & properties of MAC HMAC algorithm & structure

Lecture 9	**Cryptography-VI** Digital Signature, requirements & properties of DS Public key infrastructure (PKI), elements of PKI, X.509, Digital certificates
Lecture 10	**Revision**
First Mid-term Exam	
Lecture 11	**Software Security** Malware, types of malware (virus, worms, trojan horse, adware, spyware, backdoor, ransomware, rootkits, bootkits), malware analysis & countermeasures
Lecture 12	**Software Security-II** Control Hijacking: Integer overflow String format vulnerabilities & countermeasures
Lecture 13	**Software Security-III** Control Hijacking: Buffer overflow countermeasures
Lecture 14	**Database Security** Basics SQL Injection Attack, techniques, types of attack Countermeasures, database access control
Lecture 15	**Database Security-II** Database inference attacks & counter measures Database encryption methods
Lecture 16	**Web Security** Background Cross Site Request Forgery (CSRF) Attack Countermeasures (STP, origin header, referrer header)
Lecture 17	**Web Security-II** Cross Site Scripting (XSS) Attack Types of XSS (reflected, stored, DOM based) countermeasures (encoding, validation, input handling contexts, secure input handing)
Lecture 18	**User Authentication** Types (password, biometric, symmetric/asymmetric)

	Kerberos (overview, key exchange protocol)
Lecture 19	**Access Control** Access control policies Discretionary and Role-based Access Control
Lecture 20	**Revision**
Second Mid-term Exam	
Lecture 21	**Network Security** Secure Socket Layer (SSL) SSL certificate, architecture, handshake
Lecture 22	**Network Security-II** IP security (IPSec) IPsec modes (transport, tunnel), architecture, AH, ESP
Lecture 23	**Network Security-III** Intrusion Detection Systems (IDS) Components of IDS, classification of IDS (anomaly, signature, hybrid), types (host-based, network based)
Lecture 24	**Network Security-IV** Firewalls Types of firewall (packet-filtering, stateful packet inspection, application proxy, circuit-level proxy) Location of firewall
Lecture 25	**Theoretical models of Access Control** Confidentiality policies (BLP model) Integrity policies (Biba Model) Integrity policies (Clark-Wilson model) Hybrid policies (Chinese Wall model)
Lecture 26	**Cybercrime Laws and Ethics** Pakistan cybercrime act and the role of investigative agencies. Ethical perspective of research studies and experimentation (data privacy and anonymization techniques). Intellectual property, copyright, patent, trade secret.
Lecture 27 - onwards	**Revision & Project Evaluations**

	Final Examination			
Laboratory Projects/Experiments Done in the Course				
Programming Assignments	A programming assignment where students are expected to develop an application with a focus on identifying vulnerabilities and implementing mechanisms to address them.			
Class Time Spent on (in credit hours)	**Theory**	**Problem Analysis**	**Solution Design**	**Social and Ethical Issues**
	40	25	25	10
Oral and Written Communications	Every student is required to submit at least __2___ written reports for the given assignments and to make __1___ oral presentations of typically __10___ minute's duration for the project. Include only material that is graded for grammar, spelling, style, and so forth, as well as for technical content, completeness, and accuracy.			

Instructor Name: Dr. Rana Asif Rehman

Instructor Signature