

# CS4286: INTERNET SECURITY AND E-COMMERCE PROTOCOLS

---

## Effective Term

Semester A 2022/23

## Part I Course Overview

### Course Title

Internet Security and e-Commerce Protocols

### Subject Code

CS - Computer Science

### Course Number

4286

### Academic Unit

Computer Science (CS)

### College/School

College of Engineering (EG)

### Course Duration

One Semester

### Credit Units

3

### Level

B1, B2, B3, B4 - Bachelor's Degree

### Medium of Instruction

English

### Medium of Assessment

English

### Prerequisites

CS3201 Computer Networks or  
CHEM2808 Forensics and Modern Society or  
CHEM2809 Science Versus Crime  
(For students intending to take a Minor in Forensic Studies)  
or equivalent

### Precursors

Nil

### Equivalent Courses

Nil

### Exclusive Courses

Nil

## Part II Course Details

### Abstract

This course aims to provide an understanding of information security. Students are expected to gain a broad understanding of information security with the goal of recognising security problems and discovering the security requirements of current computer systems. The course explores existing security mechanisms and offers students the opportunity to evaluate and design techniques for enforcing computer and network security and developing secure e-commerce protocols.

### Course Intended Learning Outcomes (CILOs)

CILOs	Weighting (if app.)	DEC-A1	DEC-A2	DEC-A3
1	Identify the security requirements of various security systems.	x	x	
2	Make critique and assess the security threats of systems against various attacks and identify potential security problems on Internet services and communications.	x	x	
3	Create the design of secure e-commerce protocols or systems using cryptographic algorithms and protocols.		x	
4	Evaluate and critique the security and performance of security algorithms and protocols, and e-commerce systems.	x	x	

#### A1: Attitude

Develop an attitude of discovery/innovation/creativity, as demonstrated by students possessing a strong sense of curiosity, asking questions actively, challenging assumptions or engaging in inquiry together with teachers.

#### A2: Ability

Develop the ability/skill needed to discover/innovate/create, as demonstrated by students possessing critical thinking skills to assess ideas, acquiring research skills, synthesizing knowledge across disciplines or applying academic knowledge to real-life problems.

#### A3: Accomplishments

Demonstrate accomplishment of discovery/innovation/creativity through producing /constructing creative works/new artefacts, effective solutions to real-life problems or new processes.

### Teaching and Learning Activities (TLAs)

TLAs	Brief Description	CILO No.	Hours/week (if applicable)	
1	Lectures	The lectures focus on key topics of information security. Additional examples and case studies will be discussed.	1, 2, 3, 4	3 hours/week
2	Tutorials	Students work on problems and exercises related to the topics taught in lectures.	1, 2, 3, 4	8 hours/semester

3	Assignments	Assignments provide opportunity to solve selected theoretical and practical problems related to course topics.	1, 2, 3, 4	After class
4	Quiz	Mid-term quiz to evaluate understanding of course topics.	1, 2, 3, 4	

**Assessment Tasks / Activities (ATs)**

ATs	CILO No.	Weighting (%)	Remarks (e.g. Parameter for GenAI use)	
1	Assignments	1, 2, 3, 4	20	3 Problem Sets
2	Mid-term Test	1, 2, 3, 4	10	

**Continuous Assessment (%)**

30

**Examination (%)**

70

**Examination Duration (Hours)**

2

**Additional Information for ATs**

For a student to pass the course, at least 30% of the maximum mark for the examination must be obtained.

**Assessment Rubrics (AR)****Assessment Task**

Mid-term Test

**Criterion**

Ability to explain and apply information security principles

**Excellent (A+, A, A-)**

High

**Good (B+, B, B-)**

Significant

**Fair (C+, C, C-)**

Moderate

**Marginal (D)**

Basic

**Failure (F)**

Not even reaching marginal levels

**Assessment Task**

Assignments

**Criterion**

Exhibit understanding of information security principles in evaluating and designing secure systems

**Excellent (A+, A, A-)**

High

**Good (B+, B, B-)**

Significant

**Fair (C+, C, C-)**

Moderate

**Marginal (D)**

Basic

**Failure (F)**

Not even reaching marginal levels

---

**Assessment Task**

Assignments

**Criterion**

Demonstrate ability to engage with information security principles in real-world applications

**Excellent (A+, A, A-)**

High

**Good (B+, B, B-)**

Significant

**Fair (C+, C, C-)**

Moderate

**Marginal (D)**

Basic

**Failure (F)**

Not even reaching marginal levels

---

**Assessment Task**

Examination

**Criterion**

Ability to explain information security principles and also demonstrate the ability to evaluate and design aspects of secure systems

**Excellent (A+, A, A-)**

High

**Good (B+, B, B-)**

Significant

**Fair (C+, C, C-)**

Moderate

**Marginal (D)**

Basic

**Failure (F)**

Not even reaching marginal levels

## Part III Other Information

### Keyword Syllabus

A selection of topics from the following: network security, computer security, malicious software, access control, firewall, intrusion detection systems, classical cryptography, symmetric-key encryption, DES, AES, public key cryptography, digital signature, digital certificate, message authentication, hash functions, RSA, ECC, SHA-1, SHA-256, PKI, authentication and key establishment protocols, SSL, PEM, PGP, IPSec, IKE, e-cash, micropayment, SET, electronic voting, electronic auction, smart card, etc.

### Syllabus

A selection of topics from the following:

- Network security and computer security  
Basic notions and techniques of DDoS, phishing attacks, malicious software such as worms, Trojan horses and viruses, firewall, packet filtering, intrusion detection systems, access control mechanisms and related subjects.
- Cryptographic techniques  
Classical cryptography, symmetric-key encryption, public key cryptography, digital signature, message authentication, cryptographic hash functions and some concrete algorithms such as DES, AES, RSA, ECC (Elliptic Curve Cryptosystems), SHA-1, SHA-256, HMAC.
- Security protocols and e-commerce protocols/schemes  
Authentication protocols, password-based authentication, digital certificate, certificate authority, revocation schemes, IPSec, IKE, SET, SSL, e-cash, micropayment, blind signature
- Advanced cryptographic protocols and e-commerce systems  
Electronic voting, electronic auction, payment servers, secret-sharing schemes, fair exchange of signatures for contract signing

### Reading List

#### Compulsory Readings

Title	
1	Stallings W. (2013). Cryptography and Network Security: Principles and Practice. Prentice Hall. 6th edition.

#### Additional Readings

Title	
1	Stinson D. R. (2005). Cryptography - Theory and Practice. CRC Press, 3rd edition.
2	Anderson R. (2008). Security Engineering. Wiley, 2nd edition.