

ITEC 6323, Enterprise Security

Applied Cryptography and Information Systems Security

Week	Fundamentals of Secure Systems	Cryptography Decrypted	Outside Readings	"Hands On" Projected
24 Oct	Ch 1 Introduction Ch 2 Classic Cryptography	Ch 1 Locks and Keys Ch 2 Substitution and Caesar's Cipher Ch 3 Transposition Ciphers Ch 4 Diffuse and Confuse	<i>Selections from:</i> Guideline for Implementing Cryptography In the Federal Government, NIST 800-21, Units 1 through 6 (Pages 5 -70)	
31 Oct	Ch 3 Symmetric Key Cryptosystems Ch 4 Hash Functions Ch 5 Public Key Cryptosystems and Digital Signatures Ch 6 Other (Secret Splitting and Cryptographic Protocols, Pages 94-96, 102-109)	Ch 5 DES isn't Strong Anymore Ch 6 Evolution of Cryptography Ch 7 Secret Key Assurances Ch 8 Problems with Secret Key Exchange	Schneier, Bruce; Why Cryptography is Harder than it Looks, Information Security Bulletin, 1997.	Cryptool -Kendal
7 Nov	Ch 7 Computer Security Ch 8 Computer Security Threats	Ch 9 Pioneering Public Key Ch 10 Confidentiality Using Public Keys Ch 11 Making Public Keys Ch 12 Creating Digital Signatures	Whitten, Alma, Why Johnny Can't Encrypt, In Security and Usability, 2005.	OpenSSL - Custom
14 Nov	Ch 9 Network Security Ch 10 Network Security Threats	Ch 13 Hashes Ch 14 Message Digest Assurances Ch 15 Comparing Secret	Selections from: Guide to IPsec VPNs NIST SP 800-77	TrueCrypt

		Key, Public Key, and Message Digests		
21 Nov	Ch 11 E-mail and WWW Security Ch 12 E-mail and WWW Threats Ch 13 Intrusion Detection Systems	Ch 16 Digital Certificates Ch 17 X.509 Public Key Infrastructure Ch 18 Pretty Good Privacy and the Web of Trust	Introduction to Public Key Technology and the Federal PKI Infrastructure NIST SP800-32 Ch 1 Introduction Ch 2 Background Ch 3 Public key infrastructures Ch 4 Issues and risks in CA system operation	Advanced Protocol Analysis SSL & IPsec IP Tables? Password Auditing? SSH Demo? (Putty)
28 Nov	Thanksgiving Holiday	Holiday	Holiday	
5 Dec	Ch 14 Electronic Commerce	Part IV Real World Systems Ch 20 SSL and Ch 21 IPsec	Selections from: Guideline on Network Security Testing NIST 800-42	Network Security Monitoring Hacker Challenge?
12 Dec	Final Project Demonstrations & Final Exam			

Online Handbook of Applied Cryptography
<http://www.cacr.math.uwaterloo.ca/hac/>