**әл-Фараби атындағы Қазақ ұлттық университеті**

**Ақпараттық технологиялар факультеті**

 **«5B100300– Ақпараттық қауіпсіздік жүйелері»**

**мамандығы бойынша білім беру бағдарламасы**

**Cиллабус**

**(KABSh3302) Блокты шифрлы криптоталдау**

**Күзгі семестр 2019/2020 уч. год**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Пән коды | Пәннің аты | Тип | Апта бойынша сағат саны | Кредиттер саны | ECTS |
| Дәріс | Практ/семин | Зертханалық |
| KABSh3302 |  Блокты шифрлы криптоталдау | ЭК | 1 | 1 | 2 | 3 | 5 |
| Дәріскер   | Хомпыш АрдабекСтарший преподаватель | Офис-сағаты | Кесте бойынша  |
| e-mail | ardabek@mail.ru |
| Телефоны  | 87072433362 | Аудитория  | 419 |
| Практ/семинар /зертхана сабағын жүргізетін оқытушы | Жумабекова А. |  |  |
| e-mail | Zhumabekova2702@gmail.com |  |  |
| Телефоны | 87011066721 | Аудитория |  |

|  |  |
| --- | --- |
| Академиялық курс презентациясы | Курстың мақсаты - криптанализ әдістерін және олардың криптографияның дамуына әсерін зерттеу. Кілттерді толық есептеу әдісімен шифрларды бұзудың максималды мүмкіндіктерін бағалау. Әр түрлі крипто шабуылдардың симметриялы криптожүйелерге қолданылуын талдау. Криптанализдің перспективті технологияларымен танысу.Пәнді оқу нәтижесінде студент білуі тиіс:- қазіргі заманғы алгоритмдерге белгілі криптанализ әдістерін қолдана білу;- есептерді шығаруда математикалық әдістерді қолдана алады;- салыстырмалы талдау жүргізу, әдістер мен құралдарды таңдау;- ақпараттық ресурстарды қорғау деңгейін бағалау. |
| Пререквизиттер және постреквизиттер | 1. Пән жоғарғы оқу орында «Ақпараттық қауіпсіздік және ақпаратты қорғау», «Ақпарат теориясы»,«Дискреттік математика» пәндерінен алынған білімге негізделеді.
2. Пәнді оқып меңгерген студенттер «Криптография», «Желідегі ақпараттарды қорғау әдістері» пәндерін оқуда қолданылады.
 |
| Әдебиеттер және ресурстар | **Әдебиеттер**:**Негізгі:**1. Л.К. Бабенко, Е.А. Ищукова. Современные алгоритмы блочного шифрования и методы их анализа // Москва. Гелиос АРВ – 2006.
2. В. Столлингс Криптография и защита сетей: принципы и практика. 2-е изд. / Пер. С англ. – М.:Вильямс, 2001.
3. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тесты на языке Си. – М.: ТРИУМФ, 2003.
4. Иванов М.А., Чугунков И.В. Теория, применение и оценка качества генераторов псевдослучайных последовательностей. М.: КУДИЦ-ОБРАЗ, 2003.

**Қосымша:**1. Нечаев В.И. Элементы криптографии (Основы теории защиты информации) / Под ред. В.А.Садовничего. – М.: Высшая школа, 1999. – 109 с.
2. А. Ростовцев, "Алгебраические основы криптографии", СПб: Мир и Семья, 2000.
3. Зубов А.Ю. Криптографические методы защиты информации. Совершенные шифры. М.: Гелиос АРВ, 2005.
4. Фороузан Б.А. Криптография и безопасность сетей: Учебное пособие / Фороузан Б.А.; перевод с англ. под ред. А.Н. Берлина. – М.: Интернет-Университет Информационных технологий: БИНОМ. Лаборатория знаний, 2010
5. Алфёров А.П., Зубов А.Ю., Кузьмин А.С., Черёмушкин А.В. Основы криптографии. М.: Гелиос АРВ, 2005.
 |
| Университеттің моральдық-этикалық құндылықтарына сай курстың академиялық саясаты  | **Академиялық ереженің тәртібі:** Студенттер сабақтарға міндетті түрде кешікпей қатысуы керек, сабаққа себепсіз қатыспауға болмайды. Сабаққа себепсіз қатыспаса, кешігіп келсе 0 бал қойылады.Тапсырмаларды (СӨЖ бойынша, аралық бақылау, зертханалық, практикалық/семинарлық, жоба жұмыстарын және т.б), қорытынды емтиханды уақытында орындауға және тапсыруға міндетті.Тапсырмаларды орындап, тапсыру барысында студент тапсыру мерзімін бұзған жағдайда жоспарланған максималды балдан айыппұл (50%) шегеріліп, бағаланады.**Академиялық құндылықтар:**Академиялық құндылық және адалдық: барлық тапсырмаларды өз бетінше орындау; плагиатқа, жалғандыққа, шпаргалканы пайдалануға жол бермеу, білімді бақылаудың барлық кезеңінде көшіруге, оқытушыны алдау және оған деген қарым-қатынасының нашарлығын болдырмау (ҚазҰУ студенттерінің ар-намыс кодексі).Мүмкіндігі шектеулі студенттер арнайы ardabek@mail.ru бойынша көмек ала алады. |
| Бағалау саясаты және аттестаттау | **Критериалды бағалау:** Орындалған жұмыстар менқорытынды емтихан барысында теориялық материалдың меңгерілуі мен теориялық және практикалық дағдыларды қабылдауы дескрипторға сәйкес тексеріледі (аралық бақылау мен емтиханда құзыреттіліктің қалыптасуын тексеру).**Жиынтық бағалау:** аудиториядағы жұмыс белсенділігі, қатысуы және орындалған тапсырма бағаланады. Қорытынды баға төменде келтірілген білімді бағалау шкаласына сәйкес қойылады. |

**Білімді бағалау шкаласы**

|  |  |  |  |
| --- | --- | --- | --- |
| Әріптік жүйе бойынша бағалау | Балдардың сандық эквиваленті | Балдар (%-дық қатынаста) | Дәстүрлі жүйе бойынша бағалау |
| А | 4,0 | 95-100 | Өте жақсы  |
| А- | 3,67 | 90-94 |
| В+ | 3,33 | 85-89 | Жақсы Қанағаттанарлық  |
| В | 3,0 | 80-84 |
| В- | 2,67 | 75-79 |
| С+ | 2,33 | 70-74 |
| С | 2,0 | 65-69 |  |
| 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 жүзеге асыру күнтізбесі (графигі)**

|  |  |  |  |
| --- | --- | --- | --- |
| Неделя / дата | Название темы | Кол-во часов | Максимальный балл |
| 1 | Лекция 1. Частотный анализ. Открытые сообщения и их характеристики. Частотные характеристики открытых сообщений. Критерии на открытый текст. Анализ и способы вскрытие простых замен, шифра цезаря и вертикальный перестановки. | 2 | 0 |
| 1 | Семинарское занятие 1. Ситуационные задачи на определение свойств информации, подлежащей криптографическому преобразованию. Изучить полиалфавитный шифр замены, система Виженера. | 1 | 12 |
| 1 | СРСП 1. Шифр с использованием кодового слова. | 1.5 | 8 |
| 2 | Лекция 2. Шифры сложной замены и код. Способы их вскрытие. Весовой критерий. | 2 | 0 |
| 2 | Семинарское занятие 2. Шифры, основанные на аналитических преобразованиях. | 1 | 12 |
| 2 | СРСП 2. Биграммные замены. Шифр Плейфера и криптоанализ шифра. Шифр «двойной квадрат». | 1.5 | 8 |
| 3 | Лекция 3. Шифрование методом гаммирование. Модульное гаммирование. Случайные и псевдослучайные гаммы. Нулевая вертикальная биграмма(НВБ).  | 2 | 0 |
| 3 | Семинарское занятие 3. Псевдослучайные генераторы. Оценка свойств гаммы шифра. Снятие гаммы при повторном использования ключа. | 1 | 12 |
| 3 | СРСП 3. Анализ криптограмм, полученных применением неравновероятной и короткой гаммы. | 1.5 | 8 |
| 4 | Лекция 4. Роторные и электронные шифраторы. Обзор известных шифровальных машин. Шифровальная машина Энигма. Расшифрование шифр «Энигмы». | 2 | 0 |
| 4 | Семинарское занятие 4. Математические описание роторных шифр машин. Криптоанализ Энигмы. | 1 | 12 |
| 4 | СРСП 4. Аналоги шифровальных машин Энигмы. | 1.5 | 8 |
| 4 | **СРСП** Защита СРС1 |  |  |
| 5 | Лекция 5. Шифровальная машина **М-209(Хагелин).** Криптостойкость шифра и возможности восстоновление ключа. | 2 | 0 |
| 5 | Семинарское занятие 5. Примеры настройки роторных шифровальных машин. Шифрование открытого сообщения. | 1 | 12 |
| 5 | СРСП 5. Модификаций шифровальных машина М-209.**СРСП Коллоквиум**  | 1.5 | 8 |
| 5 | **РК1**  |  | 100 |
| 6 | Лекция 6. Сжатие данных. Типы скремблеров. Принципы сжатия данных и их применимость. | 2 | 0 |
| 6 | Семинарское занятие 6. Характеристики алгоритмов сжатия. Алгоритм метода Хаффмана. Построение кодового дерева. | 1 | 12 |
| 6 | Семинарское занятие 6. Характеристики алгоритмов сжатия. Алгоритм метода Хаффмана. Построение кодового дерева. | 1.5 | 8 |
| 7 | Лекция 7. Обзор современных систем шифрования. Принципы построения блочных шифров. Классификация алгоритмов шифрования. Требования к блочному алгоритму шифрования. Сеть Фейстеля и проектирование S блоков.  | 2 | 0 |
| 7 | Семинарское занятие 7. Американский стандарт шифрования данных DES. Стандарт шифрования ГОСТ 28147-89. Новый стандарт AES “Rijndael”. Основные режимы работы алгоритмов. | 1 | 12 |
| 7 | СРСП 7. Математические основы асимметричного шифрования. | 1.5 | 8 |
| 7 | **СРСП СРС2 Консультация** |  |  |
| 8 | Лекция 8. Задачи и принципы криптоанализа. Классификация криптоатак.  | 2 | 0 |
| 8 | Семинарское занятие 8. Атака на основе открытых текстов и соответствующих шифротекстов. | 1 | 12 |
| 8 | СРСП 8. Атака «грубой силы», метод «встречи по середине». Анализ слабых ключей. | 1.5 | 8 |
| 9 | Лекция 9. Алгебраический анализ стойкости криптографических алгоритмов. Булевы функции. Алгебраический подход.  | 2 | 0 |
| 9 | Семинарское занятие 9. Алгебраический криптоанализ однораундового AES. | 1 | 12 |
| 9 | СРСП 9. XSL атаки. | 1.5 | 8 |
| 10 | Лекция 10. Дифференциальный криптоанализ.  | 2 | 0 |
| 10 | Семинарское занятие 10. Анализ одного раунда DES. | 1 | 12 |
| 10 | СРСП 10. Особенности дифференциального криптоанализа алгаритма AES. **СРСП Коллоквиум**  | 1.5 | 8 |
|  | **МТ как РК** |  | 100 |
| 11 | Лекция 11. Дифференциальный криптоанализ S блоки алгоритмов DES, AES, ГОСТ 28147-89, ГОСТ Р 34.13.2015.  | 2 | 0 |
| 11 | Семинарское занятие 11. Дифференциальный криптоанализ DES. Вскрытие с помощью дифференциального криптоанализа. | 1 | 12 |
| 11 | СРСП 11. Дифференциальный криптоанализа шифр алгоритма Lucifer. | 1.5 | 8 |
| 12 | Лекция 12. Линейный криптоанализ. Построение линейных уравнений.  | 2 | 0 |
| 12 | Семинарское занятие 12. Уязвимость различных шифров к методу линейного криптоанализа. | 1 | 12 |
| 12 | СРСП 12. Дифференциально-линейный криптоанализ. | 1.5 | 8 |
|  | **СРСП**  |  |  |
| 13 | Лекция 13. Линейный криптоанализ S блоки алгоритмов DES, AES, ГОСТ 28147-89, ГОСТ Р 34.13.2015. Требование для S блоков к устойчивости дифференциального и линейного криптоанализа. | 2 | 0 |
| 13 | Семинарское занятие 13. Применение линейного криптоанализа к DES. | 1 | 12 |
| 13 | СРСП 13. Использование слабых блоков замены для линейного криптоанализа блочных шифров. | 1.5 | 8 |
| 13 | **СРСП прием СРС** |  |  |
| 14 | Лекция 14. Интерполяционный криптоанализ. Использование метода. Ключ восстонавления.  | 2 | 0 |
| 14 | Семинарское занятие 14. Алгоритм шифрование IDEA. Математическое описание. Режимы шифрования. | 1 | 12 |
| 14 | СРСП 14. Криптоанализ IDEA. | 1.5 | 8 |
| 15 | Лекция 15. Корреляционный криптоанализ. Базовые и другие корреляционные атаки.  | 2 | 0 |
| 15 | Семинарское занятие 15. Безусловно стойкие и вычислительно стойкие шифры. | 1 | 12 |
| 15 | СРСП 15. Имитостойкость и помехоустойчивость криптосистем**СРСП Коллоквиум**  | 1.5 | 8 |
|  | РК |  | 100 |
|  | **Экзамен**  |  | 100 |

Әдістемелік бюроның төрайымы Гусманова Ф.Р.

Кафедра меңгерушісі Мусиралиева Ш.Ж.

Дәріскер Хомпыш А