BAKI ALİ NEFT MƏKTƏBİ
BAKU HIGHER OIL SCHOOL

The Ministry of Education of the Azerbaijan Republic
The State Oil Company of the Azerbaijan Republic
Baku Higher Oil School

İnformation Technology Department

Cybersecurity major (Master degree)

Advanced Cryptography and Data Protection

Courses Syllabus

Autumn, 2024

Instructor : Agha Aghayev

Course code : CS 103 Course credit : 6

Office : White Building, BHOS Office hours :

Prerequisites:

Language of instruction: English

Schedule :

Web site : www.bhos.edu.az

Email : aga.agayev@bhos.edu.az

Description of the course

Advanced Cryptography and Data Protection is a comprehensive course designed to explore the intricate world of modern cryptographic techniques and their vital role in safeguarding digital information. This course delves deep into contemporary cryptographic algorithms and more richer cryptographic tools, including the current state-of-art research directions. The course is designed to provide a of theoretical perspective of cryptography, hardness assumptions and security

definitions. This course equips learners with ability to use correct cryptographic tool and how to talk to a cryptographer.

Learning outcomes section

After taking this course students will be able to:

- Understand the foundational principles of cryptography, including encryption, decryption, and cryptographic algorithms.
- Analyze and evaluate the security of cryptographic systems, identifying vulnerabilities and potential attack vectors.
- Design and implement cryptographic solutions for data confidentiality, integrity, and authenticity in various applications.
- Explore advanced cryptographic techniques such as public key infrastructure (PKI), homomorphic encryption, and post-quantum cryptography.
- Investigate the quantum-proof hardness assumptions and existing attacks.
- Develop privacy-preserving technologies with privacy homomorphism
- Collaborate effectively in team projects to solve complex cryptography and data protection challenges.
- Demonstrate a deep understanding of cryptographic concepts through assessments, projects, and practical demonstrations.

Assessment methods

The assignments should be scripted with LaTeX, there will be 5 assignments, you should explicitly mention your name and number of the assignment. Midterm and final exam will be done on papers, which will include open ended and multiple choice questions. After each lesson students may answer some questions, quizzes. Attendance and class performance will contribute to 10% of the overall score.

Grading

Exam	Weight	Date	Exam
Final	40%	TBA (to be announced)	
Midterm	30%	6-7th week of the semester	
Assignments	20%		
Class activity	10%		

RESIT EXAM

Resit Exam score is 40% from total score. Total score after resit exam will be calculated by this way: Resit Exam (40%) + Midterm Exam (30%) + Assignments (20%) + Subjective (10%)

Resit exam will be done **only for the Final exam**, so there will **not** be a resit exam for the Midterm exam.

Area grading scale

A 91-100

B 81-90

C 71-80

D 61-70

F ≤ 60

Rules

Exams

In order to be excused from the exam, the student must contact the dean and the instructor before the exam. Excuses will not be granted for social activities such as trips, cruises and sporting events (unless you are participating). The exams will all be cumulative. Most of the questions on each exam will be taken from the chapters covered since the last exam. However, some will come from the earlier chapters. In general, the coverage will reflect the amount of the time spend in class on the different chapters.

Withdrawal (pass / fail)

This course strictly follows the grading policy of the Process Automation Engineering Department. Thus, a student is normally expected to achieve a total mark (preexam score + exam score) of at least 61 to pass. In this case of failure, he/she will be referred or required to repeat the course the following term or year.

Late policy

Late assignment submissions won't be accepted for grading. The grade for this assignment will be **zero**.

Teaching resources

Presentation : (in site: www.lms.bhos.edu.az)

Textbook :

[1] Paar, C., & Pelzl, J. (2010). *Understanding cryptography* (Vol. 1). Springer-Verlag Berlin Heidelberg.

[2] Katz, J., & Lindell, Y. (2007). *Introduction to modern cryptography: principles and protocols*. Chapman and hall/CRC.

[3] Lecture notes of Vinod https://people.csail.mit.edu/vinodv/CS294/lecturenotes.pdf

[4] Peikert, C. (2016). *A decade of lattice cryptography*. Foundations and trends® in theoretical computer science, 10(4), 283-424.

For class presentations and discussions, we will mostly use the first textbook, for more formal and advanced algorithms students may benefit from second text book. Moreover, the course does not limit the use of learning materials available at BHOS library.

Attendance

The students are required to attend all classes as a part of their studies and those having legitimate reasons for absence (illness, family bereavement, etc.) are required to inform the instructor.

Professionalism and Participation

1. Attend class regularly, arrive on time, leave only when dismissed.

2. Attend class with all materials required, be prepared to listen and work.

3. Be well prepared for class, read all required materials, and complete all necessary preparation.

4. Be attentive in class, take notes, contribute to discussion and ask intelligent questions.

5. Demonstrate professional and respectful interpersonal relationships with peers and instructor: ATTITUDE COUNTS, AND whining is unacceptable.

6. Take responsibility for your actions, and your results.

Plagiarism

Honesty requires that any ideas or material taken from another source for written, visual, or oral use must be fully acknowledged. Offering the work of someone else as one's own is plagiarism. The language or ideas thus taken from another may range from isolated formulas, images, sentences or paragraphs to entire articles copied from books, periodicals, speeches, or the writings and creations of other students. The offering of materials assembled or collected by others in the form of projects or collections without acknowledgment also is considered plagiarism. Any student who fails to give credit for ideas or materials taken from another course is guilty of plagiarism.

Week	Topics	Textbook/Assignments
1	**Introduction to Cryptography** • Overview on the field of cryptology • Basics of symmetric cryptography • Cryptanalysis • Substitution Cipher • Modular arithmetic • Shift (or Caesar) Cipher and Affine Cipher	- Instructor's Presentations - Paar, C., & Pelzl, J. (2010). Understanding cryptography (Vol. 1). Springer-Verlag Berlin Heidelberg.
2	**Stream Ciphers** • Intro to stream ciphers • Random number generators (RNGs) • One-Time Pad (OTP) • Linear feedback shift registers (LFSRs) • Trivium: a modern stream cipher	- Instructor's Presentations - Paar, C., & Pelzl, J. (2010). Understanding cryptography (Vol. 1). Springer-Verlag Berlin Heidelberg.
3	**The Data Encryption Standard (DES)** • Introduction to DES • Overview of the DES Algorithm • Internal Structure of DES • Decryption • Security of DES	- Instructor's Presentations - Paar, C., & Pelzl, J. (2010). Understanding cryptography (Vol. 1). Springer-Verlag Berlin Heidelberg.
4	**The Advanced Encryption Standard (AES)** • Overview of the AES algorithm • Internal structure of AES • Byte Substitution layer • Diffusion layer • Key Addition layer • Key schedule • Decryption • Practical issues	- Instructor's Presentations - Paar, C., & Pelzl, J. (2010). Understanding cryptography (Vol. 1). Springer-Verlag Berlin Heidelberg.
5	**More About Block Ciphers** • Encryption with Block Ciphers: Modes of Operation • Encryption modes: ECB, CBC, OFB, CFB, CTR, GCM • Exhaustive Key Search Revisited • Increasing the Security of Block Ciphers	- Instructor's Presentations - Paar, C., & Pelzl, J. (2010). Understanding cryptography (Vol. 1). Springer-Verlag Berlin Heidelberg.

6	**Introduction to Public-Key Cryptography** • Symmetric Cryptography Revisited • Principles of Asymmetric Cryptography • Practical Aspects of Public-Key Cryptography • Important Public-Key Algorithms • Essential Number Theory for Public-Key Algorithms	- Instructor's Presentations - Paar, C., & Pelzl, J. (2010). Understanding cryptography (Vol. 1). Springer-Verlag Berlin Heidelberg.
7	**The RSA Cryptosystem** • The RSA Cryptosystem • Implementation aspects • Finding Large Primes • Attacks and Countermeasures • Lessons Learned	- Instructor's Presentations - Paar, C., & Pelzl, J. (2010). Understanding cryptography (Vol. 1). Springer-Verlag Berlin Heidelberg.
8	**Public-Key Cryptosystems Based on the Discrete Logarithm Problem** • Diffie–Hellman Key Exchange • The Discrete Logarithm Problem • Security of the Diffie–Hellman Key Exchange • The Elgamal Encryption Scheme	- Instructor's Presentations - Paar, C., & Pelzl, J. (2010). Understanding cryptography (Vol. 1). Springer-Verlag Berlin Heidelberg.
9	**Digital Signatures** • The principle of digital signatures • Security services • The RSA digital signature scheme • The Digital Signature Algorithm (DSA)	- Instructor's Presentations - Paar, C., & Pelzl, J. (2010). Understanding cryptography (Vol. 1). Springer-Verlag Berlin Heidelberg.
10	**Lattice-based cryptography** • Definitions of lattices • Hardness assumptions: LWE and SIS problems • Basic cryptographic tools from lattices	- Instructor's Presentations - Lecture notes [3]
11	**Zero-knowledge Proofs** • Definitions of ZKs • Compactness and soundness • Proofs for NP • Quadratic residue and Graph isomorphism	- Instructor's Presentations -
12	**Homomorphic encryption** • Group homomorphism • Types of HE schemes • HE constructions and applications	- Instructor's Presentations - Lecture notes [3] - Efficient Fully Homomorphic Encryption from (Standard) LWE by Zvika Brakerski and Vinod Vaikuntanathan. - Homomorphic Encryption from Learning with Errors: Conceptually-

		Simpler, Asymptotically-Faster, Attribute-Based by Gentry et al.
	Final Exam	

Instructor of the course _____

Head of the department _____