THE SAULT COLLEGE OF APPLIED ARTS AND TECHNOLOGY
SAULT STE. MARIE, ON

COURSE OUTLINE

Course Title: Cryptography

Code No.: 222-4 Semester: Three

Program: Computer Networking

Author: The Mathematics Department

Date: August 2003 Previous Outline Dated: August 2002

Approved: ______________________ ________________________
Dean Date

Total Credits: 4
Prerequisite(s): MTH122
Hours/Week: 3

For additional information, please contact Colin Kirkwood, Dean
School of Technology, Skilled Trades, and Natural Resources,
705) 759-2554, Ext. 688

I. COURSE DESCRIPTION:

Students will study basic aspects of probability and cryptography,

II. STUDENT PERFORMANCE OBJECTIVES:

The basic objectives are that the student develop an understanding of the methods studied, demonstrate a knowledge of the facts presented and show an ability to use these in the solution of problems. To accomplish these objectives, exercises are assigned. Test questions will be of near equal difficulty to questions assigned in the exercises. The level of competency demanded is the level required to obtain an overall passing average on the tests. The material to be covered is listed below.

III. TOPICS TO BE COVERED: APPROXIMATE TIME FRAME

A. Probability **20 periods**

1. Elementary combinatorics
2. Elementary Probability Theory
3. Conditional probability and independence
3. Measures of central tendency
4. Measures of dispersion
5. Random variables
6. Binomial, Normal, and Poisson Distributions

B. Cryptography **30 periods**

1. Mathematics associated with cryptography (a basic look)
2. Cryptography Fundamentals
3. DES and Symmetric Keys
4. RSA and Public Keys
5. CAST
6. IDEA
7. DSA
8. Cryptographic hash functions and MAC’s (message authentication codes)
9. Random numbers and PRNG’s
10. Real World Applications

IV. LEARNING OUTCOMES AND ELEMENTS OF THE PERFORMANCE:

a) Elementary Combinatorics – instructor handout

Potential Elements of the Performance:

- Use factorial notation
- Use permutation and combination formulae correctly

b) Elementary Probability Theory – instructor handout

Potential Elements of the Performance:

- Use basic rules of probability

c) Conditional probability and independence – instructor handout

Potential Elements of the Performance:

- Understand the difference between dependent and independent events
- Understand conditional probability
- Apply formulae for multiple dependent, independent, and conditional events

d) Measures of central tendency – instructor handout

Potential Elements of the Performance:

- Understand various measures of central tendency, and how they are used
- Correctly apply associated formulae

e) Measures of dispersion – instructor handout

Potential Elements of the Performance:

- Understand various elementary measures of dispersion
- Correctly apply associated formulae

f) Random Variables – instructor handout

Potential Elements of the Performance:

- Understand various elementary aspects of random variables and their significance in probability theory
- Correctly apply associated formulae

g) Binomial, Normal, and Poisson Distributions – instructor handout

h) Mathematics associated with Cryptography –text

Potential Elements of the Performance:

- Understand some aspects of mathematics associated with public and private key cryptography

i) Cryptography Fundamentals – text

Potential Elements of the Performance:

- Understand some aspects of network security

j) DES and Symmetric Keys – Class notes

Potential Elements of the Performance:

- Understand symmetric key protocol
- Understand DES algorithms

k) RSA Public Keys – Class notes

Potential Elements of the Performance:

- Understand public key protocols
- Understand RSA algorithm

l) CAST – Class notes

Potential Elements of the Performance:

- Understand CAST algorithm

m) IDEA – class notes

Potential Elements of the Performance:

- Understand IDEA algorithm

n) DSA – Class notes

Potential Elements of the Performance:

- Understand DSA algorithm

o) Cryptographic hash functions and MAC's – text

Potential Elements of the Performance:

- Understand basic purpose and implementation of Cryptographic hash functions and MAC's

p) Real World Applications – text

Potential Elements of the Performance:

- Understand the purpose and implementation of public key distribution, X.509 public key infrastructure, PGP, secure email, kerberos, secure socket and transport layer, IPSec

V. REQUIRED RESOURCES / TEXTS / MATERIALS:

1. **Text: <u>Cryptography Decrypted</u>, by H. X. Mel and Doris Baker, Addison-Wesley**
2. Calculator: (Recommended) SHARP Scientific Calculator EL-546V. *Note: The use of some kinds of calculators may be restricted during tests.*

VI. EVALUATION PROCESS/GRADING SYSTEM:

MAJOR ASSIGNMENTS AND TESTS

Regular topic tests will contribute a minimum of **60%** of the overall mark.

While regular tests will normally be scheduled and announced beforehand, there may be an unannounced test on current work at any time. Such tests, at the discretion of the instructor, may be used for up to **30%** of the overall mark.

The instructor will provide you with a list of test dates and other required evaluation information for your class section. Tests may be scheduled out of regular class time.

ATTENDANCE

It is your responsibility to attend all classes during the semester. Research indicates there is a high correlation between attendance and student success.

If you are absent from class, it is your responsibility to find out what work was covered and assigned and to complete this work before the next class. Your absence indicates your acceptance of this responsibility.

Unexcused absence from a test may result in a mark of zero ("0"). Absence may be excused on compassionate grounds such as verified illness or bereavement. On return from an excused absence, you should ask your instructor to schedule the writing of a make-up test. Failure to do so will be considered as an unexcused absence.

METHOD OF ASSESSMENT (GRADING METHOD)

The following semester grades will be assigned to students in postsecondary courses:

Grade	Definition	Grade Point Equivalent
A+	90 - 100%	4.00
A	80 - 89%	3.75
B	70 - 79%	3.00
C	60 - 69%	2.00
F (Fail)	59% and below	0.00

VI. EVALUATION PROCESS/GRADING SYSTEM (continued):

CR (Credit)	Credit for diploma requirements has been awarded.
S	Satisfactory achievement in field /clinical placement or non-graded subject area.
U	Unsatisfactory achievement in field/clinical placement or non-graded subject area.
X	A temporary grade limited to situations with extenuating circumstances giving a student additional time to complete the requirements for a course.
NR	Grade not reported to Registrar's office.
W	Student has withdrawn from the course without academic penalty.

The method of calculating your weighted average will be defined by your instructor. Since grades are based upon averages, it follows that good marks in some tests can compensate for a failing mark in another test.

Make-Up Test (if applicable)

An “X” grade may be assigned at the end of the regular semester if you have met ***ALL*** of the following criteria for the course:

- an overall average between 50% and 59% was achieved
- at least 50% of the tests were passed
- at least 80% of the scheduled classes were attended
- at least 80% of quizzes and assignments were submitted
- all of the topic tests were written

If you are assigned an “X” grade, you may convert it to a “C” grade by writing a make-up test on topics agreed to by the instructor. This test will be available at the time agreed to by your instructor.

At the end of the regular term, it is your responsibility to obtain your results from your instructor and, in the event of an “X” grade, to inquire when the make-up test will be available.
The score you receive on this make-up test will replace your original test score and be used to re-calculate your weighted average. If the re-calculated average is 60% or greater, a “C” grade will be assigned. If the re-calculated average is 59% or less, an “F” grade will be assigned.

“F” and “X” Grades at the end of the Semester

If an “X” grade is not cleared by the specified date, it will become an “F” grade. Except for extenuating circumstances, an “X” grade in Math will not be carried into the next semester.

VII. SPECIAL NOTES:

Special Needs:

If you are a student with special needs (e.g. physical limitations, visual impairments, hearing impairments, or learning disabilities), you are encouraged to discuss required accommodations with your instructor and/or the Special Needs office. Visit Room E1204 or call Extension 493 so that support services can be arranged for you.

Retention of course outlines:

It is the responsibility of the student to retain all course outlines for possible future use in acquiring advanced standing at other postsecondary institutions.

Plagiarism:

Students should refer to the definition of "academic dishonesty" in *Student Rights and Responsibilities*. Students who engage in "academic dishonesty" will receive an automatic failure for that submission and/or such other penalty, up to and including expulsion from the course/program, as may be decided by the professor/dean. In order to protect students from inadvertent plagiarism, to protect the copyright of the material referenced, and to credit the author of the material, it is the policy of the department to employ a documentation format for referencing source material.

Course outline amendments:

The Professor reserves the right to change the information contained in this course outline depending on the needs of the learner and the availability of resources.

Substitute course information is available in the Registrar's office.

VII. PRIOR LEARNING ASSESSMENT:

Students who wish to apply for advanced credit in the course should consult the professor or the Coordinator, Mathematics Department. Credit for prior learning will be given upon successful completion of a challenge exam or portfolio.

VIII. DIRECT CREDIT TRANSFERS:

Students who have completed an equivalent post-secondary course must bring relevant documents to the Coordinator, Mathematics Department:

- a copy of course outline
- a copy of the transcript verifying successful completion of the equivalent course

Note: A copy of the transcript must be on file in the Registrar's Office.