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. • Setting the course context: recent cyber threats overview, the field of information security in industrial and academic context.
Lecture 2	**Information Security Foundations** An overview of basic information security principles (with practical examples): *confidentiality, integrity, availability, authentication, authorization* and *non-repudiation.*
Lecture 3	**Security Design Principles** Discussion and evaluation of following primitives: Least-privilege, fail-safe defaults, complete mediation, separation of privilege.
Lecture 4	**Security Mechanisms** Access Controls, Authentication (Access control theory, access control matrix, information flow)
Lecture 5	**Cryptography** Introduction to Cryptography: symmetric cipher model, substitution and transposition techniques, stenography
Lecture 6	**Cryptography-II** Block cipher structure and design principle, the data encryption standard, DES example and strength
Lecture 7	**Cryptography-III** AES structure, transformation, key expansion mechanism, AES example and implementation, Triple DES, electronic code book, CBC mode, CF mode, OF mode
Lecture 8	**Cryptography-IV** Public Key cryptography and RSA: principles, RSA algorithm, Diffie-hellman key exchange, elliptic curve cryptography
Lecture 9	**Cryptography-V** Hash Functions, applications, SHA, SHA-3, message authentication code, security of MAC, HMAC, DAA, CMAC
Lecture 10	**Cryptography-VI** Digital Signature, elgamal digital signature scheme, schnorr digital scheme, NIST digital signature scheme, symmetric
First Mid-term Exam	

Lecture 11	**Software Security** • Vulnerabilities, Malware types • Malware countermeasures
Lecture 12	**Software Security-II** • Control Hijacking: Integer overflow • String format vulnerabilities • Buffer overflow
Lecture 13	**Database Security** • Basics • SQL Injection Attack
Lecture 14	**Web Security** • Background • Cross Site Scripting (XSS) Attack • Cross Site Request Forgery (CSRF) Attack
Lecture 15	**Network Security** • TCP/IP Security Issues • DNS Security Attacks and countermeasures
Lecture 16	**Network Security-II** • Transport Layer Security (TSL) • Secure Socket Layer (SSL)
Lecture 17	**Network Security-III** • Network Layer Security • IPSec
Lecture 18	**Network Security-IV** • Intrusion Detection Systems
Lecture 19	**Network Security-V** • Firewalls
Lecture 20	**Security Policies** • Confidentiality policies (BLP model) • Integrity policies (Biba Model)
Second Mid-term Exam	

Lecture 21	**Security Policies – II** • Integrity policies (Clark-Wilson model) • Hybrid policies (Chinese Wall model, role-based access control)
Lecture 22	**Cybercrime Laws and Ethics** Pakistan cybercrime act and the role of investigative agencies.
Lecture 23	**Cybercrime Laws and Ethics - II** • Ethical perspective of research studies and experimentation (data privacy and anonymization techniques). • Intellectual property, copyright, patent, trade secret.
Lecture 24	**Digital Forensics** Introduction to forensics, gold standards, evidentiary source identification, artefact acquisition and evidence provenance.
Lecture 25	**Digital Forensics - II** Introduction to open source forensic toolkits.
Lecture 26	**Digital Forensics – III** Contemporary issues in digital forensics: network, cloud and IoT/big data forensics.
Lecture 27	**Limitations and Future Challenges** • Issues in big data, IoT and software defined infrastructures. • Applications of blockchain in information security.
Lecture 28 - 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