Module Code and Title: DIS303 Cryptology
Programme: BE in Information Technology
Credit: 12
Module Tutor: Kezang Dema
Module Coordinator: Kezang Dema

General Objective:
The module introduces the theory and practice of cryptography, which is central to information security, network security, cybersecurity, and blockchain technology. This module provides knowledge of traditional and modern cryptography, public-key and private-key cryptography, data integrity algorithms, and key management. The module also introduces the breaking of cryptosystems to find and secure their weaknesses.

Learning Outcomes:
On completion of the module, students will be able to:

1. Elucidate the basic structure of the symmetric cryptosystems.
2. Apply modular arithmetic to the implementation of modern cryptosystems.
3. Perform encryption/decryption and verify the signature using different cryptosystems.
4. Cryptanalyze ciphers, and evaluate the security by different cryptanalysis.
5. Analyse strengths and weaknesses in different cryptosystems.
6. Assess a hash function for its suitability.
7. Differentiate block-level encryption, file-level encryption and application-level encryption.
8. Evaluate different key management and distribution approaches.

Learning and Teaching Approach:

	Approach	**Hours per Week**	**Total Credit Hours**
Contact	Lecture/Flipped Classroom	3	90
	Practical	3	
Independent study	Assignments	1	30
	Self-study	1	
	Total		120

Assessment approach:
Assessment components consist of **Continuous Assessment (CA) Theory - 35%**, **Continuous Continuous (CA) Practical - 35%** and **Semester-End Examination - 30%**. The CA Theory will consist of a Midterm Test (15%), an Assignment (10%) and a Quiz (10%). The CA Practical will consist of a laboratory report (15%), laboratory work (15%) and lab exam (10%).

Students will be divided into groups of a maximum of 24 students each to conduct the practical classes and have to sit for 3 hours of weekly practical classes in the computer laboratories allocated. The tutor shall either ask students to submit a weekly lab report for the particular lab class or assess the student's lab work by the end of the class. At least 50% of the total lab classes will be considered for evaluating lab reports and 50% for assessing lab work. The two sub-components shall be assessed out of 15 marks each.

The assessments will be carried out continuously through the following assessments:

A. Mid-term Test: (15%)

Students will undertake one closed-book mid-term test of 1-hour duration in the middle of the semester. The test will cover the units covered up to mid-semester and marked out of 15% while computing total marks for the module.

B. Assignment: (10%)

Students will undertake an individual assignment in the 7th week. The questions will be out on the VLE a week before the deadline. The assignment will be 8 - 15 questions covering topics such as encryption/decryption using various algorithms, mathematics-behind-cryptography problems, RSA, Diffie-Hellman, and ElGamal algorithms, etc. The assessment will be based on the weightage of the question given and converted to 10% while computing the total marks for the module.

C. Quiz: (10%)

Students will undertake an online or offline closed-book quiz of a maximum one-hour duration consisting of MCQ, short-answer questions, and True/False questions. The mark will be converted to 10% while computing the total marks for the module.

D. Laboratory Report: (15%)

For those lab classes identified to submit the lab report, the students have to write the report in the format prescribed by the module tutor and submit the report before the commencement of the next laboratory class. The selected report will be evaluated as per the following criteria:

5 Correctness of code (logic, syntax, according to questions)
3 Output
3 Readability and format
2 Documentation
2 Submission on deadline

The mark for the laboratory report will be evaluated out of 15% while computing the total marks for the module.

E. Laboratory Work: (15%)

Each student's work will be assessed by the end of the practical classes to keep track of students' learning and performance. The criteria for assessment are as follows:

2 Punctuality
3 Problem-solving skills
2 Debugging
3 Implementation

The mark for the laboratory work will be evaluated out of 15% while computing the total marks for the module.

F. Laboratory Exam: (5%)

A closed-book exam of 1-hour duration will be conducted in the 14th Week in a computer lab to test students' understanding of concepts applied in the lab classes. The lab exam will be marked based on the mark allocated and converted to 5% while computing the total marks for the module.

G. Semester End Examination: (30%)

There will be a 2-hour closed-book examination that will cover all the subject matter. Two sets of question papers with answer keys will be prepared and moderated for the assessment and reassessment exam. The exam will be marked out of 30% while computing the total mark for the module.

Overview of the assessment approaches and weighting:

Areas of Assignments	**Quantity**	**Weighting (%)**
A. Mid-Term Test	1	15
B. Assignment	1	10
C. Quiz	1	10
D. Laboratory Report	4	15
E. Laboratory Work	4	15
F. Lab Exam	1	5
G. Semester-end examination	1	30
Total		**100**

Prerequisite: None

Subject Matter:

Unit I: Introduction

1.1 Define cryptography, cryptanalysis and cryptology, cipher, cryptosystems, ciphertext, plaintext, encryption/enciphering, decryption/deciphering
1.2 Cryptanalysis & Brute-force attack, unconditionally vs. computationally secure
1.3 Symmetric (Secret-Key), Asymmetric (Public-Key) cryptosystem, advantages & disadvantages
1.4 Cryptography and Steganography: advantages & disadvantages
1.5 Number theory – divisibility algorithm, Euclid's algorithm, modular arithmetic, prime numbers, Fermat's & Euler's theorems, discrete logarithm

Unit II: Traditional encryption techniques

2.1 Substitution ciphers: Caesar Cipher, Monoalphabetic cipher, Play fair cipher and Polyalphabetic cipher & their cryptanalysis
2.2 Transposition ciphers: Rail fence and row transposition ciphers & their cryptanalysis
2.3 Rotor cipher, Enigma Machine, cryptanalysis of Enigma/rotor machine

Unit III: Data Encryption Standard (DES)

3.1 Block cipher and Feistel cipher structure, Shannon's Confusion and Diffusion
3.2 DES structure (Use simple DES to explain DES)
3.3 Strength and weakness of DES, Block Cipher design principles, the avalanche effect

Unit IV: Advanced Encryption Standard (AES)

4.1 Finite Field Arithmetic – GF(p), polynomial arithmetic, GF(2^n)
4.2 General AES Structure (Use simple AES to explain AES)
4.3 Avalanche Effect on AES

Unit V: Block Cipher

5.1 Block Cipher vs Stream Cipher
5.2 Multiple Encryption: double DES and triple-DES
5.3 Block Cipher Modes of operation: ECB, CBC, CFB, OFB, CTR and XTS-AES

Unit VI: Public-key cryptosystem

6.1 Principles of Public-Key Cryptosystems: Public Key Cryptosystems, Applications for Public-Key Cryptosystems, Requirements for Public-Key Cryptography
6.2 RSA algorithm: Description of the algorithm, Computational aspects, Security of RSA
6.3 Diffie-Hellman Key exchange: Algorithm, Key Exchange Protocols, Man-in-the-middle Attack
6.4 ElGamal cryptographic system
6.5 Elliptic Curve Cryptography: Elliptic Curve Encryption/Decryption, Security of Elliptic Curve Cryptography

Unit VII: Cryptographic Data Integrity Algorithms

7.1 Cryptographic hash function: Application, Requirement and Security, MD5, SHA-1, SHA-2, SHA-3
7.2 Message Authentication Codes: Requirements, message authentication functions, Security of MACs, MAC based on hash functions, block ciphers
7.3 Digital Signatures: NIST DSA, ElGamal and Schorr Digital Signature Schemes, Elliptic Curve and RSA-PSS Digital Signature Algorithms

Unit VIII: Key management and distribution

8.1 Symmetric key distributions: symmetric and asymmetric encryption
8.2 Public key distributions: Public announcement, Publicly available directory, Public-Key Authority, Public-Key certificates
8.3 X.509 Certificates and PKI: certificates, X.509 Version 3, PKIX Management Functions and Management Protocols

List of Practical(s):

1. Install and utilize of encryption/decryption tools
2. Cryptanalyze classical symmetric ciphers
3. Solve modular and finite field arithmetic problems
4. Implement Euclid's and extended Euclid's Algorithm
5. Implement private and public key cryptosystems
6. Utilize cryptographic hash functions to maintain Data Integrity
7. Simulate Digital Signature.
8. Perform certificate configuration on a web server

Reading List:

Essential Reading:

Stallings, W. (2017). *Cryptography and network security : principles and practice* (7th Ed). Pearson.

Additional Reading:

Buchmann, J. (2004). *Introduction to cryptography* (2nd ed.). Springer.

Schmeh, K. (2003). *Cryptography and public key infrastructure on the internet*. Wiley.

Forouzan, B. A. (2008). *Introduction to cryptography and network security*. McGraw-Hill Higher Education.

Date: February 2025