Knight Foundation School of Computing and Information Sciences

Course Title: Introduction to Cryptography **Date:** 11/02/2021

Course Number: CIS-5xxx

Number of Credits: 3

Subject Area: Cybersecurity	**Subject Area Coordinator:** **email:**
Catalog Description: Introduction to cryptography, including hash functions, symmetric and public key cryptosystems, applications, attack types, standards. No programming or special math skills required.	
Textbook: Menezes, Alfred J., Paul C. Van Oorschot, and Scott A. Vanstone. *Handbook of applied cryptography*. CRC press, 2018. ISBN-13: 978-0849385230	
References: None	
Prerequisites Courses: None **(M.S. or Ph.D. standing or permission of the instructor**	
Corequisites Courses: None	

Type: Required

Prerequisites Topics:

- Pre-college Mathematics

Course Outcomes: At the end of the course, students should be able to:

O1. Understand basic security functions, including confidentiality, integrity, authentication, non-repudiation
O2. Understand various attack techniques, including brute force, chosen plaintext (CPA), known plaintext, chosen cyphertext (CCA), differential and linear cryptanalysis
O3. Explain the concepts behind IND-CPA and IND-CCA games
O4. Describe the applications of hash functions, including integrity checking, data authentication, and login services (secure storage of authentication credentials)
O5. List and explain the properties of cryptographic hash functions (pre-image resistance, second pre-image resistance, collision resistance)
O6. Master hash functions concepts, including MD4, MD5, SHA-1, SHA-2, SHA-3
O7. Master the concepts of symmetric key cryptography, including DES and Twofish
O8. Explain differences between block and stream data
O9. Explain differences between various cryptographic modes, their strengths and weaknesses, including IND-CPA security
O10. Understand the evolution from DES to AES
O11. Master the concepts and implementation of public key cryptosystems, including Diffie-Hellman, RSA, Elliptic Curve Cryptography, ElGamal, and DSA, quantum crypto
O12. Describe their vulnerabilities, including man-in-the-middle and IND-CPA attacks, and solutions.
O13. Understand PKC applications including public key certificates, public key infrastructure, GPG (GNU privacy guard), SSH/OpenSSL, key management, digital signatures and authentication

O14. List cryptographic standards (FIPS 140 series)
O15. Understand implementation failures

Outline

Topic	Lecture Hours	Outcome
Introduction • Background and history of cryptography • Basic concepts and security functions	3.5	O1, O2
Cryptosystems overview • Attack types • IND-CPA and IND-CCA games	3.5	O2, O3
Cryptographic Hash Functions • Properties • Implementation • Applications • Standards	6	O4, O5, O6
Symmetric Key Cryptography • DES, AES, RC4 • Standards	3	O7, O10
Multiple encryption modes Operation modes • IND-CPA security	5	O8, O9
Public Key Cryptography • RSA, DH, ElGamal, DSA • IND-CPA security • Standards	6	O11, O12
Public Key Cryptography • Elliptic curve cryptography	3	O11
Applications • Digital Certificates • PKI • Digital Signatures • Standards	3	O13
Implementation failures	3	O14

Grading Policy

- Midterm: 30%
- Final Exam: 30%
- Assignments: 30%
- Participation: 10%