KAZAKH-BRITISH TECHNICAL UNIVERSITY

JSC «Kazakh-British Technical University»
School of IT and Engineering

APPROVED BY
Dean of SITE
Azamat Imanbayev
_____
«____» _____ 2024

SYLLABUS

Discipline: Applied Cryptography
Number of credits: 3
Course code: CSE 1204
Term: Spring 2024
Instructors full name: Temirlan Zhaxalykov

Personal Information about the Instructor	Time and place of classes		Contact information	
	Lessons	Office Hours	Tel.	e-mail
Temirlan Zhaxalykov	According to the schedule	According to the schedule		t.zhaxalykov@kbtu.kz

COURSE DURATION: 3 credits, 15 weeks, 45 class hours

GENERAL COURSE AIMS:

The general aims of the Applied Cryptography course are to provide students with a comprehensive understanding of cryptographic principles, techniques, and applications. The course aims to equip students with the knowledge and skills required to analyze, design, and implement secure cryptographic solutions in real-world scenarios.

COURSE DESCRIPTION

This course explores the foundations of cryptography and its practical applications in various fields. Students will delve into both symmetric and asymmetric cryptographic algorithms, hashing techniques, and their applications in secure communication, data integrity, and access control. Emphasis will be placed on practical implementations and real-world use cases, preparing students for challenges in modern information security.

COURSE OBJECTIVES

- Understand Cryptographic Fundamentals:
  - Gain a solid understanding of cryptographic concepts, including encryption, decryption, key management, and cryptographic protocols.
- Explore Symmetric Cryptography:
  - Study symmetric encryption algorithms, modes of operation, and their applications in secure data transmission and storage.
- Examine Asymmetric Cryptography:

- Investigate asymmetric encryption algorithms, digital signatures, and key exchange protocols used in secure communication.
- Analyze Hashing Techniques:
  - Explore cryptographic hash functions, their properties, and applications in ensuring data integrity, password storage, and digital signatures.
- Address Quantum Cryptography Concepts:
  - Introduce the basics of quantum cryptography, quantum key distribution, and strategies for securing information in a post-quantum era.
- Practical Implementation:
  - Develop practical skills in implementing cryptographic algorithms and protocols using programming languages and cryptographic libraries.
- Security Protocols and Applications:
  - Study common security protocols and their implementations in applications such as secure messaging, e-commerce, and network security.

COURSE OUTCOMES

By the end of the course, students should be able to:

- Design and analyze secure cryptographic systems for various applications.
- Implement cryptographic algorithms using programming languages and cryptographic libraries.
- Evaluate the security of existing cryptographic systems and propose improvements.
- Understand the impact of quantum computing on current cryptographic practices.
- Apply cryptographic principles to enhance the security of information systems.

LITERATURE

1. "Cryptography and Network Security: Principles and Practice" by William Stallings.
2. "Applied Cryptography: Protocols, Algorithms, and Source Code in C" by Bruce Schneier.
3. "Serious Cryptography: A Practical Introduction to Modern Encryption" by Jean-Philippe Aumasson.
4. "Introduction to Modern Cryptography" by Jonathan Katz and Yehuda Lindell.
5. "Quantum Computing for Computer Scientists" by Noson S. Yanofsky and Mirco A. Mannucci.
6. "Foundations Of Cryptography" by Oded Goldreich.

COURSE ASSESSMENT CRITERIA

Assessment occurs continuously throughout the course. The evaluation will be based on the levels of (maximums in %):

Type of activity	Final scores
Attendance /participation	**0%**
SIS(Project defence)	**28%**
Midterm	**10%**
Endterm	**10%**
Quizzes	**12%**
Final exam	**40%**
Total	**100%**

*Students who get more points than the required maximum for in-class, final testing are awarded bonus points in the amount exceeded.

TASKS

for students independent study (SIS)

Week	SIS	Cost (in points)
4	SIS 1	**7**
7	SIS 2	**7**

12	SIS 3	**7**
14	SIS 4	**7**
	Total	**28**

COURSE CALENDAR

Week	CLASS WORK		SIS (students independent study	TSIS (teacher supervised independent study)
	Topic	Lec-tures		
1	2	3	4	5
1	**Lecture #1. Introduction. History of Cryptography**	3		
2	**Lecture #2. Data Encryption Standard and its variations**	3		
3	**Lecture #3. Advanced Encryption Standard**	3		
4	**Lecture #4. Blowfish**	3	SIS 1	
5	**Lecture #5. Diffie-Hellman Key Exchange**	3		
6	**Lecture #6. RSA (Rivest-Shamir-Adleman)**	3		
7	**Lecture #7. DSA (Digital Signature Algorithm)**	3	SIS 2	
8	**MIDTERM**	3		
9	**Lecture #8. SHA-256 (Secure Hash Algorithm 256-bit)**	3		
10	**Lecture #9. MD5 (Message Digest Algorithm 5)**	3		
11	**Lecture #10. SHA-3 (Secure Hash Algorithm 3)**	3		
12	**Lecture #11. BCRYPT**	3	SIS 3	
13	**Lecture #12. BB94**	3		
14	**Lecture #13. E91**	3	SIS 4	
15	**ENDTERM**	3		
16-17	**Final Exam**			

No	Assessment criteria	1	2	3	4	5	6	7	8 /1at	9	10	11	12	13	14	15 /2 at	16-17	%
1.	Midterm								* 10									10%
2.	Endterm															* 10		10%
3.	SIS				* 7			* 7					* 7		* 7			28%
4.	Quizzes		* 1	* 1	* 1	* 1	* 1	* 1		* 1	* 1	* 1	* 1	* 1	* 1			12%
5.	Attendance and activity on lessons	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*		0%
6.	Final Exam Project Defense																* 40	40%
	Total																	**100%**

Class sessions – will be a mixture of information, discussion and practical application of skills.

In-class assessment – will prepare students for their mid-term and final assessment and identify the competence level they have achieved on a related subject matter, the aim being to diagnose potential discrepancies in students' understanding and performance in order to make specific adjustments to the course content and procedures and/or to assign additional assignments to certain individuals or the whole group.

Home assignments – will consolidate the concepts and materials taken during in-class activities, help students to expand the content through diverse background resources and/or practise certain skill areas; they will also develop the students' ability to work individually in exploring and examining related issues.

SIS (Student Independent Study) – comprises group Project to be done by students on the independent basis. Students are supposed to use knowledge and skills acquired in class to do the project. Assistance and advice will be provided by teachers during office hours.

TSIS (Teacher Supervised Student Independent Study) – student self-made project.

End-term test – a diagnostic test used to identify the students' progress, their strengths and weaknesses, intended to force student to prepare for Final Exam. It includes computer based test.

Final examination – 1) an attainment test designed to identify how successful the students have been achieving objectives.

Grading policy:
Intermediate attestations (on 8^{th} and 15^{th} week) join topics of all lectures, practice, laboratories, SIS, TSIS and materials for reading discussed to the time of attestation. Maximum number of points within attendance, activity, SIS, TSIS and laboratories for each attestation is 30 points.
Final exam joins and generalizes all course materials, is conducted in the complex form with quiz and problem. Final exam duration is 180 min. Maximum number of points is 40. At the end of the semester you receive overall total grade (summarized index of your work during semester) according to conventional KBTU grade scale.

ATTENTION!

1) If student missed without plausible reason more than **30% of lessons student receives «F (Fail)»** grade;

2) If for two attestations student receives 29 or less points, this student is not accepted to final exam and for all course he (she) receives **«F (Fail)» grade;**

3) If student receives on final exam 19 or less points, then independently on how many points he (she) received for two attestations, in whole he (she) receives **«F (Fail)» grade;**

In the case of missing or being late for final exam without plausible reason, independently on how many points he (she) received for two attestations, in whole he (she) receives **«F (Fail)» grade.**

4) It is forbidden to change the topic of the course project and change the composition of the team after 2 weeks of training.

5) If a student obtains **30 points** in theoretical knowledge, but does not have a **finished course project (15 week)**, he is not allowed to defend the project and receives an **«F (Fail)» grade** for the course automatically.

6) If a student missed more **than 50%** of the lectures due to health problems and has medical documents in the form of KBTU, but did not complete the course project, the student is not allowed to **defend the course project**, and it is recommended to take an **academic leave.**

7) In case of non-compliance of the course project with the **given assignment**, the student is not allowed to **defend the course** project and automatically receives an **«F (Fail)» grade**.

8) In case of detection **of plagiarism** in the course project, the student is automatically not allowed to defend the course project and receives **«F (Fail)» grade**.

9) At the exam, the student must prepare a **printed course project**, a **presentation** and a **software implementation** of the project. If any documents are missing, the student does not automatically give the right to defend the course project and receives an **«F (Fail)» grade**.

10) The delivery of the **electronic version** of **the course project** and **presentations in MS TEAMS** should be no later than **15 weeks**, if students do not upload the course project **on time**, they will not automatically finish the exam and receives an **«F (Fail)» grade**.

Academic Policy:

- Cheating, duplication, falsification of data, plagiarism are not permitted under any circumstances!
- Students must participate fully in every class. While attendance is crucial, merely being in class does not constitute "participation". Participation means reading the assigned materials, coming to class prepared to ask questions and engage in discussion.
- Students are expected to take an active role in learning (the instructor will provide the information and guidelines to do this).
- Students must come to class on time.
- Students are to take responsibility for making up any work missed.
- Make up tests in case of absence will not normally be allowed.
- Mobile phones must always be switched off in class.
- Students should always show tolerance, consideration and mutual support towards other students.

Students are encouraged to

- consult the teacher on any issues related to the course;
- make up within a week's time for the works undone for a valid reason without any grade deductions;
- make any proposals on improvement of the academic process;
- track down their continuous rating throughout the semester.

Senior Lecturer of SITE, MSc ***Zhaxalykov T.M.***

Minutes #34 of School of Information Technology and Engineering meeting on January 8, 2024