Global Learning Initiatives Program Course Syllabus

Please complete the following form in English. The information will be updated to the Global Learning Initiatives Program website for students' reference. If you will be offering more than one course, please fill out one form per course offered. Examples in grey.

Course Information

Course Name *provide the **English** course name of the course.	Applied Cryptography
Lecturer(s) *provide the lecturers' **English** name. If there are more than one lecturer, please indicate all lecturers in the column.	Prof. Amir Rezapour
Course Description *briefly describe the contents covered in the courses.	This course is intended for graduate students. Cryptography is one of the most crucial subjects that has made numerous breakthroughs since the discover of the WWW. In this class, we'll mainly focus on practical aspects. Besides, we'll show how to prove the security of some well-known cryptosystems.
Course Objectives *list out knowledge or skills students should acquire upon completion of course.	This course will cover the basics of symmetric cryptography, public-key cryptography, hash functions, message authentication codes, digital signatures, key management and distribution, and other fundamental cryptographic primitives. Then, we use the primitives to build provable secure protocols such as identification schemes, zero-knowledge proofs, commitment schemes, secret sharing, and electronic election system. By learning some existing secure protocols, you'll learn how to build provable secure systems.

Suggested Proficiencies (if any) *list preferred knowledge or skills students should have before taking the course.	Computer Networks Introduction to Algorithms Probability
Reading List (if any) *list out the textbooks, references, or other reading materials.	Hans Delfs, Helmut Knebl, Introduction to Cryptography: Principles and Applications (2nd Ed.), Springer, 2007. Menezes, Alfred J., Paul C. Van Oorschot, and Scott A. Vanstone. Handbook of applied cryptography. CRC press, 2018.
Grading Criteria *how would the students be assessed during the course.	Four Homework Assignments Exams •Mid-Term •Final Evaluation •Homework: 50% + o Assignments 50% o Practical experiments 2 × 10% [bonus points] ii. Mid-Term 25% iii. Final 25%

Course Schedule

Please complete the following table with the dates and expected course topics. If there are more than one lecturers instructing the course, please also indicate the lecturer for each class.

Classes	Date (YYYY/MM/DD)	Course Topic	Lecturer
2	2023/2/1	1. Introduction	Prof. Amir Rezapour
4	2023/2/15	Symmetric Key Encryption	Prof. Amir Rezapour
2	2023/3/15	Algebra and Number Theory	Prof. Amir Rezapour
4	2023/3/29	Public Key Crypto	Prof. Amir Rezapour

6	2023/4/26	Cryptographic Protocols	Prof. Amir Rezapour
19	2021/7/19	Examination	Prof. Amir Rezapour