COURSE SYLLABUS
SEC370: CRYPTOGRAPHY

Course Description

This course introduces students to the core principles of modern cryptography with emphasis on formal definitions, clear assumption and rigorous proofs of security. As an introduction to cryptography the course aims to present the foundations of cryptosystems used in the industry.

General Course Information

Number of Units/Weeks	4/10
#Hours Lecture/#Hours Laboratory/#Hours ELPs*	40/0/80
Prerequisite(s)	Discrete mathematics
Co-requisites (s)	None
Course Developer(s)	William Reid, Lars Amoo
Date Approved / Last Review	November, 2015

*Enhanced Learning Projects

Learning Outcomes

- Discuss the principles and practices of cryptographic techniques.
- Categorize the differences between secret key and public key cryptosystems, their strengths, and vulnerabilities.
- Analyze and discuss the design of security protocols and mechanisms for the provision of security services needed for secure networked applications.

Instructional Methods Employed in this Course

- Lecture and reading assignments.
- References, additional reading and exercises.
- Practical application of theory and skills in authentic design projects.(LASA1&2)
- Build on prior knowledge and experience of students to enhance richness of class activities.

Information Resources for this Course

Textbook

Introduction To Modern Cryptography Second Edition. CRC Press, Taylor & Francis Group, 2015. ISBN-13: 978-1-4665-7026-9.

Other Materials
Add text

Web Site Readings
https://www.nada.kth.se/kurser/kth/2D1441/semteo03/lecturenotes/rapport_SS-OW_semteo.pdf
http://calclab.math.tamu.edu/~rundell/m471/goldwasser-micali.pdf
http://csrc.nist.gov/about/ct.html
http://freevideolectures.com/Course/2661/Discrete-Mathematical-Structures#

Table/Topics & Assignments

Types of Assignments:

Lecture -
Considered Lecture Hours

Classroom Discussion -
Considered Lecture Hours

In Class Critique -
Considered Lecture Hours

Delivering Oral Presentations -
Considered Lecture Hours

In Class (IC) Exercise -
Considered Lecture Hours

Reading -
Considered Enhanced Learning Project (ELP), work done outside of class

WebClass lesson (non-online courses) -
Considered ELP, work done outside of class

Lab Work -
Considered Lab Hours

Quiz, Midterm or Final -
Considered Lecture Hours

Week 1						
Type	**Topic/Description**	**LEC Hours**	**LAB Hours**	**ELP Hours**	**Point Value**	**Due**
LEC 1A **Introduction** **Reading:** Sections 1.1, 1.2, 1.3, 1.4.and 2.2	• Introduction and overview / Private-key cryptography. • The syntax of private-key encryption/The shift cipher • Historical encryption schemes and their cryptanalysis. • Modern cryptography: definitions, assumptions, and	4	--	--	--	

	proofs. • Defining perfectly secret encryption.					
IC EX 1A	LASA 1 6-8 Pages of writing	--	--	16.0	200	Week 5
ELP 1A	Week 1 readings-Ch.1&2 (40 pages) Evaluated by IC EX 2A	--	--	4.0	--	
Total Week 1		4	0	20.0	200	

Week 2

Type	Topic/Description	LEC Hours	LAB Hours	ELP Hours	Point Value	Due
LEC 2A **Perfectly secret encryption** **Reading:** Sections 2.2, 2.3, 3.1.1, 3.1.2, 3.1.1, 3.1.2, 3.2.1, 3.3, 3.1.3, and 3.4.1.	• Perfect secrecy and the one-time pad/Limitations of the one-time pad. • Limitations of perfect secrecy. • A computational Security. • Constructing Secure Encryption Schemes • Pseudorandom generators. • Proofs by reduction. • Security for Multiple Encryptions.	4	--	--	--	
IC EX 2A	Chapter 1&2 Review Exercises (10 selected questions)	--	--	4.0	50	End of week 2
ELP 2A	Week 2 readings-Ch.2&3 (40 pages).Evaluated by IC EX 3A	--	--	4.0	--	
Total Week 2		4	0	8.0	50	

Week 3

Type	Topic/Description	LEC Hours	LAB Hours	ELP Hours	Point Value	Due
LEC 3A **Private –Key Encryption** **Reading:** Sections 3.4.2 , 3.5.1, 3.5.2 3.6.1 and 3.6.2. **See: https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation**	•Chosen-plaintext attacks. Formally defining CPA-security. Pseudorandom functions. •Pseudorandom functions/permutations and block ciphers. •CPA-security from pseudorandom functions. •Stream-Cipher Modes of Operation. • Block-Cipher Modes of Operation.	4	--	--	--	
IC EX 3A	Chapter 2&3 Review Exercises (10 selected questions)	--	--	4.0	50	End of week 3
ELP 3A	Week 3 readings-Ch.3 (64 pages) Evaluated by IC EX 4A.	--	--	6.4	--	
Total Week 3		4	0	10.4	50	

Week 4

Type	Topic/Description	LEC Hours	LAB Hours	ELP Hours	Point Value	Due
LEC 4A **Message Authentication Codes** **Reading:** Sections 3.71,3.7.2, 4.1-4.4 4.5- 4.6 **See http://robertheaton.com/2013/07/29/padding-oracle-attack/**	• Security against chosen-cipher text attacks. • CCA-security. Padding-oracle attacks. • Secrecy vs. Integrity • Message Aauthentication Codes (MACs). • Authenticated Encryption • Generic construction • Information theoretic MACs • A fixed-length MAC. • MACs for arbitrary-length messages.	4	--	--	--	
IC EX 4A	Chapter 3 Review Exercises (5 selected questions) / Quiz	--	--	--	50	End of week 4
ELP 4A	Read Chapter 4 (45 pages) Evaluated by IC EX 5A	0	0	4.5	0	
ELP 4B	Midterm Review Chapter 1 – 4 (144 pages) Evaluated by EXAM 5A	--	--	7.2	--	
Total Week 4		4	0	11.7	50	

Week 5

Type	Topic/Description	LEC Hours	LAB Hours	ELP Hours	Point Value	Due
LEC 5A	Course Recap/ Midterm Review	2	--	--	--	
IC EX 5A	LASA 2 5 Pages of writing	--	--	12.0	200	Week 10
ELP 5A	Chapter 4 Review Exercises (10 selected questions)	--	--	4.0	--	
EXAM 5A	Midterm exam will be on any material covered in class through to wk5	2	--	--	150	End of week 5
Total Week 5		4	0	16.0	350	

Week 6

Type	Topic/Description	LEC Hours	LAB Hours	ELP Hours	Point Value	Due
LEC 6A **Hash Functions and Applications**	• Collision Resistance. • Domain Extension • Message authentication using hash functions. • Generic Attacks on Hash Functions.	4	--	--	--	

Reading: Sections 5.1.1-2, 5.2, 5.3, 5.4, 5.5,5.6	• The Random-Oracle Model. • Additional Applications of Hash Functions.					
IC EX 6A	Chapter 5 Review Exercises (10 selected questions)	--	--	4.0	50	End of week 9
ELP 6A	Read Chapter 5 (39 pages) Evaluated by IC EX 6A	--	--	3.9	--	
Total Week 6		4	0	7.9	50	

Week 7

Type	Topic/Description	LEC Hours	LAB Hours	ELP Hours	Point Value	Due
LEC 7A **Practical and Theoretical Constructions of Symmetric-Key Primitives** **Reading:** Sections 6.1.6.2, 6.3, 7.1, 7.2, 7.3,7.4,7.5,7.6,7.7, 7.8	• Stream Ciphers/Block Ciphers/Hash functions. • Attacks on reduced-round SPNs. • Attacks on reduced-round SPNs. • The Data Encryption Standard (DES). 2DES and triple-DES. • AES -Practical constructions of hash functions. • One-Way Functions • Constructing Pseudorandom Generators. • Assumptions for Private-Key Cryptography. • Computational Indistinguishability.	4	--	--	--	
IC EX 7A	Chapter 6 Review Exercises (10 selected questions)	--	--	4.0	25	End of week 7
ELP 7A	Read Chapters 6&7 (56 pages) Evaluated by IC EX 8A	--	--	5.6	--	
Total Week 7		4	0	9.6	25	

Week 8

Type	Topic/Description	LEC Hours	LAB Hours	ELP Hours	Point Value	Due
LEC 8A **Number Theory and Cryptographic Hardness Assumptions** **Algorithms for Factoring and Computing Discrete Logarithms**	• Basic number theory and algorithmic number theory. • Modular arithmetic and efficient algorithms. Group theory. • Primes, factoring and RSA assumptions. • Cryptographic Assumptions in Cyclic Groups. • Cryptographic	4	--	--	--	

Reading: Sections 8.1(Appendices B.1, B.2.1, B.2.2, and B.2.3) 8.2, 8.3, 8.4, 9.1, 9.2 9.3	Applications. • Algorithms for Factoring. • Algorithms for Computing Discrete Logarithms. • Recommended Key Lengths					
IC EX 8A	Chapter 7 Review Exercises (10 selected questions)	--	--	4.0	25	End of week 8
ELP 8A	Read Chapters 8&9 (73 pages) Evaluated by IC EX 9A	--	--	7.3	--	
Total Week 8		4	0	11.3	25	

Week 9

Type	Topic/Description	LEC Hours	LAB Hours	ELP Hours	Point Value	Due
LEC 9A **Key Management and Public-Key Encryption** **Reading:** Sections 10.1, 10.2, 10.3, 10.4, 11.1, 11.2, 11.3,11.4, 11.5	• Key Distribution and Key Management. • Key-Distribution Centers. • Key Exchange and the Diffie-Hellaman Protocol. • Public –Key Revolution. • Public-Key Encryption. • Security against Chosen-Plaintext Attacks • Hybrid Encryption KEM/DEM • CDH/DDH-Based Encryption. • RSA Encryption	4	--	--	--	
IC EX 9A	Chapter 8 Review Exercises (5 selected questions)/Quiz	--	--	4.0	50	End of week 9
ELP 9A	Read Chapters 10&11 (78 pages) Evaluated by 10A	--	--	7.8	--	
Total Week 9		4	0	11.8	50	

Week 10

Type	Topic/Description	LEC Hours	LAB Hours	ELP Hours	Point Value	Due
LEC 10A **Digital Signatures Schemes** **Reading:** Sections 12.1, 12.3, 12.4,12.5, 12.6, 12.7	• Digital Signatures • The Hash-and-Sign Paradigm. • RSA based Signatures. • DSA and ECDSA. • Signatures from Hash Functions. • Certificates and Public-Key Infrastructures. • SSL/TLS. • Final review.	3	--			End of week10

IC EX 10A	Final review Chapters 5-12 (215 pages) Evaluated by EXAM 10A			10.5		
EXAM 10A	Finals	1	--	--	150	End of week10
Total Week 10		4	0	10.5	150	

Course Hours Summary

Week	Topic	LEC Hours	LAB Hours	ELP Hours
1	Introduction	4	--	20.0
2	Perfectly secret encryption	4	--	8.0
3	Private –Key Encryption	4	--	10.4
4	Message Authentication Codes	4	--	11.7
5	Course Recap/ Midterm Review	4	--	16.0
6	Hash Functions and Applications	4	--	7.9
7	Practical and Theoretical Constructions of Symmetric-Key Primitives	4	--	9.6
8	Number Theory and Cryptographic Hardness Assumptions / Algorithms for Factoring and Computing Discrete Logarithms	4	--	11.3
9	Key Management and Public-Key Encryption	4	--	11.8
10	Digital Signatures Schemes	4	--	10.5
Total		40	--	117.2

Table/Point Breakdown

Week	Assignment	Possible Points	Percent of Grade
1	LASA1	200	20%
2	Chapter 1&2 Review Exercises	50	5%
3	Chapter 2&3 Review Exercises	50	5%
4	Chapter 3 Review Exercises / Quiz	50	5%
5	LASA 2	200	20%
5	Midterm Exam	150	15%
6	Chapter 5 Review Exercises	50	5%
7	Chapter 6 Review Exercises	25	2.5%
8	Chapter 7 Review Exercises	25	2.5%
9	Chapter 8 Review Exercises / Quiz	50	5%
10	Final Exam	150	15%
Total		1000	100%

Your Grades for this Course

Your final grade for this course will be based on an assessment by the Instructor of your performance on a number of course activities, which may include objective tests, classroom exercises, laboratory demonstrations, project papers, or other types of activities. The chart below indicates in what activities you will engage, how many possible points can be earned for each activity, and the percentage of your final grade that will be accounted for by each activity.

Students in this course should be graded following Coleman University assessment practices and policies. A point system is used in the University to indicate student performance on various required activities or projects. For this course, it is recommended that points be distributed as follows:

Coleman University Grade Assignment Policy:
The Coleman University guidelines for the assignment of grades to total points earned is as follows:

Percent	Letter Grade	Grade Points
94-100	A	4.0
90-93	A-	3.67
87-89	B+	3.33
84-86	B	3.0
80-83	B-	2.67
77-79	C+	2.33
74-76	C	2.00
70-73	C-	1.67
67-69	D+	1.33
64-66	D	1.00
60-63	D-	0.67
N/A	INC	0
N/A	W	0
60 or above	CR	0
59 or below	NC	0
70 or above	PASS	0

Requirements

Assignments: All assignments (including projects, lab work, quizzes and exams) must be completed as scheduled. The following will apply to late assignments:

- 1-24 hours after due date = 20% off point value
- 25-48 hours after due date = 60% off point value
- 49+ hours after due date = No points given

If an assignment equals less than 5 points, no points will be given for late work. If there are extenuating circumstances, the student must submit a written explanation to the department Senior Instructor. Upon evaluation, points will be given according to the Senior Instructor's discretion.

Attendance: Classes begin and end as indicated in the published schedule. It is required that students be present at the beginning of each class session and stay until class is dismissed, including lab periods. Excessive tardiness, leaving early and/or absences (from either lecture or lab sessions) are causes for dismissal from the course. A student that arrives in class beyond 30 minutes late may be considered absent. A student that leaves over 30 minutes before the end of class may also be considered absent. Excused absences will be determined by the instructors and approved by the Dean of Academics & Director of Student Services. Students may be removed from the course(s) based on the following absence guidelines:

4 Unit Course – Allowed 2 absences per 10-week MOD (3rd absence may be excused by DOA & DOSS)

5 Unit Course – Allowed 2 absences per 5-week MOD (3rd absence may be excused by DOA & DOSS)

8 Unit Course – Allowed 5 absences per 10-week MOD (6th absence may be excused by DOA & DOSS)

Conduct: Students are expected to conduct themselves in a professional manner while on campus. Rules of conduct are outlined in the University Catalog and students are required to adhere to such policies. Students who are in violation of the Student Code of Conduct Policy can be suspended.

Student Academic Progression (SAP)

Graduate: Student must maintain an accumulative GPA of 3.0 or higher. If a student falls below the GPA requirement at any time during their program, they will be placed on Academic Probation. Once on Academic Probation, the student's accumulative GPA will be reviewed after 4 future mods have been completed (must take punitive graded courses). Failure to meet the 3.0 GPA requirements will result in an Academic

Suspension. A student is not allowed more than 150% of the standard length of the program in which to complete the requirements for graduation.

Undergraduate: Student must maintain an accumulative GPA of 2.0 or higher. If a student falls below the GPA requirement at any time during their program, they will be placed on Academic Probation. Once on Academic Probation, the student's accumulative GPA will be reviewed after 2 future mods have been completed (must take a minimum of 8 credits per mod). Failure to meet the 2.0 GPA requirements will result in an Academic Suspension. A student is not allowed more than 150% of the standard length of the program in which to complete the requirements for graduation.

Suspension and Reinstatement: If a student is suspended (SAP, plagiarism, code of conduct, etc.), the student must sit out one full MOD (currently 10 weeks for undergraduate level and 5 weeks for graduate level). The student will be required to submit a written reinstatement request, which will be reviewed by the Reinstatement Committee. The Reinstatement Committee will approve the request, deny the request, or request a meeting with the student for further consideration.

Grades: All grades listed will count as units attempted:

Letter Grade	Percentage	Grade Points
A	94% - 100%	4.00
A-	90% - 93%	3.67
B+	87% - 89%	3.33
B	84% - 86%	3.00
B-	80% - 83%	2.67
C+	77% - 79%	2.33
C	74% - 76%	2.00
C-	70% - 73%	1.67
D+	67% - 69%	1.33
D	64% - 66%	1.00
D-	60% - 63%	0.67
F	0% - 59%	0.00
INC	N/A	0.00
W	N/A	0.00
CR	N/A	0.00
NC	N/A	0.00
PASS	N/A	0.00

Failed Courses: If a student receives a FAIL grade, they may retake the course. The retake course will be charged at current tuition pricing. The student will be able to *replace* the previous FAIL grade with the grade received on the retake course.

Drop Period & Refund:

Graduate

Sessions Attended	Refund	Grade Received When Dropping Course
0	100%	No Grade
1	100%	No Grade
2	80%	W
3	70%	W
4	60%	W
5	50%	Grade Earned
6	0%	Grade Earned
7	0%	Grade Earned
8	0%	Grade Earned
9	0%	Grade Earned
10	0%	Grade Earned

Undergraduate

Week In MOD	Refund	Grade Received When Dropping Course
No Start	100%	No Grade
1	100%	No Grade
2	80%	W
3	70%	W
4	60%	W
5	50%	Grade Earned
6	0%	Grade Earned
7	0%	Grade Earned
8	0%	Grade Earned
9	0%	Grade Earned
10	0%	Grade Earned

Coleman University Policy on Academic Dishonesty:

Academic dishonesty is cause for dismissal from Coleman University. Presenting another person's ideas, methods, course work, or test answers with the intention that they be taken as one's own is theft of a special kind. It defrauds the originator of the work, the institution, its graduates, its students, and its future students.

The student has full responsibility for the authenticity of all academic work and examinations submitted. A student who appears to have violated this policy must submit to a hearing with the reporting instructor and the associate dean. If it is determined that a violation occurred, the matter will be referred to an Officer of the University with recommendations for an appropriate penalty. The student may be dismissed, suspended, or given another penalty.

Coleman University employs the plagiarism software known as Turnitin. Students are expected to use this tool in an appropriate manner with the sole purpose to support their own academic endeavors at Coleman University. Turnitin account information cannot be shared with anyone. Contact your instructor if you have any questions about plagiarism related issues.

Academic Accommodation / Adjustment Policy:

In accordance with Section 504 of the Rehabilitation Act of 1973 and the Americans with Disabilities Act (ADA), Coleman University offers accommodations to students with documented physical, psychological, and/or cognitive disabilities. Coleman University will adhere to all applicable federal, state, and local laws, regulations, and guidelines with respect to providing reasonable accommodations as required to offer equal educational opportunities to qualified disabled individuals.

To qualify for an academic accommodation under ADA, the student must provide adequate documentation of a disability. Students seeking academic accommodations should contact the campus ADA Coordinator, Ariana Marron, at 858-966-3953 or via email at ada@coleman.edu. The ADA Coordinator will review the documentation provided and verify ADA coverage. Students covered under ADA must meet with the ADA Coordinator at the beginning of every term to determine the appropriate academic accommodations. Failing to meet with the ADA Coordinator at the beginning of every term may impact the availability of accommodations.

After the academic accommodations have been determined, the students' instructors will be notified by the ADA Coordinator. If any problems or concerns regarding the provision of accommodations occur, the student must inform the ADA Coordinator. If the student feels accommodation is not being made appropriately, the student may follow the published Student Grievance Procedures.