20-ECES-653 NETWORK SECURITY

Catalog Data: 20-CS-653. Network Security. Credits 3. Current concerns, trends and techniques to ensure security and safety of data on computer and over networks. Topics include PGP, RSA, Diffie-Hellman, authentication, integrity, confidentiality, denial of service, security policy enforcement and management techniques. Prereq: 20-CS-229, 15-MATH-253.

Textbook: Kaufman, Perlman & Speciner, *Network Security: Private Communication in a Public World*, 2nd Ed., 2002.

References:

1. Schneier, Bruce, *Applied Cryptography*, 2nd Edition, Wiley, 1996.
2. Doraswamy, Neganand, *IPSec: The New Security Standard for the Internet, Intranets, and Virtual Private Networks*, 1999.
3. Denning, *Cryptography and Data Security*, 1982.
4. Stallings, *Network and Internetwork Security*, 1995.
5. Chapman and Zwicky, *Building Internet Firewalls*, 1995.
6. Daemen and Rijmen, *The Rijndael Block Cipher.*
7. Morris and Thompson, *Password Security: A Case History*, CACM, Vol. 22, Num. 11, Nov. 1979.
8. Feldmeier and Karn, *UNIX Password Security – Ten Years later*, Crypto89
9. *The Keyed-Hash Message Authentication Code (HMAC).*

Coordinator: John Franco, Professor, Computer Science

Knowledge and Comprehension Goals: The student will know:

1. What a secret key cryptosystem is
2. What a public key cryptosystem is
3. What a message digest is
4. What stream and block ciphers are
5. How to implement message integrity, confidentiality and authentication
6. Some of the mathematics behind the crypto algorithms discussed

Application Goals: The student will be able to:

1. Implement RSA, HMAC, Diffie-Hellman, Fiat-Feige-Shamir algorithms in Java.
2. Use network security principles to protect a complex system.
3. Use certificates to authenticate some party.
4. Use an asymmetric block cipher (Karn) to encrypt.

Prerequisites by Topic: The usual programming courses that a senior will have taken including 20-CS-229, Software Development in C++ and 15-MATH-253, Calculus 3. The student is expected to know what Object Oriented Programming is and is expected to have significant programming experience in OOP, especially using C++.

Topics:

1. Introduction: Firewalls, Viruses, Hashes, Message Digests, etc
2. Cryptography: Secret Key Algorithms (DES,3DES,AES,IDEA)
3. Cryptography: Hashes and Message Digests (SHA and variants)
4. Cryptography: Public Key Algorithms: (RSA,ECC,DH,Zero-knowledge)
5. Authentication, Handshake Pitfalls
6. Review and Exam
7. Kerberos
8. IPSec+IKE
9. SSL/TLS

10. PEM, PGP, GPG, etc.

Contributions to CS Student Outcomes:
(a) an ability to apply knowledge of mathematics, science, and engineering
(i) a recognition of and an ability to engage in life-long learning
(j) a knowledge of contemporary issues

Outcomes × Goals and Primary Assessment Methods:

Goal	(a)	(i)	(j)
Know-1	HW		Project
Know-2	HW		Project
Know-3	HW		Project
Know-4	HW		Project
Know-5	HW		Project
Know-6	HW		Project
App-1		Project	Project
App-2		Project	Project
App-3		Project	Project
App-4		Project	Project

Computer Usage: Four homeworks and project

Area Coverage:

AREA	HOURS
Algorithms	5
Data Strcutures	1
Computer Organization and Architecture	0
Software Design	6
Concepts of Programming Languages	0

Laboratory Projects: Final project that counts as a final examination

Prepared by: John Franco., Ph.D. **Date:** June 2009