University of Dhaka
Dept. of Computer Science and Engineering
Professional Masters in Information and Cyber Security (PMICS) Program

COURSE OUTLINE

1 General Information

Course Title:	CSE 802 Information Security and Cryptography		
Semester:	Batch 5/July 2025	**Credit Hours:**	3
Instructor:	Mohammad Humayun Kabir	**Email:**	hkshimulbd@gmail.com
Co-Instructor:	Jargis Ahmed	**Email:**	jargis@cse.du.ac.bd
Teaching Assistant:	Mukul Ahmed	**Email:**	mukul.ahmed@outlook.com
Class Location:	Auditorium & Room 707	**Class Day/Time:**	Fri/3pm - 6pm
Google Classroom Code:		**fnndr27w**	

2 Course Contents

Information and Network Security Concepts: Cybersecurity, Information Security and Network Security, CIA triad, Security Attacks, Services and mechanism, Various types of threats, and Cryptanalysis. **Symmetric Encryption:** Symmetric Cipher Model, Classical Substitution and Transposition Ciphers, Block Cipher Design Principles and Data Encryption Standard, Strength of DES, Different variants of DES like 2DES, 3DES. Attack of 2DES, AES. **Asymmetric Encryption:** Principles of Pubic Key Cryptosystems, RSA, Discrete Logarithm, Diffie-Hellman Key Exchange, Man-in-the-Middle attack on Diffie-Hellman. **Hash Functions:** Applications of cryptographic hash functions, Hash function requirements, Secure Hash Algorithm (SHA), Digital Signatures. **Key and Identity Management including certificate management:** Key exchange and random numbers, key/identity management, Symmetric key distribution using Symmetric and Asymmetric Encryption, Public Key Distribution, X.509 Certificates, PKI Architecture. **User Authentication:** Password-based authentication, Token-based authentication, Biometric authentication, Remote user authentication, security issues for user authentication, AI/ML for security systems.

3 Course Learning Outcomes

A successful CSE 802 student should be able to:

- **CO1**: Explain the core concepts of information, network, and cybersecurity, including the CIA triad, security threats, attacks, and cryptanalysis.

- **CO2**: Apply and compare symmetric and asymmetric encryption algorithms (DES, AES, RSA, Diffie–Hellman) to ensure confidentiality and secure communication.
- **CO3**: Evaluate the effectiveness of cryptographic mechanisms such as hash functions, digital signatures, and PKI in providing integrity, authentication, and non-repudiation.
- **CO4**: Design and implement secure key management and user authentication mechanisms (password, token, biometric, remote authentication), including modern AI/ML-based approaches.

4 Course Material

4.1 Textbook and References

- (**Textbook**) Willam Stallings, Cryptography and Network Security Principles and Practice, 8th Edition.
- (**Reference**) Pachghare, V. K. Cryptography and information security. PHI Learning Pvt. Ltd., 2019.

4.2 Course Pack

For each of the theory classes, a separate concise and customized course study content will be shared with the students. Similarly, lab manuals for each of the experiments will be communicated. Please keep your eyes on the Google classroom contents for the updated materials.

4.3 Power Point Slides

For each of the theory and lab classes, a separate set of slides will be shared with the students through Google classroom.

4.4 Google Classroom

The following Google classroom https://classroom.google.com/c/ODA3NzQ2MDA1NTg5 will be used for sharing study materials, and managing assignments and/or term papers. This will also serve as the online communication platform in between the instructors and students.

5 Lecture Methods

The theoretical knowledge and technical skill development activities for the students of this course will be conducted through onsite classroom teaching and laboratory exercises. For the theory classes, the major teaching tools will be power point slides, whiteboard and marker. The students must be ready to participate in discussions for problem-solving, case studies in a group and give presentations, etc.

6 Lecture Delivery Plan

Weeks	Selected Topics	Instructor
1	**Class 1 - InfoSec Fundamentals** • Cybersecurity fundamentals • Difference between InfoSec & Network Security • CIA Triad	**MHK**
2	**Class 2 - Security Threats & Attack** • Security services & mechanisms • Types of security threats and attacks • Basics of cryptanalysis	**MHK**
3	**Class 3 - Symmetric Encryption Basics** • Symmetric cipher model • Classical encryption techniques (Substitution, Transposition) • Block cipher design principles • DES, 2DES, 3DES • AES (Structure, Security) • Attacks on Symmetric Encryption	**JA**
4	**Lab 1 - Security Attack & Detection** • SIEM Configuration for attack detection • Attack Simulation: Atomic Red teaming • Use Case for Attack Detection	**MHK, JA, MK**
5	**Lab 2 - Symmetric Cryptography** • Symmetric encryption and its applications • Compare different algorithms (DES, 3DES, AES). • Impact of key size, cipher mode (ECB vs CBC), and padding. • Analyze performance and security implications.	**MHK, JA, MK**
6	MID TERM 1	**MHK, JA, MK**

Continued on next page

Weeks	Selected Topics	Instructor
7	**Class 4 - User Authentication** • Password-based Authentication • Token-based Authentication • Biometric Authentication • Remote user Authentication • Security Issues in Authentication	**MHK**
8	**Class 5 - Asymmetric Encryption** • Principles of Public Key Cryptosystems • RSA Algorithm • Discrete Logarithm • Diffie-Hellman Key Exchange • MIMT Attack on DH	**JA**
9	**Lab 3 - RSA and DH Key Exchange Implementation with MITM Attack Simulation** • Generate RSA Key pairs • Encrypt/Decrypt messages using generated keys • Implement Diffie-Hellman key exchange • Simulate MITM attack	**MHK, JA, MK**
10	**Lab 4 - Hashing, Password Cracking and Hardening** • Password hashing and storage • Demonstrate password cracking using real-world tools • Hash Collision • PGP	**MHK, JA, MK**
11	**Lab 5 - Build a Mini PKI** • Create Root CA • Create Intermediate CA • Issue Server Certificate • Issue Client Certificate • Revoke Certificate + CRL	**MHK, JA, MK**

Continued on next page

Weeks	Selected Topics	Instructor
12	MID TERM 2	**MHK, JA, MK**
13	**Class 6 - Emerging Trends** • AI/ML in security • Future of Identity and Access Management (IAM) • Zero Trust security concepts	**MHK**
14	**Class 7 - Hash Functions + PKI** • Applications & requirements of hash functions • SHA family • Digital signatures • Key Exchange & Random Number Generation • Key distribution (symmetric/asymmetric/public key) • X.509 Certificates	**JA**
15	Final Exam	**MHK, JA, MK**

Table 1: Weekly course content delivery and formative assessment plan

7 Student Evaluation and Grading

7.1 Student Evaluation

Diverse methods of assessment techniques are recommended to quantify the progressive learning and skill development of the students. While the summative assessment constitutes 50% of the total as the Final examination, the formative assessments weigh the rest half in different forms. A statement of the proportion that each evaluation component contributes toward the final grade is portrayed in Table 2.

7.2 Grading

This course will be evaluated out of 100 marks including continuous assessments and final examinations. Following the grading policy of the University of Dhaka for regular undergraduate and graduate degree programs, grades of Professional Masters in Information and Cyber Security courses will be assigned according to the mapping in Table 3.

An 'I' (Incomplete) grade will be assigned to a student absent in the course's final examination for an acceptable reason. Such a student will be given a chance to sit for the makeup examination within two weeks of the last date of the final exam routine subject to approval of the course instructor and payment of prescribed fees.

Component	Points	Remarks
Class participation	5%	
Quiz/ term paper/ case presentation	15%	Two quizzes or 1 quiz and another term paper or case presentation will be conducted.
Midterm Exams	30%	• Two midterm exams will be held • Midterm 1 will be a written exam for 1.5 hours, carrying 30 marks • Midterm 2 will be on practical experiments for 1.5 hours, carrying 30 marks • Average of the two will be taken to assign midterm mark
Final Exam	50%	• 3 hours written Final exam will be conducted. • Question will be set by two examiners and moderation will be done by the examination committee. • Two examiners will examine the answer scripts and the average will be assigned as the given mark. • If marks of two examiners vary more than 20%, the third examiner's mark and its closer one will be averaged.

Table 2: Mark distribution for student performance evaluation

Numerical Scores	Letter Grade	Grade Point
80% and above	A+	4.00
75% to < 80%	A	3.75
70% to < 75%	A-	3.50
65% to < 70%	B+	3.25
60% to < 65%	B	3.00
55% to < 60%	B-	2.75
50% to < 55%	C+	2.50
45% to < 50%	C	2.25
40% to < 45%	D	2.00
Less than 40%	F	0.00
	I	Incomplete
	W	Withdrawn

Table 3: Letter grades and grade points

A 'W' grade will be assigned to a student who withdraws himself (or herself) from this course in the middle of the semester.

8 Course Administration Policies

8.1 Class Participation

The University of Dhaka gives equal access to education for all students irrespective of their gender, ethnicity, nationality, age group, and disability status. Students are advised to bring their own materials such as a calculator, notebook, and pen to participate effectively in classroom activities. Borrowing from others inside the classroom is not allowed as it may potentially create distractions

for their classmates. The use of mobile phones during class hours is strictly prohibited. An instructor has full right to defer the entrance of a late student in the class.

If your attendance count is 75% or above, you will be termed as a regular student; if it falls below 75% but above or equal to 60%, you will have to pay the prescribed fine to get admit card for the final examination; otherwise, you will not be eligible to sit for the final examination.

8.2 Missed Class Policy

Students are advised to attend all classes regularly. If circumstances occur missing a class, resulting in a student missing a quiz, presentation, lab test, or other graded item, the student must contact the instructor in advance by email or in person. The permission for sitting a make-up is subject to the submission of valid official documentation by the student and getting its approval by the course instructor.

8.3 Makeup Exam

If the severe illness of a student (or first family members) occurs absent in the midterm or final examinations, the student will get a single chance (for each exam) to appear at the makeup examination subject to the production of official documentation and getting approval from the program conduction committee. In such cases, the student will deposit prescribed fees and collect admit card before the date of the examination.

8.4 Retaking a Course

a) Students with a grade of 'I', 'W' or 'F' in this course may retake the course offered in the subsequent available semester on payment of requisite fees.

b) The student has to pay the full tuition fee for the course unless he/she receives an 'I' in the course.

c) A student earning a grade of 'A-' or worse may also retake a course by paying the requisite fees to improve his/her grade in that course. However, in that case, the transcript will show credit, grade and R (Retake) against the retaken course.

d) A student will be allowed to retake a course only once. In order to retake a course, a student must apply to the program conduction committee at least 4 weeks before the commencement of the semester.

e) All retake applications must be approved by the program conduction committee. Any approval for retaking a course will result in auto cancellation of his/her earlier grade.

8.5 Academic Dishonesty

Any act of academic dishonesty including the adoption of unfair means in the examinations, copying from others, and submission of plagiarised term paper or case presentation or any designated report exercised by a student will result in an 'F' grade in the concerned course subject to the determination of the instructors.

8.6 Student Privacy

It is of utmost importance for instructors to uphold the privacy of individual students and not to influence their personal preferences. Instructors are prohibited from discussing a student's grades or class performance with anyone outside of the university faculty/staff without the student's written and signed consent. This includes parents and spouses.