COURSE TITLE **BLACKBOARD SITE**	Cryptography MCS 5813 Fall 2012 CRN 2154
INSTRUCTOR	David J. Fawcett Math & Computer Science dfawcett@ltu.edu 248-760-1077 Office hours by appointment
SCHEDULE	August 29 – December 21, 2012 Refer to http://www.ltu.edu/registrars_office/calendar_final_exam.index.asp for the last date to withdraw and other important registration related information.
LEVEL/HOURS **PREREQUISITE**	Graduate or Undergraduate Degree / 3 credit hours Discrete Math
REQUIRED TEXT (See Blackboard for additional resources)	Douglas R. Stinson, Cryptography Theory and Practice, 3rd Edition, Publisher, Chapman and Hall. ISBN 1-58488-0508-4 Available for online purchase through LTU Bookstore at: http://lawrence-tech1.bkstore.com/bkstore/TextbookSelection.do?st=489
ADDITIONAL RESOURCES	LTU Online student resources: http://www.ltu.edu/ltuonline/
TECHNICAL SUPPORT	Technical support for using Blackboard is provided by the Helpdesk, 248.204.2330 or helpdesk@ltu.edu. Send the Help Desk a form detailing any issues by clicking here http://tinyurl.com/3yqrvne.

COURSE SCHEDULE FOR TRADITIONAL SEMESTER COURSES

This fully online course begins with a partial week online course orientation period to familiarize yourself with the online learning environment and to meet online or via the phone with your instructor. Each subsequent week starts on a Monday and ends on a Sunday.

Dates	Modules	Topics / Readings	Assignments Due
Prior to Semester Start and Aug 29 – Sep 2	Module 0	Overview of textbook Online Learning Orientation	Review Topics in Number Theory presentation to get a head start on Module 1.
Week of Sep 3 – Sep 9	Module 1	**Topics in Number Theory** **Objectives/Outcomes** 1. You will be able to apply theorems and methods of Number Theory. 2. You will learn to use the Cryptography Workbench (CWB) software.	1. Self Assessment **#A01** 2. Discussion board (two threads). 3. No homework to turn in.
Week of Sep 10 – Sep 30	Module 2	Chapter 1. **Classical Cryptography** **Objectives/Outcomes** You will be able to discuss the history of cryptography and how the state of the art ciphers worked prior to the computer age. You will be able to apply the terminology used in cryptography. You will apply number theory and statistics to analyze classical ciphers. You will use techniques you learned in class to decrypt messages that were encrypted by classical ciphers.	1. Homework 1 Problem 1.21 parts a, b, c, d. #**A11** 2. Discussion board
Week of Oct 1 – Oct 7	Module 3	Chapter 2 – **Shannon's Theory** **Objectives/Outcomes** You will learn Shannon's original concept of Entropy in Information Systems. You will know how to and will have computed the entropy of a system. You will do research and write a short paper on Entropy.	1. Homework #**A21** 2. Paper on Entropy #**A22** 3. Discussion board

Dates	Modules	Topics / Readings	Assignments Due
		You will be able to apply the idea of "Perfect Secrecy" and its relationship to random numbers to the analysis of other cryptosystems.	
Week of Oct 8 – Oct 21	Module 4	Chapter 3 – **Block Ciphers** **Objectives/Outcomes** You will know how Substitution/Permutation networks (SPNs) work inside DES and AES. You will know what a Linear and Differential Cryptanalysis attack is and how they can be used to attack DES and AES. You will write a research paper on linear and differential cryptanalysis attacks. You will have adapted source code to run the AES on your computer. You will have applied the AES software to encrypt/decrypt a text file. You will be able to discuss the history of DES/AES and the role of NIST.	1. Compile & execute code. Turn in screen shots. **#A31** 2. Paper on linear and differential cryptographic analysis **#A32** 3. Discussion board
Week of Oct 22 – Oct 28	Module 5	Chapter 4 – **Cryptographic hash Functions (CHF)** **Objectives/Outcomes** You will adapt source code to run the SHA-1 or HMAC on your computer. You will create a "message digest" and used it in message security. You will used SHA-1 or HMAC to generate a digest of a text file. You will write a research paper on Cryptographic Hash Functions.	**1.** Compile and execute code. Turn in screen shots **#A41** 2. Paper on CHF **#A42** 3. Discussion board
Week of Oct 29 – Nov 11	Module 6	Chapter 5 – **RSA & factoring Integers** **Objectives/Outcomes** You will use RSA to decrypt several files. You will analyze algorithms for factoring integers. You will be able to explain the relationship between breaking RSA and factoring large integers. You will be introduced to Public Key Cryptography	Homework 5.12 **#A51** Homework 5.3 **#A52** Self assessment **#A53** Discussion board

Dates	Modules	Topics / Readings	Assignments Due
Week of Nov 12 – Nov 19	Module 7	**Midterm Exam**	Midterm #M
Week of Nov 19 – Dec 2	Module 8	Chapter 6 – **Public Key Cryptography and Discrete Logarithms** **Objectives/Outcomes** You will apply the ElGamal algorithm. You will be able to explain the relationship between breaking ElGamal and solving discrete logarithms in mod space. You will program and use several algorithms for solving discrete logs in mod space. You will write a paper on Elliptic Curves and their relation to cryptography. You will learn more about Public Key Cryptography and the Diffie-Helman problem. You will be able to explain the Diffie-Helman key exchange method. **Includes Thanksgiving Break**	1. Homework 6.1, 6.3 & 6.5 **#A61** Paper on Elliptic Curve Cryptography **#A62** 2. Discussion board
Week of Dec 3 – Dec 9	Module 9	Chapter 7 – **Digital Signatures and Authentication** **Objectives/Outcomes** You will apply the ElGamal signature scheme. You will write a paper on the Digital Signature Algorithm You will learn ELGamal can be broken under certain conditions.	Homework 7.3 and 7.4 **#A71** **Paper on DSA #A72** Discussion board
Week of Dec 10 – Dec 16	Module 10	Chapter 14 – **Pseudo Random Number/Bit Generators** **Objectives/Outcomes** You will apply some common PRNGs. You will program the Von Neumann, BBS and RSA PRNGs and generate a list of pseudo random numbers. You will use the CWB to decrypt a probabilistically encrypted file using the BBS PRNG with a known seed.	Homework – file decryption **#A81** Program Von Neumann PRNG **#A82** **Program BBS #A83** **Program RSA PRNG #A84** Discussion board
Week of Dec 17 – Dec 21	Final Exams	Course Summary End of Course	**Final Exam**

STUDENT EVALUATION

The course has 30 assignments (including test and discussion board) totaling 3000 points. Letter grades are awarded based on the total number of points achieved. Points are deducted for late assignments.

Assignments	Points		
A01	25	A52	50
A11	100	A53	25
A21	50	A61	100
A22	100	A62	100
A31	100	A71	100
A32	100	A72	100
A41	100	A81	100
A42	100	A82	50
A51	100	A83	50
See next column		A84	50
Midterm	300		
Final Exam	300		
Online Participation (9 DBs)	900		
Total Points	3000		

Class Points	Letter Grade
96 and above	A
90 – 95	A-
87 – 89	B+
83 – 86	B
80 – 82	B-
77 – 79	C+
73 – 76	C
70 – 72	C-
61 – 70	D (Undergrad Only)
60 and below	E

Note: Grades lower than a "B" fall below the LTU graduate standard

EDUCATIONAL GOALS/ STUDENT LEARNING OBJECTIVES / OUTCOMES

The goals of this course expressed as outcomes are:
The student will learn/understand, apply, and be able to discuss the following:

- *Number theory relevant to Cryptography*
- *The history of Cryptography including "classical ciphers"*
- *The jargon of Cryptography*
- *Shannon's theory and its impact on the field.*

- *Cryptographic Hash Functions and their relationship to security*
- *The RSA algorithm and Integer Factoring*
- *Public Key Cryptography*
- *El Gamal and Diffie Hellman cryptosystems and Discrete Logarithms*
- *Digital Signatures*
- *Pseudo random Number Generators and Probabilistic Encryption*

The student will be able to analyze and evaluate cryptosystems.

PREREQUISITE SKILLS

The student must know how to program. Visual Studio C++ is the preferred language and tool set. The student must be good a mathematics and be able to apply algorithms from Number Theory.

INSTRUCTIONAL METHODS AND COURSE ORGANIZATION

Blackboard Learning Environment – Blackboard at my.ltu.edu contains the syllabus, all assignments, reading materials, streaming videos, narrated PowerPoint mini-lectures, podcasts, written lecture notes, chapter quizzes, links to Web resources, and discussion forums. You will submit all assignments via Blackboard, and are expected to participate regularly in discussion topics. Please take time to familiarize yourself with the organization of the Blackboard site. You will want to check the site frequently for announcements reminding you of new resources and upcoming assignments.
Student/Instructor Conversations – Students keep in touch with the instructor via e-mail messages, telephone conference calls, and IM conversations.
Self-Assessments – Pre- and post- self-assessment tools will help students measure their entering skills and progress during the course.
Required Reading – Textbook chapters should be read according to the schedule outlined in the syllabus. Chapters will be discussed online.
Assignments – Please refer to the course map document "Course Map_MCS5813_Cryptography.xlsx" found in the course resources area.

CLASS POLICIES AND EXPECTATIONS

I plan to offer you a valuable learning experience, and expect us to work together to achieve this goal. Here are some general expectations regarding this course:

Each student has a LTU email account. If you wish to use a different email address for this course, please **change your email address in Blackboard under "Blackboard Tools", then "Personal Information"** and send an email to me to store your email address in my directory.

Readings, discussion forum participation, and written assignments must be completed according to the class schedule. It is important to contact the instructor as needed to discuss personal needs regarding course requirements and assignments.

It is essential that all students actively contribute to the course objectives through their experiences and working knowledge.

All assignments must be submitted on schedule, via Blackboard, and using Microsoft Office compatible software. If you need to submit an assignment via email, contact the instructor in advance.

Assignments must be completed to an adequate standard to obtain a passing grade. Requirements for each assignment are detailed in this syllabus.

Be prepared to log into Blackboard at least once each day. Please focus your online correspondence within the appropriate Blackboard discussion forums, so that your colleagues may learn from you.

At midterm and at the end of the course, you will be invited to participate in a University evaluation of this course. Your feedback is important to the University, to LTU Online, and to me as an instructor, and I strongly encourage your participation in the evaluation process.

It is important for you as students to know what to expect from me as your instructor:

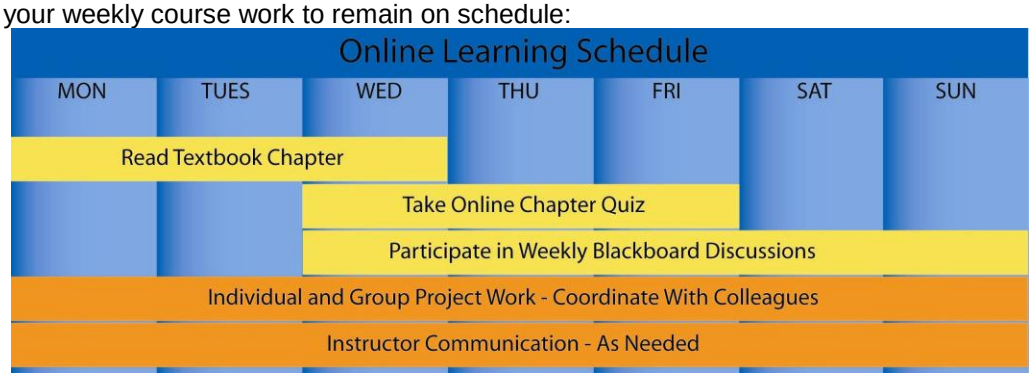
- I will be available to you via e-mail and phone, and will promptly reply to your messages.
- I will be available to you for face-to-face appointments as requested.
- I will maintain the Blackboard web site with current materials, and will resolve any content-related problems promptly as they are reported to me.
- I will send out a weekly e-mail update to all class members to guide upcoming work and remind you of assignment due dates.
- I will return all assignments to you promptly, and will include individualized comments and suggestions with each assignment.
- I will hold our personal written or verbal communications in confidence. I will not post any of your assignments for viewing by the class without requesting your approval in advance.
- I will treat all members of the class fairly, and will do my best to accommodate individual learning styles and special needs.
- If any of these points need clarification, or should special circumstances arise that require my assistance, please contact me so that we may discuss and resolve the matter.

PRACTICAL GUIDELINES FOR CLASS LOAD EXPECTATIONS

A three-credit course generally requires at least nine hours per week of time commitment. Here are some practical guidelines to help schedule your time commitments for this online course:

- A 14-week semester (the Summer semester is compressed into 10 weeks) would require at least 126 hours of time commitment to successfully complete all readings, activities, assignments, and texts as described in this syllabus.
- You should reserve at least 6 hours per week to read the required textbook chapters and resources, participate in online discussions, review presentation materials, and work through online quizzes. This effort will total at least 84 hours over the course of the semester.
- You should organize your remaining time to roughly correspond with the point value of each major assignment. This means that you should plan to spend at least:
  - 8-9 hours preparing your case study review;
  - 24-40 hours working with your group on the three parts of your semester-long project;
  - 8-9 hours working on the various components of your reflective consolidation (final exam).

These guidelines may not reflect the actual amount of outside time that you – as a unique individual with your own learning style – will need to complete the course requirements. The number of hours each week will vary based on assignment due dates, so please plan ahead to insure that you schedule your academic, work, and personal time effectively. The following graphic may be used to guide you in planning your weekly course work to remain on schedule:



ASSIGNMENT DETAILS

Course assignments and evaluation criteria are detailed below. Please review these requirements carefully. See the section Academic Resources / Assessment Guidelines for information about assessment of written and oral presentations.

Details for all assignments are shown below. Please note that you should not submit any assignments to the Blackboard "Digital Drop Box." All assignments are submitted using the Blackboard "Assignments" or "SafeAssign" function. Some assignments are also posted to the Blackboard Discussion Forum for student comments.

Assignments

Please see the "Course Map_MCS5813_Cryptography.xlsx" document (which is shown here below) for assignment details and expectations. Each assignment has a unique number (e.g. A32) that appears in the Gradebook.

Course Map for Cryptography MCS 5813

Ch	Wk #	Wks	Topic		What to do		What to turn in	GB ID
0	**1**	**1**	**Topics in Number Theory**	**1**	Watch presentation "Topics in Number Theory.pptx" and "Using the CWB.pptx"	1	**Assessment 0 - Check the Self Assessment button (not graded, but you have to do it).**	**A01**
				2	Do further research on the Internet/WIKI on the topics in the "Topics in Number Theory" presentation if you feel you do not understand them.	2	**Do the Discussion board (two threads). Discussion board - "Did I have this math in Discrete Math or other courses? Is it new to me? Is there further research or information I need, if so, what" and "What do I expect to learn in this course?"**	
				3	Review all materials in this chapter's supplemental resources	3	**No homework to turn in**	
				4	Install and run the ***Cryptography Workbench*** (CWB) software			
				5	Do the Self Assessment - Do I understand this math?			
				6	*Participate in the discussion board* -			
					Objectives/Outcomes			
				1	You will be able to apply theorems and methods of Number Theory to Cryptography problems identified in this course			
				2	You will use the CWB tool to help you solve problems and understand methods used in this course.			
1	**2**	**3**	**Classical Cryptography**	**1**	Watch presentations Classic Cryptography.pptx & Cryptanalysis.pptx	1	**Homework 1 - Turn in problem 1.21 parts a, b, c**	**A11**

			Shift, substitution, affine, vigenere, hill, autokey, one time pad ciphers	2	Read chapter 1 (concurrently)	2	**Discussion board - "Discuss how you decrypted the three problems in the homework. Use the examples in the text as an outline. Did you try any novel methods not mentioned in the text or write any computer code to help you?"**	
				3	Review all materials in this chapter's supplemental resources	3	**No Assessment to turn in**	
				4	Homework problems 1.21 parts a, b, c			
				5	Participate in the discussion board			
					Objectives/Outcomes			
				1	You will be able to discuss the history of cryptography and how the state of the art ciphers worked prior to the computer age.			
				2	You will be able to apply the terminology used in cryptography.			
				3	You will apply number theory and statistics to analyze classical ciphers.			
				4	You will use techniques you learned in class to decrypt messages that were encrypted by classical ciphers.			
2	**5**	**1**	**Shannon's Theory**	**1**	Watch presentation Shannon's Theory.pptx	1	**Homework 2 - "Suppose there are 3 messages with probabilities 0.5, 0.25, and 0.25. What is the entropy in this case? Compute and give a number, show your work."**	**A2 1**
			Perfect Secrecy	2	Read chapter 2 concurrently	2	**Assessment 2 - Turn in a 3 page paper on Entropy as it pertains to Cryptography. The paper must discuss the relationship of Entropy to the likelihood that an attack can be successful, the formula for computing Entropy, and the impact that Shannon's concept of Entropy had on the field of Cryptography, and any other ideas you think are important to be included.**	**A2 2**
			Entropy	3	Review all materials in this chapter's supplemental resources	3	**Discussion Board - Discuss the impact of Claude Shannon's concepts of Entropy and Perfect Secrecy on the field of cryptography**	
				4	Do further research on Entropy on the Internet/WIKI			
					Objectives/Outcomes			
				1	You will learn Shannon's original concept of Entropy in Information Systems.			
				2	You will know how to and will have computed the entropy of a system.			
				3	You will do research and write a short paper on Entropy.			
				4	You will be able to apply the idea of "Perfect Secrecy"			

					and it's relationship to random numbers to the analysis of other cryptosystems.			
3	**6**	**2**	**Block Ciphers**	**1**	Watch presentation AES & DES.pptx	1	**Assessment 3 - Turn in a screen shot of the AES code you got working that encrypts the file "ga.txt" using the key shown in the file "AES assignment"**	**A3 1**
			S-Boxes	2	Read chapter 3 (concurrently)	2	**Turn in a 3 page paper on linear and differential cryptographic analysis, what is it, how does it work, how is it used. The paper should explain the basics of each method and then compare the differences in the methods. Include some historical details (inventor, time period of use, success/failures). Also discuss the impact of Cryptography of these two methods of attack.**	**A3 2**
			SPN	3	Review all materials in this chapter's supplemental resources	3	**Discussion board - discuss what issues you had getting the AES code to run. If you had no issues, please use the discussion board to help other students who are having issues.**	
			Differential CA	4	Read Wiki articles on DES and AES to further your understanding			
			DES	5	Try to compile and execute the source code provided. Don't wait until the last minute; I will help you if you ask me. You may find AES code in your own preferred language and get it to run if you like.		*Please note: if you cannot get the code to run, there should be lots of discussion (by you) on the board about your issues. Also, you should ask me for help if you don't get what you need from the others.*	
			AES	6	See if you can duplicate the encryption in the picture "AES assignment"			
				7	Do web research and write a paper on linear and differential CA			
				8	Discussion board - discuss what issues you had getting the AES code to run.			

Objectives/Outcomes

1. You will know how Substitution/Permutation networks (SPNs) work inside DES and AES.
2. You will know what a Linear and Differential Cryptanalysis attack is and how they can be used to attack DES and AES.
3. You will write a research paper on linear and differential cryptanalysis attacks.
4. You will adapt source code to run the AES on your computer.
5. You will apply the AES software to encrypt/decrypt a text file.
6. You will be able to discuss

					the history of DES/AES and the role of NIST.			
	8	**1**	Midterm					**M**
4	**9**	**1**	**Cryptographic hash Functions**	**1**	Watch presentation 1 - Cryptographic Hash Functions.pptx	1	**Turn in a screen shot of the digest you created for the file ga.txt with SHA-1 or Turn in a screen shot of the digest you created with HMAC and a key of your choice. Show the key you used for HMAC**	**A4 1**
			Data Integrity	2	Read chapter 4 (concurrently)	2	**Turn in a 3 page paper on Cryptographic Hash Functions. The paper will cover methods to create CHFs, security of CHFs, differences between keyed and non keyed CHFs, iterated hash functions, and SHA and Message Authentication Codes (HMAC).**	**A4 2**
				3	Review all materials in this chapter's supplemental resources	3	**Discussion board - try to get the SHA and HMAC code to run and discuss what issues you had. If you had no issues, please use the discussion board to help other students.**	
			Security	4	Read Wiki articles on SHA-1 and HMAC			
			Iterated Hash Functions	5	Try to compile and execute the source code provided		*Please note: if you cannot get the code to run, there should be lots of discussion (by you) on the board about your issues. Also, you should ask me for help if you don't get what you need from the others.*	
			Secure Hash Functions	6	Write a paper on Cryptographic Hash Functions (CHF)			
			Message Authentication Codes	7	Discussion board - try to get the SHA and HMAC code to run and discuss what issues you had.			
					Objectives/Outcomes			
				1	You will adapt source code to run the SHA-1 or HMAC on your computer.			
				2	You will create a "message digest" and used it in message security.			
				3	You will used SHA-1 or HMAC to generate a digest of a text file.			
				4	You will write a research paper on Cryptographic Hash Functions.			
5	**10**	**2**	RSA & factoring Integers	1	Watch presentation - RSA and Integer Factoring.pptx	1	**Turn in homework problem 5.12 in the text. You will find the text files you need in the supplemental material RSA051.txt and RSA052.txt. (Hint - there are many RSA decoders online or use CWB)**	**A5 1**
			Intro to Public Key Cryptography	2	Review all materials in this chapter's supplemental resources	2	**Turn in homework problem 5.3**	**A5 2**
			Number theory	3	Read chapter 5 (concurrently)	3	**Read this URL "http://www.math.umn.edu/~garrett/crypto/overview.pdf" and complete the self assessment (the PDF is also in the supplemental file)**	**A5 3**

			RSA cryptosystem	4	Homework problem 5.12	4	**Discussion board - what are some advantages/disadvantages of RSA public key cryptography over DES/AES?**	
			Square roots/Factoring		**Objectives/Outcomes**			
			Rabin	1	You will have used RSA to decrypt several files.			
			Semantic Security of RSA	2	You will have analyzed algorithms for factoring integers.			
				3	You will be able to explain the relationship between breaking RSA and factoring large integers.			
				4	You will be introduced to Public Key Cryptography			
6	**12**	**2**	Discrete Logs	1	Watch presentation - ElGamal and Discrete Logs	1	**Turn in problems 6.1, 6.3 and 6.5 at the end of the chapter**	**A6 1**
			El Gamal Cryptosystem	2	Review all materials in this chapter's supplemental resources	2	**Discussion board - discuss the issues you had getting all the algorithms to work in doing problems 6.1, 6.3, and 6.5. If you had no issues, help other students get the code to work.**	**A6 2**
			Algorithms	3	Read chapter 6 (concurrently)	3	**Turn in a 3 page paper on Elliptic Curves and their use in Cryptography. The paper will cover the basic equation, the use in mod space, the reduction in required key length, uses in all areas of Cryptography, and the overall impact on Cryptography.**	
			Elliptic Curves		**Objectives/Outcomes**			
			Security	1	You will apply the ElGamal algorithm.			
			Diffie-Hellman	2	You will be able to explain the relationship between breaking ElGamal and solving discrete logarithms in mod space.			
				3	You will program and use several algorithms for solving discrete logs in mod space.			
				4	You will write a paper on Elliptic Curves and their relation to cryptography.			
				5	You will learn more about Public Key Cryptography and the Diffie-Helman problem(s).			
				6	You will be able to explain the Diffie-Helman key exchange method.			
7	**14**	**1**	Digital Signatures and Authentication	1	Watch the presentation - Signature Schemes.pptx		**Turn in problems 7.3 and 7.4**	**A7 1**
			Security requirements	2	Review all materials in this chapter's supplemental resources		**Turn in a 3 page paper on the DSA algorithm that includes a discussion of the algorithm, it's history, and how it can easily be broken if**	**A7 2**

						mistakes are made in parameter selection or use.	
			ElGamal Signature Scheme Variants of ElGamal Provably secure signature schemes	3 4	Read chapter 7 (concurrently) Discussion board **Objectives/Outcomes** 1 You will apply the ElGamal signature scheme. 2 You will write a paper on the Digital Signature Algorithm 3 **You will show how ELGamal can be broken under certain conditions.**		
8	**15**	**1**	**Pseudo Random Number/Bit Generators** Von Neumann Rand LCG RSA BBS	**1** 2 3 4	Watch the presentation - Pseudo Random Number Generation.pptx Review all materials in this chapter's supplemental resources Read chapter 8 (concurrently) Discussion board **Objectives/Outcomes** 1 You will apply some common PRNGs. 2 You will program the on Neumann, BBS and RSA PRNG and generate a list of pseudo random numbers from each. 3 You will use the CWB to decrypt a probabilistically encrypted file using the BBS PRNG with a known seed.	**Use CWB to decrypt the file "class_encrypted_01" using the seed 21247 and the BBS PRNG & turn in a screen shot of the answer.** **Write a computer program to do the Von Neumann PRNG algorithm and turn in the code and a list of random numbers you generated.** **Write a computer program to do the BBS PRNG algorithm and turn in the code and a list of random numbers you generated.** **Write a computer program to do the RSA PRNG algorithm and turn in the code and a list of random numbers you generated.**	**A8 1** **A8 2** **A8 3** **A8 4**
	16	**1**	**Final exam**				**F**

Online Participation (900) points)

Each student is expected to actively participate in online activities. Class participation is evaluated to a maximum of 900 points based on: Actively participating in Blackboard discussion forums, responding to questions posted by the instructor, and interacting positively with other students.

SYLLABUS ADDENDA

Please see the LTU Online "Current Students" web site http://www.ltu.edu/ltuonline/ for comprehensive information about Lawrence Tech's academic services, library services, student services, and academic integrity standards. The content of this web site is explicitly included in these syllabus requirements.

The LTU Online "Current Students" web site also includes grading rubrics used by your instructor to evaluate written assignments, discussion forum participation, and group assignments. Please note that the SafeAssign anti-plagiarism product will be used for written assignments submitted for this course. Please see the instructions included on the eHelp web site regarding the use of the SafeAssign product.

Undergraduates: Leadership Transcripts

The leadership transcript enables students to track co-curricular activities that are undertaken above and beyond the requirements of the LTU curriculum. The leadership transcript serves students by enhancing the leadership portfolio; providing the opportunity for a transcript of distinction; enhancing their resumes; and assisting in articulating leadership experience. It can be accessed by logging on to Banner Web and clicking the Student and Financial Aid tab. Leadership Activities is located at the bottom of the list. More information is available at http://www.ltu.edu/leadership.