

# EE4215: CYBERSECURITY TECHNOLOGY

---

## Effective Term

Semester A 2025/26

## Part I Course Overview

### Course Title

Cybersecurity Technology

### Subject Code

EE - Electrical Engineering

### Course Number

4215

### Academic Unit

Electrical Engineering (EE)

### 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

EE3315 Internet Technology

### Precursors

EE2302 Foundations of Information Engineering and (EE3331 Probability Models in Information Engineering or EE3001 Foundations of Data Engineering)

### Equivalent Courses

Nil

### Exclusive Courses

Nil

## Part II Course Details

### Abstract

This course aims to provide students with an understanding of the principles of cybersecurity and computer security technologies, including the principles of ethical hacking, cryptography, and blockchain technologies.

### Course Intended Learning Outcomes (CILOs)

| CILOs | Weighting (if app.)   | DEC-A1 | DEC-A2 | DEC-A3 |
|-------|---|--------|--------|--------|
| 1     | Describe the basic concepts and current technologies of cybersecurity.                  | x      |        |        |
| 2     | Apply cryptographic techniques to defend against attacks.                               | x      | x      |        |
| 3     | Describe the defensive techniques and architectures in defending against cyber attacks. | x      | x      |        |
| 4     | Apply penetration testing techniques to assess network security.                        | 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.

### Learning and Teaching Activities (LTAs)

| LTAs | Brief Description  | CILO No.   | Hours/week (if applicable) |
|------|--|------------|----------------------------|
| 1    | Lecture<br><br>Key concepts are described and illustrated.<br><br>Key concepts are worked out based on problems. | 1, 2, 3, 4 | 3 hrs/wk                   |
| 2    | Lab<br><br>Key concepts are applied to investigate or solve network security problems.                           | 1, 2, 3, 4 |                            |

### Assessment Tasks / Activities (ATs)

| ATs | CILO No.                   | Weighting (%) | Remarks ("- for nil entry) | Allow Use of GenAI? |     |
|-----|----------------------------|---------------|----------------------------|---------------------|-----|
| 1   | Tests/Quizzes (at least 2) | 1, 2, 3, 4    | 30                         | -                   | No  |
| 2   | Mini-project               | 1, 2, 3, 4    | 15                         | -                   | Yes |
| 3   | #Assignments (at least 3)  | 1, 2, 3, 4    | 20                         | -                   | Yes |

### Continuous Assessment (%)

**Examination (%)**

35

**Examination Duration (Hours)**

2

**Minimum Continuous Assessment Passing Requirement (%)**

30

**Minimum Examination Passing Requirement (%)**

30

**Additional Information for ATs**

Remarks: To pass the course, students are required to achieve at least 30% in course work and 30% in the examination. Also, 75% laboratory attendance rate must be obtained. # may include homework, classwork, or presentation

**Assessment Rubrics (AR)**

**Assessment Task**

Examination

**Criterion**

Achievements in CILOs

**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**

Coursework

**Criterion**

Achievements in CILOs

**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**Introduction to Cybersecurity and Cryptography

Computer security concepts, the CIA triad, model for network security, threats, vulnerabilities and attacks, perfect secrecy, computational security, and pseudo-randomness.

Cryptographic Techniques

Symmetrical cipher: block cipher, DES, AES, confidentiality modes; Asymmetrical cipher: public key infrastructure, RSA, Diffie-Hellman key exchange; hash functions, message integrity and digital signature; Selected advanced topics (e.g., elliptic curve cryptography, post-quantum cryptography).

Cybersecurity - Defensive Approach

Red Team vs Blue Team, Endpoint Security; Router & Switch Security; Network Security Devices: Firewalls, IDS, VPNs.

Cybersecurity - Offensive Approach

Security Assessment and Penetration Testing; Hacking Techniques; Web Hacking; Information Gathering; Vulnerability Assessment; Target Exploitation; Privilege Escalation; Maintaining Access.

**Reading List****Compulsory Readings**

| Title |     |
|-------|-----|
| 1     | Nil |

**Additional Readings**

| Title |  |
|-------|--|
| 1     | Justin Seitz, Black Hat Python: Python Programming for Hackers and Pentesters, No Starch Press; 1 edition (December 21, 2014) (ISBN-13: 978-1593275907, ISBN-10: 1593275900) |
| 2     | Andreas Bolting, Cryptographic Primitives in Blockchain Technology: a Mathematical Introduction, Oxford University Press, 2020   |
| 3     | S.J. Nielson, C.K. Monson: Practical Cryptography in Python: Learning Correct Cryptography by Example, Apress; 1st ed. edition (September 27, 2019)                          |
| 4     | Ugo Ekpo: Introduction to Cyber Security: Fundamentals, Independently published (October 12, 2018)   |
| 5     | Seymour Bosworth, Michel E. Kabay and Eric Whyne , Computer Security Handbook, Sixth Edition [electronic resource] ( John Wiley & Sons, 2014, ISBN:9781118127063)            |
| 6     | William Stallings, Cryptography and network security: principles and practice, (Pearson, 2014, ISBN 9780133354690)   |
| 7     | Richard E. Blahut , Cryptography and secure communication [electronic resource] ( Cambridge University Press, 2014, ISBN 9781107014275)                                      |
| 8     | Omar Santos, Cisco CyberOps Associate CBROPS 200-201 Official Cert Guide, (Cisco Press, 2020, ISBN-10: 0-13-680783-6)  |