CSCE 477/877, Cryptography & Security

Fall 2022

Instructor:	Nirnimesh Ghose	**Email:**	nghose@unl.edu
Time:	T R 08:00 AM – 09:15 AM	**Place:**	110 Avery Hall
Office Hours:	By appt. only	**Office:**	107 Schorr Center
TA:	Philip Oguchi	**TA Email:**	eoguchi2@huskers.unl.edu
TA Office Hours:	By appt. only	**TA Office:**	114C Schorr Center

Course Pages:

1. Piazza – Primary, Register: https://piazza.com/unl/fall2022/cse477877; Access Code: SecurityFall22.
2. Canvas – Grades and Lecture video recording.
3. Tophat - Join Code: 065803; Password: fall22 – In class Quizzes.
4. SoC Webhandin – assignment submission.

Course description: Introduction to security concepts and basic cryptographic building blocks. Implementation of fundamental security properties such as message and user authentication, confidentiality, privacy, anonymity, authorization, certification, non-repudiation, and revocation. Application of basic cryptographic primitives on building secure protocols and systems. Wireless and network security protocols.

Among the topics covered are: introduction to information Security, Shannon's approach to cryptography, symmetric key cryptography, message integrity and authentication, public key cryptosystems, user authentication protocols, key distribution systems, key agreement protocols, and Network Security. The course will cover the recent developments in cryptography and security and include a group project that will provide hands-on interaction with implementation of cryptography and security. You will have the chance to apply what you have learned in the course during the project.

Required Material:

Cryptography and Network Security: Principles and Practice, 8th Edition, W. Stallings, Pearson, 2020
Lecture notes (POWERPOINT) will be posted on Piazza.
HOMEWORKS and EXAM will be based on lecture notes and supplemental reading materials.

Recommended Reading:

- *Cryptography: Theory and Practice*, Douglas Stinson, 3rd Edition, Prentice Hall, 2005 (more suitable for graduate students).
- *Network Security (private communication in a public world)*, C. Kaufman, R. Perlman, M. Speciner, Prentice Hall, 2002 (more suitable for undergraduate students).
- *Introduction to Modern Cryptography*, J. Katz and Y. Lindell, Chapman & Hall/CRC, 2014 (more suitable for graduate students).

- *Handbook of Applied Cryptography*, A. Menezes, P. Van Oorschot, S. Vanstone, CRC Press 1996, Available Online

Prerequisites: This class is appropriate for undergraduate or graduate students with previous background in Linear Algebra, Probability Algorithm and Data Structure. CSCE 310 (Data Structures and Algorithms) or CSCE 311 (Data Structures and Algorithms for Informatics); MATH 314 (Linear Algebra); MATH 487 (Probability Theory) are prerequisites.

Course Objectives: Upon the completion of this course, students should have achieved the following objectives:

- Have a fundamental understanding of the objectives of cryptography and network security.
- Become familiar with the cryptographic techniques that provide information and network security.
- Be able to apply suitable cryptographic primitives to achieve specific security goals for communication systems and networks.
- Be able to evaluate the security of communication systems, networks and protocols based on a multitude of security metrics.

Expected Learning Outcomes: By the end of this course, the student will be able to:

- Identify the basic notions of information and network security.
- Describe and apply cryptographic primitives for achieving confidentiality in both private key and public key settings.
- Describe and apply cryptographic mechanisms for achieving information integrity.
- Evaluate the security/computation/communication tradeoffs between public key and private key cryptography.
- Apply private key or public key cryptographic primitives for building mutual authentication protocols.
- Outline key agreement and key distribution protocols and analyze their overhead.
- Explain the application of cryptographic primitives and protocols in the context of wireless and network security.

Additional Learning Outcomes for 877:

- Describe and apply cryptanalysis methods to crack early and modern ciphers.
- Describe and apply formal security definitions and proof mechanisms to reason about the security of a cryptosystem or security protocol.

Course Topics:

Introduction to Information Security (∼1 week)

- Information security objectives

- Schematic of a secure communication system
- Formal definition of a cryptosystem, and adversary models

Classical Encryption Techniques (∼1.5 weeks)

- Number theory basics
- Early cryptosystems: substitution and transposition
- Cryptanalysis of early cryptosystems

Measures of Security and Ideal Cryptosystems (∼1 week)

- Measures of security
- Perfect secrecy
- Definition of entropy
- Ideal cryptosystems, and one-time pad

Symmetric Key Cryptography (∼2 weeks)

- The notion of a symmetric key cryptography, and computational security
- Block cipher, product cipher, and substitution-permutation networks
- The Data Encryption Standard (DES)
- The Advanced Encryption Standard (AES)
- Modes of operation
- Pseudorandom numbers and stream ciphers

Public Key Cryptosystems (∼1.5 weeks)

- Principles of Public-key Cryptography (PKC)
- More number theory basics
- Common public key cryptosystems: RSA
- Diffie-Hellman key exchange and ElGamal

Message Integrity and Authentication (∼1.5 weeks)

- Definition of hash functions and security properties
- Examples of hash functions: MD series, and Secure Hash Algorithm (SHA)
- Message Authentication Codes (MAC), HMAC
- More hash applications, including commitment protocols
- Common digital signatures schemes: RSA, ElGamal, Schnorr, and DSA

Key Management and Distribution (∼1 week)

- Symmetric key distribution schemes, Key Distribution Centers (KDC), session keys
- Public key distribution and Certificate Authorities (CA)
- Public Key Infrastructure (PKI)

User Authentication (∼1.5 weeks)

- User authentication principles
- Password authentication protocols
- Challenge-response protocols and common pitfalls
- Kerberos

Network Security (∼2 weeks)

- TCP/IP Threats
- IP security: the IPSec protocol
- Transport-level security: SSL and TLS protocols

System Security (∼1 week)

- Malware, Worms, DDoS attacks, SBGP
- Firewalls and Virtual Private Networks (VPNs)
- Intrusion detection

Grading Policy:

Projects	40%
Homework	30%
Examination	20%
Piazza Discussions	5%
Class participation	5%

Grading:

Grade	**477**	**877**
A+	93 - 100.0	97 - 100.0
A	90 - 92.99	93 - 96.99
A-	87 - 89.99	90 - 92.99
B+	83 - 86.99	87 - 89.99
B	80 - 82.99	83 - 86.99
B-	77 - 79.99	80 - 82.99
C+	73 - 76.99	77 - 79.99
C	70 - 72.99	73 - 76.99
C-	67 - 69.99	70 - 72.99
D+	63 - 66.99	67 - 69.99
D	60 - 62.99	63 - 66.99
D-	57 - 59.99	60 - 62.99
F	00 - 56.99	00 - 59.99

Important Dates (Tentative):

First Project Due	October 01, 2021
Second Project Due	November 05, 2021
Examination	November 23, 2021
Third Project Due	December 10, 2021

Homework Policies: Homework submissions will be through web handin Late homework is penalized 10% per day, No homework will be accepted after the solution is posted

GROWN-UP RULE: Sometimes things come up that we have to take care of. Thus, you are allowed to turn one assignment in up to 2-days late without penalty (the first late assignment will be used. You may not choose which one to use this rule on if you turn in multiple late assignments). No questions asked. No reason wanted!

To dispute scores on assignments, please discuss with the TA. If it is not resolved to your satisfaction, please visit me during office hours or email for an appointment. This must be done within one week of when the original assignment score is posted. Also, please remember that a single point on an assignment is a very small fraction of your overall grade. So please do not overburden the TA with insignificant requests.

Examination: (20% of total grade) There will be one in-class exam. The exams are open book/notes.

Course Projects: (40% of total grade) We will have three course project assignments, which will be a hands-on experience of the topics covered till then.

First Project-Crack Ciphers: (10% of total grade) In the first project, you will be expected to develop code for a platform of your choice. The code should be able to perform an automated ciphertext-only attack. The attack will be performed in three steps: 1) recognizing the encryption scheme, 2) cracking the key, and 3) output the corresponding plaintext.

Second Project-Crack Wired Equivalent Privacy: (15% of total grade) In the second project, you will be expected to crack the key for Wired Equivalent Privacy (WEP) security standard for Wi-Fi. WEP implements the Key Scheduling Algorithm of RC4, you will be required to learn about the vulnerability and use a tool of your choice to crack the key of Wi-Fi access point set in my lab (Schorr 114C),

Third Project-Crack Wi-Fi Protected Access : (15% of total grade) In the third project, you will be expected to extend the knowledge gained from the second project to crack the password of Wi-Fi Protected Access (WPA) security standard for Wi-Fi. Again you will be required to learn about the vulnerabilities of the WPA standard and use a tool of your choice to crack the key of Wi-Fi access point set in my lab (Schorr 114C),

Attendance Policy: Class participation is 5% of the grade so it is important to miss as few classes as possible. Students are expected to have several serious critiques of the course material and textbook for each class. Make-ups for assignments and projects will be given only under circumstances beyond student's control (a university-sanctioned excuse). Prior arrangements with the instructor must be made when feasible and official verification of circumstances necessitating the absence will be required. Note that late arrivals are incredibly distracting, and as such anyone, more than 10 minutes late will lose points for class participation.

Stay Up-to-Date: It is School of Computing policy that students in SoC courses regularly (every 24 hours) check their email so that they do not miss important course announcements.

Also, utilize the student resource center at Avery 12, more details available at https://computing.unl.edu/current-undergraduate#SRC.

Academic Honesty: All homework assignments, quizzes, exams, etc. must be your own work. No direct collaboration with fellow students, past or current, is allowed unless otherwise stated. The School of Computing has an Academic Integrity Policy (https://computing.unl.edu/academic-integrity-policy). All students enrolled in any School of Computing course are bound by this policy. You are expected to read, understand, and follow this policy. Violations will be dealt with on a case by case basis and may result in a failing assignment or a failing grade for the course itself.

Students with Disabilities: The University strives to make all learning experiences as accessible as possible. If you anticipate or experience barriers based on your disability (including mental health, chronic or temporary medical conditions), please let me know immediately so that we can discuss options privately. To establish reasonable accommodations, I may request that you register with Services for Students with Disabilities (SSD). If you are eligible for services and register with their office, make arrangements with me as soon as possible to discuss your accommodations so they can be implemented in a timely manner. SSD contact information: 232 Canfield Admin. Bldg.; 402-472-3787.

Counseling and Psychological Services: UNL offers a variety of options to students to aid them in dealing with stress and adversity. Counseling and Psychological & Services (CAPS); is a multidisciplinary team of psychologists and counselors that works collaboratively with Nebraska students to help them explore their feelings and thoughts and learn helpful ways to improve their mental, psychological and emotional well-being when issues arise. CAPS can be reached by calling 402-472-7450. Big Red Resilience & Well-Being (BRRWB) provides one-on-one well-being coaching to any student who wants to enhance their well-being. Trained well-being coaches help students create and be grateful for positive experiences, practice resilience and self-compassion, and find support as they need it. BRRWB can be reached by calling 402-472-8770.

Concerns: The School of Computing has an anonymous contact form (https://computing.unl.edu/anonymous-depar that you may use to voice your concerns about any problems in the course or department if you do not wish to be identified.