ECE 471/571 Fundamentals of Information and Network Security (Spring 2024)

Note: Quizzes are only for online students

Course Schedule

Week	Topics	Assignments & Deliverables Open: Assignments Available Due: Assignments Due
Week 1 **Jan. 10 – Jan. 14**	**Module 1 – Introduction to Information Security** • Information security objectives • Schematic of a secure communication system • Formal definition of a cryptosystem and adv. models **Readings:** • Textbook sections: 1.1-1.8	**Open Wednesday, 01/10** • **Quiz 1** • **HW 1**
Week 2 **Jan. 15 – Jan. 21**	**No Class on 1/15 (holiday)** **Module 2 - Classical Encryption Techniques** • Number theory basics • Early cryptosystems: substitution and transposition **Readings:** • Textbook sections: 2.1-2.4, 3.1-3.3	**Open Tuesday, 01/16** • **Lab 1**
Week 3 **Jan. 22 – Jan. 28**	**Module 3 – Cryptanalysis and Measures of Security** • Early cryptosystems (cont'd) • Cryptanalysis of early cryptosystems • Perfect secrecy, Ideal cryptosystems & one-time pad **Readings:** • Textbook sections: 3.1 – 3.3 • Reference book sections: [Stinson's book] 2.2, 3.3;	**Open Monday, 01/22** • **Quiz 2** **Due Sunday, 01/28** • **Quiz 1**
Week 4 **Jan. 29 – Feb. 4**	**Modules 3, 4 – Measures of Security and Symmetric Key Crypto.** • The notions of symmetric key cryptography, and computational security • Block cipher, product cipher, and substitution-permutation networks **Readings:** • Textbook sections: 4.1, 4.5 • Reference book sections: [Stinson's book] 4.1-4.2	**Due Monday, 01/29** • **HW 1** **Open Friday, 02/02** • **HW 2** • **Lab 2**

Week 5 **Feb. 5 –** **Feb. 11**	**Module 4 – Symmetric Key Cryptography** • The Data Encryption Standard (DES) and its security • Finite Field Arithmetic & Advanced Encryption Standard (AES) **Readings:** • Textbook sections: 4.2-4.4, 6.1-6.6, 7.1	**Due Monday, 2/5** • **Lab 1 (Task 1)** **Due Sunday, 02/11** • **Quiz 2** **Open Monday, 02/05** • **Quiz 3**
Week 6 **Feb. 12–** **Feb. 18**	**Module 4 – Symmetric Key Cryptography (cont'd)** • Modes of operation • Pseudorandom numbers and stream ciphers **Readings:** • Textbook sections: 7.2-7.6, 8.1-8.4	**Due Monday, 2/12** • **Lab 1 (All)** **Open Friday, 2/16:** • **Lab 3**
Week 7 **Feb. 19–** **Feb. 25**	**Module 5 – Hash Functions, Message Integrity Check & Authentication** • Definition of hash functions and security properties • Examples of hash functions: MD series, and SHA • Message Authentication Codes (MAC), HMAC • Hash applications, including commitment protocols **Readings:** • Textbook sections: Textbook section: 11.1-11.3, 11.4-11.5, 12.1-12.5, 12.7, 12.9	**Due Monday, 2/19** • **HW 2** **Due Saturday, 2/24** • **Quiz 3** **Open Monday, 2/19:** • **HW 3** • **Quiz 4**
Week 8 **Feb. 26–** **Mar. 3**	**Module 6 – Public Key Cryptography** • More number theory basics • Principles of Public-key Cryptography (PKC) • Common public key cryptosystems: RSA **Readings:** • Textbook section: 2.5, 2.8, 9.1-9.2	**Due Monday, 2/26** • **Lab 2** **Due Sunday, 3/3** • **Quiz 4** **Open Friday, 3/1:** • **Quiz 5** • **Lab 4**
Week 9 **Mar. 4 –** **Mar. 10**	**Spring Recess (No class)**	**Due Monday, 3/4** • **Lab 3** **Open Monday, 3/4:** • **HW 4**
Week 10 **Mar. 11 –** **Mar. 17**	**Module 7 – PKC and Digital Signatures** • Diffie-Hellman key exchange and ElGamal • Common digital signatures schemes: RSA, ElGamal, etc. **Readings:** • Textbook sections 10.1-10.2, 13.1-13.2	**Due Monday, 3/11:** • **HW3** **Due Friday, 3/15:** • **Quiz 5** **Open Sunday, 3/17:** • **Quiz 6**

Week 11 **Mar. 18 –** **Mar. 24**	**Module 7, 8 – Key Management and Distribution** - Symmetric key distribution schemes, KDC - Public key distribution and Public Key Infrastructure (PKI) **Readings:** - Textbook sections 15.1-15.5	**Midterm Exam, TBD.**
Week 12 **Mar. 25 –** **Mar. 31**	**Module 9 – User Authentication** - User authentication principles - Password authentication protocols - Challenge-response protocols and common pitfalls **Readings:** - Textbook sections: 16.1-16.2, 16.4 - Reference book sections: [Kaufman's book] 11.1-11.5	**Due Monday, 3/25:** - **Lab 4** **Due Sunday, 3/31:** - **Quiz 6** **Open Monday, 3/25:** - **Lab 5**
Week 13 **Apr. 1 –** **Apr. 7**	**Module 9, 10 – User Authentication and Network Security** - User authentication: Kerberos - TCP/IP Threats **Readings:** - Textbook sections: 16.3, 17.1	**Due Monday, 4/1:** - **HW 4** **Open Monday, 4/1:** - **Quiz 7** - **HW5**
Week 14 **Apr. 8 –** **Apr. 14**	**Module 10 – Network Security Protocols** - IP security: the IPSec protocol - Transport-level security: SSL and TLS protocols **Readings:** - Textbook sections: 20.1-20.5; 17.2-17.4	**Due Sunday, 4/14:** - **Quiz 7**
Week 15 **Apr. 15 –** **Apr. 21**	**Modules 10, 11 – Network Security, and System Security** - Electronic mail security, S/MIME, PGP - Malware, Worms, DDoS attacks, SBGP **Readings:** - Textbook section(s): 19.1-19.4; 21.3-21.4;	**Due Monday, 4/15:** - **Lab 5** **Open Monday, 4/15:** - **Quiz 8**
Week 16 **Apr. 22 –** **Apr. 28**	**Module 11 – System Security** - Intrusion detection - Firewalls and Virtual Private Networks (VPNs) **Readings:** - Textbook sections: 21.1-21.2	
Week 17 **Apr. 29 –** **May 5**	**Module 11 – System Security (cont'd)** 5/3 (no class, reading day) **Readings:** Textbook sections: 21.1-21.2	**Due Monday, 4/29:** - **HW 5** **Due Wednesday, 5/1:** - **Quiz 8**

Finals Week **May 6**	**Final Exam**	**Monday, 5/6:** • **Final Exam**