University of Tehran
School of Electrical and Computer Engineering

<table>
<tr><td>Course:</td><td>Cryptography (Communication Security)</td></tr>
<tr><td>Course type:</td><td>
<table>
<tr><td></td><td colspan="6">EE*</td><td colspan="3">CE*</td><td rowspan="2">Credit: 3</td></tr>
<tr><td></td><td>Com</td><td>E</td><td>P</td><td>B</td><td>Con</td><td>D</td><td>SW</td><td>HW</td><td>IT</td></tr>
<tr><td>Required</td><td>☒</td><td>☐</td><td>☐</td><td>☐</td><td>☐</td><td>☐</td><td>☐</td><td>☐</td><td>☐</td><td></td></tr>
<tr><td>Elective</td><td>☐</td><td>☐</td><td>☐</td><td>☐</td><td>☐</td><td>☐</td><td>☐</td><td>☐</td><td>☐</td><td></td></tr>
</table>
</td></tr>
<tr><td>Level:</td><td>Undergraduate ☐
Graduate ■</td></tr>
<tr><td>Co-requisite(s):</td><td></td></tr>
<tr><td>Prerequisite(s):</td><td>Probability and Statistics</td></tr>
<tr><td>Prerequisite by topic:</td><td>Having background in number theory and algebra.</td></tr>
<tr><td>Textbook(s):</td><td>[1] Stinson, Douglas R. Cryptography: theory and practice. CRC press, 2005.
[2] Henry, B., and P. Fred. "Cipher Systems: The Protection of Communication." (1982).</td></tr>
<tr><td>Coordinator:</td><td>Mohammad Ali Akhaee, Assistant Professor</td></tr>
<tr><td>Goals:</td><td>For many centuries the goal of cryptography was the protection of privacy of communications. Computers, digital communication and in particular the Internet have brought an abundance of new security goals. Examples are: anonymity, authenticity, non-repudiation, authorized wiretapping (called law enforcement), and traceability. For realization of each case different security mechanisms are needed. The goal of the course is to make students familiar with such techniques and some of the foundations of these methods. By learning the concept of cryptology and its related mathematics, students are capable to design and implement new cryptographic algorithm or customization of the state of the art schemes upon the request.</td></tr>
<tr><td>Outcome:</td><td>Upon successful completion of the course, students will be able to
1. Implement and cryptanalyze classical ciphers.
2. Design and implement stream ciphers
3. Describe modern private-key cryptosystems and ways to cryptanalyze them.
4. Describe modern public-key cryptosystems and ways to cryptanalyze them.
5. Explain the mathematical concepts underlying modern cryptography.</td></tr>
<tr><td>Topics:</td><td>History and overview of cryptography
Classic Cryptology
Shannon Theory</td></tr>
</table>

	Basic symmetric-key encryption One time pad and stream ciphers Block ciphers Block cipher abstractions: PRPs and PRFs Attacks on block ciphers **Cryptographic Hash Functions** Hash functions and data integrity Security of hash functions Message Authentication code **Public key cryptography** Arithmetic modulo primes Cryptography using arithmetic modulo primes Public key encryption Arithmetic modulo composites **Digital signatures** Digital signatures: definitions and applications More signature schemes and applications (If time allows)
Computer usage:	Some parts of the course will be presented using PowerPoint.
Assignments:	Four written assignments, two computer assignments, Presenting a research paper of cryptography field.
Projects:	Students will choose a project topic from the beginning of the semester. The project consists of the research and implementation of a recent cryptographic algorithm along with its performance evaluation.
Grading:	Assignments 20% Final Project (Presentation) 10% Midterm exam: 30% Final exam: 40%
Further readings:	NIST Computer Security Publications - NIST Special Publications
Prepared by:	Mohammad Ali Akhaee
Date:	Aug, 2017

*EE: Electrical Engineering		CE: Computer Engineering	
Com	Communications	SW	Software
E	Electronics	HW	Hardware
P	Power	IT	Information Technology
B	Bioelectronics		
Con	Control		
D	Digital System		