Program Content

Semester	V	
Course Code:	IT5306	
Course Name:	Principles of Information Security	
Credit Value:	3 (3L)	
Core/Optional:	Core	
Hourly Breakdown:	**Theory**	**Independent Learning**
	45 Hrs	105 Hrs

Course Aim:

This course focuses on the fundamentals of information system security that are used in protecting both the information present in computer storage as well as information traveling over computer networks. Information security is enabled through securing data, computers, and networks. In this course, students will learn topics such as fundamentals of information security, cryptography algorithms and protocols, authentication mechanisms, and software security. By the end of this course, students will be able to identify information security issues and provide suitable solutions.

Intended Learning Outcomes:

After following this course, students should be able to:

- Explain the concepts of securing information.
- Explain the concept of symmetric key and asymmetric key cryptography.
- Contrast the encryption and decryption algorithms, and key distribution protocols.
- Differentiate the security requirements of various software systems, such as operating systems, database management systems, and other programs.
- Develop solutions for various security-related problems in information systems.

Course Content: (Main Topics, Sub topics)

Topic	**Theory (Hrs)**
1. Information Security Concepts	3
2. Hash Functions and MAC	3
3. Symmetric Key Encryption	9
4. Asymmetry Key (Public Key) Encryption	9
5. Key Distribution Protocols	5
6. Operating Systems Security	3
7. Database Security	3
8. Program Security	3
9. Electronic Payment Systems	4
10. Digital Crime and Legal Background of Information Security	3
Total	**45**

1. **Information Security Concepts (3 hours)**
   - 1.1. Computer Security Concepts: Confidentiality, Integrity, and Availability [Ref 1: Pg.(12-19)]
   - 1.2. Threats, Attacks, and Assets [Ref 1: Pg.(19-25)]
   - 1.3. Security Functional Requirements [Ref 1: Pg.(25-27)]
   - 1.4. Fundamental Security Design Principles [Ref 1: Pg.(27-31)]
   - 1.5. Attack Surfaces and Attack Trees [Ref 1: Pg.(31-34)]
   - 1.6. Computer Security Strategy [Ref 1: Pg.(34-36)]
   - 1.7. Concepts of Encryption, Decryption, Plain Text and Cipher Text [Ref 1: Pg.(41-42)]
   - 1.8. Stream and Block Ciphers [Ref 1: Pg.47, Pg.(651-655)]

2. **Hash Functions and MAC (3 hours)**
   - 2.1. Hash Concept [Ref 1: Pg.(50-51)]
   - 2.2. Description of Hash Algorithms [Ref 1: Pg.(670-675)]
   - 2.3. HMAC Algorithms [Ref 1: Pg.(48-50), Pg.(675-678)]
   - 2.4. Security Issues [Ref 1: Pg.(678-679)]

3. **Symmetric Key Encryption (9 hours)**
   - 3.1. The Data Encryption Standard (DES) [Ref 1: Pg.(43-44), Pg.(643-645)]
   - 3.2. Triple DES [Ref 1: Pg.45, Pg.(643-645)]
   - 3.3. Advanced Encryption Standard (AES) [Ref 1: Pg.45, Pg.(645-651)]
   - 3.4. Block Cipher Modes [Ref 1: Pg.(655-660)]
   - 3.5. Applications of symmetric key algorithms [Ref 1: Pg.(660-662)]

4. **Asymmetry Key (Public Key) Encryption (9 hours)**
   - 4.1. Concept and Characteristics of Asymmetric key (Public key) Encryption System [Ref 1: Pg.(55-58)]
   - 4.2. Rivest-Shamir-Adelman (RSA) algorithm [Ref 1: Pg.59, Pg.(679-684)]
   - 4.3. Introduction to Elliptic Curve (EC) Cryptography [Ref 2: Pg.(330-334)]
   - 4.4. Application of public key cryptography [Ref 1: Pg.58]
   - 4.5. Digital signatures [Ref 1: Pg.(60-61)]

5. **Key Distribution Protocols (5 hours)**
   - 5.1. Diffie-Hellman Algorithm [Ref 1: Pg.(684-688)]
   - 5.2. Key Exchange with Public Key Cryptography [Ref 1: Pg.(62-64)]
   - 5.3. Concept of Digital Certificate [Ref 1: Pg.(61-62)]
   - 5.4. Certificate Authorities and its roles [Ref 1: Pg.(61-62)]
   - 5.5. Public Key Infrastructures (PKI) [Ref 1: Pg.(727-729)]
   - 5.6. Certificate Revocations [Ref 1: Pg.(724-728)]

6. **Operating Systems Security (3 hours)**
   - 6.1. System Security Planning [Ref 1: Pg.(417-419)]
   - 6.2. Operating Systems Hardening [Ref 1: Pg.(419-423)]
   - 6.3. Application Security [Ref 1: Pg.(424-425)]
   - 6.4. Security Maintenance [Ref 1: Pg.(425-426)]
   - 6.5. Linux/Unix Security [Ref 1: Pg.(426-430)]

6.6. Windows Security [Ref 1: Pg.(430-432)]
6.7. Virtualization Security [Ref 1: Pg.(432-436)]

7. Database Security (3 hours)

7.1. The Need For Database Security [Ref 1: Pg.(156-163)]
7.2. SQL Injection Attacks [Ref 1: Pg.(163-168)]
7.3. Database Access Control [Ref 1: Pg.(169-173)]
7.4. Inference [Ref 1: Pg.(173-176)]
7.5. Database Encryption [Ref 1: Pg.(176-180)]

8. Program Security (3 hours)

8.1. Types of Malicious Software [Ref 1: Pg.(200-203)]
8.2. Advanced Persistent Threat [Ref 1: Pg.(203-204)]
8.3. Viruses and Worms [Ref 1: Pg.(204-218)]
8.4. System Corruption [Ref 2: Pg.(221-222)]
8.5. Attack Agents [Ref 1: Pg.(222-225)]
8.6. Keyloggers, Phishing, and Spyware [Ref 1: Pg.(224-226)]
8.7. Stealthing: Backdoors and Rootkits [Ref 1: Pg.(226-229)]
8.8. Countermeasures [Ref 1: Pg.(229-235)]

9. Electronic Payment Systems (4 hours)

9.1. Fundamentals of e-payment [Ref 5: Pg(05-17)]
9.2. Credit Card Payment Protocols [Ref 5: Pg(73-125)]
9.3. Digital Cash and other e-payments methods [Ref 5: Pg.(171-214), Ref 6: Pg(04-15)]
9.4. Cryptocurrency [Ref 6: Pg(23-73)]
9.5. Blockchain [Ref 6: Pg(75-95)]

10. Legal Background (3 hours)

10.1. Cybercrime and Computer Crime [Ref 1: Pg.(611-615)]
10.2. Intellectual Property [Ref 1: Pg.(615-621)]
10.3. Privacy [Ref 1: Pg.(621-626)]
10.4. Sri Lanka Computer Crime Act [Ref 3]
10.5. Sri Lanka Electronic Transaction Act [Ref 4]

Teaching /Learning Methods:

You can access all learning materials and this syllabus in the VLE: http://vle.bit.lk/, if you are a registered student of the BIT degree program.

Assessment Strategy:

In the course, case studies/Lab sheets will be introduced, and students have to participate in the learning activities.

The final exam of the course will be held at the end of the semester. This course is evaluated using a two-hour question paper consisting of 4 Structured Questions.

References/ Reading Materials:

- **Ref 1.** Computer Security - Principles and Practice (3rd Ed) by William Stallings and Lawrie Brown
- **Ref 2.** Cryptography and Network Security: Principles and Practice (7th Edition) by William Stallings
- **Ref 3.** Sri Lanka Computer Crime Act No 24 of 2007
- **Ref 4.** Electronic Transactions Act, No. 19 of 2006
- **Ref 5.** Electronic Payment Systems for E-Commerce (2nd Ed) by, Donal O'Mahony, Michael A. Peirce, and Hitesh Tewari, Artech House
- **Ref 6.** Bitcoin and Cryptocurrency Technologies by Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, Steven Goldfeder