**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 криптоталдау2 | 5 | 15 | 15 | 30 | 3 | 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 | Moodle/кейс ҚОЖ-дегі тест  |
| **Лектор** | Бегимбаева Енлик Ериковна | **Оф./с.** | ЖоспарланғанZoom жиналысына қосылыңызhttps://us04web.zoom.us/j/8506270133?pwd=bENGWlhXMDZyYTdHYWJkbWV1V2h6UT09Конференцияның идентификаторы:850 627 0133Кіру коды: 2ZapZP |
| **e-mail** | Enlik\_89@mail.ru |
| **Телефон**  | +77051000777 |  |  |

|  |
| --- |
| **Курстың академиялық презентациясы** |

|  |  |  |
| --- | --- | --- |
| **Пәннің мақсаты** | **Оқытудың күтілетін нәтижелері (ОН)** | **ОН іске асуын көрсететін ндикаторлар (әр ОН үшін кемінде 2 индикаторды келтіру керек)** |
| **Пәннің мақсаты;** Компьютерлік жүйе мен желілерде ақпаратты криптографиялық қорғаудың қазіргі кездегі құралдары мен принциптерін оқу және белгілі алгоритмдерге талдау жасау болып табылады. | 1. Ақпараттарды криптографиялық қорғау алгоритмдері қарапайым орын ауыстыру әдістерін талдау және криптоталдау жүргізіп үйрену. | 1. қарапайым орын ауыстыру әдісін талдау.2. қарапайым орын ауыстыру әдістерін криптоталдау жүргізу |
| 2. Қалдықтар класының санау жүйесін және сандар теориясын криптографияда қолдану. | 1. Қалдықтар класының санау жүйесін құру.2. Салыстыру және оның қасиеттерін талдау.3. Факторизациялау ұғымы, ЕҮОБ және Евклид алгоритмін талдау. 4. Жай сандар туралы Эйлер және Ферма теоремаларын талдау. |
| 3. Қалдықтар туралы Қытай теоремасын криптографияда қолдану. | 1. Қалдықтар туралы Қытай теоремасын үйрену.2. Бірінші дәрежелі салыстыру ұғымы және бірінші дәрежелі салыстыру жүйесін шеуді талдау. |
|  | 4.Симметриялық криптожүйелерге жататын заманауи шифрлеу алгоритмдеріне талдау жүргізу. | 1. блокты шифрларды жасау әдістерін талдау.2. заманауи блокты шифрларды қолданылатын түрлендіру әдістерін зерттеу. |
|  | 5.Ассимметриялық криптожүйелерге жататын шифрлеу алгоритмдеріне талдау жүргізу. | 1. Шифрлеу және дешифрлеу кілттерін жасау әдісін талдау.2. ассимметриялық криптожүйелерге жататын шифрлеу алгоритмдеріне талдау.3.Электронды цифрлық қолтаңба |
| 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, 1999.1. 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

**Ресурстар:** **-бағдарламалық қамтамасыздануы және Интернет- ресурстары**1. 1. intuit.ru
2. **мәліметтер базысы, ақпараттық-анықтамалық және іздестіру жүйелері:** интернет желісі

**Онлайн қол жетімділігі:** Қосымша оқу материалы, жэне үй тапсырмалары мен жобалар univer.kaznu.kz. сайтындағы өздеріңнің парақшаларыңдағы ПОЭК бөлімінде көруге болады.  |

|  |  |
| --- | --- |
| Университеттің моральдық-этикалық құндылықтары аясындағы курстың академиялық саясаты | **Оқу тәртібі:**1. Пәннің кестесіне сәйкес онлайн-курстық модульдердің уақыты қатаң сақталуы керек2. 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 |
| А | 4,0 | 95-100 | Өте жақсы |
| А- | 3,67 | 90-94 |
| В+ | 3,33 | 85-89 | Жақсы |
| В | 3,0 | 80-84 |
| В- | 2,67 | 75-79 |
| С+ | 2,33 | 70-74 |
| С | 2,0 | 65-69 | Қанағаттанарлық |
| С- | 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 | Тақырыпың атауы |  ОН | ОНИ | Сағат саны | Макс балл | Білімді бағалау түрі | Сабақ жүргізу формасы/платформа |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 |  |
| **I** | **Модуль - 1** |  |
| 1 | Д1. Курстың мақсаты мен міндеттері. Криптография және криптоанализ: тарих, философия, тәсілдер. | ОН 1 | 1.1 | 1 | 1 | Дәріске қатысу белсенділігі | Бейне дәріс Zoom.Cинхронды |
| 1 | СС1. Классикалық шифрлар. Қарапайым мәтіннің математикалық модельдері. Алмастыру шифрлары. Ауыстыру шифрлары. Ауыстыратын шифрдың математикалық моделі. Ауыстырылатын шифрлардың жіктелуі. 1 бөлім. | ОН 1 | 1.1  | 1 | 2 | Талдау жүргізу | ВебинарZoomсинхронды |
| 1 | ЗС1. Классикалық шифрларды криптоанализге арналған тапсырмалар. Бағандарды ауыстыру шифры. Қос алмастыру шифры. | ОН 1 | 1.1 | 2 | 10 | Жеке тапсырма бойынша қорғау | ВебинарZoomсинхронды |
| 1 | СОӨЖ1. Кеңес беру. СОӨЖ жеткізу кестесімен танысу. Қазақстандағы криптоанализ тарихы. | ОН 1 | 1.1 | 1 | 10 | Жеке тапсырма бойынша қорғау | ВебинарZoomсинхронды |
| 2 | Д2. Криптография мен криптоанализдегі заманауи бағыттарына шолу. Криптоанализдің жалпы әдістері. | ОН 1 | 1.2 | 1 | 1 | Дәріске қатысу белсенділігі | Бейне дәріс Zoom.Cинхронды |
| 2 | СС2. Классикалық шифрлар. Қарапайым мәтіннің математикалық модельдері. Алмастыру шифрлары. Ауыстыру шифрлары. Ауыстыратын шифрдың математикалық моделі. Ауыстырылатын шифрлардың жіктелуі. 2 бөлім. | ОН 1 | 1.2  | 1 | 2 | Талдау жүргізу | ВебинарZoomсинхронды |
| 2 | ЗС2. Мәтіндік ақпаратты қорғау үшін ауыстыру мен алмастырудың классикалық криптоалгоритмдерін қолдану. | ОН 1 | 1.2  | 2 | 10 | Жеке тапсырма бойынша қорғау | ВебинарZoomсинхронды |
| 3 | Д3. Құпия кілтпен криптографиялық жүйелерді құрудың теориялық негіздері. Керхгоф принципі. Криптографиялық жүйелердің түрлері. | ОН 2 | 2.12.22.3 | 1 | 1 | Дәріске қатысу белсенділігі | Бейне дәріс Zoom.Cинхронды |
| 3 | СС3. Абсолютті тұрақты криптографиялық жүйелер. Есептеуге тұрақты шифрлар. |  ОН 2 | 2.3  | 1 | 2 | Талдау жүргізу | ВебинарZoomсинхронды |
| 3 | ЗС3. Кілттерді таңдау негізінде мәтіндік ақпараттарды қорғаудың әр түрлі әдістерін және олардың беріктігін зерттеу. | ОН 2 | 2.3  | 2 | 15 | Жеке тапсырма бойынша қорғау | ВебинарZoomсинхронды |
| **II** | **Модуль – II** |
| 4 | Д4. Симметриялық криптожүйелердің криптоанализі: блоктық шифрлар. Блоктық шифрлау алгоритмдерінің құрылымы. Блоктық шифрлау алгоритмін анықтау. Фейстель схемасы. Блоктық шифрлаудың құрылу принциптері. | ОН 2 | 2.12.2 | 1 | 1 | Дәріске қатысу белсенділігі | Бейне дәріс Zoom.Cинхронды |
| 4 | СС4. Шифрлау айналымдарының саны. F түрлендіру функциясына қойылатын талаптар. S-блоктарының құрылымы. Кілтті есептеу алгоритмі. | ОН 2 | 2.12.2 | 1 | 2 | Талдау жүргізу | ВебинарZoomсинхронды |
| 4 | ЗС4. Feistel желілері. Feistel желісін бағдарламалық қамтамасыз ету. | ОН 2 | 2.12.2 | 2 | 10 | Жеке тапсырма бойынша қорғау | ВебинарZoomсинхронды |
| 4 | СОӨЖ2. Басқа белгілі блоктық шифрлау алгоритмдері. RC 5. IDEA. SAFER. Blowfish. | ОН 2 | 2.12.22.3 | 2,5 | 15 | Презентация | ВебинарZoomсинхронды |
| 5 | Д5. Блоктық шифрлау стандарттары. DES стандарты. Жеңілдетілген DES. S-DES кілттерін есептеу. | ОН 3 | 1.11.2 | 1 | 1 | Дәріске қатысу белсенділігі | Бейне дәріс Zoom.Cинхронды |
| 5 | СС5. Ресей стандарты - ГОСТ 28147-89. | ОН 2ОН 3 | 2.22.43.1 | 1 | 2 | Талдау жүргізу | ВебинарZoomсинхронды |
| 5 | ЗС5. Блоктық шифрлау стандарттары бойынша сұрақтар мен тапсырмалар. | ОН 2ОН 3 | 2.22.43.1 | 2 | 15 | Жеке тапсырма бойынша қорғау | ВебинарZoomсинхронды |
| 5 | **АБ 1** |  |  |  | 100 |  |  |
| 6 | Д6. AES шифрлау алгоритмі. S\_AES шифрлау алгоритмі. | ОН 3 | 1.11.2 | 1 | 1 | Дәріске қатысу белсенділігі | Бейне дәріс Zoom.Cинхронды |
| 6 | СС6. AES алгоритмінің криптоанализі. | ОН 2ОН 3 | 2.22.43.1 | 1 | 2 | Талдау жүргізу | ВебинарZoomсинхронды |
| 6 | ЗС6. AES симметриялы шифрлау стандарты. Бағдарламалық жасақтаманы енгізу. | ОН 2ОН 3 | 2.22.43.1 | 2 | 10 | Жеке тапсырма бойынша қорғау | ВебинарZoomсинхронды |
| **III** | **Модуль - III** |
| 7 | Д7. Ақпараттық қауіпсіздік жүйелеріндегі псевдо-кездейсоқ тізбектер генераторларының функциялары. ПКТ генераторларына қойылатын талаптар. Криптотұрақтылық. ПКТ генераторларын құру принциптері | ОН 3 | 3.13.2 | 1 | 1 | Дәріске қатысу белсенділігі | Бейне дәріс Zoom.Cинхронды |
| 7 | СС7. ПКТ генераторларының классификациясы. Криптографиялық ПКТ генераторлары. | ОН 3 | 3.13.2 | 1 | 2 | Талдау жүргізу | ВебинарZoomсинхронды |
| 7 | ЗС7. Конгруентті ПКТ генераторлары. Сызықтық конгруентті генераторлардың периоды және потенциалы. Мысалдар мен тапсырмалар. | ОН 3 | 3.13.2 | 2 | 10 | Жеке тапсырма бойынша қорғау | ВебинарZoomсинхронды |
| 8 | **Д8.** Сызықтық кері байланысы бар ауысымдық регистрлердегі (РСЛОС) ПКТ генераторлары. | ОН 4 | 4.14.2 | 1 | 1 | Дәріске қатысу белсенділігі | Бейне дәріс Zoom.Cинхронды |
| 8 | СС8. РСЛОС генераторларын біріктіру. Геффе генераторы. | ОН 4 | 4.14.2 | 1 | 2 | Талдау жүргізу | ВебинарZoomсинхронды |
| 8 | ЗС8. Псевдо-кездейсоқ сандардың генераторы ретінде сызықтық кері байланыс ауысымының регистрлері. | ОН 4ОН 4 | 4.14.2 | 2 | 10 | Жеке тапсырма бойынша қорғау | ВебинарZoomсинхронды |
| 8 | СОӨЖ4. РСЛОС негізіндегі ағын шифрлары | ОН 4 | 4.14.2 | 2,5 | 15 | Презентация | ВебинарZoomсинхронды |
| **IV** | **Модуль - IV** |
| 9 | Д9. ПКТ генераторларының сапасын бағалау әдістемесі. Графикалық тесттер. Элементтің таралу гистограммасы. Жазықтықтағы таралуы. Серияны тексеру. | ОН 4 | 4.14.2 | 1 | 1 | Дәріске қатысу белсенділігі | Бейне дәріс Zoom.Cинхронды |
| 9 | СС9. Монотондылықты тексеріңіз | ОН 4 | 4.14.2 | 1 | 2 | Талдау жүргізу | ВебинарZoomсинхронды |
| 9 | ЗС9. Автокорреляция функциясы | ОН 4 | 4.14.2 | 2 | 10 | Жеке тапсырма бойынша қорғау | ВебинарZoomсинхронды |
| 9 | СӨОЖ4 **–** Тесттерді бағдарламалық қамтамасыздандыру | ОН 4 | 4.14.2 | 2,5 | 20 | Презентация | ВебинарZoomсинхронды |
| 10 | Д10.Бағалау тестілері. Ықтималдықтар теориясы және математикалық статистика туралы ақпарат | ОН 4 | 4.14.2 | 1 | 1 | Дәріске қатысу белсенділігі | Бейне дәріс Zoom.Cинхронды |
| 10 | СС10. Д.Кнуттың тест тапсырмалары. Байланысыз серияларды тексеру. Аралықтарды тексеру. | ОН 4 | 4.14.2 | 1 | 2 | Талдау жүргізу | ВебинарZoomсинхронды |
| 10 | СС10. «DIEHARD» статистикалық қасиеттерін бағалау жүйесі. | ОН 4ОН 4 | 4.14.2 | 2 | 10 | Жеке тапсырма бойынша қорғау | ВебинарZoomсинхронды |
| 10 | **Midterm** |  |  |  | 100 |  |  |
| 11 | Д11. NIST нұсқаулығы. Жалпы ережелер. Жиілік тесті. Ішкі тізбектегі жиілікті тексеру тесті. | ОН 5 | 5.2 | 1 | 1 | Дәріске қатысу белсенділігі | Бейне дәріс Zoom.Cинхронды |
| 11 | СС11. "Тесік" тесті. Ішкі тізбектегі «блоктарды» тестілеу. | ОН 5 | 5.2 | 1 | 2 | Талдау жүргізу | ВебинарZoomсинхронды |
| 11 | СС11. Таңбалар бойынша тексеру. Жиілікті тексеру. Тест нәтижелерін бағалау. | ОН 5 | 5.2 | 2 | 10 | Жеке тапсырма бойынша қорғау | ВебинарZoomсинхронды |
| **V** | **Модуль V** |
| 12 | Д12. Блоктық шифрлау алгоритмдерінің сызықтық криптоанализі. Сызықтық криптоанализ туралы жалпы ақпарат. | ОН 5 | 5.2 | 1 | 1 | Дәріске қатысу белсенділігі | Бейне дәріс Zoom.Cинхронды |
| 12 | СС12. Сызықтық криптоанализді шифрлау алгоритмдеріне қолдану. | ОН 5 | 5.2 | 1 | 2 | Талдау жүргізу | ВебинарZoomсинхронды |
| 12 | ЗС12. Шифрлау алгоритмдеріне сызықтық криптоанализ бойынша сұрақтар. | ОН 5 | 5.2 | 2 | 10 | Жеке тапсырма бойынша қорғау | ВебинарZoomсинхронды |
| 12 | СӨОЖ5 RC 5 шифрлау алгоритмінің дифференциалды криптоанализі. | ОН 5 | 5.2 | 2 | 35 | Жеке тапсырма бойынша қорғау | ВебинарZoomсинхронды |
| 13 | Д13. Блоктық шифрлау алгоритмдерінің дифференциалды криптоанализі. Дифференциалды криптоанализ туралы жалпы мәліметтер. | ОН 5 | 5.1 | 1 | 1 | Дәріске қатысу белсенділігі | Бейне дәріс Zoom.Cинхронды |
| 13  | СС11. Дифференциалды криптоанализді шифрлау алгоритмдеріне қолдану. | ОН 5 | 5.1 | 1 | 2 | Талдау жүргізу | ВебинарZoomсинхронды |
| 13  | ЗС11. Шифрлау алгоритмдеріне дифференциалды криптоанализ бойынша сұрақтар. | ОН 5 | 5.1 | 2 | 10 | Жеке тапсырма бойынша қорғау | ВебинарZoomсинхронды |
| **VI** | **Модуль - VI** |
| 14 | Д14. Алгебралық криптоанализ. Негізгі ой. Алгебралық криптоанализ әдісі. | ОН 5 | 5.3 | 1 | 1 | Дәріске қатысу белсенділігі | Бейне дәріс Zoom.Cинхронды |
| 14 | СС14. Ағын шифрының криптоанализі. Мысалдарды қарастыру. | ОН 5 | 5.3 | 1 | 2 | Талдау жүргізу | ВебинарZoomсинхронды |
| 14 | ЗС14. Алгебралық криптанализ бойынша сұрақтар. | ОН 5 | 5.3 | 2 | 10 | Жеке тапсырма бойынша қорғау | ВебинарZoomсинхронды |
| 15 | Д15. Слайд криптоанализі. Негізгі ой. Әдістер. | ОН 5 | 5.3 | 1 | 1 | Дәріске қатысу белсенділігі | Бейне дәріс Zoom.Cинхронды |
| 15 | СС15. Слайд криптанализінің алгоритмі. | ОН 5 | 5.3 | 1 | 2 | Талдау жүргізу | ВебинарZoomсинхронды |
| 15 | ЗС15. KeeLog шифрының криптоанализі | ОН 5 | 5.3 | 2 | 10 | Жеке тапсырма бойынша қорғау | ВебинарZoomсинхронды |
| 15 | СӨОЖ қабылдау | ОН 5 | 5.3 | 1 |  | Жеке тапсырма бойынша қорғау | ВебинарZoomсинхронды |
| 15 | **АБ 2**  |  |  |  | 100 |  |  |
|  | Қортынды бақылау |  |  |  | 100 |  |  |
|  | БАРЛЫҒЫ (1АБ+АБ(МТ)+ 2 АБ)/3\*0,6+(ИЭ\*0,4) |  |  |  | 100 |  |  |

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.