CS 627: Cryptology, Spring 2007 Semester

Course Syllabus

Introduction and Overview:

Cryptology is a discipline that for thousands of years that dealt exclusively with the secrecy of messages, and therefore it was restricted almost entirely to the military environment. It is only within the past thirty years or so that it has become prominent in the civilian world as well. The reason for the recent civilian interest is the potential offered by cryptology for providing a variety of security services for electronic commerce. The recent proliferation of distributed and networked systems has done much to enhance the potential of cryptography to contribute to the security of the enterprise. Communications security has become a major issue. Someone who wants to deploy cryptologic techniques to maximum advantage must understand what cryptography is and how it works, and must also have some notion of cryptanalytic techniques and of the modes of hostile attacks. In addition, he/she must also have a good grasp of the principles of communications protocols, including the practical details of the major communications protocols currently in common use and under development, and in particular of how cryptology can be applied in conjunction with a variety of communications protocols to provide a substantial level of protection to the user.

Summary Course Description:

Key cryptologic terms, concepts, and principles are defined and explained. Traditional character-based cryptographic and cryptanalytic techniques are covered, perspective on successes and failures in cryptologic history, and also modern, computer-based techniques, including both single-key, i.e., symmetric algorithms, and also asymmetric, or double-key algorithms. Block ciphers and stream ciphers are described, modes of operation of symmetric ciphers, and their application in the form of several cryptographic algorithms, including DES, “triple-DES”, IDEA, Blowfish, RC5, CAST-128, RC5 and Rijndael (AES) algorithms, and also special cryptanalytic techniques. Newer uses of cryptography

are discussed, including authentication of message origin and also of message content (data integrity) to the satisfaction of a disinterested third party, and also non-repudiation (digital signature), and access control, as well as issues pertaining to cryptographic keys, including key generation, key control, key distribution, key recovery/escrow, and key certificates, including the X.509 public key infrastructure. Issues in network communications and in network security; the ISO-OSI model for data communications, OSI communications protocols, and the TCP/IP protocol suite will also be discussed, as well as the use of cryptologic protocols to provide a variety of security services in a networked environment, including the Secure Socket Layer (SSL), Transport Layer Security (TSL), IPsec, and secure E-mail. Social and public policy issues pertaining to the commercial development, availability, and marketing of both software and hardware for encryption will also be discussed.

Course Outline:

1. Introduction to, and Basic Concepts of, Cryptology
    a. Cryptography
    b. Cryptanalysis
    c. Principal Uses of Cryptology:
        (i) Secret Writing
        (ii) Authentication of Sender (Digital Signature)
        (iii) Authentication of Message Content
        (iv) Certification of Delivery
        (v) Non-Repudiation
        (vi) Various protocols
            (a) Voting
            (b) Simultaneous contract committal
            (c) Digital cash
            (d) Remote logon/passage of clearance

2. Classical Cryptography
    a. Codes vs. Ciphers
    b. Substitution Ciphers and Transposition (Permutation) Ciphers
    c. The Caesar Cipher
    d. Monoalphabetic Ciphers
    e. Cryptanalysis of Monoalphabetic Ciphers
    f. Polyalphabetic Ciphers
    g. Cryptanalysis of Polyalphabetic Ciphers
        (i) Kasiski Method
        (ii) Friedman Method
    h. Rotor Machines: Enigma and Purple

i. The One-Time Pad

3. Modern Cryptographic Methods I: Symmetric (Single-Key) Encryption
    a. Feistel Cipher Structure
        (i) Number of Rounds
        (ii) Function **F**
        (iii) S-boxes
        (iv) Diffusion
        (v) Confusion
        (vi) Key Length Issues
    b. "Data Encryption Algorithm" (DEA), the basis for the Data Encryption Standard (DES)
        (i) Sub-Key Generation
        (ii) Rounds
        (iii) S-Box Design
        (iv) Modes of Operation I: Electronic Codebook Mode (ECB)
        (v) Modes of Operation II: Cipher Block Chaining Mode (CBC)
        (vi) Modes of Operation III: Cipher Feedback Mode (CFB)
        (vii) Modes of Operation IV: Output Feedback Mode (OFB)
    c. Cryptanalytic Attacks against DES
        (i) Differential Cryptanalysis
        (ii) Linear Cryptanalysis
        (iii) Brute Force Attack
        (iv) Double-DES and the Meet-in-the-Middle Attack
        (v) Triple-DES
    d. Rijndael (Advanced Encryption Standard, AES)

4. Modern Cryptographic Methods II: Asymmetric (Dual-Key or Public Key) Encryption
    a. Principles of Dual-Key Encryption
    b. Rivest-Shamir-Adelman (RSA) Algorithm
    c. Elliptic Curve Cryptography: the El-Gamal Algorithm and DSA
    d. Massey-Omura Algorithm
    e. The problem of Key Management
    f. Diffie-Hellman Key Exchange

5. Hash Functions and Message Authentication Codes
    a. Hash Functions and Message Authentication Codes (MACs)
    b. Security of Hash Functions
    c. HMAC

6. Digital Signatures and Authentication Protocols
    a. Digital Signature using Conventional (symmetric) Encryption
    b. Digital Signature using Public-Key Encryption
    c. Digital Signature Algorithm (DSA) and the Digital Signature Standard (DSS)

7. Security in Networks
    a. Principles of Protocol Layering
    b. The ISO's OSI Model (seven protocol layers)
    c. Connection-Oriented Network Services
    d. Connectionless Network Services
    e. Details of OSI Layering
    f. Real-World Protocols: the TCP/IP Protocol Suite
    g. Provision of Cryptography in Lower Protocol Layers vs. Upper Layers
    h. Issues in the Management of Security Services

8. Use of Cryptography in Authentication
    a. Passwords, Password-Guessing, and Password Sniffing
    b. Password Spoofing and Password Verification Spoofing
    c. One-Time Passwords
    d. Authentication Protocols
    e. Kerberos
    f. Authentication Exchanges
    g. Certificate Distribution and Exchange
    h. Entity Authentication
    i. Data Origin Authentication

9. Access Control Policy and Mechanism
    a. Group-Based Access Control
    b. Individual Access Control
    c. Role-Based Access Control
    d. Category-Based Access Control
    e. Traditional Approaches to the Control of Access
        (i) Tokens
        (ii) Capabilities
        (iii) Access Control Lists (ACLs)
        (iv) Security Labels
        (v) Security Models
    f. Issues in Network Access
    g. Generation, Revocation, Distribution, and Storage of Access Control Information

10. Confidentiality and Integrity
    a. Flow Controls
    b. Data Granularity
    c. Data Padding
    d. Traffic Padding
    e. Testwords
    f. Seals or Signatures

g. Sequence Integrity
h. Redundancy
i. Integrity Recovery
j. Security Transformations
k. Security Labels

11. Non-Repudiation
    a. Phases and Roles
        (i) Generation of Evidence
        (ii) Transfer/Storage of Evidence
        (iii) Verification of Evidence
        (iv) Resolution of Disputes
    b. Non-Repudiation of Origin
    c. Non-Repudiation of Receipt

12. Security for Electronic Mail and for Electronic Data Interchange (EDI)

Course Objectives:

By the end of the course, the student should be able to:

a. Explain, implement, and make use of the commonly used forms of cryptography, as well as the principal uses of cryptography, including both public key and symmetric cryptography.

b. Make practical use of the following types of cryptosystems, and understand comprehensively the principal advantages and vulnerabilities of each: Affine and other types of monoalphabetic substitution ciphers, Vigenère and other types of polyalphabetic substitution ciphers, DES in four modes, as well as other block ciphers such as IDEA, Blowfish, and AES-Rijndael (AES), RSA, and DSA.

c. Explain the theoretical problems as well as the practical issues associated with pseudo-random number generators and with cryptographic hash functions, and both select and implement appropriate instances of each.

d. Compare, contrast, and select the appropriate cryptographic techniques for a given security application and security policy.

e. Deploy cryptography effectively in appropriate layers of the communications protocol stack to support the security of a computing facility (for example, password protection, Identification and

Authentication, Communications Security, Message Confidentiality, Confidentiality of Sender and of Recipient, Message Integrity, Authentication of Sender, Non-Repudiation, and so on).

f. Implement and make use of key control, key distribution, and key exchange algorithms.

g. Adopt a reasoned, well-thought-out position on the major contemporary public policy issues related to cryptographic technology.

h. Extend his/her knowledge of the field of cryptology by reading articles dealing with cryptology published in professional journals.

Required Textbooks and Materials:

(1) FERGUSON, NIELS; & SCHNEIER, BRUCE (2003). *Practical Cryptography* Indianapolis, IN: Wiley Publishing, Inc. 2003276249; 005.8/2 22; QA76.9.A25 F466 2003; ISBN 0-471-22894-X (hardcovered), & 0-471-22357-3 (paperback)

(2) SINGH, SIMON (1999). *The Code Book: The Evolution of Secrecy from Mary, Queen of Scots to Quantum Cryptography*. Doubleday. ISBN 03859495315. $17.47

(3) STALLINGS, WILLIAM (2006). *Cryptography and Network Security. Principles and Practices. Fourth Edition.* Upper Saddle River, NJ: Prentice-Hall. TK5105.59.S713 2006; 005.8—dc21; 2006276085; ISBN 0-13-187316-4.

Suggested Supplementary Materials:

1. Cryptology-related:

(4) BEUTELSPACHER, ALBRECHT (1994). *Cryptology: An Introduction to the Art and Science of Enciphering, Encrypting, Concealing, Hiding, and Safeguarding Described Without any Arcane Skullduggery, but not Without Cunning Waggery, for the Delectation and Instruction of the General Public.* (Transformation from German into English Succored and Abetted by J. Chris Fisher. Washington, DC: Mathematical Association of America. QA76.9.A25B49 1994; ISBN 0-88385-504-6. $34.00

(5) MEL, H. X.; & BAKER, DORIS; with math appendix by STEVE BURNETT (2001). *Cryptography Decrypted.* QA76.9.A25 M44 2000; 005.8'2-dc21; 00-046878; ISBN 0-201-61647-5.

2. Writing-related

(6) BRIANS, PAUL (2003). *Common Errors in English Usage.* Wilsonville, OR: William, James & Co. PE1464 .B75 2003; 421/.1 21; 2003044605; ISBN 1887902899. [Provides a list of common errors along with an explanation of each.]

(7) GORDON, KAREN ELIZABETH (1993a). *The Deluxe Transitive Vampire: The Ultimate Handbook of Grammar for the Innocent, the Eager, and the Doomed.* New York, NY: Pantheon Books. ISBN: 0679418601. [This book is a concise, wittily written tutorial on the fine points of grammar.]

(8) GORDON, KAREN ELIZABETH (1993b). *The New Well-Tempered Sentence: A Punctuation Handbook for the Innocent, the Eager, and the Doomed.* New York, NY: Pantheon Books. PE1450.G65 1993; 428.2—dc20; 93-18454; ISBN 0-395-62883-0. [This book is a concise, wittily written tutorial on the fine points of punctuation.]

(9) DUPRE, LYN (1998). *Bugs in Writing Revised. A Guide to Debugging Your Prose.* Reading, MA: Addison-Wesley. ISBN: 0-201 37921-X. [The author specifically

addresses the needs of computer professionals and other technical people to write clearly.]

(10) STRUNK, WILLIAM, JR.; & White, E.B. (2000). *The Elements of Style. With Revisions, an Introduction, and a Chapter on Writing. Fourth Edition.* New York, NY: Longman. PE1408.S772 1999; 808'.042—dc21; 99-16419; ISBN 0-205-30902-X (paperback) or 0-205-31342-6 (casebound). [A classic on clarity in writing.]

Additional Reading Materials:

Three lists of additional reading materials are provided. Two of these are traditional paper-based materials, one consisting of textbooks and other book-length materials (REFERENCES-ON-INFOSEC-AND-CRYPTO.PDF), and the other consisting principally of articles published in cryptographic or other Computer Science journals (LANDMARK-JOURNAL-ARTICLES-ON-CRYPTO.PDF). In addition to the two lists of conventionally published materials, a list of Uniform Resource Locator (URL) references is also provided (URLS-ON-CRYPTOLOGY.PDF).

Instructor:

Dr. Charles Abzug

Course Practices:

Attendance Policy, and Relationship of Course Sessions to Readings: In class, announcements are sometimes made of new or changed course policies, requirements, modifications to assignments, etc. Information provided in such announcements may not appear anywhere in the course documentation. Furthermore, course sessions will cover *some* of the material in the readings, but will *also* include some material *not* covered by the readings. Therefore, students **must** not only do all of the readings, but must **also** attend **all** classes.

There are only three acceptable grounds for a student's missing a class: (1) grave medical or (2) serious personal problems affecting the student him/herself, or in some cases affecting a member of the student's immediate family. Immediate family is defined for the purpose of this policy as father/grandfather, mother/grandmother, sister, brother, spouse, or fiancé to whom you are formally engaged. (NOTE: I do **not** consider your girlfriend/boyfriend to be a member of your immediate family.) The other acceptable excuse for a student's missing a class is (3) ***force majeur*** (overpowering force due to an unexpected and uncontrollable event). An example of ***force majeur*** is the occurrence of a flat tire or of a motor vehicle accident involving your vehicle while you are traveling to class. If you want to claim exemption on one of these three grounds, be prepared to submit evidence (e.g., a note from a licensed physician on physician's stationery, or copy of police accident report).

I normally take attendance at every class. Attendance does not get factored directly into the grading process. Why, then, do I take attendance? The purpose is two-fold: (i) attendance data sometimes provide me with advance information that a student may be experiencing academic difficulty because of medical or personal problems, or for some other reason. In addition, I may also consult attendance records in deciding how much I am willing to extend myself in providing help should you get into academic difficulty during the semester. You are in a much better position to get a "break" if you have been conscientiously attending class.

Note that if you do miss out on a class, it is **your** responsibility to find out what we covered in class, as well as what announcements might have been made. It is also your responsibility to obtain the missed material. "I wasn't in class when you made that announcement" is **not** an acceptable excuse for your failure to comply with any directives issued in class. Please see the companion to this section entitled, "Policy on Classes Missed by Students".

E-mail on Course-Related Matters: All E-mail messages related to the course must be identified by a Subject header of the form: ***CS-xyz-n {additional subject identification},*** where ***xyz*** is the three-digit course number, ***n*** is the section number, and additional subject identification is appended following the course and section numbers. Thus, a submission of homework assignment 47 for course CS-789 Section 13 would have a Subject header: ***CS-789-13-Assignment-47.***

Grading of Tests and Assignments, and the JMU Honor Code: You will eventually be assigned an overall course grade. The course grade will be based principally upon your performance on quizzes, exams, homework assignments, projects, etc. Integrity of the grading process requires that you be graded on the basis of **your own work** and not on someone else's. Yet, sometimes a student may get stymied and not be able to complete an assignment on his/her own. ***If you find it necessary to obtain help from someone else in completing your assignment, you are required to indicate that by clearly marking it on your assignment.*** Thus, if one of your colleagues contributes a line of code to your

computer program, you should plainly mark that via a comment inserted into the text of the program, as in the following example:

```
//Hieronymous Johnson kindly contributed the following line of code to my program:
for (int i=0, k=4-I; i<10; k=Math.abs(4-++I+(i>4?1:0)));
```
[1]

Similarly, non-programming assignments should be clearly footnoted or annotated to indicate where someone else's help contributed to the product. In the absence of a clear annotation in your submitted assignment, you will be assumed to be the sole author of all work that you submit. Should that turn out not to be the case, it will be accounted as an honor code violation and will be dealt with severely. Details of the JMU Honor Code are to be found at: http://www.jmu.edu/honor/

The JMU Honor Code specifies that every assignment, whether written or electronically submitted by a student, is submitted pursuant to the Honor Code, and **must contain a declaration** stating that "This work complies with the JMU Honor Code.", together with your signature. **I** personally require that you place this signed declaration **on the first page** of your assignment. If the Honor Code declaration is not included *at the time that the assignment was submitted*, your grade for that assignment will be a zero.

Assignment, Homework, and Term Project Policy: Assignments of problems or exercises from the course text must be submitted in **legible** hard copy. Programming projects and major assignments, such as a term project or an essay ("paper") must be machine-generated (i.e., not hand-written), and must be submitted **both** in hard- and in soft-form.

Format: The source code of your program and the program's output should be on separate sheets of paper. Multiple pages of hard-copy must be **stapled** together[2], and **both** hard and soft copies must have, in the upper left corner of the first page:

(a) your name
(b) course number
(c) section number
(d) semester (e.g., Fall 2001)
(e) date of submission, and
(f) Honor Code declaration, with your signature.

[1] I am indebted to Prof. David Brunner for contributing the coding example shown above.

[2] If you do not own a stapler, there is one available for student use in the Copy Center (HHS Room 1002).

Please note that I have no trouble remembering my own name. Therefore, you do not need to write my name on your homework assignments, term projects, etc.

Content: All written work should be thoroughly professional in accordance with the highest standards. Your writing should be clear, should comply with the rules of grammar of the language in which it is written (for most of my courses, this will be English), as well as with good writing practice, and should be correctly spelled and punctuated and free of both slang and jargon.

Late Submissions Policy: All work is due at the designated date and time. Under some circumstances, I might be willing to accept a late submission. If so, then late submissions are subjected to the following penalties:

Date Submitted	Penalty from Maximum Credit
One day late	10%
Two days late	20%
Up to one week late	40%
Up to two weeks late	60%
Over two weeks late	100%

Grading Policy:

Overall Meaning/Definition of Grades: A grade of ***A,*** either on an individual assignment or for the entire semester, indicates work that is truly outstanding in the opinion of the instructor, demonstrating excellent mastery of the material covered. A grade of ***B*** indicates very good work, meeting minimum expectation for a graduate student. A graduate grade of ***C*** indicates work that is not satisfactory, although adequate to receive credit for passing the course. A grade of ***D*** cannot be awarded for graduate study. A grade of ***F*** indicates work far below the minimum level considered to be satisfactory, demonstrating insufficient achievement in the skills or level of knowledge required even at the undergraduate level, and certainly at the graduate level.

Extra-Credit Opportunities. Grades are based only on assignments given to every student in the class. Opportunities to earn extra credit may be announced to the entire class at various times during the semester, but extra-credit assignments will NOT be custom-crafted for the sake of an individual student. Your best strategy is to learn the course material by conscientiously studying and doing your

assigned homeworks throughout the semester. If you wake up at the end of the semester and suddenly realize that you are in trouble, there may not be anything that you can do.

Extra Tutorial Assistance: I will be pleased to provide extra help in most instances to any student who requests it. However, the student who needs help must **both:** (i) take the initiative on his/her own to seek me out, **and** (ii) seek help in a timely manner and not wait until the last minute, when the examination or assignment due date is already imminent. You must also understand that I am willing to help when your own assiduous efforts to learn the material prove to be inadequate. I can**not** provide tutorial assistance to a student who cannot find the time to do the assigned readings and homeworks.

Homework Assignments and Projects, Term Project, and Final Examination: There will be a term project and a final examination. In addition, there will be several homework assignments or possibly projects or presentations or reports assigned at various points during the semester. The examination will be based **both** upon the reading assignments, regardless of whether or not the readings were covered in class, **and** also upon the material covered in class, regardless of whether or not the assigned readings also cover the same material. Please note that you will be held responsible not only for material that the instructor presents in class, but also for any presentations made by yourself or by your fellow students.

Class Participation: Vigorous student participation in class discussion makes for a much more lively and interesting class for all. To encourage participation in class discussion, the grading mechanism includes the opportunity for the student to earn a reward (details given below) for participating both **vigorously and constructively** in class. Note that your mere attendance can **not** considered to be "class participation", and will **not** be rewarded with class participation points. Attendance is mandatory, and therefore rewards will not be meted out merely for attendance. However, your vigorous and constructive participation in class discussion will certainly make the class more interesting both for me and for your fellow students as well as for yourself, and this therefore can possibly result in an enhancement to your grade, as well.

Assignment of Grades: Makeup of overall grade for the semester will be as follows: First, a numeric score will be calculated based upon the student's performance on all the examinations, on the quizzes and homeworks, and on the term project. The basis for calculating the numeric score is:

Homework Assignments, Projects, and Presentations:	30 pts
Term Project:	35 pts
Final Exam:	35 pts
TOTAL:	100 pts
Opportunities possibly to be announced, and class participation points :	$\leq$10 pts

After the numeric scores have been determined, letter grades will be assigned, based upon the distribution of the numeric scores. I make **no** commitment in advance regarding the letter-grade equivalent of specific numeric grades. The standard cutoff scores for grades are: 90 for ***A,*** 80 for ***B,*** and 70 for ***C.*** However, I reserve the right to lower the cutoff points in accordance with my judgment after studying the actual distribution of numeric scores.

Enhancement of Grades for Vigorous Class Participation: An initial assignment of grades is made to all members of the class as described above. After the initial assignment of grades has been made, additional points will be dispensed to those students who participated vigorously and effectively in class discussion. This may result in the improvement of the grades for such students. Thus, non-participation will **not** lower anyone's grade, but high-quality participation may **possibly** raise it.

Legibility and Clarity-of-Communication Requirements for Quizzes, Examinations, Homeworks, and Term Papers: It is up to you, the student, to demonstrate to the satisfaction of your instructor that you have mastered the course material. We know that at the time of your birth you knew nothing about the subject matter of this course. If a change has occurred between then and now, then *you* must demonstrate that this has taken place. Therefore, your writing and drawing must be clear and unambiguous, and your answer should be obviously correct on its own, without benefit of any verbal explanation of your answer that you may provide *post hoc*. What this means is that:

(i) your handwriting must be legible to the instructor;
(ii) you must, yourself, bear the burden of choosing the correct words and technical terms that answer the question;
(iii) your drawings must be neat, technically correct, and properly labeled;
(iv) your sentences must be properly structured, and paragraphs must be correctly and logically organized;
(v) you must thoroughly address **all** the specific issues raised by the question; and
(vi) for multiple-choice, fill-in-the-blank and other short-answer type questions, you are responsible for marking the answer in the correct place on the answer sheet. The grader will **not** be responsible for searching for the correct answer in other places, nor can credit be given after the fact for notations made on your question booklet that

were not reflected in the answer marked on your answer sheet. Be careful, and check what you are doing. It can be very frustrating for student and instructor alike when a student who knows the material has to take a lower grade than he or she could have earned, because of the student's carelessness in marking the answer properly on the answer sheet. Nevertheless, Computer Science, like airline piloting, is notoriously unforgiving of mistakes, and minute attention to detail is one of the personal properties that the faculty tries to inculcate in our students.

Errors in Grading: Unclear answers will be marked **wrong.** Instructors are human and sometimes make mistakes, too. You are entitled to complain politely after class if you honestly feel that your answer is both clear and correct, but was misunderstood at grading time by the instructor. If the instructor agrees that a mistake was made, then your grade will be cheerfully corrected.

Rules for Examinations:

(1) No calculators, no books, no notes.
(2) The JMU Honor Code must be scrupulously observed.
(3) All work **must** be shown on your examination paper. You will certainly be given extra paper if you ask for it.
(4) You must provide exactly ONE answer to each test question. In the event that you should provide more than one answer, the answer that is **wrong** is the one that will be graded.
(5) All examinations **must** be taken at the scheduled time. If you miss the scheduled examination, you are responsible for providing **timely** documentation to support a medical or other *bona fide* emergency to avoid getting a grade of zero for the examination. Medical exemption requires certification from a licensed medical practitioner or facility. The documentation must be provided on the practitioner's letterhead and must be dated and signed by the practitioner, and must clearly certify the time range over which you were incapacitated. The practitioner's telephone number must also appear on the document.

Note that there is a deadline for submitting your documentation to support medical or other excused absence. The deadline is one calendar week after you return to class.

Homework Assignments:

Educational Philosophy: There are three ways for a student to learn complex technical subject matter, such as you will encounter in this course. First is by reading. Second is by coming to class and both watching and listening **interactively.** Third is by working selected problems and examples. This course has been carefully designed to integrate at least the first two, and perhaps all three modes of teaching and learning. There may be some material covered in the reading assignments that will **not** also be covered in the classroom, and there is other material **not** covered in the reading assignments that will be covered **only** in the classroom. Students will be held responsible **both** for the content of all assigned readings, ***whether or not covered in class,*** **and** also for all classroom material, ***whether or not covered in the assigned readings.*** To assist you in reviewing both the readings and the classroom materials, and in preparation for the examinations, review questions covering the main points may be provided, and in some cases answers as well. Students are **well advised** to answer review questions in writing, and, where applicable, also to work out solutions to assigned problems in detail before peeking at the answers. The reason for this recommendation is that in first crafting your own answers or your own solutions you will be much more seriously stress-testing your own level of comprehension of the material. Then, when you compare your own answers with those provided to you, you will gain much better insight into any deficiencies in comprehension that you may have. If you look at the answers first, it will go much faster for you, but you will suffer in the depth of learning that you will attain. I treat you as adult by providing the answers up front in some cases and by trusting you to use good judgment in working through the problems before consulting the answers. Please don't disappoint me.

Types of Assignments: Details of homework assignments for this course are specified in a separate document. In general, a homework assignment may have one or more of four components: readings, review questions, practical exercises, and reports (oral and/or written). Readings **must** be done on time, so that you will be properly prepared for, and get full benefit from the class. Review questions are also extremely important for you to answer prior to the class when they are due. In most cases, your answers to review questions will *not* be collected and graded, but these questions are excellent preparation both for a brief quiz that you may possibly encounter when you come to class and for the lengthier scheduled examinations. Readings, review questions, practical exercises, and reports must all be completed no later than the scheduled due date and must be ready for submission on the due date at the beginning of class. Some or all of the homeworks will be collected. These will be graded **not** on the basis of whether the answers are correct, but merely on the basis of whether the homework was done completely and conscientiously.

Group Projects: One or more projects may be assigned during the semester. Any assigned projects, including the Term Project, may be assigned either as individual projects or as Group Projects. Any project assigned as a group project **must** be done as a group project. Even if you prefer to work by yourself and are willing to do by yourself all the work required for the project, you must nevertheless join a group to work on any project designated as a group project, and you must also participate as a full partner with your fellow-students in the group. Group members are **advised** to exchange **both** telephone numbers **and** E-mail addresses immediately upon formation of the group, to facilitate inter-member communication (this is a ***recommendation,*** not a requirement). Each member of the group is responsible for cooperating fully with the other members of the group, and for doing his/her full agreed-upon share of the work *in concert with* the rest of the group. For every group project assignment, the

group is required to deliver, along with their written project report, a written ***Work Breakdown*** statement, indicating precisely what contribution each member of the group made to the overall project.

Policy Regarding Classes Missed by Students:

In the university environment, there is an implied contract between students and faculty. You (students) expect us (faculty) to come to class. I, as a faculty member, also expect all of my students to come to class. Occasionally, you may find it necessary to miss a class. If you must miss an occasional class, I trust you, as a responsible adult, to do so only for adequate reason. Therefore, you don't need to seek my permission before skipping a solitary class, nor do you need explain afterwards why you were absent. Please note, however, that I do look particularly askance at students who miss the last class prior to a vacation period and/or the first class after vacation. The university is very generous with scheduled vacations, and I expect you to make do with the allotted vacation days and **not** to take for yourself an extension of your vacation period beyond what the university has generously scheduled for all students and faculty. Airline tickets can usually be procured for travel ***during*** the scheduled vacation period, if they are purchased sufficiently in advance. In the event that you are unable to obtain a ticket without committing yourself to straying into the time scheduled for classes, then I invite you to make alternate plans and to spend your vacation closer to Harrisonburg.

If you have missed the class for good and valid reason, nevertheless you **are** responsible for making up the work you missed, as well as for complying with any announcements, directives, or instructions that might have been issued during the class that you missed. Therefore, it is up to **you** both to find out what was covered or announced, **and** to make up in a timely fashion any missed work.

You would be wise to prepare, as early as the very first day of the semester, for the possible occurrence of sudden brief acute illness (tummy ache, head ache, etc.), or of other, non-medical emergencies, such as a flat tire, traffic jam, family emergency, or the like. I suggest that you exchange phone numbers and E-mail addresses on the first day of class with several of your classmates. If at all possible, give notice to one of your colleagues prior to the class you will miss. Follow up as soon as possible after the missed class, so that you will be able to stay abreast of what is happening in class. Also, if you know in advance that you must miss a class, you should arrange to have someone hand in for you any assignments you may have done that are due that day. If you did not make advance arrangements, then it is even more important both that you follow up rapidly to find out what you missed and that you make up for missed work.

Do **not** send me E-mail, either asking in advance of the class you must miss what do I intend to cover, or querying me subsequently to the class on what did I cover. I teach many students each semester, and I just don't have the time to answer a blizzard of "What will I miss?" and "What did I miss?" E-mails. In the fortunately rare case that a student encounters a serious health problem or an

issue in his/her personal or family life that spans several consecutive classes, it is my experience that I have almost always been able to make a special accommodation to try to help the student through the crisis, and I will certainly make every effort to do so in the future, as well. But I must insist that you take care of the onesies and twosies on your own.

Class Meetings:

Classes meet during the Spring 2007 semester on Tuesday and Thursday evenings from 1830 to 1945 hrs in ISAT/CS Room 243.