Green University of Bangladesh
Department of Computer Science and Engineering

Course Outline

1 General Information

Fall 2023 CSE 323

Faculty	Faculty of Science and Engineering (FSE)
Department	Department of Computer Science and Engineering (CSE)
Programme	Bachelor of Science in Computer Science and Engineering
Semester	**Fall 2023**
Course Title	*Computer and Cyber Security*
Course Code	CSE 323
Course Credit	3.0 units
Contact Hours	2.5/week
Course Status	Core CSE Course
Prerequisite Course	

2 Course Instructors

Section	Name	Office	Email
203 D1	Md. Riad Hassan	A-510	riad@cse.green.edu.bd
221 D2	Md. Riad Hassan	A-510	riad@cse.green.edu.bd
211 D1	Md. Jahidul Islam	A-403	jahid@cse.green.edu.bd

3 Class Hours

Section	Room	Weekday	Time	Weekday	Time
203 D1	K-103	Monday	09:45 AM - 11:00 AM	Wednesday	09:45 AM - 11:00 AM
221 D2	J-107	Tuesday	08:30 AM - 09:45 AM	Thursday	08:30 AM - 09:45 AM
211 D1	J-110	Tuesday	11:00 AM - 12:15 AM	Thursday	11:00 AM - 12:15 AM

4 Counseling Hours

Section	Weekday	Time	Weekday	Time
203 D1	Tuesday	11:00 AM - 12:15 AM	Thursday	11:00 AM - 12:15 AM
221 D2	Monday	12:15 AM - 01:30 PM	Wednesday	12:15 AM - 01:30 PM
211 D1	Wednesday	09:45 AM - 11:00 AM	Thursday	09:45 AM - 11:00 AM

5 Course Rationale

The course covers the theory and practice of theoretical and practical security including computer security, cryptography, network security, and ethical hacking; focusing on particulars on the security aspects of data transmission, the web, and the Internet. It surveys cryptographic tools used to provide security, such as

shared key encryption (AES); public-key encryption, key exchange, and digital signature (Diffie-Hellmann, RSA, etc.). It then reviews how these tools are utilized in Internet protocols and applications such as KDC, SSL/TLS, IPSEC, PGP, S/MIME, SET, Blockchain, SDN, and others (including wireless). System security issues, such as protection from malware and harmful bots, intrusion detection systems, and firewalls will also be covered. Be noted, based on all these aspects, cyber laws and ethical hacking will be introduced as well.

6 Course Description

Security Basics: CIA triad, Authentication, Access Control, Non-repudiation, Authorization, Digital Signature; Computer and Network Security: Cryptosystem and Cryptanalysis, Modern block cipher, Public key Cryptosystem, Layered network security; vulnerability assessment; Advanced cryptography: Authenticated key exchange, TLS key exchange, Key distribution center (KDC), Homomorphic encryption, Multiparty secure computation; Secure systems and application software design and development; Principles of Software and Hardware reverse engineering; Intrusion Detection systems: Honeypot, Network monitoring; Mobile computing security; Wireless network security; Computer and network forensics: Attack traceback, fingerprinting, footprint, log monitoring; Web Security; Ethical hacking; Cyberlaw in Bangladesh.

7 Teaching Methods

All topics will be covered from the web and textbook. Some class notes will be uploaded on the web. White boards will be used most of the time. For some cases, multimedia projector will be used for the convenience of the students. Students must participate in classroom discussions for case studies, problems solving and project developments. Students may have to bring their own laptops to use tools and perform practical work.

8 Course Outcomes

CO	CO Description	PO	Domain (LoBT)	Weight	WK	WP	EA	Assessment Methods
CO1	Apply fundamental security concepts, including cryptographic algorithms and network security techniques to address real-life security concerns.	PO1	Cognitive (C3)	60%	WK3			Please refer to Section 9.
CO2	Analyzing cryptographic algorithms, secure system design, and development, vulnerability assessment, and solution to measure the performance and troubleshoot of cyber security systems.	PO2	Cognitive (C4)	30%	WK4			
CO3	Analyze, Design and Implement secured system to develop skill related to cyber security systems and cryptographic algorithms.	PO10	Psychomotor (P6)	10%			EA2	

Legend:

CO: *Course Outcome*
PO: *Program Outcome* (Appendix: A)
WK: *Knowledge Profile* (Appendix: B)
WP: *Complex Problem Solving* (Appendix: C)
EA: *Complex Engineering Activities* (Appendix: D)
LoBT: *Level of Bloom's Taxonomy* (Appendix: E)

9 Assessment Methods of COs

Assessment Method	CO1	CO2	CO3	Total
Final Exam	30%	10%		40%
Midterm Exam	20%	10%		30%
Class Tests	10%			10%
K/S/A Test 1		10%		10%
K/S/A Test 2			10%	10%
Total	60%	30%	10%	100%

10 Topic Outline

Lecture	Selected Topic	Article	Problems
(1)	Socialization and Introduction to the course	-	-
(2-3)	Security Basics Security Attacks Security Services & Mechanism	1.1, 1.3, 1.4, 1.5	1.1-1.4
(4)	Mathematics of Cryptography (GCD using Euclidean Algorithm, Mod Function, Additive & Multiplicative Inverse)		
(5-8)	Traditional Symmetric Key ciphers Cryptanalysis Substitution Ciphers (Additive, Multiplicative, Affine, Monoalphabetic Substitution Cipher, Autokey, Vigenere, Playfair ciphers) Security Services & Transposition Cipher (Keyless transposition - Rail Fence Cipher, Keyed Transposition - Row, Column transposition & Double transposition) Block & Stream Ciphers	3.1-3.4	2.2-2.9, 3.3-3.7
(9-10)	Modern Block Cipher Difference between substitution and transposition ciphers Components of a Modern Block Cipher, P-Boxes, and S-Boxes, X-OR, Circular Shift and Swap operation Diffusion and Confusion with appropriate examples		
(11-12)	Advanced Encryption Standard (AES) AES Algorithm in details Key Expansion technique in AES - 128, AES- 192, AES - 256	5.2-5.5	6.1-6.10
(12-13)	Asymmetric ciphers Difference between Asymmetric-Key and Symmetric Key RSA Cryptosystem	10.1-10.2	
(14)	Cryptographic Data Integrity Modification Detection Code (MDC) Message Authentication Code (MAC)	11.1,11.3	
	Mid Term Examination		
(15-16)	Chinese Remainder Theorem, Little Fermat's Theorem Euler Phi Function Rabin Cryptosystem	16.1-16.5	
	Cryptographic Hash Functions (MD5, SHA - 512)		

(17-18)	Message Preparation and padding Word Expansion Technique Word Expansion Technique Structure of SHA 512, Majority, Conditional, Rotation and Shift Operations	12.1, 12.2	
(19)	Key Management & Distribution (Diffie-Hellman Key Agreement)	15.3	
(20-21)	Application Layer Security (PGP, S/MIME)	16	
(22 - 23)	Web Security Secure Socket Layer (SSL) TLS		
(24 - 25)	SQL Injection Attack, Man-in-the-Middle (MITM) attack, DDoS Attacks	Web Resources	
(26-27)	SDN Technology (concept) & BlockChain technology	Web Resource	-
(27-28)	IDS, IPS, Firewall	Web Resources	-
(29 - 30)	Cyber Law in BD, Security Research, Capstone Project Presentation	-	-

For the definitions of **T** and **R** , Please refer to Section 11.

11 Text and Reference Materials

T Textbook:

- *Behrouz A. Forouzan*, **Introduction to Cryptography and Network Security**, 5th Ed., McGraw Hill Networking Series, 2012.

R References:

- *William Stallings*, **Cryptography and Network Security: Principles and Practice**, 7th Ed., Pearson, 2016.

12 Grading Policy

Marks Obtained	Letter Grade	Numerical Evaluation	Definition
80% and above	A+	4.00	Excellent
75% <80%	A	3.75	Excellent
70% <75%	A-	3.50	Very Good
65% <70%	B+	3.25	Good
60% <65%	B	3.00	Good
55% <60%	B-	2.75	Good
50% <55%	C+	2.50	Average
45% <50%	C	2.25	Average
40% <45%	D	2.00	Below Average
below 40%	F	0.00	Failing

13 Additional Course Policies

1. **Equipment and Aids**: Bring your own materials such as a calculator, notebook, and pen to participate effectively in classroom activities. You are NOT allowed to borrow from others inside the classroom which may potentially create distractions for your classmates.

2. **Assignments**: There will be a number of assignments for formative assessment purposes. The average of the assignment marks will be used for computing the final grade. Late submission of homework will carry a zero mark.

3. **Class Tests**: There will be at least three Class Tests taken during the semester and the best two will be counted for final grading. A class test can be taken with/without prior announcement.

4. **Examinations**: The midterm and final examinations will be a closed book, closed notes. Mobile phones are strictly prohibited in the exam hall. Please bring your own watch (non-smart) and synchronize at the beginning of the examination.

5. **Test Policy**: In case of missing a test without prior notice to the respected faculty member, a zero mark will be given. No makeup tests will be taken as the best two test scores will be considered for grading out of three tests.

6. **Mobile Devices Policy**: Empirical evidence of using multitasking devices such as laptops and smartphones in the classroom hinders the learning experience. Thus, the use of multitasking devices is strictly discouraged. Switch off your laptop/mobile devices during class activities.

14 Additional Information

Please click or scan:

Academic Calendar Fall, 2023:

Academic Information and Policies:

Proctorial Rules:

Grading and Performance Evaluation:

Palash Roy
Course Coordinator, CSE 323
October 25, 2023

Dr. Md. Aminur Rahman
Chairman, Department of CSE
October 25, 2023

Appendix A : Program Outcomes

POs	Category	Program Outcomes
PO1	Engineering Knowledge	Apply the knowledge of mathematics, science, engineering fundamentals and an engineering specialization to the solution of complex engineering problems.
PO2	Problem Analysis	Identify, formulate, research the literature and analyze complex engineering problems and reach substantiated conclusions using first principles of mathematics, the natural sciences and the engineering sciences.
PO3	Design/Development of Solutions	Design solutions for complex engineering problems and design system components or processes that meet the specified needs with appropriate consideration for public health and safety as well as cultural, societal and environmental concerns.
PO4	Investigations	Conduct investigations of complex problems, considering design of experiments, analysis and interpretation of data and synthesis of information to provide valid conclusions.
PO5	Modern tool usage	Create, select and apply appropriate techniques, resources and modern engineering and IT tools including prediction and modeling to complex engineering activities with an understanding of the limitations.
PO6	The engineer and society	Apply reasoning informed by contextual knowledge to assess societal, health, safety, legal and cultural issues and the consequent responsibilities relevant to professional engineering practice.
PO7	Environment and sustainability	Understand the impact of professional engineering solutions in societal and environmental contexts and demonstrate the knowledge of, and need for sustainable development.
PO8	Ethics	Apply ethical principles and commit to professional ethics, responsibilities and the norms of the engineering practice.
PO9	Individual work and teamwork	Function effectively as an individual and as a member or leader of diverse teams as well as in multidisciplinary settings.
PO10	Communication	Communicate effectively about complex engineering activities with the engineering community and with society at large. Be able to comprehend and write effective reports, design documentation, make effective presentations and give and receive clear instructions.
PO11	Project management and finance	Demonstrate knowledge and understanding of the engineering and management principles and apply these to one's own work as a member or a leader of a team to manage projects in multidisciplinary environments.
PO12	Life Long Learning	Recognize the need for and have the preparation and ability to engage in independent, life-long learning in the broadest context of technological change.

Appendix B : Knowledge Profile

Knowledge Profile	Attribute
WK1	A systematic, theory-based understanding of the natural sciences applicable to the discipline
WK2	Conceptually based mathematics, numerical analysis, statistics and the formal aspects of computer and information science to support analysis and modeling applicable to the discipline
WK3	A systematic, theory-based formulation of engineering fundamentals required in the engineering discipline
WK4	Engineering specialist knowledge that provides theoretical frameworks and bodies of knowledge for the accepted practice areas in the engineering discipline; much is at the forefront of the discipline
WK5	Knowledge that supports engineering design in a practice area
WK6	Knowledge of engineering practice (technology) in the practice areas in the engineering discipline
WK7	Comprehension of the role of engineering in society and identified issues in engineering practice in the discipline: ethics and the engineer's professional responsibility to public safety; the impacts of engineering activity; economic, social, cultural, environmental and sustainability

WK8	Engagement with selected knowledge in the research literature of the discipline

Appendix C : Range of Complex Engineering Problem Solving

Attribute	Identity	Complex Engineering Problem Description
Depth of knowledge required	WP1	Cannot be resolved without in-depth engineering knowledge at the level of one or more of K3, K4, K5, K6 or K8 which allows a fundamentals-based, first principles analytical approach
Range of conflicting requirements	WP2	Involve wide-ranging or conflicting technical, engineering and other issues
Depth of analysis required	WP3	Have no obvious solution and require abstract thinking, originality in analysis to formulate suitable models
Familiarity of issues	WP4	Involve infrequently encountered issues
Extent of applicable codes	WP5	Are outside problems encompassed by standards and codes of practice for professional engineering
Extent of stakeholder involvement and conflicting requirements	WP6	Involve diverse groups of stakeholders with widely varying needs
Interdependence	WP7	Are high-level problems including many component parts or sub-problems

Note: Complex Engineering Problems have identity P1 and some or all of P2 to P7.

Appendix D : Range of Complex Engineering Activities

Attribute	Identity	Activity Description
Range of resources	EA1	Involve the use of diverse resources (and for this purpose resources include people, money, equipment, materials, information and technologies)
Level of interaction	EA2	Require resolution of significant problems arising from interactions between wide-ranging or conflicting technical, engineering or other issues
Innovation	EA3	Involve creative use of engineering principles and researchbased knowledge in novel ways
Consequences for society and the environment	EA4	Have significant consequences in a range of contexts, characterized by difficulty of prediction and mitigation
Familiarity	EA5	Can extend beyond previous experiences by applying principles-based approaches

Note: Complex activities means (engineering) activities or projects that have some or all of the above activities.

Appendix E : Domain and Level of Bloom's Taxonomy

Cognitive Domain		Psychomotor Domain		Affective Domain	
C1	Remembering	P1	Perception	A1	Receive
C2	Understanding	P2	Set	A2	Respond
C3	Applying	P3	Guided Response	A3	Value
C4	Analyzing	P4	Mechanism	A4	Organize
C5	Evaluating	P5	Complex Overt Response	A5	Internalize
C6	Creating/ Designing	P6	Adaption		
		P7	Origination		