Course Deliverables

Course Deliverable (Sorted by Due Date)	Due Date (11:59pm CST)
Homework 1	Friday, September 16
Project 1	Friday, September 30
Homework 2	Friday, October 14
Project 2	Friday, November 04
Homework 3	Friday, November 11
Examination	**Tuesday, November 22**
Homework 4	Friday, December 09
Project 3	Sunday, December 11

Course Flow

Week	Topics	Assignments & Deliverables Open: Assignments Available Due: Assignments Due
Week 1 **Aug. 22 – Aug. 26**	**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 Monday, 08/22** • **HW 1**
Week 2 **Aug. 29 – Sep. 02**	**Module 2 - Classical Encryption Techniques** • Number theory basics • Early cryptosystems: substitution and transposition **Readings:** • Textbook sections: 2.1-2.5, 3.1-3.3	**Open Monday, 08/29** • **Project 1**
Week 3 **Sep. 05 – Sep. 09**	**Module 3 – Cryptanalysis and Measures of Security** • Early cryptosystems (cont'd) • Cryptanalysis of early cryptosystems • Perfect secrecy, Ideal cryptosystems & one-time pad **Readings:** • Reference book sections: [Stinson's book] 2.2, 3.3; • Textbook sections: 3.2	
Week 4 **Sep. 12 – Sep. 16**	**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:** • Reference book sections: [Stinson's book] 4.1-4.2 • Textbook sections: 4.1-4.5	**Due Friday, 09/16** • **HW 1**
Week 5 **Sep. 19 – Sep. 23**	**Module 4 – Symmetric Key Cryptography** • The Data Encryption Standard (DES) and its security • Finite Field Arithmetic & Advanced Encryption Standard (AES) **Readings:** • Textbook section: 5.1-5.6, 6.1-6.5, 7.1	**Open Monday, 09/19** • **HW 2**

Week 6 **Sep. 26 – Sep. 30**	**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 Friday, 09/30** • **Project 1**
Week 7 **Oct. 03 – Oct. 07**	**Module 5 – Public Key Cryptography** • Principles of Public-key Cryptography (PKC) • More number theory basics • Common public key cryptosystems: RSA **Readings:** • Textbook sections: 2.5, 9.1-9.2	**Open Monday, 10/03** • **Project 2**
Week 8 **Oct. 10 – Oct. 14**	**Module 6 – Public Key Cryptography and Hash Functions** • Diffie-Hellman key exchange and ElGamal • Definition of hash functions and security properties **Readings:** • Textbook section: 10.1-10.2, 11.1-11.3	**Due Friday, 10/14** • **HW 2**
Week 9 **Oct. 17 – Oct. 21**	**Module 7 – Message Integrity and Authentication** • **No - Class (Oct. 19)** • Examples of hash functions: MD series, and SHA • Message Authentication Codes (MAC), HMAC **Readings:** • Textbook section: 11.4-11.5, 12.1-12.5, 12.7	**Open Monday, 10/17** • **HW 3**
Week 10 **Oct. 24 – Oct. 28**	**Module 7, 8 – Digital Signatures, Key Management and Distribution** • More hash applications, including commitment protocols • Common digital signatures schemes: RSA, ElGamal, etc. • Symmetric key distribution schemes, KDC • Public key distribution and Public Key Infrastructure (PKI) **Readings:** Textbook sections: 12.9 , 13.1-13.2, 14.1-14.5	
Week 11 **Oct. 31 – Nov. 04**	**Module 9 – User Authentication** • User authentication principles • Password authentication protocols • Challenge-response protocols and common pitfalls **Readings:** • Textbook sections: 15.1-15.2, 15.4,	**Due Friday, 11/04:** • **Project 2**

Week 12 **Nov. 07 – Nov. 11**	**Module 9, 10 – User Authentication and Network Security** • User authentication: Kerberos • TCP/IP Threats **Readings:** • Textbook sections: 15.3, 17.1	**Open Monday, 11/07** • **Project 3** **Due Friday, 11/11** • **HW 3**
Week 13 **Nov. 14 – Nov. 18**	**Module 10 – Network Security Protocols** • IP security: the IPSec protocol • Transport-level security: SSL and TLS protocols **Readings:** Textbook sections: 20.1-20.5; 17.2-17.3	**Open Monday, 11/14:** • **HW 4** **Open Friday, 11/18:** • **Examination**
Week 14 **Nov. 21 – Nov. 25**	• Examination • **No - Class (Nov. 24)**	**Due Tuesday, 11/22** • **Examination**
Week 15 **Nov. 28 – Dec. 02**	**Modules 10, 11 – Network Security, and System Security** • Electronic mail security, S/MIME, PGP • Malware, Worms, DDoS attacks, SBGP **Readings:** • Textbook section(s): 19.1-19.5; 21.1-21.10;	
Week 16 **Dec. 05 – Dec. 09**	• **Dead Week – No Class (Dec. 06, 08)**	**Due Friday, 12/09** • **HW 4** **Due Sunday, 12/11** • **Project 3**