CMSE491 - Selected Topics in Software Engineering I

Department:
Software Engineering

Program Name:
Software Engineering

Program Code: ?

Course Number:
CMPE112

Credits:
5 Cr

Year/Semester:
2022-2023 Fall

□ Required Course ☒ Elective Course

Prerequisite(s):

Catalog Description:
This course has been organized to give fundamental knowledge about cryptography science. Encryption, decryption and cryptoanalysis methods are considered as the core concept of this course. Symmetric and asymmetric encryption algorithms are aimed to be implemented. Perfect secrecy and the randomness is the another topic to be discussed. Hash functions will be studied as the hot topic in encryption method for perfect secrecy.

Aims and Objectives
A student who successfully fulfills the course requirements will learn the key topics of cryptography science as encryption, decryption and the cryptoanalysis methods.

Textbook(s):
"Introduction to Modern Cryptography", Jonathan Katz and Yehuda Lindell, 2/E (ISBN 13: 978-1-4665-7027-6) CRC Press, 2015.

Indicative Basic Reading List:
"Introduction to Modern Cryptography", Jonathan Katz and Yehuda Lindell, 2/E (ISBN 13: 978-1-4665-7027-6) CRC Press, 2015.

Extended Reading List:
"C: The Complete reference", Herbert Schildt, McGraw-Hill, 1995.

Topics Covered, Class Schedule and Lab Schedule: (Tentative)
(4 hours of lectures per week) (2 hours of laboratory per week)

WEEK	Starting Day	LABS
1	October, 3	**No Lab**
2	October, 10	**No Lab**
3	October, 17	**No Lab**
4	October, 24	Lab 1 – Caesar Shift Encryption
5	October, 31	Lab 2 – Vernam Encryption
6	November, 7	Lab 3 – Cryptoanalysis
7	November, 14	Lab 4 – Cryptoanalysis
8-9		**No Lab**
10	December, 5	Lab 5 – Public Key Encryption
11	December, 12	Lab 6 – Public Key Encryption
12	December, 19	Lab 7 – Hash Functions
13	December, 26	**No Lab**
14	January, 2	**No Lab**
15-17		**No Lab**

Course Learning Outcomes:
On successful completion of the course, the student is expected to be able to:
(1) Have knowledge about cryptography science.
(2) Use cryptoanalysis and randomness.
(3) Implement stream cipher and hash functions.

	Method	No.	Percentage
Assessment	Midterm Exam	1	35%
	Labs	7	15 %
	Final Examination	1	50%

Exams:

- You have re-sit exam chance at the end of semester if you fail. Note that; if your letter grade is “D” or above and you have no warning, you will not be able to enter re-sit exam. Yet, be aware that if you attend the re-sit exam, grade you get will be replace your midterm and final exam grades even if your grade is decreased.
- If you miss the midterm or the final exam, you **MUST submit a medical report to the course instructor, stating your excuse, within 3 days of that examination. The report will be evaluated by the committee of instructors. If the committee approves, you will be able to take a make-up exam. You will be able to take only one make-up exam.**
- If you miss both midterm and final exams and do not submit any written report, you will get an “NG” grade. In the same case, if you submit report for both missed exams, you will be able to enter make-up for one of them only.

Labs:

- There will be no makeup for the missed lab experiments. The sum of the highest 5 grades will be the overall lab grade. Exemption for lab work will not be provided.

Plagiarism

Plagiarism (which also includes any kind of cheating in exams, assignments, and lab works) is a disciplinary offence and will be dealt with accordingly. Furthermore, the penalty of plagiarism is to get zero for the corresponding exam, assignment, or lab work.

Important Remarks

- You should have regular attendance to the lectures for being successful in the course.
- Course related materials, exercises, laboratory experiments, past exam questions and announcements will be published on the course web site and you will be responsible from all. Note that the course web site can update during the semester. Therefore, check it regularly.

Contribution of Course to Criterion 5

Credit Hours for:
Mathematics & Basic Science : 2
Engineering Sciences and Design : 2
General Education : 0

Relationship of Course to Program Outcomes

The course has been designed to contribute to the following program outcomes:
a) an ability to apply knowledge of mathematics, science, and engineering
e) an ability to identify, formulate, and solve engineering problems
k) an ability to use the techniques, skills, and modern engineering tools necessary for engineering practice

Prepared by: Asst.Prof. Dr. Mehtap KÖSE ULUKÖK	**Date Prepared:** November 03, 2022