Course Description and Outcome Form
Department of Computer Science and Engineering
School of Engineering and Computer Science
Brac University

A. Course General Information:

Course Code:	CSE 447
Course Title:	Cryptography and Cryptanalysis
Credit Hours (Theory):	3
Contact Hours (Theory + Lab):	3+1.5
Category:	Elective
Type:	Lecture

B. Course Catalog Description (Content):

This course features a rigorous introduction to classical and modern cryptography, with an emphasis on classical systems, information theory, symmetrical cryptosystems, block ciphers, stream ciphers, Asymmetric cryptosystems, DES, AES, Public key cryptography, RSA, ECC, Cryptanalysis, types of attack, provable security, key-exchange and management, and digital signatures, different cryptanalysis techniques, and real-time protocol.

C. Course Objective

After completing this course, the student should have the following competencies:

a. Understand basic principles of cryptography and general cryptanalysis
b. Acquainted with the concepts of symmetric encryption, public key encryption, digital signatures, and key establishment.
c. Know and understand common examples and uses of cryptographic schemes, including the AES, RSA, the Digital Signature Algorithm, and the basic Diffie-Hellman key establishment protocol, and know how and when to apply them.
d. Understand the protocols and how real-world protocols work.

D. Course Outcomes (COs):

Upon successful completion of this course, students will be able to

Sl.	CO Description	Weightage (%)
CO1	Explain the fundamental concepts of cryptography.	25
CO2	Analyze and Break down private key and public key algorithms and the usages	40
CO3	Investigate different security protocol and vulnerabilities	20
CO4	Examine different cryptographic algorithm and how to break it.	15

- **Mapping of CO-PO-Taxonomy Domain & Level- Delivery-Assessment Tool:**

Sl.	CO Description	PLOs	Bloom's taxonomy domain/level	Delivery methods and activities	Assessment tools
CO1	Explain the fundamental concepts of System analysis and design.	PO1	Cognitive/Understand	Lectures, notes	Quiz,exam
CO2	Analyze and Break down private key and public key algorithms and their usages	PO2	Cognitive/Analyze	Lectures, notes	Quiz,exam
CO3	Investigate different security protocols and vulnerabilities	PO9	Cognitive/Analysis	Lectures, notes	Quiz,exam
CO4	Examine different cryptographic algorithms and how to break them.	PO4	Cognitive/Evaluate	Lab task	Lab work

- **Course Materials:**

i. Text and Reference Books:

Title	Author(s)	Publication Year	Edition	Publisher	ISBN
Information security	Mark Stamp	2012	2nd	willey	978-0470626399
Cryptography And Network Security Principles And Practice	William Stallings	2005	4th	Pearson Education	978-0134444284
Understanding Cryptography	Christof Paar, January Pelzl	2014	2nd	Springer	978-3642446498

ii. Other materials (if any)

Lecture Notes and presentation slides

Lab Handouts

- **Lesson Plan:**

Lecture	Topic Details
Week 1	Intro to Crypto and Historical Ciphers, Substitution Cipher and Cryptanalysis, Double transposition, one-time pad, Codebook cipher, History and taxonomy
Week 2	Symmetric Key Crypto, A5/1,
Week 3-4	Block cipher, DES, AES, MAC, Cryptanalysis
Week 5 - 6	Public Key Crypto, Modular arithmetic, Knapsack, RSA
Week 7	Midterm Exam
Week 8	Diffie-Hellman Key exchange, Uses of public key crypto,
Week 9	Digital Signature, Hash functions
Week 10	Public key: Elliptic Curve cryptography
Week 11-12	Symmetric key Authentication Protocols, public key authentication protocol, Zero

	Knowledge Proof
Week 13-14	Real World Protocols, SSH, SSL, Kerberos, IPSec
	Final Exam

- **Assessment Tools:**

Assessment Tools Weightage (%)	
1. Participation in class	5%
2. Quizzes/Class Tests	10%
3. Assignments	15%
4. Mid Term Examination	25%
5. Lab	20%
6. Final	25%

- **CO Assessment Plan:**

Assessment Tools				
	CO1	**CO2**	**CO3**	**CO4**
Homework	x	x	x	x
Quizzes	x	x	x	x
Examinations	x	x	x	x
Lab		x	x	

- **CO Attainment Policy:**

As per Department of CSE course outcome attainment policy

- **Grading policy:**

As per brac grading policy

- **Course Coordinator:**

Dr. Muhammad Iqbal Hossain (MIH)