Course Number, Title, Credits, Contact hours

CYBR 463/563; 4 Credits; 5 Contact Hours

Course Description

This course covers the general principles of modern cryptography, including symmetric cryptosystems, asymmetric cryptosystems, secure hash functions, and cryptographic level randomness. Other topics may include historic cryptosystems and their cryptanalysis, information entropy, zero knowledge proofs, trusted computing architectures, and information theory as it relates to cryptography. Programming assignments are required, writing and class presentations may be required.

Required, Elective or Selected elective

This is a required course for CYBR degree.

Prerequisites or Co-requisites

Prerequisites: MATH 225 or MATH 301 or equivalent.

Reference Text, Title, Author

Cryptography and Network Security, Behrouz A. Forouzan, McGraw-Hill, Inc

Cryptography and Network Security, William Stallings, Pearsons.

Course Learning Objectives

1. Understand the basic principles, goals, and foundational concepts of cryptography.
2. Learn to implement cryptographic techniques such as encryption, decryption, and hashing.
3. Explore the strengths, limitations, and security implications of cryptographic systems.
4. Study advanced topics like secure communication protocols, zero-knowledge proofs, and post-quantum cryptography.
5. Apply cryptographic methods to real-world security challenges and key management practices.
6. Analyze the ethical considerations and the impact of emerging technologies on cryptography.

Weekly Course Outline

The tentative weekly outline of the topics is as follows

Week	Topics
1-2	**Introduction to Cryptography and Security Concepts:** Overview of cybersecurity, Security architecture, security attacks, services, mechanisms, cryptography **Introduction to Number Theory**: Division algorithm, Euclidean algorithm, modular arithmetic, prime numbers, Fermat's and Euler's theorems, primality testing, Chinese remainder theorem, and discrete logarithms. **Classical Encryption Techniques:** Symmetric cipher model, substitution, and transposition techniques.
3	**Block Ciphers and DES:** Block cipher structures, Data Encryption Standard (DES), examples, strength of DES, Triple DES, block cipher design principles.

Week	Topics
4	**Finite Fields and Advanced Encryption Standard (AES):** Groups, rings, fields, finite fields, polynomial arithmetic, AES structure, transformation functions, key expansion, examples, and implementation.
5	**Block Cipher Operation:** Modes like ECB, CBC, CFB, OFB, CTR, XTS-AES, and format-preserving encryption. Random Bit Generation and Stream Ciphers: Pseudorandom number generation, stream ciphers (RC4), feedback shift registers, and true random number generators.
6	**Public-Key Cryptography and RSA:** Principles of public-key cryptosystems, RSA algorithm, Diffie-Hellman key exchange, and ElGamal. Elliptic Curve Cryptography (ECC): Elliptic curve arithmetic and its application in cryptography.
7	**Cryptographic Hash Functions**: Applications, requirements, and security, including SHA family (SHA-2 and SHA-3). Message Authentication Codes (MACs): MAC requirements, HMAC, DAA, CMAC, authenticated encryption (CCM, GCM), and pseudorandom generation with MACs.
8	**Digital Signatures**: Concepts and algorithms, including ElGamal, Schnorr, NIST Digital Signature Algorithm, ECDSA, and RSA-PSS. **Zero-Knowledge Proofs**: Introduction to zero-knowledge proofs and their applications in cryptographic protocols.
9	**Emerging Cryptographic Concepts**: Lightweight cryptography, post-quantum cryptography, and resilience against quantum computing threats, Blockchain
10	**Cryptographic Key Management and User Authentication:** Symmetric and asymmetric key distribution, public key infrastructure (PKI), X.509 certificates, Kerberos, and federated identity management..

GRADING

Type	% of Final Grade
Assignments	30%
Exams and Quizzes	40%
Labs	30%

This course utilizes the standard university letter grades

Grade	Percentage Range	Description
A	93-100%	Excellent work demonstrating a high level of understanding and application of research methods.
A-	90-92%	Strong work with minor errors or omissions.
B+	87-89%	Good understanding with some areas needing improvement.
B	83-86%	Satisfactory work meeting basic requirements.
B-	80-82%	Adequate work but with several significant issues.
C+	77-79%	Below satisfactory performance, lacking depth or clarity.
C	73-76%	Minimal comprehension and application of concepts.
C-	70-72%	Poor performance with serious deficiencies.
D	60-69%	Very poor performance fails to meet course standards.

Grade	Percentage Range	Description
F	Below 60%	Unacceptable work, significant failure to understand key concepts.

GENERAL POLICIES

Americans with Disabilities Act: Students requiring accommodations need to contact Disability Support Services (DSS) at (509) 359-6871. The DSS Office is located in TAW 125.

Exams and Quizzes

Exams and quizzes will be announced at least one week in advance, with review sessions held prior to each assessment to ensure adequate preparation. Makeup exams or quizzes will only be granted if arrangements are made in advance or in the case of a documented emergency after the fact. It is your responsibility to communicate any conflicts as early as possible.

Homework and Assignments

Homework will include programming projects, laboratory exercises, written assignments, and research papers based assignments. Timely submission of assignments is critical to maintaining the pace of the course and receiving valuable feedback.

Late Submission Policy

Assignments submitted after the deadline will incur a 10% deduction per day. Extensions will only be considered if arrangements are made before the deadline. Planning and time management are essential to avoid unnecessary penalties.

Attendance and Participation

Participation in all class sessions is essential and expected. While occasional absences may occur, more than two unexcused absences will negatively impact your final grade. Your active engagement not only benefits your learning but also contributes to the collective classroom experience.

Academic Integrity

All assignments must be your own original work. Plagiarism or any form of academic dishonesty will be dealt with in accordance with university policies and may result in serious consequences. If you are uncertain about what constitutes academic misconduct, seek clarification before submitting your work.

Professional Behavior

You are expected to uphold the department's Code of Professional Conduct, maintaining professionalism in all interactions, whether in class, online, or during group work. Respectful communication and collaboration are fundamental to a positive learning environment.

Class Attendance

Although attendance is not formally graded, it is expected. Classroom activities are designed to complement the textbook and other course materials, and missing class may leave you at a disadvantage. If you are unable to attend, you are responsible for catching up on missed material and notifying me via email in advance.

Preparation for Lectures

To get the most out of this course, you are expected to read the assigned material from the textbook prior to class. This preparation ensures you can actively engage in discussions and follow along with in-class examples. Verifying the examples provided in the textbook independently is strongly encouraged to enhance your understanding.

Cell Phone Policy

Cell phones must be silenced during class. If you need to take an urgent call, step outside the classroom to avoid disruption. A ringing phone during class may be answered by the instructor as a gentle reminder to adhere to this policy.

Final Grade Policy

Your final grade will be calculated based on the percentages outlined in the syllabus and is not subject to negotiation. Work cannot be resubmitted after the deadline, and final grades, once assigned, are final. To avoid disappointment, focus on meeting the course requirements and maintaining consistent effort throughout the quarter.

EWU Academic Policy/Cheating Policy: You are allowed to discuss your thoughts with and help other classmates; however, you must do your own work, meaning ALL work should be your own. Plagiarism and cheating WILL NOT BE TOLERATED. Plagiarism includes using someone else' programs or parts of programs as your own; copying another person's work; handing in another person's work for your own. If you work with someone else to understand the content, it is important that each person does the assignment separately. Any infractions will be handled in accordance with the academic integrity policy of Eastern Washington University and Washington State civil law.

Code of Ethics and Professional Conduct

Students are expected to uphold a code of ethics and professional behavior that promotes the highest standards of integrity, honesty, trustworthiness, and professionalism when exploring cybersecurity-related topics and exercises. Students are required to sign the NCAE-C Student Code of Ethics and Professional Conduct during the first week of class to proceed in the course. Copies are available by emailing cybersecurity@ewu.edu.

Inclement Weather/ Emergency Closure

In the event of inclement weather or emergencies that impact in-person meetings, updates regarding class plans will be communicated through Canvas announcements and email. If the university declares remote operations, this course will transition to an online format, with instructions and updates provided promptly.

Students are encouraged to reach out with any questions or concerns via email or Canvas messaging. To stay informed about emergency alerts and campus notifications, it is highly recommended to download the EagleSafe app, available on the Apple Store and Google Play Store. This app will provide real-time updates and important information regarding campus operations.

Title IX and Mandatory Reporting

Eastern Washington University recognizes the inherent dignity of all individuals and promotes respect for all people. Sexual misconduct will NOT be tolerated at EWU. If you have been subjected to sexual misconduct, we encourage you to report this matter promptly. As a faculty member, I am interested in promoting a safe and healthy environment, and should I learn of any sexual misconduct I must report the matter to the Title IX Coordinator. Should you want to report to a confidential source you may contact the following:

- Sexual Assault Family Trauma (SAFeT) – 509-624-7273 – 24 hours
- YWCA Domestic Violence Crisis Line – 509-326-2255 – 24 hours
- Suicide and Mental Health – 509-838-4428 – 24 hours
- Employee Assistance Program (EAP) – 360-407-9490 (employees)
- Counseling and Psychological Services (CAPS) – 509-359-2366 (students)