2020

Advanced Network Security Applications

North Carolina Agricultural and Technical State University

NORTH CAROLINA AGRICULTURAL AND TECHNICAL STATE UNIVERSITY

COURSE SYLLABUS

College Name: College of Science and Technology
Department Name: Department of Computer Systems Technology
Course Name: Advanced Network Security Applications

COURSE INFORMATION

- Course Number/Section: CST 615
- Term:
- Semester Credit Hours: 3
- Times and Days:
- Class Location:

INSTRUCTOR CONTACT INFORMATION

- Instructor:
- Office Location:
- Office Phone:
- Email Address:

Faculty must notify students of the approximate time and method they can expect to receive an answer to all communications (e.g., email, phone, course messages). Excluding holidays, the response should be provided within 48 hours.

If there's a graduate teaching assistant assigned to work with this course, please include their names also.

STUDENT HOURS

These are times students may visit the professor without an appointment to request the assistance they need.

NOTE: Students are responsible for reading, understanding, and following the syllabus.

: AM ☐ / PM ☐ – : AM ☐ / PM ☐

Monday ☐ Tuesday ☐ Wednesday ☐ Thursday ☐ Friday ☐

COURSE PREREQUISITES

None.

COURSE DESCRIPTION

This course explores security terms, definitions, concepts, and issues that face industries today. This course also will examine how the concept of security, and being secure, integrates into the overall enterprise mission. The importance of user involvement, security training, ethics, trust, and informed management will be explored.

STUDENT LEARNING OBJECTIVES/OUTCOMES (SLO)

Learning outcomes should be specific, measurable, and focused on the content knowledge the students are expected to master and not what the faculty will teach.

If the course is a General Education Course, the SLO should be listed and labeled as "General Education."

SLO 1: Describe basic cryptographic functionality, including symmetric ciphers, public key encryption, digital signatures, hash functions, and related concepts;
SLO 2: Describe how basic cryptographic building blocks are combined to meet high-level security goals in protocols like SSL and IPsec;
SLO 3: Identify specific security technologies that can improve aspects of a system design;
SLO 4: Justify the use of particular technologies, settings, and parameters to meet specified security goals;
SLO 5: Evaluate the security of systems that use cryptography and secure communication techniques;
SLO 6: Discuss how security and privacy issues can impact system design;
SLO 7: Explore research-level computer security and cryptography topics.

REQUIRED TEXTBOOKS AND MATERIALS

Any course-level subscriptions and tools linked in Blackboard Learn learning management system (LMS) should be listed here. The Blackboard LMS must have links to their student data privacy statement.

REQUIRED TEXTS:

William Stallings (2017). *Cryptography and Network Security: Principles and Practice (7 ed.).* Pearson.

REQUIRED MATERIALS:

None.

SUGGESTED COURSE MATERIALS

SUGGESTED READINGS/TEXTS:

SUGGESTED MATERIALS:

GRADING POLICY

ASSIGNMENTS AND GRADING POLICY

94% and above	A		76% - 74%	C
93% - 90%	A-		73% - 70%	C-
89% - 87%	B+		69% - 67%	D+
86% - 84%	B		66% - 64%	D
83% - 80%	B-		63% - 0%	F
79% - 77%	C+			

For GRADUATE COURSES: See 2019-2020 Graduate Catalog p.38 for graduate grading scale and Non-Graded Courses

GRADING ALLOCATION

Course grades are based on a weighted grading scale of 100%. The breakdown for the course is as follows: *[Faculty, please adjust according to your course.]*

Category	# of Activities	Percentage Grade Weight
Discussion Board (includes *Self-Intro)*	1	0%
Assignment/ Homework	7	40%
Hands-on Project/ Project Report	1	20%
Exam	2	40%
Total	**11**	**100%**

COURSE POLICIES

USE OF BLACKBOARD AS THE LEARNING MANAGEMENT SYSTEM

Blackboard is the primary online instructional and course communications platform. Students can access the course syllabus, assignments, grades, and learner support resources. Students are encouraged to protect their login credentials, complete a Blackboard orientation, and log in daily to the course.

Note: Uploading assignments through Blackboard presents a challenge for Chromebook users in locating the files for submission. If you use a Chromebook, please be sure you also have access to a Mac computer or Windows computer so you can fully participate in your Blackboard class. For more information about student computer recommendations, please visit https://hub.ncat.edu/administration/its/computer-recommendations.php.

MAKE-UP EXAMS

See << Update Academic Year >>*Undergraduate Bulletin:*

https://www.ncat.edu/provost/academic-affairs/bulletins/index.php

For GRADUATE STUDENTS: See 2019-20 Graduate Catalog p. 54

EXTRA CREDIT

LATE WORK

SPECIAL ASSIGNMENTS

For GRADUATE STUDENTS: FAILING TO MEET COURSE REQUIREMENTS (Graduate Catalog p.40)

For GRADUATE STUDENTS: CLASS ATTENDANCE (see 2019-20 Graduate Catalog p. 53-54)

Students are expected to attend class and participate on a regular basis in order to successfully achieve course learning outcomes and meet federal financial aid requirements (34 CFR 668.22). Class attendance in online courses is defined as active participation in academically-related course activities. Active participation may consist of course interactions with the content, classmates, and/or the instructor. Examples of academically-related course activities include, but are not limited to:

- Completing and submitting assignments, quizzes, exams, and other activities within Blackboard or through Blackboard (3rd-party products).
- Participating in course-related synchronous online chats, discussions, or meeting platforms such as Blackboard Collaborate in which participation is tracked.

CLASSROOM CITIZENSHIP

Courtesy, civility, and respect must be the hallmark of your interactions.

COMPLIANCE WITH THE AMERICANS WITH DISABILITIES ACT

North Carolina A&T State University is committed to following the requirements of the Americans with Disabilities Act Amendments Act (ADAAA) and Section 504 of the Rehabilitation Act.
If you need an academic accommodation based on the impact of a disability, you must initiate the request with the Office of Accessibility Resources (OARS) and provide documentation in accordance with the Documentation Guidelines at N.C. A&T. Once documentation is received, it will be reviewed. Once approved, you must attend a comprehensive meeting to receive appropriate and reasonable accommodations. If you are a student registered with OARS, you must complete the Accommodation Request Form to have accommodations sent to faculty.

OARS is located in Murphy Hall, Suite 01 and can be reached at 336-334-7765, or by email at accessibilityresources@ncat.edu. Additional information and forms can be found on the internet at https://www.ncat.edu/provost/academic-affairs/accessibility-resources/index.php.

Please note: Accommodations are not retroactive and begin once the Disability Verification Form is provided to faculty.

TITLE IX

North Carolina A&T State University is committed to providing a safe learning environment for all students—free of all forms of discrimination and harassment. Sexual misconduct and relationship violence in any form are inconsistent with the university's mission and core values, violates university policies, and may also violate federal and state law. Faculty members are considered "Responsible Employees" and are required to report incidents of sexual misconduct and relationship violence to the Title IX Coordinator. If you or someone you know has been impacted by sexual harassment, sexual assault, dating or domestic violence, or stalking, please visit the Title IX website to access information about university support and resources. If you would like to speak with someone confidentially, please contact Counseling Services at 336-334-7727 or the Student Health Center at 336-334-7880.

TECHNICAL SUPPORT

If you experience any problems with your A&T account, you may call Client Technology Services (formerly Aggie Tech Support and Help Desk) at 336-334-7195, or visit https://hub.ncat.edu/administration/its/dept/ats/index.php.

FIELD TRIP POLICIES / OFF-CAMPUS INSTRUCTION AND COURSE ACTIVITIES

If applicable:

Off-campus, out-of-state, foreign instruction, and activities are subject to state law and university policies and procedures regarding travel and risk-related activities. Information regarding these rules and regulations may be found at https://www.ncat.edu/campus-life/student-affairs/index.php.

STUDENT HANDBOOK

https://www.ncat.edu/campus-life/student-affairs/departments/dean-of-students/student-handbook.php

STUDENT TRAVEL PROCEDURES AND STUDENT TRAVEL ACTIVITY WAIVER

https://hub.ncat.edu/administration/student-affairs/staff-resources/studen_activity_travel_waiver.pdf

OTHER POLICIES *(e.g., Copyright Guidelines, Confidentiality, etc.)*

STUDENT HANDBOOK

https://www.ncat.edu/campus-life/student-affairs/departments/dean-of-students/student-handbook.php

Graduate Catalog

SEXUAL MISCONDUCT POLICY

https://www.ncat.edu/legal/title-ix/sexual-harassment-and-misconduct-policies/index.php

FAMILY EDUCATIONAL RIGHTS AND PRIVACY ACT (FERPA)

https://www.ncat.edu/registrar/ferpa.php

STUDENT COMPLAINT PROCEDURES

https://www.ncat.edu/current-students/student-complaint-form.php

STUDENT CONDUCT AND DISCIPLINE

North Carolina A&T State University has rules and regulations that govern student conduct and discipline meant to ensure the orderly and efficient conduct of the educational enterprise. It is the responsibility of each student to be knowledgeable about these rules and regulations.

Please consult the following about specific policies such as academic dishonesty, cell phones, change of grade, disability services, disruptive behavior, general class attendance, grade appeal, incomplete grades, make-up work, student grievance procedures, withdrawal, etc.:

- Undergraduate Bulletin
  https://www.ncat.edu/provost/academic-affairs/bulletins/index.php
- Graduate Catalog
  https://www.ncat.edu/tgc/graduate-catalog/index.php
- Student Handbook
  https://www.ncat.edu/campus-life/student-affairs/departments/dean-of-students/student-handbook.php

ACADEMIC DISHONESTY POLICY

Academic dishonesty includes but is not limited to the following:

1. Cheating or knowingly assisting another student in committing an act of cheating or other academic dishonesty;
2. Plagiarism (unauthorized use of another's words or ideas as one's own), which includes but is not limited to submitting exams, theses, reports, drawings, laboratory notes or other materials as one's own work when such work has been prepared by or copied from another person;
3. Unauthorized possession of exams or reserved library materials; destroying or hiding source, library or laboratory materials or experiments or any other similar actions;
4. Unauthorized changing of grades, or marking on an exam or in an instructor's grade book or such change of any grade record;
5. Aiding or abetting in the infraction of any of the provisions anticipated under the general standards of student conduct;
6. Hacking into a computer and gaining access to a test or answer key prior to the test being given. N.C. A&T reserves the right to search the emails and computers of any student suspected of such computer hacking (if a police report of the suspected hacking was submitted prior to the search); and
7. Assisting another student in violating any of the above rules.

A student who has committed an act of academic dishonesty has failed to meet a basic requirement of satisfactory academic performance. Thus, academic dishonesty is not only a basis for disciplinary action, but may also affect the evaluation of a student's level of performance. Any student who commits an act of academic dishonesty is subject to disciplinary action.

In instances where a student has clearly been identified as having committed an act of academic dishonesty, an instructor may take appropriate disciplinary action, including loss of credit for an assignment, exam, or project; or awarding a grade of "F" for the course, **subject to review and endorsement by the chairperson and dean**.

For GRADUATE STUDENTS: Reference for academic dishonesty – 2010-2020 Graduate Catalog, p.58-59

For GRADUATE STUDENTS: STUDENT RELIGIOUS OBSERVANCE (see Graduate Catalog, p.55)

ASSIGNMENTS AND ACADEMIC CALENDAR

Include topics, reading assignments, due dates, exam dates, withdrawal dates, pre-registration and registration dates, all holidays, and convocations.*

THE WEEK OF MM/DD/YY	SUBJECT	UNIT LEARNING OUTCOMES (ULO)	READING IN TEXT, ACTIVITY, HOMEWORK, EXAM
	Unit 1: Computer and Network Security Concepts	ULO 1: Describe the key security requirements of confidentiality, integrity, and availability. (SLO 1 to 7) ULO 2: Describe the X.800 security architecture for OSI. (SLO 1 to 7) ULO 3: Discuss the types of security threats and attacks that must be dealt with and give examples of the types of threats and attacks that apply to different categories of computer and network assets. (SLO 1 to 7) ULO 4: Explain the fundamental security design principles. (SLO 1 to 7) ULO 5: Discuss the use of attack surfaces and attack trees. (SLO 1 to 7) ULO 6: List and briefly describe key organizations	1. **Read from textbook**: William Stallings (2017). *Cryptography and Network Security: Principles and Practice (7 ed.).* Pearson. Read the following chapter(s): a. Chapter 1 b. Module A "Networking Concepts" from Page 578 to Page 617 2. **Read**: Syllabus

		involved in cryptography standards. (SLO 1 to 7)	
	Unit 2: Introduction to Number Theory	ULO 1: Understand the concept of divisibility and the division algorithm. (SLO 1 to 7) ULO 2: Understand how to use the Euclidean algorithm to find the greatest common divisor. (SLO 1 to 7) ULO 3: Present an overview of the concepts of modular arithmetic. (SLO 1 to 7) ULO 4: Explain the operation of the extended Euclidean algorithm. (SLO 1 to 7) ULO 5: Discuss key concepts relating to prime numbers. (SLO 1 to 7) ULO 6: Understand Fermat's theorem. (SLO 1 to 7) ULO 7: Understand Euler's theorem. (SLO 1 to 7) ULO 8: Define Euler's totient function. (SLO 1 to 7) ULO 9: Make a presentation on the topic of testing for primality. (SLO 1 to 7) ULO 10: Explain the Chinese remainder theorem. (SLO 1 to 7)	**1. Read from textbook**: William Stallings (2017). *Cryptography and Network Security: Principles and Practice (7 ed.).* Pearson. Read the following chapter(s): a. Chapter 1 and b. Chapter 2 **2. Complete**: Assignment #1 (ULO 1 to 11)

		ULO 11: Define discrete logarithms. (SLO 1 to 7)	
	Unit 3: Classical Encryption Techniques	ULO 1: Present an overview of the main concepts of symmetric cryptography. (SLO 1 to 7) ULO 2: Explain the difference between cryptanalysis and brute-force attack. (SLO 1 to 7) ULO 3: Understand the operation of a monoalphabetic substitution cipher. (SLO 1 to 7) ULO 4: Understand the operation of a polyalphabetic cipher. (SLO 1 to 7) ULO 5: Present an overview of the Hill cipher. (SLO 1 to 7) ULO 6: Describe the operation of a rotor machine. (SLO 1 to 7) ULO 7: Understand the distinction between stream ciphers and block ciphers. (SLO 1 to 7) ULO 8: Present an overview of the Feistel cipher and explain how decryption is the inverse of encryption. (SLO 1 to 7) ULO 9: Present an overview of Data	**1.Read from textbook**: William Stallings (2017). *Cryptography and Network Security: Principles and Practice (7 ed.).* Pearson. Read the following chapter(s): a. Chapter 3: “Classical Encryption Techniques” (i.e., pp. 67-99); b. Chapter 4: "Block Ciphers and the Data Encryption Standard" (i.e., pp. 100-122)

		Encryption Standard (DES). (SLO 1 to 7) ULO 10: Explain the concept of the avalanche effect. (SLO 1 to 7) ULO 11: Discuss the cryptographic strength of DES. (SLO 1 to 7) ULO 12: Summarize the principal block cipher design principles. (SLO 1 to 7)	
	Unit 4: Block Ciphers and the Data Encryption Standard	ULO 1: Present an overview of the main concepts of symmetric cryptography. (SLO 1 to 7) ULO 2: Explain the difference between cryptanalysis and brute-force attack. (SLO 1 to 7) ULO 3: Understand the operation of a monoalphabetic substitution cipher. (SLO 1 to 7) ULO 4: Understand the operation of a polyalphabetic cipher. (SLO 1 to 7) ULO 5: Present an overview of the Hill cipher. (SLO 1 to 7) ULO 6: Describe the operation of a rotor machine. (SLO 1 to 7) ULO 7: Understand the distinction between stream ciphers and	**1.Read from textbook**: William Stallings (2017). *Cryptography and Network Security: Principles and Practice (7 ed.).* Pearson. Read the following chapter(s): a. Chapter 3: "Classical Encryption Techniques" (i.e., pp. 67-99); b. Chapter 4: "Block Ciphers and the Data Encryption Standard" (i.e., pp. 100-122) **2. Complete**: Assignment #2 (ULO 1 to 12)

		block ciphers. (SLO 1 to 7) ULO 8: Present an overview of the Feistel cipher and explain how decryption is the inverse of encryption. (SLO 1 to 7) ULO 9: Present an overview of Data Encryption Standard (DES). (SLO 1 to 7) ULO 10: Explain the concept of the avalanche effect. (SLO 1 to 7) ULO 11: Discuss the cryptographic strength of DES. (SLO 1 to 7) ULO 12: Summarize the principal block cipher design principles. (SLO 1 to 7)	
	Unit 5: Finite Field	ULO 1: Define finite fields of the form GF(p). (SLO 1 to 7) ULO 2: Distinguish among groups, rings, and fields. (SLO 1 to 7) ULO 3: Explain the differences among ordinary polynomial arithmetic, polynomial arithmetic with coefficients in Zp, and modular polynomial arithmetic in GF(2n) (SLO 1 to 7) ULO 4: Define finite fields of the form	**1.Read from textbook**: William Stallings (2017). *Cryptography and Network Security: Principles and Practice (7 ed.).* Pearson. Read the following chapter(s): **1.** Chapter 5: Finite Fields" (i.e., pp. 123-152); **2.** Chapter 6: "Advanced Encryption Standard" (i.e., pp. 153-188)

		GF(2n). (SLO 1 to 7) ULO 5: Explain the two different uses of the mod operator. (SLO 1 to 7) ULO 6: Present an overview of the general structure of Advanced Encryption Standard (AES). (SLO 1 to 7) ULO 7: Understand the four transformations used in AES. (SLO 1 to 7) ULO 8: Explain the AES key expansion algorithm. (SLO 1 to 7) ULO 9: Understand the use of polynomials with coefficients in GF (28). (SLO 1 to 7)	
	Unit 6: Advanced Encryption Standard	ULO 1: Define finite fields of the form GF(p). (SLO 1 to 7) ULO 2: Distinguish among groups, rings, and fields. (SLO 1 to 7) ULO 3: Explain the differences among ordinary polynomial arithmetic, polynomial arithmetic with coefficients in Zp, and modular polynomial arithmetic in GF(2n) (SLO 1 to 7) ULO 4: Define finite fields of the form GF(2n). (SLO 1 to 7)	**1. Read from textbook**: William Stallings (2017). *Cryptography and Network Security: Principles and Practice (7 ed.).* Pearson. Read the following chapter(s): a. Chapter 5: Finite Fields" (i.e., pp. 123-152); b. Chapter 6: "Advanced Encryption Standard" (i.e., pp. 153-188 **2. Complete**: Exam #1(ULO 1 to 9) **3. Complete**: Assignment # 3 (ULO 1 to 9)

		ULO 5: Explain the two different uses of the mod operator. (SLO 1 to 7) ULO 6: Present an overview of the general structure of Advanced Encryption Standard (AES). (SLO 1 to 7) ULO 7: Understand the four transformations used in AES. (SLO 1 to 7) ULO 8: Explain the AES key expansion algorithm. (SLO 1 to 7) ULO 9: Understand the use of polynomials with coefficients in GF (28). (SLO 1 to 7)	
	Unit 7: Block Cipher Operation	ULO 1: Analyze the security of multiple encryption schemes. (SLO 1 to 7) ULO 2: Explain the meet-in-the-middle attack. (SLO 1 to 7) ULO 3: Compare and contrast ECB, CBC, CFB, OFB, and counter modes of operation. (SLO 1 to 7) ULO 4: Present an overview of the XTS-AES mode of operation. (SLO 1 to 7) ULO 5: Explain the concepts of randomness and unpredictability with respect to random numbers. (SLO 1 to 7)	**1.Read from textbook**: William Stallings (2017). *Cryptography and Network Security: Principles and Practice (7 ed.).* Pearson. Read the following chapter(s): a. Chapter 7: "Block Cipher Operation" (i.e., pp. 189-231), b. Chapter 8: "Random Bit Generation and Stream Ciphers" (i.e., pp.232-264

		ULO 6: Understand the differences among true random number generators, pseudorandom number generators, and pseudorandom functions. (SLO 1 to 7) ULO 7: Present an overview of requirements for pseudorandom number generators. (SLO 1 to 7) ULO 8: Explain how a block cipher can be used to construct a pseudorandom number generator. (SLO 1 to 7) ULO 9: Present an overview of stream ciphers and RC4. (SLO 1 to 7) ULO 10: Explain the significance of skew. (SLO 1 to 7)	
	Unit 8: Random Bit Generation and Stream Ciphers	ULO 1: Analyze the security of multiple encryption schemes. (SLO 1 to 7) ULO 2: Explain the meet-in-the-middle attack. (SLO 1 to 7) ULO 3: Compare and contrast ECB, CBC, CFB, OFB, and counter modes of operation. (SLO 1 to 7) ULO 4: Present an overview of the XTS-AES mode of operation. (SLO 1 to 7)	**1.Read from textbook**: William Stallings (2017). *Cryptography and Network Security: Principles and Practice (7 ed.).* Pearson. Read the following chapter(s): a. Chapter 7: “Block Cipher Operation” (i.e., pp. 189-231), b. Chapter 8: “Random Bit Generation and Stream Ciphers” (i.e., pp. 232-264 **2. Complete:** Assignment #4

		ULO 5: Explain the concepts of randomness and unpredictability with respect to random numbers. (SLO 1 to 7) ULO 6: Understand the differences among true random number generators, pseudorandom number generators, and pseudorandom functions. (SLO 1 to 7) ULO 7: Present an overview of requirements for pseudorandom number generators. (SLO 1 to 7) ULO 8: Explain how a block cipher can be used to construct a pseudorandom number generator. (SLO 1 to 7) ULO 9: Present an overview of stream ciphers and RC4. (SLO 1 to 7) ULO 10: Explain the significance of skew. (SLO 1 to 7)	
	Unit 9: Public-Key Cryptography and RSA	ULO 1: Present an overview of the basic principles of public-key cryptosystems. (SLO 1 to 7) ULO 2: Explain the two distinct uses of public-key cryptosystems. (SLO 1 to 7)	**1.Read from textbook**: William Stallings (2017). *Cryptography and Network Security: Principles and Practice (7 ed.).* Pearson. Read the following chapter(s): **a.** Chapter 9: "Public-Key Cryptography and RSA" (i.e., pp. 265-294), **b.** Chapter 10: "Other Public-Key Cryptosystems" (i.e., pp.295-320)

		ULO 3: List and explain the requirements for a public-key cryptosystem. (SLO 1 to 7) ULO 4: Present an overview of the RSA algorithm. (SLO 1 to 7) ULO 5: Understand the timing attack. (SLO 1 to 7) ULO 6: Summarize the relevant issues related to the complexity of algorithms. (SLO 1 to 7) ULO 7: Define Diffie–Hellman key exchange. (SLO 1 to 7) ULO 8: Understand the man-in-the-middle attack. (SLO 1 to 7) ULO 9: Present an overview of the Elgamal cryptographic system. (SLO 1 to 7) ULO 10: Understand elliptic curve arithmetic. (SLO 1 to 7) ULO 11: Present an overview of elliptic curve cryptography. (SLO 1 to 7) ULO 12: Present two techniques for generating pseudorandom numbers using an asymmetric cipher. (SLO 1 to 7)	

	Unit 10: Other Public-Key Cryptosystems	ULO 1: Present an overview of the basic principles of public-key cryptosystems. (SLO 1 to 7) ULO 2: Explain the two distinct uses of public-key cryptosystems. (SLO 1 to 7) ULO 3: List and explain the requirements for a public-key cryptosystem. (SLO 1 to 7) ULO 4: Present an overview of the RSA algorithm. (SLO 1 to 7) ULO 5: Understand the timing attack. (SLO 1 to 7) ULO 6: Summarize the relevant issues related to the complexity of algorithms. (SLO 1 to 7) ULO 7: Define Diffie–Hellman key exchange. (SLO 1 to 7) ULO 8: Understand the man-in-the-middle attack. (SLO 1 to 7) ULO 9: Present an overview of the Elgamal cryptographic system. (SLO 1 to 7) ULO 10: Understand elliptic curve arithmetic. (SLO 1 to 7)	**1.Read from textbook**: William Stallings (2017). *Cryptography and Network Security: Principles and Practice (7 ed.).* Pearson. Read the following chapter(s): a. Chapter 9: "Public-Key Cryptography and RSA" (i.e., pp. 265-294), b. Chapter 10: "Other Public-Key Cryptosystems" (i.e., pp.295-320) 2. **Complete**: Assignment # 5 (ULO 1 to 12)

		ULO 11: Present an overview of elliptic curve cryptography. (SLO 1 to 7) ULO 12: Present two techniques for generating pseudorandom numbers using an asymmetric cipher. (SLO 1 to 7)	
	Unit 11: Cryptographic Hash Functions	ULO 1: Summarize the applications of cryptographic hash functions. (SLO 1 to 7) ULO 2: Explain why a hash function used for message authentication needs to be secured. (SLO 1 to 7) ULO 3: Understand the differences among preimage resistant, second preimage resistant, and collision resistant properties. (SLO 1 to 7) ULO 4: Present an overview of the basic structure of cryptographic hash functions. (SLO 1 to 7) ULO 5: Describe how cipher block chaining can be used to construct a hash function. (SLO 1 to 7) ULO 6: Understand the operation of SHA-512. (SLO 1 to 7)	**1.Read from textbook**: William Stallings (2017). *Cryptography and Network Security: Principles and Practice (7 ed.).* Pearson. Read the following chapter(s): a. Chapter 11: "Cryptographic Hash functions" (i.e., pp. 321-362), b. Chapter 12: "Message Authentication Codes" (i.e., pp. 363-400) **3. Complete:** Hands-on Project# 1 (ULO 1 to 17)

		ULO 7: Understand the birthday paradox and present an overview of the birthday attack. (SLO 1 to 7) ULO 8: List and explain the possible attacks that are relevant to message authentication. (SLO 1 to 7) ULO 9: Define the term message authentication code. (SLO 1 to 7) ULO 10: List and explain the requirements for a message authentication code. (SLO 1 to 7) ULO 11: Present an overview of HMAC. (SLO 1 to 7) ULO 12: Present an overview of CMAC. (SLO 1 to 7) ULO 13: Explain the concept of authenticated encryption. (SLO 1 to 7) ULO 14: Present an overview of CCM. (SLO 1 to 7) ULO 15: Present an overview of GCM. (SLO 1 to 7) ULO 16: Discuss the concept of key wrapping and explain its use. (SLO 1 to 7) ULO 17: Understa nd how a hash	

		function or a message authentication code can be used for pseudorandom number generation. (SLO 1 to 7)	
	Unit 12: Message Authentication Codes	ULO 1: Summarize the applications of cryptographic hash functions. (SLO 1 to 7) ULO 2: Explain why a hash function used for message authentication needs to be secured. (SLO 1 to 7) ULO 3: Understand the differences among preimage resistant, second preimage resistant, and collision resistant properties. (SLO 1 to 7) ULO 4: Present an overview of the basic structure of cryptographic hash functions. (SLO 1 to 7) ULO 5: Describe how cipher block chaining can be used to construct a hash function. (SLO 1 to 7) ULO 6: Understand the operation of SHA-512. (SLO 1 to 7) ULO 7: Understand the birthday paradox and present an overview of the	**1.Read from textbook**: William Stallings (2017). *Cryptography and Network Security: Principles and Practice (7 ed.).* Pearson. Read the following chapter(s): a. Chapter 11: "Cryptographic Hash functions" (i.e., pp. 321-362), b. Chapter 12: "Message Authentication Codes" (i.e., pp. 363-400); 2.**Complete:** Assignment #6 (ULO 1 to 17)

		birthday attack. (SLO 1 to 7) ULO 8: List and explain the possible attacks that are relevant to message authentication. (SLO 1 to 7) ULO 9: Define the term message authentication code. (SLO 1 to 7) ULO 10: List and explain the requirements for a message authentication code. (SLO 1 to 7) ULO 11: Present an overview of HMAC. (SLO 1 to 7) ULO 12: Present an overview of CMAC. (SLO 1 to 7) ULO 13: Explain the concept of authenticated encryption. (SLO 1 to 7) ULO 14: Present an overview of CCM. (SLO 1 to 7) ULO 15: Present an overview of GCM. (SLO 1 to 7) ULO 16: Discuss the concept of key wrapping and explain its use. (SLO 1 to 7) ULO 17: Understa nd how a hash function or a message authentication code can be used for	

		pseudorandom number generation. (SLO 1 to 7)	
	Unit 13: Digital Signatures	ULO 1: Present an overview of the digital signature process. (SLO 1 to 7) ULO 2: Understand the Elgamal digital signature scheme. (SLO 1 to 7) ULO 3: Understand the Schnorr digital signature scheme. (SLO 1 to 7) ULO 4: Understand the NIST digital signature scheme. (SLO 1 to 7) ULO 5: Compare and contrast the NIST digital signature scheme with the Elgamal and Schnorr digital signature schemes. (SLO 1 to 7) ULO 6: Understand the elliptic curve digital signature scheme. (SLO 1 to 7) ULO 7: Understand the RSA-PSS digital signature scheme. (SLO 1 to 7)	**1.Read from textbook**: William Stallings (2017). *Cryptography and Network Security: Principles and Practice (7 ed.).* Pearson. Read the following chapter(s): a. Chapter 13: "Digital Signatures" (i.e., pp. 401 --422), b. Chapter 14 "Key Management and Distribution" (i.e., pp. 423 --454
	Unit 14: Key Management and Distribution	ULO 1: Discuss the concept of a key hierarchy. (SLO 1 to 7) ULO 2: Understand the issues involved in using asymmetric encryption to distribute symmetric keys. (SLO 1 to 7)	**1.Read from textbook**: William Stallings (2017). *Cryptography and Network Security: Principles and Practice (7 ed.).* Pearson. Read the following chapter(s): a. Chapter 13: "Digital Signatures" (i.e., pp. 401 --422), b. Chapter 14: "Key Management and

		ULO 3: Present an overview of approaches to public-key distribution and analyze the risks involved in various approaches. (SLO 1 to 7) ULO 4: List and explain the elements in an X.509 certificate. (SLO 1 to 7) ULO 5: Present an overview of public-key infrastructure concepts. (SLO 1 to 7)	Distribution" (i.e., pp. 423 --454 2.**Complete:** Assignment #7 (ULO 1 to 5)
	Unit 15: User Authentication	ULO 1: Understand the distinction between identification and verification. (SLO 1 to 7) ULO 2: Present an overview of techniques for remote user authentication using symmetric encryption. (SLO 1 to 7) ULO 3: Give a presentation on Kerberos. (SLO 1 to 7) ULO 4: Explain the differences between versions 4 and 5 of Kerberos. (SLO 1 to 7) ULO 5: Describe the use of Kerberos in multiple realms. (SLO 1 to 7) ULO 6: Present an overview of techniques for	**1.Read from textbook**: William Stallings (2017). *Cryptography and Network Security: Principles and Practice (7 ed.).* Pearson. Read the following chapter(s): a. Chapter 13: "Digital Signatures" (i.e., pp. 401 --422), b. Chapter 14 "Key Management and Distribution" (i.e., pp. 423 --454 2.**Complete:** Hands-On Project: Project Report #2 (ULO 1 to 8) 3.**Complete:** Exam # II (ULO 1 to 8)

		remote user authentication using asymmetric encryption. (SLO 1 to 7) ULO 7: Understand the need for a federated identity management system. (SLO 1 to 7) ULO 8: Explain the use of PIV mechanisms as part of a user authentication system. (SLO 1 to 7)	

** These descriptions and timelines are subject to change at the discretion of the instructor.*