Course name	Theory of Cryptography (Advanced Cryptography)

Course ID: *40-???*	**Credits:** 3	**Program:** Graduate
Prerequisites: Data and Network Security		**Co-requisites:**
Prepared by: Rasool Jalili & Mahdi Kharrazi		

1. Aim

This course aims to connect current knowledge of graduate student in information security to advanced cryptography through these detailed targets:

1. Deep understanding of cryptography concepts.
2. Understanding of fundamentals of cryptographic mathematics.
3. Understanding of introductions, concepts, and fundamentals of the modern cryptography.
4. Understanding recent researches of this topic in journals and libraries.

2. Outline

1. Introductions
   - 1.1. Cryptography and Modern Cryptography
   - 1.2. Private-key Cryptography
   - 1.3. Classic Cryptography and it's analysis
   - 1.4. Principles of Modern Cryptography (Definitions, Assumptions, and Proof of Security)
2. Completely Secure Cryptography
   - 2.1. Basic Definitions and Properties
   - 2.2. Limitations of Completely Secure Cryptography
3. Symmetric and Pseudo-random Cryptography
   - 3.1. Computational View of Cryptography
   - 3.2. Definition of Secure Computational Cryptography
   - 3.3. Pseudo-random Number Generators
   - 3.4. Building Secure Cryptographic Schemes
   - 3.5. Security against Chosen Plain-text Attacks
   - 3.6. Security against Chosen Cipher-text Attacks
4. Elliptic-curve Cryptography
   - 4.1. Abstract Algebra
   - 4.2. Group Theory
   - 4.3. Field Theory
5. Measuring Computational Difficulty/Complexity

5.1. Problems in P

5.2. Problems in NP

6. One-way Functions
7. Commitment Methods
8. Oblivious Transfer
9. Zero-knowledge Proof Systems
10. Cryptographic Schemes
11. Digital Signature Schemes
12. Two/Multi-party Secure Protocols

3. Evaluation Criteria

1. Mid-term Exam: 25%
2. Final Exam: 35%
3. Assignments and Survey Paper: 40%

4. References

[1] Jonathan Katz & Yehuda Lindell, Introduction to Modern Cryptography, Chapman & Hall CRC Press, 2007.

[2] Oded Goldreich, Foundations of Cryptograph: Vol. 1: Basic Tools. Cambridge University Press, 2001.

[3] Oded Goldreich, Foundations of Cryptograph: Vol. 1: Basic Applications. Cambridge University Press, 2004.

[4] Alfred J. Menezes, Paul C. van Oorschot, & Scott A. Vanstone, Handbook of Applied Cryptography, CRC Press, 1996.