СИЛЛАБУС
2024-2025 оқу жылының күзгі семестрі
«8D06303- Криптология» білім беру бағдарламасы

Пәннің ID және атауы	Білім алушының өзіндік жұмысын (ДӨЖ)	Кредиттер саны			Кредиттердің жалпы саны	Оқытушының жетекшілігімен білім алушының өзіндік жұмысы (ОДӨЖ)
		Дәрістер (Д)	Семинар сабақтар (СС)	Зерт. сабақтар (ЗС)		
104453 Ақпараттық қауіпсіздік криптографиялық құралдарын жобалау	4	1,7	0	3,3	5	7

ПӘН ТУРАЛЫ АКАДЕМИЯЛЫҚ АҚПАРАТ

Оқыту түрі	Циклы, компонент	Дәріс түрлері	Семинар сабақтарының түрлері	Қорытынды бақылаудың түрі мен платфомасы
Оффлайн	БП.ТК	Пробемалы аналитикалық	Тәжірибелік есептер шешу	Жазбаша оффлайн

Дәріскер	Омаров Батырхан Султанович
e-mail:	Batyrkhan.omarov2@kaznu.kz
Телефон:	87054545882
Ассистент	Алтаева Айгерім Бакаткалиевна
e-mail:	Altayeva.aigerim@kaznu.kz
Телефон:	+77075181188

ПӘННІҢ АКАДЕМИЯЛЫҚ ПРЕЗЕНТАЦИЯСЫ

Пәннің мақсаты	Оқытудан күтілетін нәтижелер (ОН)*	ОН қол жеткізу индикаторлары (ЖИ)
криптографиялық қорғау мен криптоталдаудың заманауи әдістерін қолдану қабілетін қалыптастыру.	1. Ақпаратты криптографиялық қорғау алгоритмдерін зерттеу. Тарихи шифрларға талдау және криптоталдаумеңгеру.	1.1 криптография және криптоталдау ұғымдарын түсіндіреді
		1.2 ақпаратты қорғау әдістерін талдайды
	2. Криптографияда математикалық әдістерді қолдану.	2.1 қалдықтар класын санау жүйесін құра алады.
		2.2 салыстыру және оның қасиеттерін талдайды.
		2.3 факторизация ұғымы, ЕҮОБ және Евклид алгоритмін талдайды.
		2.4 жай сандар туралы Эйлер және Ферма теоремаларын талдайды.
	3. Қазіргі шифрлардың құрылымы мен сипаттамаларын білу. Қазіргі криптографияда қолданылатын логикалық функциялардың негізгі сипаттамаларын, олардың қасиеттерін білу.	3.1 криптографияның негізгі есептері мен ұғымдарын, қазіргі шифрларға криптографиялық беріктіліктің негізгі талаптарын біледі.
		3.2 шифрлардың негізгі сипаттамаларын, қазіргі криптографияда қолданылатын логикалық функциялардың сипаттамаларын біледі
		3.3 криптожүйелердің беріктігін талдай алады және криптожүйенің беріктігін арттыру бойынша ұсыныстар бере алады;
	4. Қазіргі шифрларға сызықтық, дифференциалды және алгебралық криптоталдауәдістерін қолдана білу.	4.1 сызықтық криптоталдауәдісі бойынша заманауи шифрларды бағалай алады.
		4.2 қазіргі шифрларды дифференциалды криптоталдауәдісі бойынша бағалай алады.
		4.3 алгебралық криптоталдауәдісі бойынша заманауи шифрларды бағалай алады.
		5.1 шифрлау және шифрды ашу кілттерін құру әдістерін талдай алады

	5. Асимметриялық криптожүйелерге қатысты шифрлау алгоритмдеріне талдау жүргізу. Кілттермен бөлуді құру дағдыларын меңгеру.	5.2 асимметриялық криптожүйелерге қатысты шифрлау алгоритмдерін талдайды
		5.3 электрондық цифрлық қолтаңба ұғымдарын түсіндіре алады
		5.4 кілттердің таралуын түсіндіре алады және кілттерді бөлудің заманауи әдістерін қолдана біледі.
Пререквизиттер	Дискретті математика, ақпаратты қорғаудың ақпараттық негіздері	
Постреквизиттер	Диссертация жазу	
Оқу ресурстары	**Әдебиет:** *Негізгі*: 1. Albrecht, M. (2021). Cryptography Engineering: Design Principles and Practical Applications. Wiley. 2. Misra, S., & Roy, P. (2023). Advances in Cryptography and Network Security. Springer. 3. Menezes, A. J., Van Oorschot, P. C., & Vanstone, S. A. (2022). Handbook of Applied Cryptography (2nd ed.). CRC Press. 4. Омассон Ж.-Ф. О криптографии всерьез / пер. с англ. А. А. Слинкина. – М.: ДМК Пресс, 2021. – 328 с.: ил. 5. Gupta, M., & Saxena, A. (2024). Post-Quantum Cryptography: Theory and Practice. Springer. 6. Liu, J., & Zhou, S. (2023). Quantum-Safe Cryptography: Algorithms and Protocols for the Post-Quantum World. CRC Press. 7. Chen, L., & Chen, M. (2022). Advanced Cryptography in Digital Networks. Wiley. 8. Bhargava, B. (2021). Blockchain and Cryptography: A Comprehensive Introduction. Springer. *Қосымша*: 1. Huang, X., & Yu, C. (2024). Applied Cryptography in Cybersecurity. Springer. 2. Shannon W. Bray, *Implementing cryptography using Python.* 1st ed. Hoboken, NJ, USA: John Wiley & Sons, 2020. 3. C. Easttom, *Modern Cryptography: Applied Mathematics for Encryption and Information Security.* 1st ed. New York, NY, USA: McGraw-Hill, 2016. 4. J. Daemen and V. Rijmen, *The Design of Rijndael*, 2nd ed. Berlin, Germany: Springer, 2020. 5. Song, S., & Zhang, Y. (2023). Modern Cryptographic Techniques for Secure Communication. Elsevier. **Зерттеушілік инфрақұрылымы** 1. Бағдарламалық жасақтама орнатылған Компьютер 2. Интернетке кіру **Интернет-ресурстар** 1. http://elibrary.kaznu.kz/kz 2. дополнительные учебные материалы, домашние задания и проекты можно найти на своих страницах (УМКД) на сайте univer.kaznu.kz.	

Пәннің академиялық саясаты	Пәннің академиялық саясаты әл-Фараби атындағы ҚазҰУ-дың Академиялық саясатымен және академиялық адалдық Саясатымен айқындалады. Құжаттар Univer ИЖ басты бетінде қолжетімді. **Ғылым мен білімнің интеграциясы.** Студенттердің, магистранттардың және докоранттардың ғылыми-зерттеу жұмысы – бұл оқу үдерісінің тереңдетілуі. Ол тікелей кафедраларда, зертханаларда, университеттің ғылыми және жобалау бөлімшелерінде, студенттік ғылыми-техникалық бірлестіктерінде ұйымдастырылады. Білім берудің барлық деңгейлеріндегі білім алушылардың өзіндік жұмысы заманауи ғылыми-зерттеу және ақпараттық технологияларды қолдана отырып, жаңа білім алу негізінде зерттеу дағдылары мен құзыреттіліктерін дамытуға бағытталған. Зерттеу университетінің оқытушысы ғылыми-зерттеу қызметінің нәтижелерін дәрістер мен семинарлық (практикалық) сабақтар, зертханалық сабақтар тақырыбында, силлабустарда көрініс табатын және оқу сабақтары мен тапсырмалар тақырыптарының өзектілігіне жауап беретін ОБӨЖ, БӨЖ тапсырмаларына біріктіреді. **Сабаққа қатысуы.** Әр тапсырманың мерзімі пән мазмұнын іске асыру күнтізбесінде (кестесінде) көрсетілген. Мерзімдерді сақтамау баллдардың жоғалуына әкеледі. **Академиялық адалдық.** Практикалық/зертханалық сабақтар, БӨЖ білім алушының дербестігін, сыни ойлауын, шығармашылығын дамытады. Плагиат, жалғандық, шпаргалка пайдалану, тапсырмаларды орындаудың барлық кезеңдерінде көшіруге жол берілмейді. Теориялық оқыту кезеңінде және емтихандарда академиялық адалдықты сақтау негізгі саясаттардан басқа «Қорытынды бақылауды жүргізу Ережелері», «Ағымдағы оқу жылының күзгі/көктемгі семестрінің қорытынды бақылауын жүргізуге арналған Нұсқаулықтары», «Білім алушылардың тестілік құжаттарының көшіріліп алынуын тексеру туралы Ережесі» тәрізді құжаттармен регламенттеледі. **Инклюзивті білім берудің негізгі принциптері.** Университеттің білім беру ортасы гендерлік, нәсілдік/этникалық тегіне, діни сенімдеріне, әлеуметтік-экономикалық мәртебесіне, студенттің физикалық денсаулығына және т.б. қарамастан, оқытушы тарапынан барлық білім алушыларға және білім алушылардың бір-біріне әрқашан қолдау мен тең қарым-қатынас болатын қауіпсіз орын ретінде ойластырылған. Барлық адамдар құрдастары мен курстастарының қолдауы мен достығына мұқтаж. Барлық студенттер үшін жетістікке жету, мүмкін емес нәрселерден гөрі не істей алатындығы болып табылады. Әртүрлілік өмірдің барлық жақтарын күшейтеді. Барлық білім алушылар, әсіресе мүмкіндігі шектеулі жандар, телефон/e-mail nazarbayev.dauren@kaznu.kz немесе MS Teams-тегі бейне байланыс арқылы https://teams.microsoft.com/l/meetup-join/19:JZUCJSk15AsJ8HTSxI27j-f3rdE_9iD6aM0XOaMulc81@thread.tacv2/1694960378754?context=%7B%22Tid%22:%22b0ab71a5-75b1-4d65-81f7-f479b4978d7b%22,%22Oid%22:%2264544ccf-36de-44aa-9757-9034e3f9129a%22%7D кеңестік көмек ала алады. **Назар салыңыз!** Әр тапсырманың мерзімі пәннің мазмұнын іске асыру күнтізбесінде (кестесінде) көрсетілген. Мерзімдерді сақтамау баллдардың жоғалуына әкеледі.

БІЛІМ БЕРУ, БІЛІМ АЛУ ЖӘНЕ БАҒАЛАНУ ТУРАЛЫ АҚПАРАТ

Оқу жетістіктерін есептеудің баллдық-рейтингтік әріптік бағалау жүйесі

Баға	Баллдардың сандық баламасы	% мәндегі баллдар	Дәстүрлі жүйедегі баға
A	4,0	95-100	Өте жақсы
A-	3,67	90-94	
B+	3,33	85-89	Жақсы
B	3,0	80-84	
B-	2,67	75-79	
C+	2,33	70-74	
C	2,0	65-69	Қанағаттанарлық
C-	1,67	60-64	
D+	1,33	55-59	
D	1,0	50-54	
FX	0,5	25-49	Қанағаттанарлықсыз
F	0	0-24	

Бағалау әдістері

Критериалды бағалау – айқын әзірленген критерийлер негізінде оқытудың нақты қол жеткізілген нәтижелерін оқытудан күтілетін нәтижелерімен ара салмақтық процесі. Формативті және жиынтық бағалауға негізделген.

Формативті бағалау – күнделікті оқу қызметі барысында жүргізілетін бағалау түрі. Ағымдағы көрсеткіш болып табылады. Білім алушы мен оқытушы арасындағы жедел өзара байланысты қамтамасыз етеді. Білім алушының мүмкіндіктерін айқындауға, қиындықтарды анықтауға, ең жақсы нәтижелерге қол жеткізуге көмектесуге, оқытушының білім беру процесін уақтылы түзетуге мүмкіндік береді. Дәрістер, семинарлар, практикалық сабақтар (пікірталастар, викториналар, жарыссөздер, дөңгелек үстелдер, зертханалық жұмыстар және т.б.) кезінде тапсырмалардың орындалуы, аудиториядағы жұмыс белсенділігі бағаланады. Алынған білім мен құзыреттілік бағаланады.

Жиынтық бағалау – пән бағдарламасына сәйкес бөлімді зерделеу аяқталғаннан кейін жүргізілетін бағалау түрі. БӨЖ орындаған кезде семестр ішінде 3-4 рет өткізіледі. Бұл оқытудан күтілетін нәтижелерін игеруді дескрипторлармен арақатынаста бағалау. Белгілі бір кезеңдегі пәнді меңгеру деңгейін анықтауға және тіркеуге мүмкіндік береді. Оқу нәтижелері бағаланады.

Формативті және жиынтық бағалау	**% мәндегі баллдар**
Дәрістердегі белсенділік	-
Семинарлық сабақтарда жұмыс істеуі	15
Лабораториялық сабақтарда жұмыс істеуі	30
Өзіндік жұмысы	15
Жобалық және шығармашылық қызметі	-
Қорытынды бақылау (емтихан)	40
ЖИЫНТЫҒЫ	100

Оқу курсының мазмұнын іске асыру күнтізбесі (кестесі). Оқытудың және білім берудің әдістері.			
Аптасы	**Тақырып атауы**	**Сағат саны**	**Макс. Балл**
МОДУЛЬ 1 КВАНТТЫҚ ТӨЗІМДІ КРИПТОГРАФИЯ ЖӘНЕ КРИПТОЖҮЙЕЛЕР			
1	**Д 1.** Криптография мен ақпараттық қауіпсіздіктің заманауи міндеттеріне кіріспе.	1	
	С 1. Криптография бойынша ғылыми жарияланымдарды сыни талдау.	1	2
	ЛС 1. Кванттық криптографияның математикалық негіздері: теоремалар, есептеу күрделілігі.	4	8
2	**Д 2.** Кванттық криптографияның математикалық негіздері мен теориялық аспектілері.	1	
	С 2. Кванттық кілттерді бөлуді жүзеге асыру (QKD)	1	2
	ЛС 2. Күрделілік теориясы және оны криптографияда қолдану.	4	8
	ОДӨЖ 1. ДӨЖ 1 орындау бойынша кеңестер	1	
3	**Д 3.** Торлы Криптография: кванттық шабуылға төзімділік және қолдану.	1	
	С 3. Кестелері негізделген схеманы іске асыру (NT RU).	1	2
	ЛС 3. Криптографияда кестелер теориясын қолдану.	4	8
	ОДӨЖ 2. ДӨЖ 1 орындау бойынша кеңестер	1	
МОДУЛЬ 2 ГОМОМОРФТЫ ШИФРЛАУ			
4	**Д 4.** Алгебралық топтар теориясы және эллиптикалық қисықтардың криптографияда қолданылу принциптері.	1	
	С 4. Эллиптикалық қисықтар арқылы қауіпсіз шифрлау схемаларын жүзеге асыру.	1	2
	ЛС 4. Математикалық қауіпсіздікті қамтамасыз етудің алгебралық негіздері.	4	8
	ДӨЖ1 Жетілдірілген криптографиялық әдістер және қазіргі қауіп-қатерлерге төзімділік.		15
5	**Д 5.** Толық гомоморфтық шифрлау әдісі және оның бұлттық есептеулерде деректер құпиялығын қорғаудағы рөлі.	1	
	С 5. Бұлттық деректердің қауіпсіздігін қамтамасыз ету үшін FHE схемаларын қолдану.	1	2
	ЛС 5. Гомоморфтық шифрлаудың ақпараттық қауіпсіздікті сақтау мүмкіндіктері.	4	8
	ОДӨЖ 3. ДӨЖ 2 орындау бойынша кеңестер	1	
6	**Д 6.** Көпқырлы криптографиялық жүйелер, мультибазистік кілттер және олардың қауіпсіздікке қосар үлесі.	1	
	С 6. Көпқырлы кілттік криптографиялық жүйелерді құру және тестілеу.	1	2
	ЛС 6. Көпқырлы кілттерді қолданудың криптографиялық артықшылықтары.	4	8
	ОДӨЖ 4. ДӨЖ 2 орындау бойынша кеңестер	1	
МОДУЛЬ 3 КӨП ЖАҚТЫ ЕСЕПТЕУ (MPC)			
7	**Д 7.** Қауіпсіз көпжақты есептеулер (MPC) және олардың деректерді құпия түрде өңдеудегі қолданбалы маңызы.	1	
	С 7. Қаржылық деректерді құпия сақтай отырып MPC протоколдарын құру.	1	2
	ЛС 7. Деректерді қорғауда көпжақты есептеулерді қолдану мүмкіндіктері.	4	8
	ДӨЖ 2. Қаржы және мемлекеттік жүйелер үшін дәлелді қауіпсіздігі бар криптографиялық хаттамалар		15
Аралық бақылау 1			**100**
8	**Д 8.** Нөлдік білім дәлелдемелері және олардың аутентификация және блокчейн жүйелеріндегі рөлі.	1	
	С 8. Нөлдік білім дәлелдеу протоколдарын құру.	1	2
	ЛС 8. Ақпарат алмасуда нөлдік білім дәлелдемелерінің рөлі.	4	8
МОДУЛЬ 4 ЖАНАМА АРНАЛЫҚ ШАБУЫЛДАР ЖӘНЕ ОЛАРДЫҢ АЛДЫН АЛУ ӘДІСТЕРІ			
9	**Д 9.** Постквантық криптографияның негізгі әдістері, кодтық және мультимерлік криптографияның болашағы.	1	
	С 9. Кодтық криптография әдістерін қолдану арқылы постквантық жүйе құру.	1	2
	ЛС 9. Постквантық қауіпсіздікті қамтамасыз етудің стандарттары.	4	8
	ОДӨЖ 5. ДӨЖ 3 орындау бойынша кеңестер	1	
10	**Д 10.** Кванттық криптоанализ: кванттық шабуылдар, алгоритмдер, қарсы қорғаныс шаралары.	1	
	С 10. RSA және ECC жүйелеріне кванттық шабуылдар жасай отырып олардың әлсіздігін зерттеу.	1	2
	ЛС 10. Кванттық шабуылдарға қарсы қорғаныс шаралары	4	8
МОДУЛЬ 5 БҰЛТТЫҚ ИНФРАҚҰРЫЛЫМДАР КРИПТОГРАФИЯЛЫҚ ШИФРЛАУ			
11	**Д 11.** Бүйірлік арналар арқылы шабуыл жасау әдістері және қауіпсіздік шаралары.	1	
	С 11. RSA криптографиялық жүйесіне бүйірлік арналар арқылы шабуыл жасауға қарсы шаралар енгізу.	1	2
	ЛС 11. Физикалық деңгейдегі қорғаныс және оның маңызы.	4	8

	ОДӨЖ 6. ДӨЖ 3 орындау бойынша кеңестер	1	
12	**Д 12.** Бұлттық және бөлінген жүйелерде қолданылатын криптографиялық қауіпсіздік шаралары.	1	
	С 12. Бұлттық инфрақұрылымдарда криптографиялық шифрлау схемаларын құру.	1	2
	ЛС 12. Бұлттық есептеулердегі деректер қауіпсіздігі.	4	8
	ДӨЖ 3 Толық гомоморфты шифрлау (FHE): артықшылықтары, шектеулері және практикалық қолданылуы		10
13	**Д 13.** Блокчейн технологияларындағы криптографиялық әдістер және деректердің өзгермейтіндігін қамтамасыз ету.	1	
	С 13. Блокчейн жүйелерінде транзакция қауіпсіздігін талдау және шифрлау.	1	2
	ЛС 13. Ақпараттық қауіпсіздік пен блокчейннің өзара байланысы.	4	8
МОДУЛЬ 6 ЖАСАНДЫ ИНТЕЛЛЕКТ ПЕН АҚПАРАТТЫҚ ҚАУІПСІЗДІК			
14	**Д 14.** Жасанды интеллекттің криптоанализдегі рөлі және қауіпсіздікке тигізетін әсері.		
	С 14. Криптографиялық жүйелерге қарсы шабуыл жасау үшін машиналық оқыту әдістерін қолдану.	1	2
	ЛС 14. Жасанды интеллект пен ақпараттық қауіпсіздіктің интеграциясы.	1	8
	ОДӨЖ 7. ДӨЖ 4 орындау бойынша кеңестер	4	
15	**Д 15.** Ақпараттық қауіпсіздік криптографиясының болашағы: кванттық және жасанды интеллектпен қақтығысқан кездегі проблемалар мен перспективалар.	1	
	С 15. Қорғау жүйелерін кванттық шабуылдарға төзімді ету моделін құру.	1	2
	ЛС 15. Ақпараттық қауіпсіздіктің болашағы мен даму бағыттары.	4	8
	ДӨЖ 4. Криптографиялық жүйелерге қарсы шабуыл жасау үшін жасанды интеллект пен ақпараттық қауіпсіздіктің интеграциясы.		10
Аралық бақылау 2			**100**
Қорытынды бақылау (емтихан)			**100**
Пән үшін жиынтығы			**100**

ДӨЖ 1. Жетілдірілген криптографиялық әдістер және қазіргі қауіп-қатерлерге төзімділік.(100% дың 15% АБ 1)

Критерий	14-15 %	11-13%	8-10%	0-7%
Тапсырмаға сәйкестік, талдау тереңдігі және әдісті түсіну, дәлелдеу және шешімдердің дұрыстығы	Студент шифрланған мәтін үшін сәйкестік индексін дұрыс есептеп, оны кездейсоқ мәтін мен табиғи тілдегі мәтіндер үшін күтілетін мәндермен салыстырды. Сәйкестік индексін есептеу негізінде кілт ұзындығы дұрыс бағаланады, индекс пен кілт ұзындығы арасындағы байланысты толық түсіну көрсетіледі. Фридман әдісінің әр қадамына, оның ішінде есептеулер мен тұжырымдарға нақты және дұрыс негіздемелермен егжей-тегжейлі түсініктемелер берілген. Балама шешімдерді немесе ықтимал қателерді қарастыруды қамтитын нәтижелерді тексеру жүргізілді. Барлық есептеулер мен қадамдар дәл орындалады, қатесіз, әдіс толығымен және дұрыс қолданылады.	Студент сәйкестік индексін дұрыс есептеді, бірақ мәндерді түсіндіруде немесе нақты деректермен салыстыруда шамалы қателер болуы мүмкін. Кілт ұзындығы дұрыс бағаланады, бірақ есептеу түсіндірмелері толық немесе егжей-тегжейлі болмауы мүмкін. Әдістің қадамдары дұрыс орындалды, бірақ негіздеме жеткілікті терең болмауы мүмкін, түсініктемелерде шамалы кемшіліктер болуы мүмкін. Есептеулерде кішігірім қателіктер болуы мүмкін, бірақ олар маңызды емес және соңғы нәтижеге қатты әсер етпейді.	Студент әдістің негізгі қадамдарын орындайды, бірақ сәйкестік индексін есептеуде немесе оны түсіндіруде қателіктер жіберіледі. Кілттің ұзындығы қатемен бағаланады немесе оның қалай есептелгені толық түсінілмейді. Түсініктемелерде олқылықтар бар және қорытынды логикасы жеткіліксіз. Әдіс соңына дейін қолданылмайды немесе барлық кезеңдер дұрыс орындалмайды. Есептеудегі немесе нәтижелерді түсіндірудегі қателер қорытындылардағы елеулі ауытқуларға әкеледі.	Фридман әдісінің негізгі қадамдары дұрыс орындалмаған немесе өткізіп жіберілген. Студент сәйкестік индексін дұрыс есептей алмады немесе нәтижелерді түсіндіре алмады. Кілттің ұзындығы есептелмеген немесе алынған нәтижелер шындыққа жанаспайды. Шешім қадамдары туралы түсініктемелер жоқ немесе олар Үстірт және нәтижесіз. Әдіс жалпы қолданылмайды немесе өрескел қателіктермен орындалмайды, бұл дұрыс емес нәтижеге әкелді.
Тапсырманы орындау мерзімдерін сақтау	Жұмыс белгіленген кестеге сәйкес мерзімінде көрсетіледі.	Жұмыс аз ауытқумен мерзімге жақын, бірақ қолайлы шеңберде қалады.	Жұмыс көрсетілді, бірақ белгіленген мерзімнен айтарлықтай ауытқу бар.	Жұмыс белгіленген мерзімнен кейін айтарлықтай кідіріспен көрсетіледі.

ДӨЖ 2. Қаржы және мемлекеттік жүйелер үшін дәлелді қауіпсіздігі бар криптографиялық хаттамалар. (100% дың 15% АБ 1)

Критерий	14-15 %	11-13%	8-10%	0-7%
Тапсырмаға сәйкестік, талдау тереңдігі және әдісті түсіну, дәлелдеу және шешімдердің дұрыстығы	Студент ағындық және блоктық симметриялы шифрларды дұрыс орындайды немесе сипаттайды. Кілттерді құру, шифрлау және шифрды ашу сияқты барлық қадамдар дәл орындалады. Егер практикалық іске асыру қажет болса, ол дұрыс жұмыс істейді, дұрыс нәтиже береді және студенттер шифрдың жұмыс істеуі туралы толық түсінік берді. Жұмыс қисынды түрде құрылымдалған, нақты криптографиялық примитивтерді қолдана отырып шифрлау/шифрды ашу кезеңдері егжей-тегжейлі көрсетілген. Барлық терминдер дұрыс қолданылады, есептеулерде немесе іске асыруда қателер жоқ.	Жалпы, тапсырма дұрыс орындалды, бірақ алгоритмдерді сипаттау немесе енгізу сияқты кейбір аспектілерде шамалы қателер болуы мүмкін. Егер тапсырма бағдарламалық жасақтаманы іске асыруды қамтыса, онда ол көп жағдайда дұрыс жұмыс істейді, бірақ кішігірім кемшіліктер болуы мүмкін. Алгоритмдерді түсіну көрсетілген, бірақ кейбір ұғымдарды түсіндіруде немесе түсіндіруде ұсақ қателіктер болуы мүмкін (мысалы, ағындық шифрлар үшін жалған кездейсоқ сандарды құру ерекшеліктері). Жалпы жұмыстың құрылымы мен логикасы жақсы деңгейде, бірақ түсініктемелердің дәйектілігі мен тереңдігінде шамалы олқылықтар болуы мүмкін.	Студент тапсырманы тек ішінара орындады немесе оның жұмысында криптографиялық алгоритмдерді іске асыруда немесе сипаттауда айтарлықтай қателіктер бар. Бағдарламалық жасақтаманы іске асыруда қателер бар немесе есептеулер дұрыс нәтиже бермейді. Студент алгоритмдердің негізгі аспектілерін дұрыс түсіндіре алмады (мысалы, кілттерді құру, блоктық шифрлау режимдерінің арасындағы айырмашылық). Жұмыстың логикасы әрдайым айқын бола бермейді, шешім қадамдары дәйекті немесе жеңілдетілмеген, кейбір ұғымдарды түсіндіруде олқылықтар бар.	Тапсырманың негізгі аспектілерінің көпшілігі немесе барлығы теориялық бөлімде де, бағдарламалық жабдықтама да дұрыс орындалмаған. Практикалық бөлік (егер бар болса) жұмыс істемейді немесе өрескел қателіктермен орындалады, бұл нәтижелерді жарамсыз етеді. Жұмыстың логикасы мен құрылымы әлсіз, тапсырмалар талаптарға сәйкес келмейді немесе аз күш жұмсалады, көбінесе дәлелдер мен түсіндірулерсіз.
Тапсырманы орындау мерзімдерін сақтау	Жұмыс белгіленген кестеге сәйкес мерзімінде көрсетіледі.	Жұмыс аз ауытқумен мерзімге жақын, бірақ қолайлы шеңберде қалады.	Жұмыс көрсетілді, бірақ белгіленген мерзімнен айтарлықтай ауытқу бар.	Жұмыс белгіленген мерзімнен кейін айтарлықтай кідіріспен көрсетіледі.

ДӨЖ 3. Толық гомоморфты шифрлау (FHE): артықшылықтары, шектеулері және практикалық қолданылуы. (100% дың 10% АБ 2)

Критерий	9-10 %	7-8%	5-6%	0-4%
Тапсырмаға сәйкестік, талдау тереңдігі және әдісті түсіну, дәлелдеу және шешімдердің дұрыстығы	Студент асимметриялық алгоритмдерді (мысалы, RSA, ECC, ElGamal), оның ішінде теориялық аспектілер мен практикалық іске асыруды терең түсінеді. Негізгі ұғымдар дұрыс түсіндірілген: ашық және жеке кілттерді құру, шифрлау және шифрды ашу, цифрлық қолтаңба, қауіпсіздік принциптері (мысалы, RSA-дағы факторизацияның күрделілігі, ecc-дегі дискретті логарифм мәселесі). Егер практикалық іске асыру қарастырылса (бағдарламалау тілінде немесе криптографиялық кітапханаларды қолдану арқылы), ол толығымен дұрыс, күтілетін нәтиже береді. Алгоритмдердің кезең-кезеңімен түсіндірумен және талдаумен, соның ішінде үлкен сандармен және өнімділік мәселелерімен жұмыс істеу ерекшеліктерімен жұмыс істеуінің нақты мысалдары келтірілген. Жұмыс құрылымдалған, дәйекті түрде берілген, бір кезеңнен екінші кезеңге нақты және логикалық ауысу.	Студент алгоритмдерді сенімді түсінетіндігін көрсетеді, бірақ қауіпсіздікті терең талдау немесе алгоритмдердің барлық қадамдарын толық сипаттау сияқты кейбір мәліметтерді жіберіп алуы мүмкін. Асимметриялық алгоритмдердің негізгі элементтері келтірілген, бірақ кейбір аспектілерді үстірт немесе толық емес сипаттауға болады (мысалы, кілт генерациясының толық түсіндірмесі немесе алгоритмдердің ерекшеліктері, мысалы, кілт ұзындығы және оның қауіпсіздікке әсері). Практикалық іске асыру дұрыс орындалды, бірақ оңтайландыруда аздаған кемшіліктер немесе алгоритмдердің өнімділігін талдау жеткіліксіз болуы мүмкін. Шифрлау/шифрды ашу мысалдары мен қадамдары сипатталған, бірақ ықтимал шабуылдарды немесе қосымша мүмкіндіктерді тереңірек талдау жеткіліксіз. Жұмыс жақсы ұйымдастырылған, бірақ кішігірім логикалық сәйкессіздіктер немесе тапсырма құрылымынан шамалы ауытқулар болуы мүмкін.	Асимметриялық алгоритмдерді түсіну шектеулі, мүмкін студент қате алгоритмдерді сипаттайды немесе жеткілікті егжей-тегжейлі емес. Шифрлау / шифрды шешудің негізгі қадамдары қателіктермен, логикадағы кемшіліктермен немесе жіберіп алулармен түсіндірілуі мүмкін. Практикалық іске асыру, егер қарастырылған болса, қателіктермен орындалуы мүмкін, дұрыс нәтиже бермейді немесе дұрыс жұмыс істемейді. Студент алгоритмдердің жалпы тармақтарын егжей-тегжейлі талдаусыз ғана айтады (мысалы, математика мен крипто-төзімділікті дұрыс қарастырмай, RSA немесе ECC-тің жеңілдетілген түсіндірмесі). Жұмыстың логикасы әрдайым дәйекті бола бермейді, дәлелді тұжырымдар немесе егжей-тегжейлі талдау жоқ. Жұмыс құрылымының кемшіліктері бар, тапсырманың барлық бөліктері орындалмайды немесе бөлшектелмейді.	Студент асимметриялық криптографиялық алгоритмдерді түсінбеді. Шифрлау, кілттерді құру және шифрды шешудің негізгі тұжырымдамалары дұрыс орындалмаған немесе мүлдем жоқ. Жұмыста алгоритмдерді сипаттауда немесе қолдануда өрескел қателер бар (мысалы, ашық және жеке кілттермен жұмыс істеу туралы қате түсініктеме). Тапсырманың практикалық бөлігі жоқ немесе өрескел қателіктермен орындалады, алгоритмдер жұмыс істемейді немесе дұрыс жұмыс істемейді. Жұмыстың логикасы нашар құрылымдалған, шешім қадамдары ретсіз түрде берілген, түсініктемелерде олқылықтар бар.
Тапсырманы орындау мерзімдерін сақтау	Жұмыс белгіленген кестеге сәйкес мерзімінде көрсетіледі.	Жұмыс аз ауытқумен мерзімге жақын, бірақ қолайлы шеңберде қалады.	Жұмыс көрсетілді, бірақ белгіленген мерзімнен айтарлықтай ауытқу бар.	Жұмыс белгіленген мерзімнен кейін айтарлықтай кідіріспен көрсетіледі.

ДӨЖ 4. Криптографиялық жүйелерге қарсы шабуыл жасау үшін жасанды интеллект пен ақпараттық қауіпсіздіктің интеграциясы. (100% дың 10% АБ 2)

Критерий	9-10 %	7-8%	5-6%	0-4%
Тапсырмаға сәйкестік, талдау тереңдігі және әдісті түсіну, дәлелдеу және шешімдердің дұрыстығы	Жұмыс тапсырманың барлық талаптарына толық сәйкес келеді. Студент S қораптарының криптографиялық қасиеттерін анықтауда қолданылатын әдістер мен тәсілдерді нақты және толық сипаттайды. Оның талаптарын қолдау үшін нақты мысалдар мен иллюстрациялар келтіреді. Криптографиялық қасиеттерін кешенді және терең талдауды ұсынады. Жұмыстың нақты және логикалық құрылымы бар. Кіріспе S-қораптардың қасиеттерді анықтаудың мақсаты мен әдістерін нақты тұжырымдайды. Жұмыс дәйекті және әр бөлім логикалық түрде ұйымдастырылған. Барабар және егжей-тегжейлі негіздемелер мен қорытындылар берілген.	Жалпы жұмыс тапсырманың негізгі талаптарына сәйкес келеді. Студент S-қораптардың криптографиялық қасиеттерін анықтау әдістерінің нақты және барабар сипаттамаларын ұсынады. Егжей-тегжейлі кемшіліктер немесе бірнеше түсініксіз сәттер болуы мүмкін. Талдаудың жақсы деңгейін білдіреді, бірақ біршама үстірт болуы мүмкін. Жұмыс жақсы құрылымға ие, бірақ бірнеше түсініксіз сәттерді қамтуы мүмкін. Кіріспе мен қорытынды анық, бірақ негізгі бөлімдерді ұйымдастыруда кейбір сәйкессіздіктер болуы мүмкін. Негізделген тұжырымдар берілген, бірақ олардың егжей-тегжейлі деңгейі әр түрлі болуы мүмкін.	Жұмыс тапсырманың минималды талаптарына сәйкес келеді. Студент әдістердің негізгі сипаттамаларын ұсынады, бірақ олар шектеулі болуы мүмкін. Талдау үстірт болуы мүмкін және әрқашан толық негізделмейді. Жұмыс ұйым мен құрылымның минималды талаптарына сәйкес келеді. Кіріспе мен қорытынды анық, бірақ негізгі бөлімдер біршама шашыраңқы болуы мүмкін немесе әрқашан қисынды емес. Қорытындылар берілген, бірақ олар шектеулі немесе әрқашан анық болмауы мүмкін.	Жұмыс тапсырма талаптарына сәйкес келмейді. Студент S қораптарының криптографиялық қасиеттерін анықтау әдістерін дұрыс түсінбеуі мүмкін. Минималды немесе кейбір ғана сипаттамаларды ұсынады немесе оларды мүлдем көрсетпейді. Жұмыс тіпті ұйымдастырылмаған және құрылымы нашар. Кіріспе және / немесе қорытынды түсініксіз немесе жоқ болуы мүмкін. Негізгі бөлімдер бір-бірімен байланысты емес, бұл жұмысты оқуға және түсінуге қиын .
Тапсырманы орындау мерзімдерін сақтау	Жұмыс белгіленген кестеге сәйкес мерзімінде көрсетіледі.	Жұмыс аз ауытқумен мерзімге жақын, бірақ қолайлы шеңберде қалады.	Жұмыс көрсетілді, бірақ белгіленген мерзімнен айтарлықтай ауытқу бар.	Жұмыс белгіленген мерзімнен кейін айтарлықтай кідіріспен көрсетіледі.

Декан м.а. _____ Тұрар О.Н.

Оқыту және білім беру сапасы бойынша
Академиялық комитетінің төрағасы _____ Адилжанова С.А.

Кафедра меңгерушісі _____ Мусиралиева Ш.Ж.

Дәріскер _____ Омаров Б.С.