Lecture #0

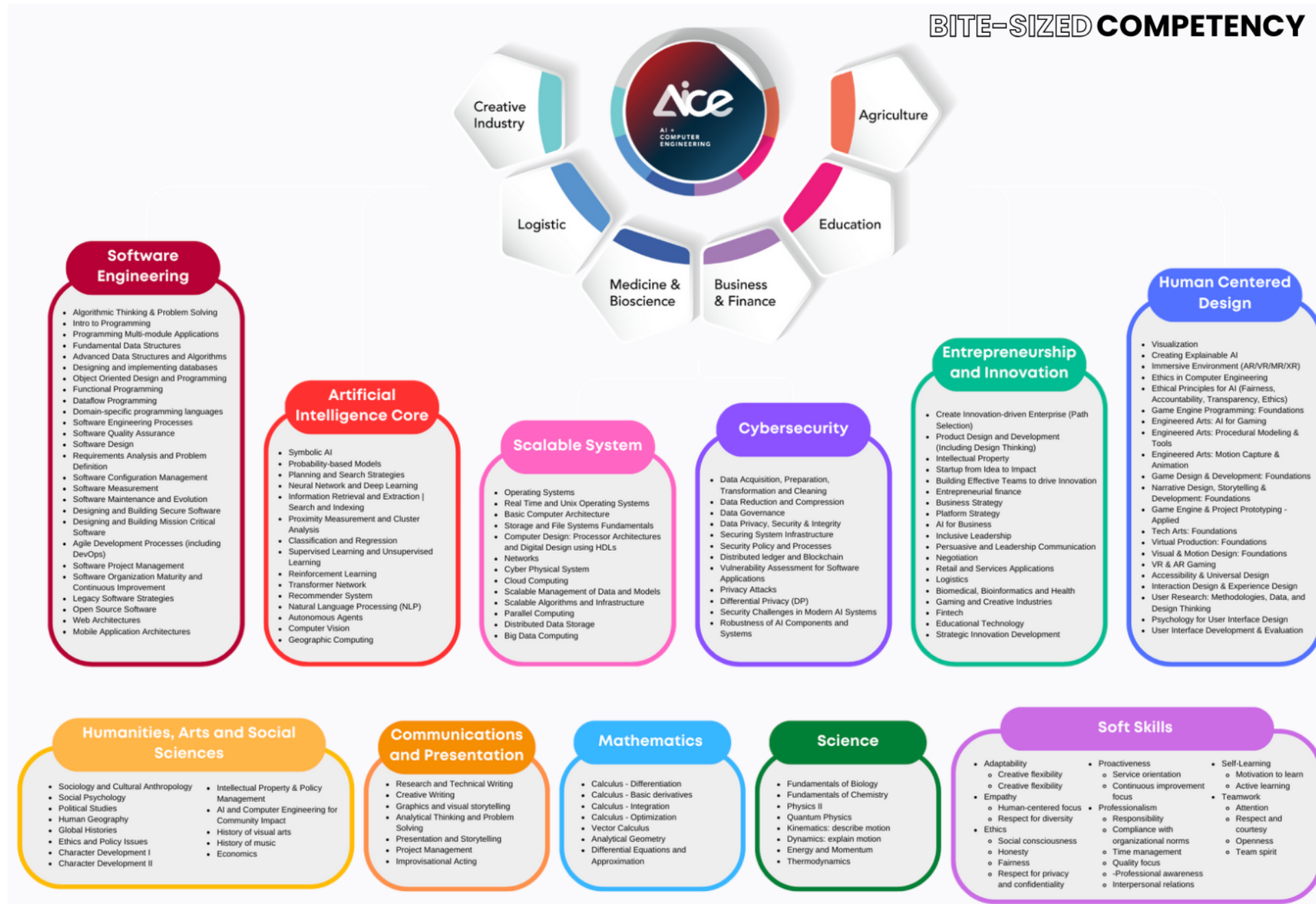## Competency Overview and Assessment

Dr. Charnon Pattiyanon

Assistant Director of IT, Instructor

Department of Artificial Intelligence and Computer Engineering
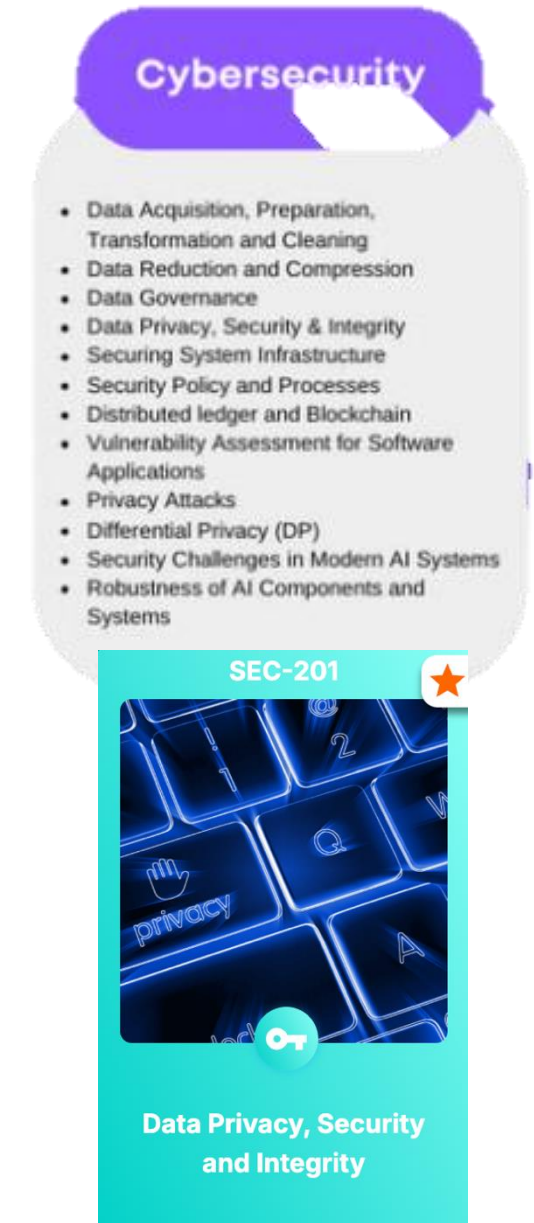
CMKL University

Welcome to
SEC-201: Data Privacy, Security, and Integrity

and the world of Cybersecurity

Competency Information

- **Competency Code:**   SEC-201

- **Competency Title:**   Data Privacy, Security, and Integrity

- **Competency Credit:**   **4**   (= **52 Hours** of work throughout an entire semester)

- **Class Timetable:**

  - **Lecture:**   Every Monday, from 14:00 – 15:00 @ Room 607, CMKL University

  - **Lab/Practical Session:**   Every Monday, from 15:00 – 16:00 @ Room 607, CMKL University

  - **Office Hours:**   Every Tuesday, from 09:00 – 10:00 @ Office 706, CMKL University

- **Class Material and Channels:**

  - Lecture Material: https://cmkl.instructure.com/courses/801/modules

  - Lab Instruction and Submission: https://cmkl.instructure.com/courses/801/assignments

  - Assessment Submission: https://cmkl.instructure.com/courses/801/assignments

  - Announcement: https://cmkl.instructure.com/courses/801/announcements

  - Discussion and Communication: https://cmkl.instructure.com/courses/801/discussion_topics

Cybersecurity

- Data Acquisition, Preparation, Transformation and Cleaning
- Data Reduction and Compression
- Data Governance
- Data Privacy, Security & Integrity
- Securing System Infrastructure
- Security Policy and Processes
- Distributed ledger and Blockchain
- Vulnerability Assessment for Software Applications
- Privacy Attacks
- Differential Privacy (DP)
- Security Challenges in Modern AI Systems
- Robustness of AI Components and Systems

SEC-201

Data Privacy, Security and Integrity

Data Privacy, Security, Integrity

Data Privacy
(Overview)

You will learn about how we can ensure **data privacy** of an information system, which means that your can share your data, and it will not be harmful to your personal life. We will explore privacy protection mechanisms, such as data anonymization, and zero-knowledge proofs.

Data Security
(Overview)

You will learn about how we can ensure **data security and confidentiality**, which means that your data will not be read by any unauthorized parties. We will explore many cryptographic techniques, from simple to advance. Also, we will explore the concept of keyed encryption, from both private and public key infrastructure.

Data Integrity
(Overview)

You will learn about how we can verify **data integrity** during both at rest and transmission over internet, which means that no one can modify or tamper your data. We will explore hash functions, message authentication code, and digital signature schemes.

Assessment

- Your skills in this competency will be assessed throughout **<u>a group project (70% Report, 30% Presentation)</u>**.

- You have to team up with your friends. (Your team must have **3 to 5 members**).

- You will be asked to develop ***a command-line-based information processing system*** that have to share data or information among components.

Important Dates

Project Announcement:	Monday, 8 September 2025, 14:00 PM
Submission Deadline for Team Member List:	Monday, 15 September 2025, 11:59 PM
Submission Deadline for Project Presentation:	Sunday, 9 November 2025, 11:59 PM
Project Presentation Date:	Monday, 10 November 2025
Submission Deadline for Project Final Report:	Friday, 28 November 2025, 11:59 PM

Competency Schedule

Week	Date	Lecture Topic	Lab Topic
1	8 September 2025	**Lecture 0:** Competency Overview and Assessment **Lecture 1:** Pillars of Cybersecurity, History of Cyber Threats and Cyber Crimes, Data Security and Privacy Properties	**Assessment Announcement**
2	15 September 2025	**Lecture 2:** Cryptography • Historical and Classical Cryptography • Symmetric Key Cryptography • Asymmetric Key Cryptography • Keyless Cryptography for Data Integrity Verification	**Lab 1:** Playing with Classical Cipher **Submission Deadline for Team Member List**
3	22 September 2025		**Lab 2:** Understand Stream Cipher and Block Ciphers
4	29 September 2025		**Lab 3:** Implementing Data Encryption Schemes (DES, AES)
5	6 October 2025		**Lab 4:** Implementing a Secure Chat Application
6	20 October 2025		**Lab 5:** Implementing Message Authentication Features in the Chat Application
7	27 October 2025	**Lecture 3:** Data Privacy Preservation • Data Privacy Techniques • Data Privacy Legislative Compliance	**Lab 6:** Playing with Zero-Knowledge Proofs Problems
8	3 November 2025		------- Free time for assessment project finalization -------
9	**9 November 2025 (23:59)**	**Submission Deadline for Project Presentation**	
	10 November 2025	**Project Presentation (30%)**	
	28 November 2025	**Submission Deadline for Project Final Report (70%)**	

Class Discipline

**Discussion and Engagement
are highly expected**

**Please do not disturb others
with noisy chit chat**

Please focus on the study

**The more you tried, the more you gain.
Please do not copy others' work**

**Be on time. You must not
miss any funny stuff**

Academic Integrity

- "In any manner of *presentation*, it is the responsibility of each student to **produce her/his own original academic work**."

- "In all academic work to be graded, **the citation of all sources is required**. When collaboration or assistance is permitted by the course instructor(s) [...], the *acknowledgement* of *any collaboration or assistance* is likewise required. This citation and acknowledgement must be incorporated into the work submitted and not separately or at a later point in time."

- "**Cheating** occurs when a student avails her/himself of an unfair or disallowed advantage [...]"

- "**Plagiarism** is defined as the use of work or concepts contributed by other individuals without proper attribution or citation. Unique ideas or materials taken from another source for either written or oral use must be fully acknowledged in academic work to be graded."

End of the Lecture

Please don't hesitate to raise your hand and ask questions if you're curious about anything!