

COURSE DESCRIPTION

Department and Course Number: **CSC 252**

Course Coordinator: **Ted Krovetz**

Course Title: **Cryptography Theory and Practice**

Total Credits: **3**

Current Catalog Description: Introduction to design and analysis of cryptographic systems. Symmetric cryptography: block ciphers and secure hash functions. Asymmetric cryptography: key exchange and public-key systems. Authentication and encryption in an adversarial model. Simple cryptanalysis. Protocol design and analysis. Prerequisite: Fully classified graduate standing in Computer Science, Software Engineering or Computer Engineering.

Textbook: Stinson, *Cryptography Theory and Practice, Second Edition*, Chapman & Hall/CRC, 2002.
Rescorla, *SSL and TLS*, Addison-Wesley, 2001.

References: Menezes, van Oorschot and Vanstone, *Handbook of Applied Cryptography*, CRC, 1996. Online at <http://www.cacr.math.uwaterloo.ca/hac/>.

Bellare and Rogaway, *Introduction to Modern Cryptography*. Lecture notes online at <http://www-cse.ucsd.edu/users/mihir/cse207/classnotes.html>.

Course Goals: To give an appreciation of (i) the basic use and construction of cryptographic primitives, (ii) the complexity-theoretic assumptions made in their use, (iii) the fragility of secure network protocols, and (iv) experience using cryptography and cryptography toolkits in programming.

Prerequisite by Topic:

Thorough Understanding of:

- Programming in C, C++ or Java, including the use of libraries.
- Basic probability.
- Analysis of algorithms: Big-Oh.

Basic Understanding of:

- Programming in C, including the use of pointers.
- Proof methods, especially contradiction.
- Networks, including ISO network model, TCP, UDP and IP.
- Network programming using sockets.

Major Topics Covered in the Course:

1. Goals of Cryptography. Adversarial model. Examples of achieving goals using a random function. (1 week)
2. Block ciphers. Random permutations. Modeling block ciphers as collection of random permutations. (1 week)
3. Cryptanalysis. Historical ciphers. Cryptanalysis of simple block ciphers. (2 weeks)
4. Block cipher encryption. Modes of operation. Attacks on encryption schemes. (1 week)
5. Cryptographic hash functions. Properties. Constructions. (1 week)
6. Authentication. Message and password authentication. (1 weeks)
7. Public-key primitives: Diffie-Hellman and RSA. Discrete logarithm and large-number factorization is thought to be hard. (2 weeks)
8. Public-key cryptography. Encryption and signature schemes. Certificates. (1 weeks)
9. Network protocols. Breaking poor protocols. Proving good protocols. Key distribution. (1 weeks)

10. Case studies: SSL, IPSec. (2 weeks)
11. Security is more than cryptography. Secure programming. Social engineering. Policies. (1 weeks)
12. Exams, reviews and evaluations. (1 week)

Outcomes:

Thorough Understanding of:

- Adversarial model in cryptography.
- Properties of cryptographic primitives: block ciphers, secure hash functions, public-key cryptosystems.
- Encryption modes-of-operation.
- Key-exchange and distribution goals, assumptions and protocols.

Basic Understanding of:

- Cryptographic programming using a cryptographic toolkit.
- Goals and techniques of cryptanalysis.
- SSL and IPSec protocols.

Exposure to:

- Programming to avoid security vulnerabilities.

Laboratory Projects: Several programming projects involving the use of OpenSSL will be assigned.

Estimated CSAB Category Content:

	CORE	ADVANCED		CORE	ADVANCED
Data Structures			Computer Organization and Architecture		
Algorithms		2.0	Concepts of Programming Languages		
Software Design		1.0			

Oral and Written Communications: No significant component

Social and Ethical Issues: No significant component

Theoretical Content: This course addresses the complexity theoretic assumptions made by modern cryptographers.

Problem Analysis: Assigned homework will require analysis of the usages of cryptographic primitives and the design of cryptographic protocols with regard to security and vulnerabilities.

Solution Design: Students will be asked to design solutions to several problems mimicking design techniques learned in the course.

Last modified 10 November 2005.