COURSE SYLLABUS

Information Security

Course code: 220126

1. General information

Course type		*Number of credits*	*Number of learning periods*
General	☐	Theory: 02 Exercise: 00 Practice: 01	Theory: 30 Exercise: 00 Practice: 30
Basic	☐		
Specialized	☑		
Required	☑		
Elective	☐		

Learners

Level	Bachelor
Discipline	Information Technology

Course requirements

Prerequisites	Computer network, Data structures and Algorithms Course code: ……..
Parallels	Course code: ……..
Other requirements	

2. Learning resources

Books	*Cryptography and Network Security Principles and Practice 5th Edition William Stalling*
References	*Cryptography and Network Security, The McGraw Hill Companies, Behrouz A. Forouzan* *Applied Cryptography Protocol, Algorithm, and Source code in C,John Wiley & Son Inc, Bruce Schneier*
Other learning materials	

3. Course description

The course provides students with the basics of data security and security; the need for data protection and information security; methods of penetration attacks. Research on symmetric encryption methods and public key infrastructure, digital authentication, and some other security solutions.

4. Course learning outcomes (CLOs)

After finishing the course, students will be able to:

		Satisfy LOs of the program	*Satisfy LOs of the ABET*
❖ ***Topic 1: Disciplinary Knowledge and Reasoning***			B.1.1 B.1.2 B.1.3 B.1.4 B.1.5 B.1.6
L1.	Apply math in informatics and standardize database	1.2.4	
L2.	Effective use of specialized English	1.2.7	
L3.	Applying secure transaction models in the network environment	1.3.5	
L4.	Building and deploying web application system	1.3.6	
L5.	Applying soft skills and scientific research methods to develop	1.4.5	
❖ ***Topic 2: Personal and Professional Skills and Attributes***			
L6.	Problem identification and formulation	2.1.1	
L7.	Modeling	2.1.2	
L8.	Estimation and qualitative analysis	2.1.3	
L9	Solution and recommendation	2.1.4	
L10.	Active learning	2.4.3	
L11.	Self-develop career knowledge	2.4.4	
L12.	Demonstrating morality, honesty and social responsibility	2.5.1	
❖ ***Topic 3: Interpersonal Skills: Teamwork and Communication***			
L13	Forming effective teams	3.1.1	
L14	Organizing team activities	3.1.2	
L15	Leadership	3.1.5	

L16	Written communication	3.2.2	
L17	Presentation and negotiation skills	3.2.4	
L18	Skills of listening, speaking, reading and writing	3.3.1	
L19	Using technical terms	3.3.2	
❖ ***Topic 4: Conceiving, Designing, Implementing and Operating Systems in The Enterprise, Societal and Environmental Context – The Innovation Process***			
L20	Roles and responsibilities of an information technology engineer	4.1.1	
L21	Setting goals and requirements	4.2.2	
L22	Analyzing the feasibility of the projects	4.2.3	
L23	Project management	4.2.4	

5. Course content

Course content	**CLOs**	**Number of learning periods**		
		Theory	**Practice**	**Others**
Chapter 1: Introduction	**L2**			
1.1 Introduction 1.2 To define three security goals 1.3 To define security attacks that threaten security goals 1.4 To define security services and how they are related to the three security goals 1.5 To define security mechanisms to provide security services 1.6 To introduce two techniques, cryptography and steganography, to implement security mechanisms				
☑ ***Personal and Professional Skills and Attributes***	L6 (T), L10, L12, L13(I)			
☑ ***Interpersonal Skills: Teamwork and Communication***	L17-L22 (I), L23(T)			
☑ CDIO	L24 (I)			
Chapter 2: Mathematics of Cryptography	**L1, L2**			

2.1 To review integer arithmetic, concentrating on divisibility and finding the greatest common divisor using the Euclidean algorithm 2.2 To understand how the extended Euclidean algorithm can be used to solve linear Diophantine equations, to solve linear congruent equations, and to find the multiplicative inverses 2.3 To emphasize the importance of modular arithmetic and the modulo operator, because they are extensively used in cryptography 2.4 To emphasize and review matrices and operations on residue matrices that are extensively used in cryptography 2.5 To solve a set of congruent equations using residue matrices				
☑ ***Personal and Professional Skills and Attributes***	L6 (T), L10, L12, L13(I)			
☑ ***Interpersonal Skills: Teamwork and Communication***	L17-L22 (I), L23(T)			
☐ CDIO	L24 (I)			
Chapter 3: Traditional Symmetric-Key Ciphers	**L2, L3**			
3.1 To define the terms and the concepts of symmetric key ciphers 3.2 To emphasize the two categories of traditional ciphers: substitution and transposition ciphers 3.3 To describe the categories of cryptanalysis used to break the symmetric ciphers 3.4 To introduce the concepts of the stream ciphers and block ciphers 3.5 To discuss some very dominant ciphers used in the past, such as the Enigma machine				
☑ ***Personal and Professional Skills and Attributes***	L6 (T), L10, L12, L13(I)			
☑ ***Interpersonal Skills: Teamwork and Communication***	L17-L22 (I), L23(T)			
☐ CDIO	L24 (I), L25, L26 (T)			
Chapter 4: Introduction to Modern Symmetric-key Ciphers	**L2, L3, L5**			
4.1 To distinguish between traditional and modern symmetric-key ciphers. 4.2 To introduce modern block ciphers and discuss their characteristics.				

4.3 To explain why modern block ciphers need to be designed as substitution ciphers. 4.4 To introduce components of block ciphers such as P-boxes and S-boxes				
☑ ***Personal and Professional Skills and Attributes***	L6 (T), L10, L12, L13(I)			
☑ ***Interpersonal Skills: Teamwork and Communication***	L17-L22 (I), L23(T)			
☑ CDIO	L24, L25, L26 (U)			
Chapter 5: Data Encryption Standard (DES)	**L2, L3, L5**			
5.1 To review a short history of DES 5.2 To define the basic structure of DES 5.3 To describe the details of building elements of DES 5.4 To describe the round keys generation process 5.5 To analyze DES				
☑ ***Personal and Professional Skills and Attributes***	L6, L10, L12, L13(U)			
☑ ***Interpersonal Skills: Teamwork and Communication***	L17-L22 (U), L23(U)			
☑ CDIO	L24 , L25, L26 (U)			
Chapter 6: Advanced Encryption Standard (AES)	**L2, L3, L5**			
6.1 To review a short history of AES 6.2 To define the basic structure of AES 6.3 To define the transformations used by AES 6.4 To define the key expansion process 6.5 To discuss different implementations				
☑ ***Personal and Professional Skills and Attributes***	L6, L10, L12, L13(U)			
☑ ***Interpersonal Skills: Teamwork and Communication***	L17-L22 (U), L23(U)			
☑ CDIO	L24 - L26(U), L27-L29(I)			
Chapter 7: Asymmetric-Key Cryptography	**L2, L3, L4**			
7.1 To distinguish between two cryptosystems: symmetric-key and asymmetric-key 7.2 To introduce trapdoor one-way functions and their use in asymmetric-key cryptosystems				

7.3 To introduce the knapsack cryptosystem as one of the first ideas in asymmetric-key cryptography 7.4 To discuss the RSA cryptosystem 7.5 To discuss the Rabin cryptosystem 7.6 To discuss the ElGamal cryptosystem 7.7 To discuss the elliptic curve cryptosystem				
☑ ***Personal and Professional Skills and Attributes***	L6, L10, L12, L13(U)			
☑ ***Interpersonal Skills: Teamwork and Communication***	L17-L22 (U), L23(U)			
☑ CDIO	L24 - L26(U), L27-L29(T)			
Chapter 8: Cryptographic Hash Functions	**L1-L5**			
8.1 To introduce general ideas behind cryptographic hash functions 8.2 To discuss the Merkle-Damgard scheme as the basis for iterated hash functions 8.3 To distinguish between two categories of hash functions 8.4 To discuss the structure of SHA-512				
☑ ***Personal and Professional Skills and Attributes***	L6, L10, L12, L13(U)			
☑ ***Interpersonal Skills: Teamwork and Communication***	L17 - L23(U)			
☑ CDIO	L24 - L29(U)			
Chapter 9: Digital Signature	**L1-L5**			
9.1 To define a digital signature 9.2 To define security services provided by a digital signature 9.3 To define attacks on digital signatures 9.4 To discuss some digital signature schemes, including RSA, ElGamal, Schnorr, DSS, and elliptic curve 9.5 To describe some applications of digital signatures				
☑ ***Personal and Professional Skills and Attributes***	L6, L10, L12, L13(U)			
☑ ***Interpersonal Skills: Teamwork and Communication***	L17 - L23(U)			
☑ CDIO	L24 - L29(U)			
Summary of skills in course level				

☑ ***Personal and Professional Skills and Attributes***	Identify and state the problem; Modeling the problem; Inference and resolution; Reviews and recommendations; Self-develop career knowledge; Demonstrating morality, honesty and social responsibility; Have a professional attitude
☑ ***Interpersonal Skills: Teamwork and Communication***	Organize group activities; Teamwork technique; Written communication skills; Multimedia communication skills; Listening, speaking, reading and writing skills; Use technical terms.
☑ CDIO	The role and responsibilities of an information technology engineer; Determine requirements and set goals; Analyze the feasibility of the topic; Managing topics.

6. Teaching and learning methods

ID	Teaching method/technique		Description
M1.	Lecturing	☒	
M2.	Questions – Answers	☒	
M3.	Group-based Learning	☒	
M4.	Problem-based Learning	☐	
M5.	Project-based Learning	☒	
M6.	Case studies	☒	
M7.	Role play	☐	
M8.	Demo	☒	
M9.	Simulations	☐	
M10.	Debate	☐	
M11.	Game	☐	

M12.	Brainstorming	☒	
M13.	Think-Pair-Share	☐	

7. Course assessment

ID	Assessment activity		Quantity	Weight	LOs assessed
T1.	Text-based midterm exam	☒	01	10%	L1, L2, L3
T2.	Text-based final exam	☒	01	50%	L1-L5
T3.	Practice midterm exam	☒	01	15%	L1-L5
T4.	Practice final exam	☐			
T5.	Report	☐			
T6.	In-class exercises	☐			
T7.	Homework assignments	☒	06	25%	L1-L5
T8.	Question – Answer	☐			
T9.	Term Project	☐			
T10.	Final Exam	☐			
Formula for Overall score	T1*0.1+T3*0.15+T7*0.25+T2*0.5				

8. Course requirements and expectations

8.1. Requirements on attendance

- Students are responsible for attending all classes. In case of absence due to force majeure circumstances, there must be sufficient and reasonable evidence.
- Students who do not attend more than 20% of the class sections, whether for reason or not, are deemed not to have completed the course and must re-enroll in the following semester.

8.2. Requirements and expectations on student behaviors

- Students must show their respects for teachers and other learners.
- Students must be on time. Students who are late more than five minutes will not be allowed to attend the class.
- Students should not make noise and interfere with others in the learning process.
- Students should not eat, chew gum, and use devices such as cell phones, music players during class hours.
- Laptops and tablets can only be used in class for the purpose of learning.
- Students who violate the above principles will be asked to leave the class and considered absent from the class.

8.3. Requirements on learning issues

Issues related to applying for score reservation, scoring complaints, scoring, exam disciplines are done according to the Learning Regulation of Tra Vinh University.

9. Tentative course instructor

Vo Phuoc Hung

DEAN	DEPARTMENT HEAD	LECTURER
		Vo Phuoc Hung