«Л.Н. Гумилев атындағы Еуразия ұлттық университеті» КеАҚ

«Ақпараттық технологиялар» факультеті

«Ақпараттық қауіпсіздік» кафедрасы

6B06306 – «Ақпараттық қауіпсіздік жүйелері»
білім беру бағдарламасы бойынша білім алушылар үшін
КК3302 «Криптология» пәні бойынша
COMS 33010 Криптографиялық жүйелер және стеганография

Оқу (модульдік) жұмыс бағдарламасы (Syllabus)

Астана
2024

Бұл құжат 2003 жылғы 7 қаңтардағы «Электрондық құжат және электрондық цифрлық
қолтаңба туралы» ҚРЗ 7-бабының 1-тармағына сәйкес қағаз жеткізгіштегі құжатпен бірдей

Құжатқа қол қойғандар

№	Аты-жөні	Қызметі
1	Конырханова Асем Адилбеккызы	Доцент (міндетін атқарушы)
2	Конырханова Асем Адилбеккызы	Доцент (міндетін атқарушы)
3	Сагнаева Сауле Кайроллиевна	доцент
4	Сеилов Шахмаран Журсинбекович	Факультет деканы

Әзірлеуші:
Конырханова Асем Адилбеккызы, Доцент (міндетін атқарушы)

КК 3302 «Криптология» пәні бойынша оқу жұмыс бағдарламасы (Syllabus) «6В06306-Ақпараттық қауіпсіздік жүйелері» білім беру бағдарламасы негізінде құрастырылған.

«Ақпараттық қауіпсіздік» кафедрасының отырысында қарастырылды, хаттама №1 «27» тамыз 2024 ж.

Факультеттің оқу-әдістемелік комиссиясының отырысында мақұлданды, хаттама №1 «28» тамыз 2024 ж.

ТҮСІНІКТЕМЕ ХАТ

1. Пәннің қысқаша сипаттамасы:

Пәннің мақсаты	**Білім беру бағдарламасы бойынша оқыту нәтижелері (ОН)***	**Пән бойынша күтілетін оқыту нәтижелері (ОН)** Пәнді оқыту нәтижесінде білім алушы қабілетті болады:
Криптоталдау негіздерін үйрену. Әртүрлі криптография алгоритмдерімен, шабуыл бұзу әдістерімен танысу, криптографиялық примитивтердің қауіпсіздігін бағалау. Криптоалгоритмдердің математикалық негіздерімен танысу. Криптографиялық жүйелердің негізгі құрылымы мен маңызды қасиеттерін түсіну; криптографиялық кітапханалар мен үлкен сандармен жұмыс істеуге (C++ тілінде) арналған кітапханаларды зерттеу. Қиын есептелетін криптографиялық мәселелерді зерттеу. Қауіпсіз әзірлеу принциптерімен танысу, бағдарламалық құралдармен криптоталдай білу, оларды тиімді қолдану. Криптоталдау үшін бағдарламалық қамтама құра білу. Белгілі заманауи алгоритмдерді криптоталдау нәтижелерімен танысу, шабуылдарды түсіну және білу (олардың практикалық орындалатындығын бағалай білу)	$ОН_{12}$ – Криптография, криптоталдау саласында формальды аппараты және кодтау теориясының матматикалық негіздерін меңгеру, криптографиялық стандартты алгоритмдер мен протоколдардын және оларды деректерді қорғау мәселесінде қолдану	- қауіпсіздікті қамтамасыз ететін заманауи криптографиялық технологияларды білу, криптоберіктікті бағалай білу. - қауіпсіздік міндеттерін түсіну, криптографиялық жүйелерге жасалатын шабуылдар мен қойылатын талаптарды білу. - шабуылдардың практикалық орындалуын бағалай білу. - криптографиялық кітапханалар, үлкен сандармен жұмыс істеуге арналған кітапханалар, ғылыми есептеулер пакеттері, криптоталдау құрал-саймандарын білу және қолдана білу.

**Білім беру бағдарламасына сәйкес*

2. **Пререквизиттер**

Аталған пәнді меңгеру үшін «Ақпарат және кодтау теориясы», «Криптографияның математикалық негіздері» меңгеру барысында игерілген білімдер, біліктер және дағдылар қажет.

Постреквизиттер

Криптографиялық хаттамалар, мамандық бойынша мемлекеттік емтихан тапсыру, дипломдық жұмысты/жобаны жазу және қорғау кезінде қажет болып табылады

3.Оқу жоспарынан үзінді
Курс 3
Семестр 5
Кредиттер саны 8

Қызмет	**Жалпы сағаттар саны**
Дәрістер	30
Практикалық оқыту	15
Семинар сабағы	
Зертханалық сабақ	30
Студия сабағы	
SRO	165
Барлығы	240

4. Модульдер бойынша пәннің тақырыптық жоспары
(академиялық сағатта)

Модуль №	Модульдің атауы
1	Шифрлеудің криптографиялық алгоритмдері. Криптоберіктік және күрделілік
2	Криптоталдауға арналған программалық-аппараттық криптографиялық құралдар мен аспаптар. Криптографиялық қосымшалар мен криптоталдау құралдарын жасаудың мәселелері
3	Симметриялық шифрлердің криптографиялық талдауының әдістері
4	Асимметриялық шифрлеу алгоритмдерін криптоталдаудың әдістері. Шифрлеудің заманауи алгоритмдерінің криптоталдаулары жайлы мақалаларға зерттеу жасау.

Дәріс сабақтары				
Апталар №	**Модуль №**	**Дәріс тақырыбының атауы**	**Сағат саны**	**Оқытудың түрлері мен әдістері**
1	1	Пәнге кіріспе. Терминоглогия. Криптографиялық шифрлер. Криптоталдау	2	дәріс, пікірталас, жеке тапсырмалар, әдістемелік ұсыныстар
2	1	Симметриялық шифрлеу. Криптоберіктік сұрақтары	2	дәріс, пікірталас, жеке тапсырмалар, әдістемелік ұсыныстар
3	1	Асимметриялық шифрлеу. Криптоберіктік мәселелері. Криптографияның математикалық негіздері	2	дәріс, пікірталас, жеке тапсырмалар, әдістемелік ұсыныстар
4	1	Асимметриялық шифрлеудің алгоритмдері. Криптографиялық хэш-функциялар. Цифрлық қолтаңбалар. Криптоберіктік мәселелері	2	талқылау, тапсырмалардың мысалдарын көрсету
5	2	Криптоталдауға арналған программалық-аппараттық криптографиялық құралдар мен аспаптар. Криптографиялық алгоритмдер мен криптографиялық хаттамалардың әлсіздігі	2	дәріс, пікірталас, сауалнама, жеке тапсырмалар, әдістемелік нұсқаулар
6	2	Криптоталдау есептерін шешуге арналған аспаптарды құру мен қосымшаларды жасау мәселелері	2	дәріс, пікірталас, жеке тапсырмалар, әдістемелік ұсыныстар
7	3	Классикалық шифрлерді криптоталдау	2	әдістемелік нұсқаулар
8	3	Симметриялық шифрларды криптоталдаудың әдістері I	2	дәріс, пікірталас, жеке тапсырмалар, әдістемелік ұсыныстар
9	3	Симметриялық шифрларды криптоталдаудың әдістері II	2	дәріс, пікірталас, жеке тапсырмалар, әдістемелік ұсыныстар
10	3	Заманауи симметриялық шифрларды криптоталдау I	2	дәріс, пікірталас, жеке тапсырмалар, әдістемелік ұсыныстар
11	3	Заманауи симметриялық шифрларды криптоталдау II	2	дәріс, пікірталас, жеке тапсырмалар
12	4	Асимметриялық шифрлеу алгоритмдерін криптоталдаудың әдістері. Хэш-функцияларға шабуылдар және цифрлық қолтаңбалар	2	әріс, сауалнама, жеке тапсырмалар, әдістемелік ұсыныстар
13	4	Асимметриялық шифрлердің криптоталдау	2	дәріс, пікірталас, әдістемелік ұсыныстар
14	4	Криптографиялық хэш-функцияларға жасалған криптографиялық шабуылдар, цифрлық қолтаңбалар	2	дәріс, пікірталас, жеке тапсырмалар, әдістемелік ұсыныстар
15	4	Заманауи шифрлеу алгоритмдерін криптоталдаудың нәтижелері, оны жүзеге асыру мен жетілдіру мәселелері	2	дәріс, пікірталас, жеке тапсырмалар, әдістемелік ұсыныстар
		БАРЛЫҒЫ	30	

Тәжірибелік (семинар) сабақтар				
Апталар №	**Модуль №**	**Тәжірибелік (семинар) сабақ тақырыбының атауы**	**Сағат саны**	**Оқытудың түрлері мен әдістері**

1	1	Криптографиялық программалық құралдар. Криптографиялық қосымшаларды дайындаудың практикалық мәселелері. Деректерді шифрлеу негіздері. Классикалық шифрлерді криптоталдау	1	талқылау, тапсырмаларды орнындауға арналған мысалдарды көрсету және түсіндіру
2	1	Ағындық шифрлер. Әлсіздік. Криптоберіктік мәселелері	1	сауалнама, жеке тапсырмалар, әдістемелік нұсқаулар
3	1	Блоктық симметриялық шифрлер. Әлсіздік. Криптоберіктік мәселелері	1	талқылау, зерттеу
4	1	Криптологияның математикалық негіздері. Асимметриялық шифрлеу. Криптоберіктік мәселелері	1	жеке тапсырмалар, әдістемелік ұсыныстар
5	1	Криптографиялық хэш-функциялар. Электронды цифрлық қолтаңба. Әлсіздіктер	1	талқылау, тапсырмаларды орындауға арналған мысалдарды көрсету
6	2	Криптоталдауға арналған программалық қаматама және әзірлеу құралдары	1	талқылау, тапсырмалардың орындалуын көрсету
7	2	Симметриялық шифрлеудің алгоритмдерін криптоталдау	1	талқылау, тапсырмалардың мысалдарын көрсету
8	3	Криптоталдаудың математикалық есептері	1	сауалнама, жеке тапсырмалар
9	3	Деректерді шифрлеудің Американдық стандарты (DES)	1	талқылау, тапсырмалардың мысалдарын көрсету
10	3	Шифрлеудің жетілдірілген американдық стандарты (AES) I	1	мысалдарды көрсету және түсіндіру
11	3	Шифрлеудің жетілдірілген американдық стандарты (AES) II	1	сауалнама, әдістемелік нұсқаулар
12	3	Асимметриялық шифрлеудің алгоритмдерін криптоталдау	1	талқылау, зерттеу
13	4	Криптоталдау есептеріндгі жәй сандар	1	талқылау
14	4	Асимметриялық шифрлеу. RSA криптожүйесі. Криптоталдау I	1	сауалнама, жеке тапсырмалар
15	4	Асимметриялық шифрлеу. RSA криптожүйесі. Криптоталдау II	1	талқылау, зерттеу
		БАРЛЫҒЫ	15	

Лабораториялық сабақтар				
Апталар №	**Модуль №**	**Лабораториялық сабақ тақырыбының атауы**	**Сағат саны**	**Оқытудың түрлері мен әдістері**
1	1	Криптографиялық программалық құралдар. Криптографиялық қосымшаларды дайындаудың практикалық мәселелері	1	талқылау, тапсырмаларды орнындауға арналған мысалдарды көрсету
1	1	Деректерді шифрлеу негіздері. Классикалық шифрлерді криптоталдау	1	талқылау, тапсырмалардың мысалдарын көрсету
2	1	Ағындық шифрлер. Әлсіздік. Криптоберіктік мәселелері	2	мысалдарды көрсету және түсіндіру
3	1	Блоктық симметриялық шифрлер. Әлсіздік. Криптоберіктік мәселелері	2	сауалнама, әдістемелік нұсқаулар
4	1	Криптологияның математикалық негіздері. Асимметриялық шифрлеу. Криптоберіктік мәселелері	2	талқылау, зерттеу
5	1	Криптографиялық хэш-функциялар. Электронды цифрлық қолтаңба. Әлсіздіктер	2	талқылау
6	1	Криптоталдауға арналған программалық қаматама және әзірлеу құралдары	2	сауалнама, жеке тапсырмалар
7	2	Симметриялық шифрлеудің алгоритмдерін криптоталдау	2	талқылау, зерттеу
8	2	Криптоталдаудың математикалық есептері	2	талқылау, тапсырмалардың мысалдарын көрсету
9	2	Деректерді шифрлеудің Американдық стандарты (DES)	2	мысалдарды көрсету және түсіндіру

10	2	Шифрлеудің жетілдірілген американдық стандарты (AES) I	2	сауалнама, әдістемелік нұсқаулар
11	2	Шифрлеудің жетілдірілген американдық стандарты (AES) II	2	талқылау, зерттеу
12	3	Асимметриялық шифрлеудің алгоритмдерін криптоталдау	2	талқылау
13	3	Криптоталдау есептеріндгі жәй сандар	2	сауалнама, жеке тапсырмалар
14	2	Асимметриялық шифрлеу. RSA криптожүйесі. Криптоталдау I	2	талқылау, зерттеу
15	2	Асимметриялық шифрлеу. RSA криптожүйесі. Криптоталдау II	2	талқылау, тапсырмалардың мысалдарын көрсету
		БАРЛЫҒЫ	30	

БӨЖ				
Апталар №	**Модуль №**	**БӨЖ тақырыбының атауы. БӨЖ тапсыру мерзімі**	**Сағат саны**	**Оқытудың түрлері мен әдістері**
1	1	Ақпаратты қорғаудың криптографиялық әдістері мен құралдары. Криптографиялық қосымшаларды жасаудың тәжірибелік мәселелері **СӨЖ тапсыру уақыты:** СӨЖ кестесі бойынша	11	Презентация, баяндама, программалар және құжатталған негізгі кодтар
2	1	Криптоталдау мен криптографияның математикалық негіздері. Программалық құрал-жабдық **СӨЖ тапсыру уақыты:** СӨЖ кестесі бойынша	11	Мазмұндау. Есептерді шығару. Қолданбалы пакеттредегі шешімдермен презентация жасау. Құжаттандырылған бастапқы кодтар
3	1	Лондон университетінің криптоталдау курсында **(Computer Science Department, University College London, авторлары N. Courtois және C. Petit)** қолданылатын материалдар мен аспаптарды оқу– **http://www.cs.ucl.ac.uk/students/syllabus_index_2015_16/mscisec/ga18_cryptanalysis/** **СӨЖ тапсыру уақыты:** СӨЖ кестесі бойынша	11	Шолу мен оқу нәтижелері және аспапты қолдану бойынша баяндама.
4	1	**Криптограф М. Стивенстің аспаптары мен мақалаларымен танысу:** - Марк Стивенстің материалдарын, аспаптары мен мақалаларын оқу (hashclash – https://marc-stevens.nl/p/hashclash/, http://www.cwi.nl/research/cwi-cryptanalysis, https://marc-stevens.nl/research/) *Мазмұндау. Шолу мен оқу нәтижелері және аспапты қолдану бойынша баяндама.* **СӨЖ тапсыру уақыты:** СӨЖ кестесі бойынша	11	Мазмұндау. Шолу мен оқу нәтижелері және аспапты қолдану бойынша баяндама
5	2	**Криптоталдау бойынша қолжетімді мақалалар мен материалдарды оқу (**NESSIE жобасының сайты (New European Schemes for Signatures, Integrity, and Encryption) — https://www.cosic.esat.kuleuven.be/nessie/index.html) **СӨЖ тапсыру уақыты:** СӨЖ кестесі бойынша	11	Презентация, баяндама
6	2	**Программалық қаматама және әзірлеу құралдары:** Терминал, bash-script, утилиталар - Математикалық есептерге арналған жоғары дәрежелі математикалық тілдер мен қолданбалы пакеттер (R, SciLab, Octave, Maple, Matematica, CryptoMiniSat, SageMath), оның ішінде ашық бастапқы кодты. - CrypTool пакеті - Параллельді есептеуге арналған C++11 (C++14) стандарттарының құралдары,	11	программалық жүзеге асыру

		таратылған есептеулерге арналған MPI интерфейсі.. Криптошабуылдарда қолдану - Куртуа тобының мақалалары мен аспаптары, нұсқаулар, материалдар– http://blog.bettercrypto.com/?page_id=1368 (СӨЖ 3-ті қараңыз) - Марк Стивенстің аспаптары мен мақалалары (hashclash – https://marc-stevens.nl/p/hashclash/, http://www.cwi.nl/research/cwi-cryptanalysis, https://marc-stevens.nl/research/) (СӨЖ 4-ті қараңыз) - Аспаптарhttps://sourceforge.net/directory/os:windows/?q=cryptanalysis - ПҚ http://resources.infosecinstitute.com/cryptanalysis-tools/		
7	3	**Ағындық симметриялық шифрлеу. Криптоталдау** **Тапсырмалар:** -Ағындық симметриялық шифрлеу. Алгоритмдер классификациясы -Негізгі ақпараттар. Классикалық ағындық шифрлер -Ағындық симметриялық шифрлеудің алгоритмдері -Жүзеге асыру мәселелері - Ағынның синхрондалған және синхрондалмаған шифрлері және блоктық шифрлерді шифрлеу режимдері - RC4 алгоритмі - A5/1 алгоритмі - пернатақтадан және файлдан енгізілетін деректерді шифрлеудің ұсынылған алгоритмін бағдарламада жүзеге асыру -Симметриялық шифрлеудің алгоритмдерін криптоталдау - Негізгі ақпараттар -Сииметриялық шифрлеудің қазіргі заманғы алгоритмдерін криптоталдаудың әдістері -Белгілі криптографиялық шабуылдарға мысалдар келтіру -Сызықтық талдау әдістерін оқу. Ұсынылған криптографиялық шабуылды жүзеге асыру **СӨЖ өткізу мерзімі:** СӨЖ кестесі бойынша	11	Презентация, баяндама, программалық өнім, талқылау
8	3	**Блоктық симметриялық шифрлеу. Асимметриялық шифрлеудің алгоритмдерін криптоталдау** **Тапсырмалар:** - негізгі ақпараттар -Алгоритмдер мысалы. Сипаттама. Криптоберіктік. Күрделілік. Салыстырмалы шолу. Жүзеге асыру мәселелері. -Берілген шифрлау режимінде көрсетілген шифрлау режимінде параметрлерді таңдау мүмкіндігі бар (кілт өлшемі, раунд саны) симметриялы блоктық деректерді шифрлау жүйесін жасау а) криптографиялық кітапханаларды пайдалану, б) криптографиялық кітапханаларды пайдаланбастан. -Криптографияның симметриялық алгоритмдерін криптоталдаудың әдістерін ары қарай оқу. - Алгоритмдердің біріне криптографиялық шабуылды жасау және оқу	11	Презентация, баяндама, программалық жүзеге асыру, құжатталған бастапқы кодтар, талқылау.

		-Толық іріктеу (криптографияның симметриялық алгоритмдерінің біріне) әдісімен шифрлеудің құпия кілтін параллельді түрде іздеуді жүзеге асыру. -параллельді алгоритмдер көмегімен слайдтық жұптарды іздеу **СӨЖ өткізу мерзімі:** СӨЖ кестесі бойынша		
9	3	**Деректерді шифрлеудің стандарты (DES)** **Тапсырмалар:** - DES тарихы - DES құрылымы. Алгоритмнің негізгі сатылары. Алгоритм раунды - Раундтарға арналған кілттерді генерациялау процессі -DES талдауы. DES-те Файстель шифрын қолдану - Көпреттік DES - DES-ті программалық жүзеге асыру. - DES-дегі криптографиялық шабуылдарға шолу - DES криптоталдауына арналған аспаптар - DES-дегі белгілі криптошабуылдарды жүзеге асыру және өз нұсқаларын ұсыну. - толық іріктеу әдсімен S-DES және DES шабуылын жүзеге асыру, сонымен қатар шифрлеудің түрлі режимдерінде сызықтық, дифференациалды, алгебралық криптоанализды қолдану. Ортада кездесу әдісін жүзеге асыру. Зерттеу және жүзеге асыру барысында осы тақрыптағы мақалаға сүйену. **СӨЖ өткізу мерзімі:** СӨЖ кестесі бойынша	11	Презентация, баяндама, программалық жүзеге асыру
10	3	**Алгебралық құрылымдар** **Тапсырмалар:** - Топтар. Операциялар. Мысалдар - Сақиналар. Операциялар. Мысалдар - Өрістер. Ақырлы өрістер. Операциялар. Мысалдар - Криптоталдау есептерінде қолдану. Программалық құралдар. **СӨЖ өткізу мерзімі:** СӨЖ кестесі бойынша	11	Презентация, баяндама, программалық жүзеге асыру
11	3	**Шифрлеудің жетілдірілген американдық стандарты (AES)** **Тапсырмалар:** - Конкурс тарихы, критерийлер, раундтар - AES құрылымы, айналдырудың 4 типі - Кілттерді ұлғайту, талдау - AES -те шифрлеу және дешифрлеу (бұзу емес), кері шифрлеуді жүзеге асырудың 2 әдісі - AES талдауы - AES -ті түрлі жүзеге асыру. - Криптоталдауға арналған программалық құралдармен (Desktop-, Web-қосымшалар) жұмыс жасау - Криптоталдауға арналған аспаптар және криптоталдаудың нәтижелеріне шолу талқылау, тапсырмалардың мысалдарын көрсету және түсіндіру, сауалнама, жеке тапсырмалар, әдістемелік ұсыныстар **СӨЖ өткізу мерзімі:** СӨЖ кестесі бойынша	11	Презентация, баяндама, программалық жүзеге асыру
12	4	**Криптоталдаудағы жәй сандар** **Тапсырмалар:** - Жәй сандар және оларды криптографияда қолдану -Сандардың қарапайымдылығын тексеретін кейбір алгоритмдер және олардың тиімділігі	11	Есептерді шешу. Қолданбалы пакеттерде есеп шешімдерін көрсетіп презентация жасау. Баяндама

		- Көбейткіштерге жіктеу алгоритмдері және олардың криптографиядағы қолданыстары - Қалдықтар жайлы қытай теоремасыжәне оның қолданыстары - Квадраттық салыстыру - Модуль бойынша дәрежеге шығару және логарифмдер -Программалық аспаптар, есептеуге арналған қолданбалы пакеттер, қарастырылған бірнеше алгоритмдер мен операцияларды жүзеге асыру **СӨЖ өткізу мерзімі:** СӨЖ кестесі бойынша		
13	4	4.2. СӨЖ №13. **Асимметриялық шифрлеу. Шифрлеудің асимметириялық алгоритмдерін криптоталдау** **Тапсырмалар:** - Асимметриялық шифрлерлеу. Жалпы идея - асимметриялық және симметриялық шифрлеудің алгоритмдеріне салыстырмалы талдау жүргізу - Функциялар. Біржақты функциялар - Тарих («дорбалы» криптожүйе, сипаттама, кілттерді генерациялау, талдау) - Diffie-Hellman экспоненциалды кілт алмасу әдісі - Асимметриялық шифрлау алгоритмдері - Асимметриялық-кілттік криптографиялық жүйелер: Рабиннің (Rabin), Эль-Гамальдың (EIGamal), Эллипстік қисық әдісі негізіндегі криптожүйе (ECC – Elliptic Curve Cryptosystem) -Іске асыру мәселелері - Берілген алгоритм көмегімен параметрлерді таңдау мүмкіндігімен (негізгі өлшем, кілт генерациясы, хабарлар және т.б.) асимметриялық деректерді шифрлау жүйесін енгізу. а) криптографиялық кітапханаларды пайдалану б) стандартты C++ арқылы криптографиялық кітапханаларды пайдаланбастан, с) криптографиялық кітапханаларды пайдаланбастан, бірақ үлкен сандармен жұмыс істеу кітапханаларын пайдалану арқылы. - асимметриялық шифрлеудің алгоритмдерін криптоталдау. Негізгі ақпараттар - асимметриялық шифрлеудің заманауи алгоритмдерін криптоталдау тәсілдері - танымал криптшабуылдарға мысал келтіру -шифрлеудің асимметриялық алгоритмдерін талдау тәсілдерін оқу. Ұсынылған криптографиялық шабуылды жүзеге асыру **СӨЖ өткізу мерзімі:** СӨЖ кестесі бойынша	11	Презентация, баяндама. Бастапқы кодтармен программалық әзірлеулер

14	4	4.3. СӨЖ №14. Хэш-функциялар. **Электронды цифрлық қолтаңба. Объектінің дұрыстығын растайтын хаттамалар және әлсіздіктер. Шифрлеудің асимметриялық алгоритмдерін криптоталдау** **Тапсырмалар:** - Хэш-функциялар. Электронды цифрлық қолтаңба - Негізгі ақпараттар - Ақпаратты хэштеу - Заманауи хэш-функциялардың параметрлері - Хэштеу алгоритмдері - ЭЦҚ алгоритмдері - Мұғалім ұсынған асимметриялық шифрі мен хэш-функцияны пайдаланып ЭЦҚ жүйесін жасау. Келесі мүмкіндіктерді жүзеге асыру: деректері бар таңдалған файл үшін ЭЦҚ жасау, оны дискіде сақтау, шынайылығын тексеру, кілт өлшемін беру, файл үшін ЭЦҚ таңдау - Объектінің дұрыстығын растайтын хаттамалар және әлсіздіктер -Кілттерді басқару - Хаттамалар - Әлсіздіктер - Асимметриялық шифрлеудің заманауи алгоритмдерін криптоталдау әдістері -Цифрлық қолтаңбаларға және хэш-функцияларға жасалған белгілі криптографиялық шабуылдар мысалдары - Ұсынылған криптографиялық шабуылды жүзеге асыру **СӨЖ өткізу мерзімі:** СӨЖ кестесі бойынша	11	Презентация, баяндама, талқылау
15	4	**RSA криптожүйесі** **Тапсырмалар**: - RSA криптожүйесі. Кілттерді генерациялау, шифрлеу, дешифрлеу, мысалдар. - Құрылымға негізделген RSA шабуылдар - Көбейткіштерге жіктеуге шабуылдар - Шифрленген мәтінді іріктеу мүмкіндігімен шабуылдау - Шифрлеу кілтіне шабуыл (шифрлеу дәрежесінің көрсеткішіне) - Куперсмит теоремасының шабуылы - кеңінен таратушы шабуыл - өзара байланысқан хаттардың шабуылы - қысқа тізім (қысқа толтырылулар) шабуылы - Шифрлеу кілтіне шабуыл (дешифрлеу дәрежесінің көрсеткішіне) - дешифрлеудің ашық дәрежесіне шабуыл - дешифрлеудің аз дәрежесінің көрсеткішіне шабуыл - Бастапқы мәтінге шабуыл - қысқа хатқа шабуыл - циклдік қайталануға шабуыл - айқын шабуыл - Модульдерге шабуыл - Жүзеге асыру шабуылдары - уақыт талдауымен шабуыл - күштілік шабуылы -Шабуылдарға қарсылық. «Асимметриялық шифрлеудің тиімді толықтырылуы» процесі - OAEP (Optimal Assimetric Encryption Padding) -Келесі сілтеме арқылы қолжетімді https://factorable.net/weakkeys12.extended.pdf N. Heninger бастаған зерттеушілер тобының	11	Презентация, баяндама

		жұмысымен RSA шабуылдарын (жалпы модульдер) жүзеге асыру. Шабуылды ұйымдастыру және нәтижелер талдауын орындау. Қосымша материал: http://www.loyalty.org/~schoen/rsa/. **СӨЖ өткізу мерзімі:** СӨЖ кестесі бойынша		
			БАРЛЫҒЫ	165	

5. Пәннің қысқаша ұйымдастырушылық-әдісттемелік сипаттамасы

Оқу нәтижелерін бақылау түрлері:

Аралық бақылау, СӨЖ орындау сапалығын бақылау, екі кезеңді бақылау, қорытынды бақылау.

Аралық бақылау 1 Жазбаша жұмыстар, тапсырмалар, есептер

Аралық бақылау 2 Жазбаша жұмыстар, тапсырмалар, есептер

Қорытынды бақылау: Ауызша емтихан (теориялық және тәжірибелік тапсырмалар)

Курстың саясаты мен процедурасы

Оқу пәнін оқытуда білім алушылар оқытушының қоятын нақты талаптарын орындауға міндетті:

- Білім алушылар кестеге сәйкес барлық сабақтарға міндетті түрде қатысуы қажет;
- Сабақтарға алдын-ала дайындықпен келу керек;
- БӨЖ уақтылы орындау және тапсыру керек;
- Сабақтың барлық түрлеріне дайындық тәуелсіз, шығармашылық сипатта болуы керек;
- Сабақ барысында белсенді жұмыс пен шығармашылық көрсету қажет;
- Бақылаудың барлық түрлеріне қатысу керек;
- Университеттің академиялық адалдық саясатын ұстану қажет.

6. Пәннің оқу-әдістемелік қамтамасыз етілуі

№ п/п	Автор, атауы, баспасы, шығарылған жылы	Ақпарат көзі	Бары (дана)	
			Кітапханада	Кафедрада
1	2	3	4	5
Негізгі әдебиеттер				
1	Криптографиядан есептер жинағы : оқу құралы / Қ. Жетпісов, Д.А. Түсіпов, Ж.С. Иксебаева [et al.]. - Нұр-Сұлтан : Л.Н. Гумилев атындағы ЕҰУ, 2020	Оқу құралы	50	-
2	Әбдіқалықов Қ.Ә. Криптографияның негіздері : оқулық / Қ.Ә. Әбдіқалықов; Қазақстан Республикасы Білім және ғылым министрлігі. - Алматы : ҚР жоғары оқу орындарының қауымдастығы, 2012	Оқулық	19	-
3	Өтелбаев М. Ақпарат қорғау мен криптография негіздері : оқу құралы / М. Өтелбаев, С. Зәуірбеков, Ә. Адамов; Қазақстан Республикасы Білім және ғылым министрлігі, Л.Н.Гумилев атындағы Еуразия ұлттық университеті. - Астана : Л.Н. Гумилев атындағы ЕҰУ, 2012	Оқу құралы	25	-
4	Герман О.Н. Теоретико-числовые методы в криптографии : учебник для студентов учреждений высшего профессионального образования, обучающихся по направлениям подготовки "Информационная безопасность" и "Математика" / О.Н. Герман, Ю.В. Нестеренко. - Москва : Академия, 2012	Оқулық	10	-
5	Романьков В.А. Алгебраическая криптология : монография /	Монография	2	-

	В.А. Романьков; Министерство науки и высшего образования Российской Федерации, Федеральное государственное бюджетное образовательное учреждение высшего образования Омский государственный университет им. Ф.М. Достоевского. - Омск : ОмГУ им. Ф.М. Достоевского, 2020			
6	Зарубин М.Ю. Криптографиялық жүйелер = Криптографические системы : оқу құралы / М.Ю. Зарубин, Г.С. Ыбытаева; Қазақстан Республикасы Білім және ғылым министрлігі. - Алматы : Бастау, 2019	Оқу құралы	100	-
Қосымша әдебиеттер				
12	Мүсірәлиева Ш.Ж. Қолданбалы криптография **:** оқу құралы / Ш.Ж. Мүсірәлиева; Әл-Фараби атындағы Қазақ ұлттық университеті. - Алматы : Қазақ университеті, 2012.	Оқу құралы	9	-
13	Рябко Б.Я. Криптографические методы защиты информации : учебное пособие для высших учебных заведений, обучающихся по специальностям: 201000 (210404)-"Многоканальные телекоммуникационные системы", 201100(210405)-"Радиосвязь, радиовещание и телевидение", 201800(210403)-"Защищенные системы связи" / Б.Я. Рябко, А.Н. Фионов. - Москва : Горячая линия-Телеком, 2013	Оқу құралы	1	-
Электрондық және интернет-ресурстар				
17	https://factorable.net/weakkeys12.extended.pdf			
18	http://www.loyalty.org/~schoen/rsa/			

7. Білім алушылардың оқу нәтижелерін бағалау жүйесі

Білім алушылардың білімі, шеберлігі, дағдылары келесі жүйе бойынша бағаланады.

Әріптік жүйе бойынша баға	Баллдардың сандық эквиваленті	Пайыздық көрсеткіші	Дәстүрлі жүйе бойынша баға	Бағалау критерийлері
A	4,0	95-100	Өте жақсы	**A** бағасы студент бағдарламалық материалды терең және берік игерсе, оны толық, жүйелілікпен, сауатты және логикалық үйлесімді баяндаса, тапсырманың түрі өзгергенде жауап беруге қиналмаса, қойылған сұрақтарға еркін жауап берсе, монографиялық материалдарды білетіндігін көрсетсе, қабылданған шешімдерді дұрыс дәлелдей алса, практикалық жұмыстарды орындаудакриптография мен криптоталдау бойынша жан-жақты дағдылар мен әдістерді пайдалана білсе, материалды өз бетімен қатесіз тұжырымдай білетіндігін және баяндай алатындығын көрсетсе қойылады.
A-	3,67	90-94		**A-** бағасы студент бағдарламалық материалды терең және берік игерсе, оны толық, жүйелілікпен, сауатты және логикалық үйлесімді баяндаса, тапсырманың түрі өзгергенде жауап беруге қиналмаса, қойылған сұрақтарға еркін жауап берсе, монографиялық материалдарды білетіндігін көрсетсе, қабылданған шешімдерді дұрыс дәлелдей алса, практикалық жұмыстарды орындауда шифрлау және дешифрлау әдістері бойынша жан-жақты дағдылар мен әдістерді пайдалана білсе, материалды өз бетімен қатесіз тұжырымдай білетіндігін және баяндай алатындығын көрсетсе қойылады. Студенттің өзімен дұрысталатын, негізгі түсініктерде байқалатын кемшіліктер рұқсат етіледі.
B+	3,33	85-89	Жақсы	**B+** бағасы студент бағдарламалық материалды берік білсе, оны сауатты және мәні бойынша әдеби тілде баяндаса, қойылған сұраққа берген жауабында елеулі дәлелсіздікке жол бермесе, теориялық ережелерді дұрыс қолдана білсе және практикалық мәселелерді шешетін қажетті дағдылары болса қойылады. Жауап беру кезінде оқытушының көмегімен кемшіліктерді дұрыстау рұқсат етіледі.
B	3,0	80-84		B бағасы студент бағдарламалық материалды берік білсе, оны сауатты және мәні бойынша әдеби тілде баяндаса, қойылған сұраққа берген жауабында елеулі дәлелсіздікке жол бермесе, теориялық ережелерді дұрыс қолдана білсе және практикалық мәселелерді шешетін қажетті дағдылары болса қойылады. Жауап беру кезінде оқытушының көмегімен кемшіліктерді дұрыстау немесе елеусіз қателіктер рұқсат етіледі.
B-	2,67	75-79		B- бағасы студент бағдарламалық материалды берік білсе, оны сауатты және мәні бойынша әдеби тілде баяндаса, қойылған сұраққа берген жауабында елеулі дәлелсіздікке жол бермесе, теориялық ережелерді дұрыс қолдана білсе және практикалық мәселелерді шешетін қажетті дағдылары болса қойылады. Бірақ, жауап беру кезінде елеулі кемшіліктер мен қателіктер, оқытушының жетектеуші

				сұрақтарды қою кезінде студенттің кемшіліктерді дұрыстауы рұқсат етіледі.
C+	2,33	70-74		**C+** бағасы студент толық жауап берсе, бірақ оны егжей-тегжейлі білмесе, дәлсіздіктерге, жеткіліксіз тұжырымдамаларға жол берсе, бағдарлама материалын баяндаудағы жүйелікті бұзса және практикалық тапсырмаларды орындауда қиыншылықтар көретін болса. Негізгі тұжырымдамаларды анықтау кезінде студент өзін-өзі дұрстауда қиыншылық көретін болса 1–2 қаттелік рұқсат етіледі.
C	2,0	65-69	Қанағаттанар-лық	**C** егер студент толық жауап бермесе, логикалық үйлесімділігі мен реттілігі бұзылса, оны егжей-тегжейлі білмесе, дәлсіздіктерге, жеткіліксіз тұжырымдамаларға жол берсе, бағдарлама материалын баяндаудағы жүйелікті бұзса және практикалық тапсырмаларды орындауда қиыншылықтар көретін болса қойылады. Студент жалпы білімін мысал ретінде оқытушының көмегімен айқындай алады.
C-	1,67	60-64		**C-** бағасы студент толық жауап бермесе, логикалық үйлесімділігі мен реттілігі бұзылса, оны егжей-тегжейлі білмесе, дәлсіздіктерге, жеткіліксіз тұжырымдамаларға жол берсе, бағдарлама материалын баяндаудағы жүйелікті бұзса және практикалық тапсырмаларды орындауда қиыншылықтар көретін болса, ұғымдардың сипатын анықтауда өрескел қателіктер жасалатын болса қойылады. Жауап беру кезінде қорытындылар жасалмайды, Жалпыланған білімді нақты көріністерін анықтауға қабілеті көрсетілмейді.
D+	1,33	55-59		**D+** бағасы студент толық жауап бермесе, мысал келтіруге қиналса, логикалық үйлемсімсіз жауап берілсе, терминдерге, ұғымдар мен фактілерге сипаттама, құбылыстарға анықтама беруде едәуір үлкен материалдық қателіктер жасалса, берілген жауаптарға қорытынды жасалмаса, жауап сауатсыз болса, қосымша сұрактарға жауап беру кезінде, студент берілген жауаптың байланысы туралы тек оқытушының көмегімен ғана түсінсе қойылады.
D	1,0	50-54		**D-** бағасы студент толық жауап бермесе, логикалық үйлемсімсіз жауап берілсе, терминдерге, ұғымдар мен фактілерге сипаттама, құбылыстарға анықтама беруде едәуір үлкен материалдық қателіктер жасалса, берілген жауаптарға қорытынды жасалмаса, жауап сауатсыз болса, мысалдар келтірілмесе, студент берілген жауап пен басқа модульдердің немесе басқа пәндердің объектілерімен байланысын көрмесе, оқытушының қосымша және нақтылаушы сұрақтарынан кейін жасалған қателіктер дұрысталмаса қойылады.

FX	0,5	25-49	Қанағаттанар-лықсыз	FX ағымдағы, аралық және қорытынды бақылау формаларымен қарастырылған жеке тапсырманы орындай алмаса, бағдарламамен қарастырылған негізгі әдебиеттермен жұмыс істемесе қойылады. F цифрлы эквиваленті ретінде 0-24 бағасы қолданылады, студент бағдарламалық материалдың едәуір бөлігін білмейтін болса, елеулі қателерге жол берсе, практикалық жұмыстарды үлкен қиындықпен орындайтын болса, модульдің жартысынан көп бөлігін игермесе, жауап беру кезінде карапайым сұрақтарға жауап бере алмаса қойылады
F	0	0-24		