CRYPTOGRAPHY: ALGORITHMS AND APPLICATIONS

CS627

Spring 2003

This syllabus is available in both PDF format and HTML format. Compared to the PDF format, the HTML version contains many URL links, including the links to teaching slides (in the COURSE CONTENTS section).

TIME AND PLACE

Time	:	Monday – Friday
Place	:	On the Web

INSTRUCTOR INFORMATION

Name	:	Drs Steven J. Greenwald and Xunhua Wang
E-Mail	:	sjg6@gate.net and wangxx@jmu.edu
Phone	:	(540) 568-3668
Fax	:	(540) 568-2745 (add Attn: Xunhua Wang)
Office	:	ISAT/CS 205
Web Site	:	Blackboard. Copies of syllabus and course content will also be available from http://www.cs.jmu.edu/users/wangxx/2003spring-cs627/index.html
Office Hours	:	Monday–Friday. May also be available on weekends but not guaranteed

CATALOG DESCRIPTION

Cryptographic techniques to achieve confidentiality, integrity, authentication and non-repudiation are examined. The underlying mathematical concepts are introduced. Topics to be covered include symmetric and public key encryption, hashing, digital signature, cryptographic protocols and other recent developments in the field.

PREREQUISITES

CS 515	Fundamentals of Computer Science for Information Security
or	
CS252	Discrete Structures
or	the permission of the instructor
NOTE	CS240 (Algorithms and Data Structures) will also be helpful

TEXTBOOK

Required	:	William Stallings. *Cryptography and Network Security Principles and Practices (The* **3rd** *Edition).* Prentice Hall Press. 2002. ISBN: 0130914290. Visit author's website about this book and errata on this book.
Optional	:	Douglas R. Stinson. *Cryptography: Theory and Practice (The* **2nd** *Edition).* CRC Press. 2002. ISBN: 1584882069. See the author's page. Here is Amazon's link. Important: errata A. Menezes, P. van Oorschot and S. Vanstone. *Handbook of Applied Cryptography.* CRC Press. 1996. Note that this book is available electronically on-line *for free* at http://www.cacr.math.uwaterloo.ca/hac

GRADING

Your grade in the course will be earned / calculated as follows:

Class participation				40%	
Homework				20%	
Final				40%	
GRADE		POINT	RANGE		DESCRIPTION
A	→	90	–	100	Excellent
B^+	→	87	–	89	Very Good
B	→	80	–	86	Good
C	→	70	–	79	Poor
F	→	0	–	69	Failure

Notes

1. Each lecture starts 12:01AM, Monday and ends 11:59PM, Sunday of the same week.
2. In-class participation. This class will be taught as a distance learning course and in-class participation is in the form of on-line discussion. Students are expected to participate in the on-line discussions.

   The class participation grade will be based on the quality of the questions you ask, your answers to and comments on other students' questions. There are 3 points for each discussion. Your grades in each discussion will be available the following week **in the Blackboard system**.
3. The final exam will last 2 hours and will be administrated by Prometric. Additional 30 minutes will be given to allow students familiar themselves with the final exam environment.
4. A student will be able to see only his/her grades. The Blackboard system is designed to protect students' privacy.
5. There will be no extensions to homework and exams unless students can provide convincing evidences (such as documented medical or family emergencies).
6. This grading policy is subject to change, depending on the performance of the students. Notice will be given if this is necessary.
7. Homework must be submitted through the Blackboard system. **When submitting your homework, please use *your-first-name_your-last-name_Homework_homework-unit-number* as the file name**.

LATE PENALTIES

Each lecture starts from Monday and ends on the Sunday of the same week. An assignment is considered late if it is not submitted before the 11:59pm/23:59 of the Sunday of the due week. Late assignments that are submitted within one week of the due date will receive a 20% point penalty. Assignment submitted after the 1 week deadline will receive a 50% point penalty.

IMPORTANT DATES

First class	:	January 13th
Drop deadline without tuition liability	:	January 28th
Add deadline	:	
Drop deadline without Dean's permission	:	
Midterm exam	:	
Last class	:	May 2nd
Final Exam	:	May 5th - 9th

ACADEMIC HONOR CODES

You are required to read the JMU Academic Honor Code and abide by it.

The details of the JMU academic honor code can be found in Section VI of the JMU Student Handbook.

STUDENTS WITH DISABILITIES

Students with disabilities who require reasonable accommodations to fully participate in course activities and/or meet course requirements are strongly encouraged to register with the Office of Disability Service (ODS) and contact me to privately discuss access issues. ODS will provide you with an Access Plan Letter that will verify your need for services and make recommendations for accommodations to be used in my classroom. ODS is located in the Wilson Hall Learning Center, Room 107. Phone/TTY 8-6705.

COURSE CONTENTS

Table 1 gives the tentative schedule for this course. In the HTML version of this syllabus, for each lecture, you can find the URL links to the teaching slides.

COURSE OBJECTIVES

By the end of this semester, you should be able to

1. explain in your own words the following terminologies:
   (a) cryptology, cryptography, cryptanalysis, steganography, threat, assets, vulnerability, confidentiality, integrity, availability, authentication, non-repudiation, general use cryptosystem, restricted use cryptosystem, code
   (b) plaintext, ciphertext/cryptogram, encryption/encipherment, key, symmetric key, public key, private key, Kerckhoff assumption, perfect secrecy, one-time pad, unconditional secrecy, conditional/computational secrecy, substitution, transposition, unicity distance, diffusion, confusion, Feistel cipher, DES weak keys, DES semi-weak keys, stream cipher, block cipher, AES, DES, Triple-DES, Blowfish, IDEA, RC2, RC5, ECB, CBC, CFB, OFB, brute-force attack, ciphertext-only attack, known-plaintext attack, chosen plaintext attack, chosen ciphertext attack, adaptive chosen ciphertext attack, differential cryptanalysis, linear cryptanalysis.
   (c) one-way function, RSA, ElGamal, DH, DSA/DSS, elliptic-curve cryptosystem, Rabin cryptosystem, Chinese Remainder Theorem (CRT), discrete algorithm, GCD, extended GCD, prime, key exchange, authenticated key exchange, mutual authentication

Table 1: Course Contents (Tentative)

Date			Topic / Activity	Text	Notes
Week	Starting Date	Ending Date			
1	Jan 13th	Jan 19th	Syllabus & Introduction	Chap 1	
2	Jan 20th	Jan 26th	The confidentiality model, classical techniques	Chap 2	
3	Jan 27th	Feb 2nd	DES	Chap 3	
4	Feb 3rd	Feb 9th	AES	Chap 4, 5	
5	Feb 10th	Feb 16th	Other Modern Symmetric Ciphers	Chap 6	
6	Feb 17th	Feb 23rd	Applied Confidentiality	Chap 7	
7	Feb 24th	March 2nd	Number theory	Chap 8	
8	March 3rd	March 9th	Public key encryption: RSA, Elliptic Curve	Chap 9	
9	March 10th	March 16th	Spring Break (no class)		
10	March 17th	March 23nd	Key management	Chap 10	
11	March 24th	March 30th	The authentication model, MAC, HMAC	Chap 11	
12	March 31st	April 6th	Hash algorithms	Chap 12	
13	April 7th	April 13th	Digital signature: RSA,DSA	Chap 13	
14	April 14th	April 20th	Authentication applications	Chap 14	
15	April 21st	April 27th	E-mail Security	Chap 15	
16	April 28th	May 2nd	Course Review	NOTES	
17	May 5th	May 9th	**Final Exam**		

(d) authentication, digital signature, hash function, MD5, SHA-1, RIPEMD-160, MAC, HMAC, dictionary attack

(e) digital certificate, PKI

(f) replay attack, active attack, passive attack.

(g) link encryption, end-to-end encryption, traffic analysis, random, pseudo-random

(h) PGP, GPG, S/MIME

(i) Kerberos

(j) PKCS, FIPS

2. explain the confidentiality model.

   (a) For the symmetric key cryptography model, the students should be able to compare and contrast block cipher with stream cipher, AES with DES, ECB with CBC.

   (b) For the Public key cryptography model, one should know

      i. how RSA encryption/decryption works (how to find two large primes, how RSA decryption works, how to do modulo exponentiation efficiently), why we need PKCS#1, why and how we can use Chinese Remainder Theorem to speed up the computation.

      ii. how ElGamal works

3. explain the authentication model. Students should be able to explain the difference between authentication and non-repudiation

   (a) how RSA digital signature works
   (b) how DSA works

4. explain the difference between key transport and key agreement; how DH works; what is vulnerability of the original DH key agreement.

5. explain what is Birthday attack? what is dictionary attack?

6. explain how Kerberos achieves the property of stateless. Why do we need TGT server in Kerberos?

7. Understand that cryptography always assume secure implementation, which is hard to achieve in real world. Explain side channel attack, power attack, timing attack, fault analysis.

STUDY HINTS

- You do not need to be a mathematician to understand cryptography. Mathematical background necessary to understand cryptography will be covered/reviewed in class. But be prepared to think hard and review the course materials from time to time.

- Exams are based on the course objectives. If you or your team can master the objectives, you will do well. Also restudying your course objectives from time to time may help a lot.

- For each homework/exam, after returning the grades, please see me after class (rather than later) if you have any questions.

- The course slides are designed to help you master the important points quickly. They are not intended to replace the textbooks and you are required to read the textbooks after reading the slides.

- Applied cryptography (to network security) is a very hot area. There is an increasing demand for information security professional (please see me if you need more information). Your efforts will be greatly rewarded (for instance, you will be able to easily pass the cryptography part of the CISSP exam).

- Applied cryptography is a fast developing area which might even make those books recently published obsolete. For instance, PKCS #1, which is about how RSA is implemented, is not covered in Stallings' book (instead, raw RSA is covered there which is not considered secure in real world!); AES is recently announced and DSA is recently modified (p should be 1024-bit long in DSA now and a new pseudorandom number generator is adopted), which are not reflected in many course textbooks. Secret sharing, which is a very important topic, is not covered in William Stallings' book; password-based cryptography (PBE, SRC, SPEKE, etc) is not covered in any selected textbooks.

  This course is structured for the most recent development (at least to my best knowledge). So, stick to your notes.

- This course focuses on the practical aspect of cryptography. Many advanced topics (such as unconditional security, threshold cryptography, secure distributed computing and zero knowledge proof) are not covered in this course. If you need some further reading, please send me emails.

- Do NOT hesitate to ask questions. Cryptography is a tricky subject. Many protocols and cryptosystems designed by smart cryptographers were broken some years later. Indeed, many ciphers and security applications provide *no* provable security. There are no silly questions in this field. So, do not get intimidated.
- This is an Internet-based course and I will try to make myself available as possible. Normally you can expect fast responses from me during weekdays. Occasionally I will also check the Blackboard and my emails on Saturday. I might not be available on Sunday.
- In addition to the discussion board, there will be at least one 1-hour Virtual Classroom session per week, which allows students and instructor to have **real time** communications. It is not mandatory but is highly recommended. *It is highly recommend that students prepare some questions before each Virtual Classroom session.* Both the discussion boards and the Virtual Classroom are archived and students who miss them can read the transcripts later.
- Please use Blackboard for communication to me and avoid personal email as possible. In case of emergency, you can call me.

QUOTES

``It is insufficient to protect ourselves with laws; we need to protect ourselves with mathematics''

— Anonymous

``Skill in production cryptanalysis has always been heavily on the side of the professionals, but innovation, particularly in the design of new type of cryptographic systems, has come primarily from the amateurs.''

— Whitfield Diffie and Martin Hellman

``...all the great cryptographic papers in the world do not protect a single bit of traffic''. Codes do.

— Whitfield Diffie