

СИЛЛАБУС
2025__-2026__оқу жылының күзгі семестрі
« 6B05402 Математика __» білім беру бағдарламасы

Пәннің ID және атауы	Білім алушының өзіндік жұмысын (БӨЖ)	Кредиттер саны			Кредиттердің жалпы саны	Оқытушының жетекшілігімен білім алушының өзіндік жұмысы (ОБӨЖ)	
		Дәрістер (Д)	Семинар сабақтар (СС)	Зерт. сабақтар (ЗС)			
Заманауи криптожүйелер	3	4,5	4,5	0	6	4	
ПӘН ТУРАЛЫ АКАДЕМИЯЛЫҚ АҚПАРАТ							
Оқыту түрі	Циклы, компоненті	Дәріс түрлері	Семинар сабақтарының түрлері		Қорытынды бақылаудың түрі мен платформасы UNIVER, жазбаша		
Оффлайн	Базалық пән. Жоғарғы оқу орны компоненті	Теориялық	Есептер шығару				
Дәріскер (лер)	к.ф.-м.н Туленбаев Кайсар Маратович						
e-mail:	kaysart1@mail.ru						
Телефоны:	87071608400						
Ассистент (тер)	к.ф.-м.н Туленбаев Кайсар Маратович						
e-mail:	kaysart1@mail.ru						
Телефоны:	87071608400						
ПӘННІҢ АКАДЕМИЯЛЫҚ ПРЕЗЕНТАЦИЯСЫ							
Пәннің мақсаты	Оқытудан күтілетін нәтижелер (ОН)*				ОН қол жеткізу индикаторлары (ЖИ)		
	1. Кіріспе, классикалық шифрлар мысалдары				1.1 Ығысу шифрымен шифрлау		
					1.2 Аффиндік шифрдың криптоанализі		
	2. Бүтін сандар жиыны және салыстырулар теориясы				2.1 Бүтін сандар жиыны, Евклид алгоритмі және оның салдары. Ең үлкен ортақ бөлгішті ұсыну		
					2.2 Салыстырулар теориясы. Модуль бойынша салыстырулар қасиеттері. Кері элементтер.		
	3. RSA-криптожүйе				3.1 RSA-шифр, шифрлау және оқу процесі, негіздеме		
					3.2 RSA-ашық кілтпен берілген мәтінді шифрлау		
Пререквизиттер	Алгебра негіздері, сызықтық алгебра, сандар теориясы, бағдарламалау тілдері						
Постреквизиттер	Криптография, ақпаратты қорғау негіздері, ақпаратты қорғаудың математикалық негіздері						
Оқу ресурстары	Әдебиет:						

	Негізгі 1. Е.Р. Байсалов, Криптографияның математикалық негіздері, Алматы, «Қазак университеті», 2003 ж. 2. А.П. Алферов және т.б., Криптография негіздері, Москва, «Гелиос АРВ», 2002 ж. 3. В.И. Нечаев, Криптография элементтері. Ақпаратты қорғаудың негіздері, М., «Жоғары мектеп», 1999 ж. Қосымша 1. А.А. Бухштаб, <i>Сандар теориясының негіздері</i>, М., «Просвещение», 1966 ж. 2. D.R. Stinson, <i>Криптография. Теория және практика</i>, CRC Press, Boca Raton, 1995 Интернет-ресурстар 1. http://elibrary.kaznu.kz/ru 2. MOOC/видеодәрістер
--	--

пәннің академиялық саясаты	Пәннің академиялық саясаты әл-Фараби атындағы ҚазҰУ-дың <u>Академиялық саясатымен және академиялық адалдық Саясатымен</u> айқындалады. Құжаттар Univer ИЖ басты бетінде қолжетімді. Ғылым мен білімнің интеграциясы. Студенттердің, магистранттардың және докторанттардың 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 ОБӨЗ, БӨЗ тапсырмаларына біріктіреді. Сабаққа қатысуы. Әр тапсырманың мерзімі пән мазмұнын іске асыру күнтізбесінде (кестесінде) көрсетілген. Мерзімдерді сақтамау балдардың 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 <u>«Қорытынды бақылауды жүргізу Ережелері», «Ағымдағы оқу жылының күзгі/көктемгі семестрінің қорытынды бақылауын жүргізуге арналған Нұсқаулықтары», «Білім алушылардың тестілік құжаттарының көшіріліп алынуын тексеру туралы Ережесі»</u> 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. Өртүрлілік өмірдің барлық жақтарын күшейтеді. Барлық білім алушылар, әсіресе мүмкіндігі шектеулі жандар, телефон/e-mail <u>оқытушының байланыстарын енгізіңіз</u> немесе MS Teams-тегі бейне байланыс арқылы <u>жиналысқа тұрақты сілтеме жасаңыз</u> кеңестік көмек ала алады. MOOC интеграциясы (massive openlline course). MOOC-тың пәнге интеграциялануы жағдайында барлық білім алушылар MOOC-қа тіркелуі қажет. MOOC модульдерінің өту мерзімі пәнді оқу кестесіне сәйкес қатаң сақталуы керек. Назар салыңыз! Әр тапсырманың мерзімі пәннің мазмұнын іске асыру күнтізбесінде (кестесінде) көрсетілген, сондай-ақ MOOC-та көрсетілген. Мерзімдерді сақтамау балдардың жоғалуына әкеледі.
-----------------------------------	--

БІЛІМ БЕРУ, БІЛІМ АЛУ ЖӘНЕ БАҒАЛАНУ ТУРАЛЫ АҚПАРАТ				
Білім алушылардың оқудағы жетістіктерін төрт балдық жүйе бойынша сандық эквивалентке сәйкес бағалаудың әріптік жүйесі				Бағалау әдістері
Әріптік жүйе	Балдардың сандық эквиваленті	Пайыздық мазмұны	Дәстүрлі жүйе бойынша бағалау	Критериалды бағалау – айқын әзірленген критерийлер негізінде оқытудың нақты қол жеткізілген нәтижелерін оқытудан күтілетін нәтижелерімен ара салмақтық процесі. Формативті және жиынтық бағалауға негізделген.

			Өте жақсы	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.														
4,0	95-100																	
3,67	90-94																	
3,33	85-89	Жақсы	<table><tr><th>Формативті және жиынтық бағалау</th><th>% мәндегі баллдар</th></tr><tr><td>Дәрістердегі белсенділік</td><td>5</td></tr><tr><td>Практикалық сабақтарда жұмыс істеуі</td><td>20</td></tr><tr><td>Өзіндік жұмысы</td><td>25</td></tr><tr><td>Жобалық және шығармашылық қызметі</td><td>10</td></tr><tr><td>Қорытынды бақылау (емтихан)</td><td>40</td></tr><tr><td>ЖИЫНТЫҒЫ</td><td>100</td></tr></table>		Формативті және жиынтық бағалау	% мәндегі баллдар	Дәрістердегі белсенділік	5	Практикалық сабақтарда жұмыс істеуі	20	Өзіндік жұмысы	25	Жобалық және шығармашылық қызметі	10	Қорытынды бақылау (емтихан)	40	ЖИЫНТЫҒЫ	100
Формативті және жиынтық бағалау	% мәндегі баллдар																	
Дәрістердегі белсенділік	5																	
Практикалық сабақтарда жұмыс істеуі	20																	
Өзіндік жұмысы	25																	
Жобалық және шығармашылық қызметі	10																	
Қорытынды бақылау (емтихан)	40																	
ЖИЫНТЫҒЫ	100																	
3,0	80-84																	
2,67	75-79																	
2,33	70-74																	
2,0	65-69	Қанағаттанарлық																
1,67	60-64																	
1,33	55-59																	
1,0	50-54																	
0,5	25-49		Қанағаттанарлықсыз															
0	0-24																	

Оқу курсының мазмұнын іске асыру күнтізбесі (кестесі). Оқытудың және білім берудің әдістері.

Апта	Тақырып атауы	Сағат саны	Бағалау (%)
1-модуль. Кіріспе, классикалық шифрлар мысалдары			
1	Дәріс 1. Кіріспе. Классикалық шифрлар және оларды бұзу. Ығысу шифры және аффиндік шифр, оларды дешифрлеу және бұзу. Шифрлау және дешифрлеудің негізгі схемасы.	2	0
	Семинар 1. Ығысу шифрымен шифрлау.	2	0
2	Дәріс 2. Классикалық шифрлар және оларды бұзу. Орнына қою шифрын бұзудың жиілік әдісі. Классикалық шифрлардың кемшіліктері, қазақ және орыс тілдеріндегі мәтіндерге жиілік талдау және олардың тұрақтылығын бағалау.	2	0
	Семинар 2. Аффиндік шифрды жүзеге асыру.	2	0
2-модуль. Бүтін сандар жиыны және салыстырулар теориясы			
3	Дәріс 3. Бүтін сандар жиыны, Евклид алгоритмі және оның салдары. Ең үлкен ортақ бөлгішті ұсыну.	2	0
	Семинар 3. Евклид алгоритміне қатысты есептер.	2	0
4	Дәріс 4. Салыстырулар теориясы. Модуль бойынша салыстырулар қасиеттері. Кері элементтер.	2	10
	Семинар 4. Модуль бойынша кері элементтерді табуға есептер.	2	10
	БӨЖ 1: Салыстырулар бойынша тапсырмалар, кері элементтерді табу	2	10
5	Дәріс 5. Эйлер функциясы және оның қасиеттері. Жай сандар үшін Эйлер функциясы.	2	5
	Семинар 5. Модуль бойынша қалдықтар өрісі және оның қасиеттері.	2	5
6	Дәріс 6. Эйлер функциясының мультипликативтігі туралы теорема.	2	5
	Семинар 6. Эйлер функциясын қолдануға есептер шығару.	2	5
7	Дәріс 7. Эйлер функциясының мәнін табу формуласы. Эйлер функциясы арқылы дәрежеге шығару.	2	5
	Семинар 7. Эйлер функциясы көмегімен дәрежеге шығару есептері.	2	5
8	Дәріс 8. Эйлер-Ферма теоремасы және RSA шифрының негізгі теоремасы	2	5
	Семинар 8 Эйлер-Ферма және RSA шифры теоремаларына есептер	2	5
	БӨЖ 2: Эйлер-Ферма және RSA шифры теоремасына тапсырмалар орындау	2	30
	Аралық бақылау 1		100
3-модуль. RSA-криптожүйе			
9	Дәріс 9. RSA-шифр, шифрлау және оқу процесі, негіздеме.	2	5
	Семинар 9. RSA-шифрды мысалдарда талдау.	2	5

10	Дәріс 10. RSA-ашық кілтпен берілген мәтінді шифрлау.	2	5
	Семинар 10. RSA-ашық кілтпен шифрлауды мысалда жүзеге асыру.	2	5
11	Дәріс 11. RSA-жабық кілтпен берілген мәтінді дешифрлау.	2	5
	Семинар 11. RSA-жабық кілтпен дешифрлауды мысалда жүзеге асыру.	2	5
12	Дәріс 12. RSA-электрондық қолтаңба, идеясы және негіздемесі.	2	5
	Семинар 12. RSA-электрондық қолтаңбаны жасау процесі.	2	5
	БӨЖ 3: RSA-электрондық қолтаңбаны негіздеу тапсырмалары.	2	5
13	Дәріс 13. RSA-электрондық қолтаңба рәсімін жүзеге асыру, қолтаңба қою бөлігі.	2	5
	Семинар 13. RSA-электрондық қолтаңба рәсімін жүзеге асыру, қолтаңба қоюды жабық кілтпен шифрлау арқылы орындау.	2	5
14	Дәріс 14. RSA-электрондық қолтаңба рәсімін жүзеге асыру, қолтаңбаны ашық кілтпен шифрлау. RSA-электрондық қол қоюды жүзеге асыру, электрондық қол қойылған шифрды ашу.	2	5
	Семинар 14. RSA-электрондық қолтаңбаны дешифрлау.	2	5
15	Дәріс 15. RSA-бағалау. Натурал қатардағы жай сандардың таралуы.	2	5
	Семинар 15. RSA-электрондық қолтаңбаны қолдану есептері.	2	5
	БӨЖ 4: RSA-электрондық қолтаңбаны дешифрлау тапсырмаларын орындау.	2	25
	Аралық бақылау 2		100
	Емтихан		100
	Барлығы		100

Механика-математика факультетінің деканы

Ж. М. Бектемесов

Оқыту және білім беру сапасы бойынша
Академиялық комитетінің төрағасы

Б. И. Ахметова

Математика
кафедрасының меңгерушісі

С. Е. Касенов

Дәріскер

К. М. Туленбаев



ЖИЫНТЫҚ БАҒАЛАУ РУБРИКАТОРЫ
ОҚУ НӘТИЖЕЛЕРІН БАҒАЛАУ КРИТЕРИЙЛЕРІ

Әрбір жоспарланған жиынтық бағалау (БӨЖ) үшін ресімделеді

ҮЛГІ (Шаблон) Тапсырма атауы (100% Аралық бақылаудан % баллдар мөлшері, оқу курсының мазмұнын іске асыру күнтізбесінен (кестесінен) көшіру, оқыту және білім беру әдістері)		«Қанағаттанарлықсыз» % макс. салмағы	
Критерий	«Өте жақсы» % макс. салмағы	«Жақсы» % макс. салмағы	«Қанағаттанарлық» % макс. салмағы