Keio University Syllabus and Timetable

INTRODUCTION TO CYBERSECURITY

Lecturer(s)	BANA, GERGELY I.
Credit(s)	2
Academic Year/Semester	2025 Fall
Day/Period	Fri.4
Campus	Mita
Classroom	445
Class Format	Face-to-face classes (conducted mainly in-person)
Registration Number	19715
Faculty/Graduate School	INTERNATIONAL CENTER
Year Level	2, 3, 4
Grade Type	S, A, B, C, D
K-Number ▼ Detail	CIN-CO-00313-212-60

Course Contents/Objectives/Teaching Method/Intended Learning Outcome

In this course we introduce the basic concepts of Cybersecurity. We talk about the challenges the interconnectedness of the cyberspace poses to computer networks, the concept or risk, typical patterns of vulnerabilities, attacks and mitigation strategies. We introduce, in a non-technical fashion, the basic concepts of cryptography, and the typical cryptographic building blocks: encryption, digital signatures, authentication codes, public key and secret key infrastructures. We talk about how these building blocks are used to build secure networks. We also touch upon the legal frameworks handling cyber attacks. Finally we talk about cybersecurity in the context of Japan and East Asia.

Active Learning Methods Description

Discussions, Debates
Problem-based learning

Preparatory Study

Weekly review of previous lectures - 1-2 hours
1 take-home midterm assignment
1 take-home final assignment

Course Plan

Lesson 1

Introduction: Security in an Interconnected World.

Lesson 2

Modern notions of security:Confidentiality, Authentication, Privacy.

Lesson 3

Securing accounts: user side, server side. Role of hash functions and their security properties.

Lesson 4

Securing data: encryptions, classical approaches to secure communication and their vulnerabilities.

Lesson 5

Perfect secrecy, One-time pad.

Lesson 6

Symmetric encryptions: Stream ciphers, block ciphers.

Lesson 7

Hardness assumptions: Discrete logarithm problem, integer factorization problem.

Lesson 8

Public-key encryption, public-key infrastructures, digital signatures.

Lesson 9

Privacy. How browsers work, and what we can do for private browsing.

Lesson 10

Virtual private networks (VPN), TOR network for secure, private communication.

Lesson 11

Malware and what we can do against it. Firewalls.

Lesson 12

Instant Messaging, Social Media and Security.

Lesson 13

Evolving cybersecurity: Blockhains, Quantum computing.

Lesson 14

Special cybersecurity challenges in Japan and East Asia.

Other

Review and Conclusions

Method of Evaluation

1 take-home midterm exam - 50%
1 take-home final exam - 50%
More than 4 absences during the semester will be considered as an abandonment of the course. Please notify the instructor in case of illness.

Textbooks

There are no prescribed textbooks.
Handouts are available for download from K-LMS.

Reference Books

Ajay Singh: Introduction to Cybersecurity
Robin Sharp: Introduction to Cybersecurity
My lecture notes

Lecturer's Comments to Students

The use of generative AI, or the internet and other materials in general is permitted in limited contexts. Specifically, students may use any source, including AI as supplemental tools for researching assignment problems, however, students must verify the accuracy of the information themselves. Furthermore, when preparing the submission, the AI or other texts must not be copied. The student should verify the information given by the resource, absorb it, close it, and write the answer themselves. Furthermore, the sources of any information that is included in the assignment but was not given by the instructor should be clearly indicated.

Question/Comments

I will be available for students after class for questions and consultation.
Please contact me through the K-LMS messaging tool.
I will also answer any questions and offer consultation via e-mail.