

Syllabus for INFA640 (Cryptography and Data Protection)

Course Description

(Formerly CSMN 681.) An overview of the theory of encryption using symmetric and asymmetric keys, current protocols for exchanging secure data (including the Data Encryption Standard and the Advanced Encryption Standard), and secure communication techniques. A review of the historical development of cryptographic methods and cryptanalysis tools is provided. Public Key Infrastructure and the use of digital signatures and certificates for protecting and validating data are examined. Strategies for the physical protection of information assets are explored.

Course Goals/Objectives

At the end of the course, students should be able to:

1. Assess threats to stored and communicated data and vulnerabilities inherent in networked information systems that can be exploited to attack stored and communicated data.
2. Compare and contrast the basic mathematical characteristics of commonly available commercial cryptographic algorithms and their relative strengths and weaknesses.
3. Analyze various encryption techniques and their appropriate uses in the assurance of privacy, integrity, and authentication in information systems.
4. Distinguish among applicable cryptographic protocols and other security countermeasures and assess tradeoffs of security, performance and cost.
5. Assess the security impacts on cryptographic systems of technological advances in computing, networks, and telecommunications.
6. Evaluate the technical and non-technical issues involved with using cryptography for data protection in the burgeoning controversies surrounding security, privacy, electronic commerce, computer crime, information sharing, and cyberwar, and be able to relate these issues to their own environment wherever applicable.

Course Materials

Schneier, Bruce. (1995). Applied Cryptography: Protocols, Algorithms, & Source Code in C, 2nd ed. John Wiley & Sons

Project Descriptions

Topic/Themes: PGP Project

Due Date: Monday (12/3/2007) by 11:59 pm (Eastern)

- Download and implement PGP. (**Note:** You can download a copy of the program <http://www.pgp.com/products/freeware.html>, or at a wide variety of sites that you

can find with a search engine online. Use of PGP by students is free. The current download is version 9.0, which has advanced features. After 30 days, it will revert to a freeware version, which includes all of the components needed for this class. As always, be very careful to know that you are downloading what you think before you execute any program on your computer. Malicious code sometimes masquerades as legitimate software.)

- Create a key pair (Be SURE to keep track of your passphrase.)
- Export your public key to an .asc file
- Submit your public key to the professor by email to be signed by the professor.
- Import all keys from the class PGP assignment to your keyring

Project Report Description: The report for the PGP Project will be in the form of a short journal that describes your experiences using PGP. Additional information on the project and the report format will be provided early in the semester.

IMPORTANT NOTES:

- Your downloaded version of PGP may expire after 30 days and revert to the freeware version. DO NOT WORRY. None of the features that we use for this class will expire.
- **DO NOT LOSE TRACK OF YOUR PASSPHRASE!!!**

Topic/Themes: Short Paper #1

Due Date: Monday (10/1/2007) by 11:59 pm (Eastern)

Description: Instructions for Short Paper #1 will be posted early in the semester.

Topic/Themes: Short Paper #2

Due Date: Monday (11/5/2007) by 11:59 pm (Eastern)

Description: Instructions for Short Paper #1 will be posted early in the semester.

Course Schedule

Readings/Assignments		
Session	Date	Readings, Assignments, and Due Dates
		<ul style="list-style-type: none"> • Administrative and Ethics Topics • Course Overview • How Cryptography Works and Historical Lessons from Classical Cryptography • Information Security Overview-The Context

<p>Session 1 Introduction and Course Overview</p>	<p>9/4 - 9/10</p>	<p>in which Cryptography Functions</p> <ul style="list-style-type: none"> • Confidentiality, Integrity and Availability • What Needs Protection, How Much and How Long • Protection, Detection and Correction • Risk Management • Threats, Vulnerabilities, Countermeasures and Impacts <p>Readings: Schneier: Section 1.1</p>
<p>Session 2 Encryption Basics</p>	<p>9/11 - 9/17</p>	<ul style="list-style-type: none"> • Introduction to Cryptography • Historical Context • Encryption Terms and Basic Concepts • Steganography, Transposition and Substitution <p>Readings: Schneier: Sections 1.2 - 1.3</p>
<p>Session 3 Cryptography and Cryptanalysis: From Paper to Machines</p>	<p>9/18 - 9/24</p>	<ul style="list-style-type: none"> • Multiliteral Substitutions and Polyalphabetic Substitutions • One-time Pads • Machine Ciphers-Cipher Wheels, Hagelin Machines, Enigma and Purple <p>Readings: Course Content: i) <i>Claude Shannon on Cryptography</i>, and ii) Cryptanalysis Document Schneier: Sections 1.4 - 1.7</p>
<p>Session 4 Modern Symmetric Encryption Algorithms</p>	<p>9/25 - 10/1</p>	<ul style="list-style-type: none"> • Modern Symmetric Key Algorithms • Overview of XOR Substitution • Pseudorandom Number Generation • Data Encryption Standard (DES) • Key Management for Symmetric Key Systems <p>Readings: Course Content: i) DES Tutorial, and ii) Rijndael Tutorial Schneier: Sections 2.1 - 2.2; 12.1 - 12.7; 15.1 - 15.2 Short Paper #1 due on Monday (10/1/2007) by 11:59 pm (Eastern)</p>
	<p>10/2 -</p>	<p>Public Key Algorithms</p>

<p>Session 5 Asymmetric Encryption Algorithms</p>	<p>10/8</p>	<p>Diffie-Hellman Rivest-Shamir-Adelman Encryption (RSA) El Gamal Digital Signature and the Digital Signature Standard (DSS) Key Management and Certificate Authorizes Readings: Course Content: <i>The Mathematics of RSA</i> Schneier: Sections 2.5 - 2.7; 19.1 - 19.10; 20.1 - 20.8; 22.1 - 22.7</p>
<p>Session 6 Authentication and Hash Functions</p>	<p>10/9 - 10/15</p>	<ul style="list-style-type: none"> • Authentication Overview • Kerberos • Hash Function Overview • Hash Algorithms <p>Readings: Course Content: Authentication Paper Schneier: Sections 2.3 - 2.4; 2.8; 3.1 - 3.3; 18.1 - 18.14; 24.5</p>
<p>Session 7 Security Protocols and Tradeoffs</p>	<p>10/16 - 10/22</p>	<ul style="list-style-type: none"> • Overview of Security Protocols • IP Security • Digital Notary Publics • Certified Time Stamping <p>Readings: Schneier: Sections 4.1; 10.1 - 10.9</p>
<p>Session 8 Mid-Term Examination</p>	<p>10/23 - 10/29</p>	<p>The Mid-Term Examination will be posted on Tuesday (10/23/2007) by 12:01 am and is due on Monday (10/29/2007) by 11:59 pm (Eastern)</p>
<p>Session 9</p>	<p>10/30 - 11/5</p>	<ul style="list-style-type: none"> • Database Concepts • Relational Databases • Object-Oriented Databases • Statistical Databases • Multilevel Secure Databases • Database Security • Identification and Authentication • Access Control

<p>Cryptography and Database Security</p>		<ul style="list-style-type: none"> • Concurrency Control • Authorization Models • Inference <p>Readings: Schneier: Section 3.8 Short Paper #2 due on Monday (11/5/2007) by 11:59 pm (Eastern)</p>
<p>Session 10</p> <p>Email and Distributed Security</p>	<p>11/6 - 11/12</p>	<ul style="list-style-type: none"> • Electronic Mail Security • Security Services and Controls • Encryption/Protocol Tradeoffs • "Pretty Good Privacy" (PGP) • S/MIME <p>Readings: Schneier: Sections 24.10; 24.12</p>
<p>Session 11</p> <p>Security Standards, Web Security, e-Government, and e-Commerce</p>	<p>11/13 - 11/19</p>	<ul style="list-style-type: none"> • Standards • Web Security • e-Government Security • e-Commerce Security <p>Note: Next week (11/20 - 11/26) is Fall Break. There won't be class - enjoy the break!</p>
<p>Session 12</p> <p>Cryptography Policy: Encryption Controversy, Export Control, and Key Escrow</p>	<p>11/27 - 12/3</p>	<ul style="list-style-type: none"> • The Encryption Controversy • Export Control of Cryptography • Access to Enciphered Traffic • Key Escrow • Skipjack and the Clipper Chip • CALEA • The President's Commission on Critical Infrastructure Protection • Presidential Decision Directive 63 • Cyber Defense Initiative <p>Readings: Schneier: Sections 25.1 - 25.16 PGP Project due on Monday (12/3/2007) by 11:59 pm (Eastern)</p>
	<p>12/4 - 12/10</p>	<ul style="list-style-type: none"> • Folklore • Elliptic Curve Cryptography

<p>Session 13</p> <p>Emerging Issues in Cryptography</p>		<ul style="list-style-type: none"> • Wireless Networks • Quantum Cryptography • Biometric Encryption <p>Readings: Course Content: i) <i>Cryptography and Physical Locks</i>, ii) <i>Chaffing and Winnowing</i>, and iii) <i>Cryptography and Computer Virii</i> Schneier: Section 23.16</p>
<p>Session 14</p> <p>Final Examination</p>	<p>12/11 - 12/17</p>	<p>The Final Examination will be posted on Tuesday (12/11/2007) by 12:01 am and is due on Monday (12/17/2007) by 11:59 pm (Eastern)</p>