Силлабус
Көктемгі семестр 2020-2021 о.ж.
Білім беру бағдарламасы бойынша

Пәннің коды	**Пәннің атауы**	**СӨЖ**	**Аптасына сағат саны**			**Кредит-тер саны**	**СӨОЖ**
			Дәріс	**Практ.**	**Зертхан.**		
KK3224	Криптография және криптоталдау 2	4	15	15	30	6	37,6

Академиялық курс туралы ақпарат

Оқыту түрі	Курстың түрі /сипаты	Дәріс түрі	Практикалық сабақтар типтері	СӨЖ саны	Қортынды бақылау түрі
Онлайн / біріктірілген	теориялық	Проблемалы, аналитикалық	Есептерді шешу	3-тен кем емес	«Универ» жүйесіндегі тестілеу
Лектор	Бегимбаева Енлик Ериковна			**Оф./с.**	Жоспарланған Zoom жиналысына қосылыңыз https://us04web.zoom.us/j/85062701333?pwd=bENGWlhXMDZyYTdHYWJkbWV1V2h6UT09 Конференцияның идентификаторы: 850 6270 0133 Кіру коды: 2ZapZP
e-mail	Enlik_89@mail.ru				
Телефон	+77051000777				

Курстың академиялық презентациясы

Пәннің мақсаты	**Оқытудың күтілетін нәтижелері (ОН)**	**ОН іске асуын көрсететін индикаторлар (әр ОН үшін**

		кемінде 2 индикаторды келтіру керек)
Пәннің мақсаты; Криптография және криптоталдау 2 пәнін игерудің мақсаты - криптожүйелердің ықтималдық және алгебралық модельдерін, соның ішінде негізгі криптографиялық алгоритмдерді, криптографиялық күшті шифрлық компоненттерді құру әдістерін, сонымен қатар блоктық және ағындық шифрларды криптоанализдеу кезінде қолданылатын математикалық әдістерді білуді қолдана отырып., теориялық және қолданбалы криптография мен криптоталдау саласындағы мәселелердің кең ауқымын шешуге қажетті теориялық және практикалық білімді үйрету.	ОН 1. Ақпаратты қорғаудың криптографиялық әдістері шеңберінде ғылыми білім мен зерттеу әдістемесінің ерекшеліктерін жүйелі түрде ұсыну және түсіну мүмкіндігі.	ЖИ 1.1 - криптография ұғымын, өзіндік криптографиялық терминологияны түсіндіру; ЖИ 1.2 - ақпаратты қорғау әдістерін талдау.
	ОН 2. Симметриялық криптографиялық алгоритмдердің негізіндегі математикалық принциптерді білу.	ЖИ 2.1 - асимметриялық криптожүйелерге жасалған шабуылдарды білу; ЖИ 2.2 - криптографиялық алгоритмнің беріктігін талдау.
	ОН 3. Ақпараттық қауіпсіздік алгоритмдерін криптографиялық әдістерді қолдана отырып қолдану, ақпараттық қауіпсіздік бағдарламаларымен жұмыс істеуді білу.	ЖИ 3.1 -деректердің алгоритмдік түрленуін түсіндіру; ЖИ 3.2 - кез-келген файл пішімін қорғау үшін асимметриялық және симметриялық криптография әдістерін қолдану; ЖИ 3.3 – АҚ бағдарламаларын пайдалана отырып, ақпаратты қорғауды қамтамасыз ету.
	ОН 4. Ақпараттық қауіпсіздік құралдары мен жүйелерін тестілеу бағдарламалары мен әдістерін жасау мүмкіндігі.	ЖИ 4.1 - криптожүйелердің беріктігін талдау; ЖИ 4.2 - криптожүйенің беріктігін арттыру бойынша ұсыныстар әзірлеу.
	ОН 5. Ақпаратты қорғаудың қолданбалы міндеттерін бағдарламалау тілдерінде және крипто-қорғауға арналған қолданбалы бағдарламалар пакеттерін жүзеге асыру.	ЖИ 5.1 - ақпаратты қорғаудың криптографиялық әдістерін түсіндіру; ЖИ 5.2 - қауіпсіздік жүйесін зерттеу мен жобалау кезінде крипто-қорғаныстың әдістерін қолдану жүзеге асыру.
Адыңғы реквизиттер мен постреквизиттер	**Пререквизиттер:** Ақпараттық қәуіпсіздік жүйесі, ақпаратты қорғау **Постреквизиттер:** Web қәуіпсіздік, Желілік қәуіпсіздікті талдау	
Әдебиетт және ресурстар	**Әдебиет**: **Негізгі:** 1. Акушский И.Я., Юдицкий Д.И. Машинная арифметика в остаточных классах, Издательство «Советское радио» Москва, 1968. 438 б. 2. Рожков А.В., Ниссенбаум О.В. Теоретико-числовые методы в криптографии , Тюмень 2007.-175б.	

	3. Фомичев В.М. Симметричные криптосхемы. Краткий обзор основ криптологии для шифрсистем с открытым ключом. — М.: МИФИ, 1995. 4. Нечаев В.И. Элементы криптографии. Основы теории защиты информации. — М.: Высшая школа, 1999. 5. Синьков М.В., Губарени Н.М. Непозиционные представления многомерных числовых систем. Киев, Наукова думка, 1977, 149 б. 6. Зубов А.Ю. Криптографические методы защиты информации. Совершенные шифры. М.: Гелиос АРВ, 2005. 7. Диффи У., Хеллмэн М.Э. Защищенность и имитостойкость: введение в криптографию. // ТИИЭР N 3, т. 67, 1979 г., б.71-109. 8. Хоффман Л.Д. Современные методы защиты информации / Под ред. В.А. Герасименко. – М.: Сов. радио, 1980. – 264 б. 9. Брюс Шнайер. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. - М.: Издательство ТРИУМФ, 2002 - 816 с.: ил. 10. Алферов А.П., Зубов А.Ю., Кузьмин А.С. и др. Основы криптографии. – М.: Гелиос АРВ, 2001. – 122 б. 11. Фомичев В.М. Дискретная математика и криптология. – М.: ДИАЛОГ-МИФИ, 2003. - 400 б. 12. А.Ж. Асамбаев., Криптография негіздері, Оқу құралы. – Павлодар, 2012. – 173 бет. Қосымша 1. Тұрым А.Ш., Мұстафина Б.М., Ақпарат қорғау және қауіпсіздендіру негіздері. – Алматы: Алматы энергетика және байланыс институты, 2002ж. 2. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. –М.: РАДИО И СВЯЗЬ, 1999. 3. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии: Учебное пособие. – М.: Гелиос АРВ, 2002. – 480 с. **Қолданылатын көрнекі құралдырымен аспаптар тізімі:** • Бағдарламалау тілдері **<u>Ресурстар:</u>** **-бағдарламалық қамтамасыздануы және Интернет-ресурстары** 4. 1. intuit.ru 5. **мәліметтер базысы, ақпараттық-анықтамалық және іздестіру жүйелері:** интернет желісі **Онлайн қол жетімділігі:** Қосымша оқу материалы, және үй тапсырмалары мен жобалар univer.kaznu.kz. сайтындағы өздеріңнің парақшаларындағы ПОЭК бөлімінде көруге болады.
Университеттің моральдық-этикалық құндылықтары аясындағы курстың академиялық саясаты	**Оқу тәртібі:** 1. Пәннің кестесіне сәйкес онлайн-курстық модульдердің уақыты қатаң сақталуы керек 2. Академиялық құндылықтар: - практикалық / зертханалық зерттеулер, СӨЖ тәуелсіз, шығармашылық болуы керек; - плагиат, жалған құжат, парақтарды пайдалану, бақылаудың

	барлық кезеңдерінде жасырын көшіріп жазуға жол берілмейді; - Мүмкіндігі шектеулі студенттер электрондық пошта Enlik_89@mail.ru арқылы консультациялық көмек ала алады.
Бағалау және аттестаттау саясаты	**Критерийлік бағалау:** оқу нәтижелерін дескрипторларға қатысты бағалау (аралық бақылау мен емтихандарда құзыреттіліктің қалыптасуын тексеру). **Жиынтық бағалау:** сыныптағы жұмыс белсенділігін бағалау; орындалған тапсырманы бағалау.

Бағалау шкаласы

Бағалау әріптер жүйесі арқылы	Сандық эквивалент	Ұпайлар (мазмұны %-бен)	Бағалау дәстүрлі жүйе бойынша
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	

Оқу курсының мазмұнын іске асырудың күнтізбесі (кестесі)

Апта	Тақырыптың аталуы	ОН	ЖИ	Сағат саны	Ең жоғарғы балл	Білімді бағалау формасы	Сабақты өткізу формасы/платформа
1	2	3	4	5	6	7	
I	**Модуль - 1** Криптографияның негіздері кіріспе						
1	**Д 1.** Курстың мақсаты мен міндеттері. Криптография және криптоанализ: тарих, философия, тәсілдер.	ОН 1	ЖИ 1.1 ЖИ 1.2	1			Асинхронды/МООК 1.https://nsk.compsciclub.ru/courses/cryptoanalysis/2020-spring/classes/5461/ 2.https://learning.edx.org/course/course-v1:MEPhIx+MEPHI017x+1T2020/block-v1:MEPhIx+MEPHI017x+1T2020+type@sequential+block@397ed914e8b948f8a962eb1f11e85a59/block-v1:MEPhIx+MEPHI017x+1T2020+type@vertical+block@3431d9cfa2fa46c489217ffa5b04e630
1	**СС 1:** Шифрлардың жіктелуі. Криптожүйелердің классификациясы.	ОН 1	ЖИ 1.1 ЖИ 1.2	1	3	Сұхбат-сауалнама	Синхронды Мұғаліммен өткізілетін вебинар: кесте бойынша, Zoom
1	**ЗС 1.** Классикалық шифрларды криптоанализге арналған тапсырмалар. Бағандарды ауыстыру шифры. Қос алмастыру шифры.	ОН 1	ЖИ 1.1 ЖИ 1.2	2	10	Жеке практикалық тапсырмаларды қабылдау	Аралас: Синхронды - тапсырманы орындау әдісі бойынша Zoom бейне(1 сағат) Асинхронды-тапсырманы «Универ» жүйесінде қабылдау(2 сағат) (Сабақ кестесіне Zoom бейнелерге сілтемелер бар)

II	**Модуль - 2** Симметриялық криптожүйелер						
2	**Д 2.** Криптография мен криптоталдаудағы заманауи әдістер.	ОН 1	ЖИ 1.1 ЖИ 1.2	1			Асинхронды/МООК https://nsk.compsciclub.ru/courses/cryptoanalysis/2020-spring/classes/5462/
2	**СС 2:** Ағынды шифрлар. Синхронды ағынды шифрлар. Өздігінен синхронды ағынды шифрлар.	ОН 1	ЖИ 1.1 ЖИ 1.2	1	3	Сұхбат-сауалнама	Аралас: Асинхронды/МООК https://learning.edx.org/course/course-v1:MEPhIx+MEPHI017x+1T2020/block-v1:MEPhIx+MEPHI017x+1T2020+type@sequential+block@1b9d2c4d71aa49cb9165165b95187a54/block-v1:MEPhIx+MEPHI017x+1T2020+type@vertical+block@0f2c4272d75843b398aa6c968d9e385c Синхронды - Мұғаліммен өткізілетін вебинар: кесте бойынша, Zoom
2	**ЗС 2.** Мәтіндік ақпаратты қорғау үшін ауыстыру мен алмастырудың классикалық криптоалгоритмдерін қолдану. Кілттерді таңдау негізінде мәтіндік ақпараттарды қорғаудың әр түрлі әдістерін және олардың беріктігін зерттеу.	ОН 1	ЖИ 1.1 ЖИ 1.2	2	10	Жеке практикалық тапсырмаларды қабылдау	Аралас: Синхронды - тапсырманы орындау әдісі бойынша Zoom бейне(1 сағат) Асинхронды-тапсырманы «Универ» жүйесінде қабылдау(2 сағат) (Сабақ кестесіне Zoom бейнелерге сілтемелер бар)
3	**Д 3.** Блоктық шифрлар және оларды құру принциптері. Блокты шифрларды құру принциптері. Шифрлау режимдері.	ОН 1	ЖИ 1.1 ЖИ 1.2	1			Асинхронды/МООК https://learning.edx.org/course/course-v1:MEPhIx+MEPHI017x+1T2020/block-v1:MEPhIx+MEPHI017x+1T2020+type

							@sequential+block@9c230ab7ce184907a7f8c4272fa2cf37/block-v1:MEPhIx+MEPHI017x+1T2020+type@vertical+block@a65464f1b8d84ff583b1cdf36cc1e5b7
3	**СС 3.** Симметриялық криптожүйелердің криптоанализі. Фейстель схемасы.	ОН 1	ЖИ 1.1 ЖИ 1.2	1	3	Сұхбат-сауалнама	Аралас: Асинхронды/МООК https://nsk.compsciclub.ru/courses/cryptoanalysis/2020-spring/classes/5462/ Синхронды - Мұғаліммен өткізілетін вебинар: кесте бойынша, Zoom
3	**ЗС 3.** Фейстель желілері. Зерттеу және талдау.	ОН 1	ИД 1.1 ИД 1.2	2	10	Жеке практикалық тапсырмаларды қабылдау	Аралас: Синхронды - тапсырманы орындау әдісі бойынша Zoom бейне(1 сағат) Асинхронды-тапсырманы «Универ» жүйесінде қабылдау(2 сағат) (Сабақ кестесіне Zoom бейнелерге сілтемелер бар)
3	**СОӨЖ 1.** Іске асыру бойынша кеңес беру. Дәріс 1 – 3 тақырыптары бойынша сауалнама. СӨЖ 1. Асимметриялық шифрлаудың математикалық негіздері.	ОН 1	ЖИ 1.1 ЖИ 1.2	1	15	Сұхбат-сауалнама	Мұғаліммен өткізілетін вебинар: кесте бойынша, Zoom
4	**Д 4.** DES деректерді шифрлаудың американдық стандарты. Шифрлау стандарты ГОСТ 28147-89. Жаңа AES стандарты «Rijndael». Алгоритмдердің негізгі жұмыс режимдері.	ОН 2	ЖИ 2.1	1			Асинхронды/МООК https://nsk.compsciclub.ru/courses/cryptoanalysis/2020-spring/classes/5462/
4	**СС 4.** AES алгоритмінің криптоталдауы.	ОН 2	ЖИ 2.2	1	3	Сұхбат-сауалнама	Аралас: Асинхронды/МООК

							https://nsk.compsciclub.ru/courses/cryptoanalysis/2020-spring/classes/5462/ Синхронды - Мұғаліммен өткізілетін вебинар: кесте бойынша, Zoom
4	**ЗС 4.** AES симметриялы шифрлау стандарты. Бағдарламалық жасақтаманы енгізу.	ОН 2	ЖИ 2.1 ЖИ 2.2	2	10	Жеке практикалық тапсырмаларды қабылдау	Аралас: Синхронды - тапсырманы орындау әдісі бойынша Zoom бейне(1 сағат) Асинхронды- тапсырманы «Универ» жүйесінде қабылдау(2 сағат) (Сабақ кестесіне Zoom бейнелерге сілтемелер бар)
4	**СОӨЖ 2:** Дәріс 3 – 4 тақырыптары бойынша сауалнама. СӨЖ 2 іске асыру бойынша кеңес беру. Блокты шифрлау алгоритмдері. RC 5. IDEA. SAFER. Blowfish. **СӨЖ 1.** Оқушылардың жұмысын қорғау және талдау	ОН 2	ЖИ 2.1 ЖИ 2.2		20	Орындалған тапсырмалар туралы есеп	«Универ» жүйесінде жұмысты тексеру.
III	**Модуль - 3** Асимметриялық криптожүйелер						
5	**Д 5.** Ашық кілт жүйелері. Есептеу күрделі математикалық есептер. RSA, El Gamal криптожүйелері. Қосымша функционалдығы бар криптожүйелер.	ОН 3	ЖИ 3.1 ЖИ 3.2 ЖИ 3.3	1			Асинхронды/МООК https://learning.edx.org/course/course-v1:MEPhIx+MEPHI017x+1T2020/block-v1:MEPhIx+MEPHI017x+1T2020+type@sequential+block@3c5b3dafbff04157be8fbc83c1992169/block-v1:MEPhIx+MEPHI017x+1T2020+type@vertical+block@a2c75d8212c54092b6225a2b9ff6cbd2

5	**СС 5.:** Қауіпсіз электрондық құжат айналымы принциптері және электрондық цифрлық қолтаңбаны (ЭЦҚ) орнату алгоритмдері.	ОН 3	ЖИ 3.1 ЖИ 3.2 ЖИ 3.3	1	3	Сұхбат-сауалнама	Синхронды Мұғаліммен өткізілетін вебинар: кесте бойынша, Zoom
5	**ЗС 5.** Асимметриялық шифрлау жүйелерінде қолданылатын жай сандарды генерациялау. Электрондық цифрлық қолтаңба.	ОН 3	ЖИ 3.1 ЖИ 3.2 ЖИ 3.3	2	10	Жеке практикалық тапсырмаларды қабылдау	Аралас: Синхронды - тапсырманы орындау әдісі бойынша Zoom бейне(1 сағат) Асинхронды-тапсырманы «Универ» жүйесінде қабылдау(2 сағат) (Сабақ кестесіне Zoom бейнелерге сілтемелер бар)
	1 АБ				**100**		
IV	**Модуль - 4** Тұтастықты қамтамасыз ету әдістері						
6	**Д 6.** Тұтастықты қамтамасыз ету әдістері. Аутентификация кодтары.	ОН 3	ЖИ 3.2	1			Асинхронды/МООК https://learning.edx.org/course/course-v1:MEPhIx+MEPHI017x+1T2020/block-v1:MEPhIx+MEPHI017x+1T2020+type@sequential+block@3e76b46970de4607b13fde0cf6437b90/block-v1:MEPhIx+MEPHI017x+1T2020+type@vertical+block@3255ad98a6864b2d93be234b75c1baab
6	**СС 6.** Криптографияның қолданбалы аспектілері. Негізгі басқару. Криптографияны күнделікті қолдану.	ОН 3	ЖИ 3.2	1	3	Сұхбат-сауалнама	Аралас: Асинхронды/МООК https://learning.edx.org/course/course-v1:MEPhIx+MEPHI017x+1T2020/block-v1:MEPhIx+MEPHI017x+1T2020+type@sequential+block@0b7a49e315404867baf1b35db6ff491a/

							block-v1:MEPhIx+MEPHI017x+1T2020+type@vertical+block@eb24fdb110134e378781f3c6ea50227c Синхронды - Мұғаліммен өткізілетін вебинар: кесте бойынша, Zoom
6	**ЗС 6.** Ақпараттық қауіпсіздік бағдарламалық жасақтамасын зерттеу. PGP бағдарламасы.	ОН 4	ЖИ 4.1 ЖИ 4.2	2	10	Жеке практикалық тапсырмаларды қабылдау	Аралас: Синхронды - тапсырманы орындау әдісі бойынша Zoom бейне(1 сағат) Асинхронды- тапсырманы «Универ» жүйесінде қабылдау(2 сағат) (Сабақ кестесіне Zoom бейнелерге сілтемелер бар)
V	**Модуль - 5** Криптоталдау						
7	**Л 7.** Криптоталдаудың мақсаттары мен принциптері. Крипто-шабуылдардың жіктелуі.	ОН 4	ЖИ 4.1 ЖИ 4.2	1			Синхронды - Мұғаліммен өткізілетін вебинар: кесте бойынша, Zoom
7	**СС 7.** Қарапайым мәтінге және тиісті шифрлық мәтіндерге негізделген шабуыл.	ОН 4	ЖИ 4.1	1	3	Сұхбат-сауалнама	Синхронды - Мұғаліммен өткізілетін вебинар: кесте бойынша, Zoom
7	**ЗС 7.** Қарапайым мәтінге және тиісті шифрлық мәтіндерге негізделген шабуылға тапсырма беру.	ОН 4	ЖИ 4.1	2	10	Жеке практикалық тапсырмаларды қабылдау	Аралас: Синхронды - тапсырманы орындау әдісі бойынша Zoom бейне(1 сағат) Асинхронды- тапсырманы «Универ» жүйесінде қабылдау(2 сағат) (Сабақ кестесіне Zoom бейнелерге сілтемелер бар)

7	**СООӨЖ 3.** Консультация по выполнению СӨЖ 3. XSL атаки. **СӨЖ 2.** Оқушылардың жұмысын қорғау және талдау**.**	ОН 4	ЖИ 4.1	2	10	Орындалған тапсырмалар туралы есеп	«Универ» жүйесінде жұмысты тексеру.
8	**Д 8.** Блоктық шифрлау алгоритмдерінің сызықтық криптоанализі. Сызықтық криптоанализ туралы жалпы ақпарат.	ОН 2-ОН 4	ЖИ 2.2 ЖИ 4.1	1			Синхронды - Мұғаліммен өткізілетін вебинар: кесте бойынша, Zoom
8	**СС 8.** Сызықтық криптоанализді шифрлау алгоритмдеріне қолдану.	ОН 2-ОН 4	ЖИ 2.2 ЖИ 4.1	1	3	Сұхбат-сауалнама	Синхронды - Мұғаліммен өткізілетін вебинар: кесте бойынша, Zoom
8	**ЗС 8.** Шифрлау алгоритмдеріне сызықтық криптоанализ бойынша сұрақтар.	ОН 2-ОН 4	ЖИ 2.2 ЖИ 4.1	2	10	Сұхбат-сауалнама	Аралас: Синхронды - тапсырманы орындау әдісі бойынша Zoom бейне(1 сағат) Асинхронды-тапсырманы «Универ» жүйесінде қабылдау(2 сағат) (Сабақ кестесіне Zoom бейнелерге сілтемелер бар)
9	**Д 9.** Блоктық шифрлау алгоритмдерінің дифференциалды криптоанализі. Дифференциалды криптоанализ туралы жалпы мәліметтер.	ОН 2-ОН 4	ЖИ 2.2 ЖИ 4.1	1			Асинхронды/МООК https://nsk.compsciclub.ru/courses/cryptoanalysis/2020-spring/classes/5463/
9	**СС 9.** Дифференциалды криптоанализді шифрлау алгоритмдеріне қолдану.	ОН 2-ОН 4	ЖИ 2.2 ЖИ 4.1	1	3	Сұхбат-сауалнама	Аралас: Асинхронды/МООК https://nsk.compsciclub.ru/courses/cryptoanalysis/2020-spring/classes/5463/ Синхронды - Мұғаліммен өткізілетін вебинар: кесте бойынша, Zoom
9	**ЗС 9.** Шифрлау алгоритмдеріне дифференциалды	ОН 2-	ЖИ 2.2 ЖИ 4.1	2	10	Жеке практикалық	Аралас: Синхронды - тапсырманы

	криптоанализ бойынша сұрақтар.	ОН 4				тапсырмаларды қабылдау	орындау әдісі бойынша Zoom бейне(1 сағат) Асинхронды-тапсырманы «Универ» жүйесінде қабылдау(2 сағат) (Сабақ кестесіне Zoom бейнелерге сілтемелер бар)
9	**СОӨЖ 4:** СӨЖ 4 іске асыру бойынша кеңес беру. RC 5 шифрлау алгоритмінің дифференциалды криптоанализі. Дәріс 8 – 9 тақырыптары бойынша сауалнама. **СӨЖ 3.** Оқушылардың жұмысын қорғау және талдау.	ОН 2-ОН 4	ЖИ 2.2 ЖИ 4.1		25	Орындалған тапсырмалар туралы есеп	«Универ» жүйесі бойынша жұмысты тексеру
10	**Д 10.** Алгебралық криптоанализ. Негізгі ой. Алгебралық криптоанализ әдісі.	ОН 2-ОН 4	ЖИ 2.2 ЖИ 4.1 ЖИ 4.2	1			Асинхронды/МООК https://nsk.compsciclub.ru/courses/cryptoanalysis/2020-spring/classes/5464/
10	**СС 10.** Ағын шифрының криптоанализі. Мысалдарды қарастыру.	ОН 2-ОН 4	ЖИ 2.2 ЖИ 4.1 ЖИ 4.2	1	3	Сұхбат-сауалнама	Синхронды Мұғаліммен өткізілетін вебинар: кесте бойынша, Zoom
10	**ЗС 10.** «Дөрекі шабуыл», «ортаңғы әдіс» бойынша кездесу. Әлсіз кілттерді талдау.	ОН 2-ОН 4	ЖИ 2.2 ЖИ 4.1 ЖИ 4.2	2	10	Фронтальный и индивидуальный опрос	Аралас: Синхронды - тапсырманы орындау әдісі бойынша Zoom бейне(1 сағат) Асинхронды-тапсырманы «Универ» жүйесінде қабылдау(2 сағат) (Сабақ кестесіне Zoom бейнелерге сілтемелер бар)
	МТ (Midterm Exam)				**100**		
11	**Л 11.** Буль функцияларының криптографиялық қасиеттері.	ОН 4	ЖИ 4.1 ЖИ 4.2	1			Асинхронды/МООК https://nsk.compsciclub.ru/courses/crypto

							analysis/2020-spring/classes/5465/
11	**СС 11.** CAST раундық шифр функциясы.	ОН 4	ЖИ 4.1 ЖИ 4.2	1	3	Сұхбат-сауалнама	Аралас: Асинхронды/МООК https://nsk.compsciclub.ru/courses/cryptoanalysis/2020-spring/classes/5465/ Синхронды - Мұғаліммен өткізілетін вебинар: кесте бойынша, Zoom
11	**ЗС 11.** Бір раундтық AES алгебралық криптоанализі.	ОН 4	ЖИ 4.1 ЖИ 4.2	2	10	Презентация Сұхбат-сауалнама	Аралас: Синхронды - тапсырманы орындау әдісі бойынша Zoom бейне(1 сағат). Асинхронды-тапсырманы «Универ» жүйесінде қабылдау(2 сағат). (Сабақ кестесіне Zoom бейнелерге сілтемелер бар)
12	**Д 12.** Слайд криптоанализі. Негізгі ой. Әдістер. KeeLog шифрының криптоанализі	ОН 4	ЖИ 4.1 ЖИ 4.2	1			Асинхронды/МООК https://nsk.compsciclub.ru/courses/cryptoanalysis/2020-spring/classes/5464/
12	**СС 12.** Интерполяция криптоанализі.	ОН 4	ЖИ 4.1 ЖИ 4.2	1	3	Сұхбат-сауалнама	Синхронды Мұғаліммен өткізілетін вебинар: кесте бойынша, Zoom
12	**ЗС 12.** Корреляциялық криптоанализ. Негізгі және басқа корреляциялық шабуылдар.	ОН 4	ЖИ 4.1 ЖИ 4.2	2	10	Жеке практикалық тапсырмаларды қабылдау	Аралас: Синхронды - тапсырманы орындау әдісі бойынша Zoom бейне(1 сағат) Асинхронды-тапсырманы «Универ» жүйесінде қабылдау(2 сағат)

							(Сабақ кестесіне Zoom бейнелерге сілтемелер бар)
12	**СОӨЖ 5.** Тақырып 11-12 бойынша сауалнама. **СӨЖ 4.** Оқушылардың жұмысын қорғау және талдау.	ОН 4	ЖИ 4.1 ЖИ 4.2		15	Орындалған тапсырмалар туралы есеп	«Универ» жүйесі бойынша жұмысты тексеру.
13	**Д 13** «Адал емес» криптоанализ: бүйірлік каналдардағы шабуылдар.	ОН 4	ЖИ 4.1 ЖИ 4.2	1			Асинхронды/МООК https://nsk.compsciclub.ru/courses/cryptoanalysis/2020-spring/classes/5466/
13	**СС 13.** Криптожүйелердің имитациялық тұрақтылығы және шуға қарсы иммунитеті.	ОН 4	ЖИ 4.1 ЖИ 4.2	1	3	Сұхбат-сауалнама	Синхронды Мұғаліммен өткізілетін вебинар: кесте бойынша, Zoom
13	**ЗС 13.** IDEA шифрлау алгоритмі. Математикалық сипаттама. Шифрлау режимдері.	ОН 4	ЖИ 4.1 ЖИ 4.2	2	10	Жеке практикалық тапсырмаларды қабылдау	Аралас: Синхронды - тапсырманы орындау әдісі бойынша Zoom бейне(1 сағат) Асинхронды-тапсырманы «Универ» жүйесінде қабылдау(2 сағат) (Сабақ кестесіне Zoom бейнелерге сілтемелер бар)
14	**Д 14.** Асимметриялық жүйелерді криптоанализдеу: факторизация алгоритмдері.	ОН 5	ЖИ 5.1	1			Асинхронды/МООК https://nsk.compsciclub.ru/courses/cryptoanalysis/2020-spring/classes/5467/
14	**СС 14.** Ықтималдық шифрлау.	ОН 5	ЖИ 5.1	1	3	Презентация Сұхбат-сауалнама	Асинхронды/МООК https://nsk.compsciclub.ru/courses/cryptoanalysis/2020-spring/classes/5467/ Синхронды - Мұғаліммен өткізілетін вебинар: кесте бойынша, Zoom

14	**ЗС 14.** Фиат-Шамир хаттамасы.	ОН 5	ЖИ 5.1	2	10	Жеке практикалық тапсырмаларды қабылдау	Аралас: Синхронды - тапсырманы орындау әдісі бойынша Zoom бейне(1 сағат) Асинхронды-тапсырманы «Универ» жүйесінде қабылдау(2 сағат) (Сабақ кестесіне Zoom бейнелерге сілтемелер бар)
14	**СОӨЖ 6.** Тақырып 12-13 бойынша сауалнама.	ОН 5	ЖИ 5.1	2	10	Сұхбат-сауалнама	Мұғаліммен өткізілетін вебинар: кесте бойынша, Zoom
15	**Д 15.** Асимметриялық жүйелерді криптоанализдеу: дискретті логарифм.	ОН 5	ЖИ 5.1 ЖИ 5.2	1			Асинхронды/МООК https://nsk.compsciclub.ru/courses/cryptoanalysis/2020-spring/classes/5468/
15	**СС 15.** RSA алгоритмінің криптоанализі.	ОН 5	ЖИ 5.1 ЖИ 5.2	1	3	Презентация Сұхбат-сауалнама	Аралас: Асинхронды/МООК https://nsk.compsciclub.ru/courses/cryptoanalysis/2020-spring/classes/5468/ Синхронды - Мұғаліммен өткізілетін вебинар: кесте бойынша, Zoom
15	**ЗС 15.** Винердің RSA-ға шабуылы. Мысал және тапсырмалар	ОН 5	ЖИ 5.1 ЖИ 5.2	2	10	Жеке практикалық тапсырмаларды қабылдау	Аралас: Синхронды - тапсырманы орындау әдісі бойынша Zoom бейне(1 сағат) Асинхронды-тапсырманы «Универ» жүйесінде қабылдау(2 сағат) (Сабақ кестесіне Zoom бейнелерге сілтемелер бар)

15	**СОӨЖ 7.** 14 - 15 тақырыптар бойынша сауалнама. Пән бойынша қорытынды емтиханға кеңес беру.	ОН 5	ЖИ 5.1 ЖИ 5.2		10	Сұхбат-сауалнама	Мұғаліммен өткізілетін вебинар: кесте бойынша, Zoom
	2 АБ				**100**		
	Пән бойынша қорытынды емтихан				100	Тест тапсырмалары	«Универ» жүйесі

Декан ф-та, к.ф.м.н., доцент Урмашев Б.А.

Әдістемелік бюроның төрайымы Баймулдина Н.С.

Кафедра меңгерушісі Мусиралиева Ш.Ж.

Дәріс беруші, аға оқытушы Бегимбаева Е.Е.