УТВЕРЖДЕНО
на заседании Ученого совета
НАО «КазНУ им. аль-Фараби»
Протокол №11 от 11.06.2024 г.

Программа вступительного экзамена для поступающих в докторантуру на группу образовательных программ D195 – «Криптология»

I. Общие положения

1. Программа составлена в соответствии с Приказом Министра образования и науки Республики Казахстан от 31 октября 2018 года № 600 «Об утверждении Типовых правил приема на обучение в организации образования, реализующие образовательные программы высшего и послевузовского образования» (далее – Типовые правила).

2. Вступительный экзамен в докторантуру состоит из собеседования, написания эссе и экзамена по профилю группы образовательных программ.

Блок	Баллы
1. Собеседование	30
2. Эссе	20
3. Экзамен по профилю группы образовательной программы	50
Всего/проходной	100/75

3. Продолжительность вступительного экзамена - 3 часа 10 минут, в течение которых поступающий пишет эссе, отвечает на электронный экзаменационный билет. Собеседование проводится на базе вуза до вступительного экзамена.

II. Порядок проведения вступительного экзамена

1. Поступающие в докторантуру на группу образовательных программ D195 – «Криптология» пишут проблемное / тематическое эссе. Объем эссе – не менее 250 слов.

Цель эссе – определить уровень аналитических и творческих способностей, выраженных в умении выстраивать собственную аргументацию на основе теоретических знаний, социального и личного опыта.

Виды эссе:

- мотивационное эссе с раскрытием побудительных мотивов к исследовательской деятельности;

- научно-аналитическое эссе с обоснованием актуальности и методологии планируемого исследования;
- проблемное/тематическое эссе, отражающее различные аспекты научного знания в предметной области.

Темы для подготовки к экзамену по профилю группы образовательной программы:

Дисциплина «Организация систем информационной безопасности»

Тема: криптоанализ

Подтемы:

1. Классические шифры и их вскрытие. Шифр сдвига и афинный шифр и их дешифрование и взлом методом перебора. Частотный метод вскрытия шифра замены. Недостатки классических шифров, частотный анализ таких шифров текстов на казахском и русском языках.
2. Кольцо целых чисел, алгоритм Евклида и следствия. Представление наибольшего общего делителя. Теория сравнений. Свойства сравнений по данному модулю. Обратимые элементы по данному модулю.
3. Функция Эйлера и ее свойства. Функция Эйлера на простых числах. Теорема о мультипликативности функции Эйлера. Формула нахождения значений функции Эйлера, возведение в степень с использованием функции Эйлера.
4. Теорема Ферма-Эйлера и основная теорема RSA-шифра.
5. RSA-шифр, процесс шифрования и чтения, обоснование. RSA-шифрование открытым ключем заданного текста. RSA-дешифрование закрытым ключем заданного текста.
6. RSA-электронная подпись, идея и обоснование.
7. Реализация процедуры RSA-электронной подписи, часть подписывания электронной подписью документа.
8. Реализация процедуры RSA-электронной подписи, часть шифрование подписи открытым ключом.
9. Распределение простых чисел в натуральном ряду и оценка RSA шифра.
10. Кольцо многочленов над полем < F2 ; +,* > алгоритм Евклида, представление наибольшего общего делителя двух многочленов. Неприводимые многочлены в этом кольце. Неприводимые многочлены степеней 2,3,4,5.
11. Конструкция поля < F2n ; +,* > как поля построенного из остатков по модулю неприводимого многочлен. Задание сложения и умножения в этом поле. Обратные элементы по сложению и обратные элементы по умножению для ненулевых элементов этого поля. Построить поле < F16 ; +, * > .
12. Теорема Лагранжа о делимости порядка группы на порядок подгруппы. Следствия о том, что порядок элемента делит порядок группы. Примеры подгрупп группы Zn. Теорема о первообразном элементе в поле < F2n ; +,* >. Первообразные элементы поля < F16 ; +,* >.

13. Конструкция поля, построенного из n-разрядных двоичных блоков. Задание сложения и умножения в этом поле. Обратные элементы по сложению и обратные элементы по умножению для ненулевых элементов этого поля, первообразные элементы этого поля. Построить поле 4-разрядных двоичных блоков, указать первообразные элементы этого поля.

14. Задача Дифи-Хеллмана. Создание общего секрета для удаленных пользователей, опираясь на «неразрешимость» задачи Дифи-Хеллмана. Решение проблемы обмена ключами для удаленных пользователей.

15. Шифр Эль-Гамаля, прецесс обмена ключами, шифрование и дешифрования. Реализация на примере.

Дисциплина «Методы и средства защиты компьютерной информации»

Тема: модели и методы шифрования информации

Подтемы:

1. Краткие исторические сведения о возникновении и развитии методов криптологии. Криптография. Конфиденциальность. Целостность. Аутентификация. Цифровая подпись.

2. Модель Белла-Лападулы. Предварительное распределение ключей. Пересылка ключей. Открытое распределение ключей. Схема разделения секрета. Инфраструктура открытых ключей. Сертификаты. Центры сертификации. Формальные модели шифров. Модели открытых текстов. Математические модели открытого текста. Критерии распознавания открытого текста. Классификация шифров по различным признакам. Математическая модель шифра замены. Классификация шифров замены.

3. Модель Low-Water-Mark (LWM). Маршрутные перестановки. Элементы крипто- анализа шифров перестановки. Шифры замены.

4. Модели J. Goguen, J. Meseguer. Табличное гаммирование. О возможности восстановления вероятностей знаков гаммы. Восстановление текстов, зашифрованных неравно-вероятной гаммой. Повторное использование гаммы. Криптоанализ шифра Виженера. Ошибки шифровальщика.

5. Модель выявления нарушения безопасности. Энтропия и избыточность языка. Расстояние единственности. Стойкость шифров. Теоретическая стойкость шифров. Практическая стойкость шифров. Вопросы имитостойкости шифров. Шифры, не распространяющие искажений. Шифры, не распространяющие искажений типа "замена знаков. Шифры, не распространяющие искажений типа" пропуск-вставка знаков.

6. Блочные системы шифрования. Принципы построения блочных шифров. Примеры блочных шифров. Американский стандарт шифрования данных DES. Стандарт шифрования данных ГОСТ 28147-89. Режимы использования блочных шифров. Комбинирование алгоритмов блочного шифрования. Методы анализа алгоритмов блочного шифрования. Рекомендации по использованию алгоритмов блочного шифрования.

7. Поточные системы шифрования. Синхронизация поточных шифрсистем. Принципы построения поточных шифрсистем. Примеры поточных шифрсистем. Шифрсистема A5. Шифрсистема Гиффорда. Линейные регистры сдвига. Алгоритм Берлекемпа-Месси. Усложнение линейных рекуррентных последовательностей. Фильтрующие генераторы. Комбинирующие генераторы. Композиции линейных регистров сдвига. Схемы с динамическим изменением закона рекурсии. Схемы с элементами памяти. Методы анализа поточных шифров.

8. Управление безопасностью. Стандарты, аудит безопасности. Особенности речевых сигналов. Скремблирование. Частотные преобразования сигнала. Временные преобразования сигнала. Стойкость систем временных перестановок. Системы цифровой телефонии.

9. Системы шифрования с открытыми ключами. Шифрсистема RSA. Шифрсистема Эль-Гамаля. Шифрсистема Мак-Элиса. Шифрсистемы на основе "проблемы рюкзака".

10. Идентификация. Правила составления паролей. Усложнение процедуры проверки паролей. "Подсоленные" пароли. Парольные фразы. Атаки на фиксированные пароли. Повторное использование паролей. Тотальный перебор паролей. Атаки с помощью словаря. Личные идентификационные номера. Одноразовые пароли. «Запрос-ответ» (сильная идентификация). "Запрос-ответ" с использованием симметричных алгоритмов шифрования. "Запрос-ответ" с использованием асимметричных алгоритмов шифрования. Протоколы с нулевым разглашением. Атаки на протоколы идентификации.

11. Криптографические хэш-функции. Функции хэширования и целостность данных. Ключевые функции хэширования. Бесключевые функции хэширования. Целостность данных и аутентификация сообщений. Возможные атаки на функции хэширования.

12. Цифровые подписи. Общие положения. Цифровые подписи на основе шифрсистем с открытыми ключами. Цифровая подпись Фиата-Шамира. Цифровая подпись Эль-Гамаля. Одноразовые цифровые подписи.

13. Протоколы распределения ключей. Передача ключей с использованием симметричного шифрования. Двусторонние протоколы. Трехсторонние протоколы. Передача ключей с использованием асимметричного шифрования. Протоколы без использования цифровой подписи. Протоколы с использованием цифровой подписи. Сертификаты открытых ключей. Открытое распределение ключей. Предварительное распределение ключей. Схемы предварительного распределения ключей в сети связи. Схемы разделения секрета. Способы установления ключей для конференцсвязи. Возможные атаки на протоколы распределения ключей.

14. Управление ключами. Жизненный цикл ключей. Услуги, предоставляемые доверенной третьей стороной. Установка временных меток. Нотаризация цифровых подписей.

15. Некоторые практические аспекты использования шифрсистем. Анализ потока сообщений. Ошибки операторов. Физические и

организационные меры при использовании шифрсистем. Квантово-криптографический протокол открытого распределения ключей. Квантовый канал и его свойства. Протокол открытого распределения ключей.

Дисциплина «Элементы средств защиты информации»

Тема: защита информации компьютерных систем

Подтемы:

1. Компьютерная система (КС). Основные понятия. Электронный документ (ЭД). Виды информации в КС.
2. Уязвимость компьютерных систем. Понятие доступа, субъект и объект доступа. Понятие несанкционированного доступа (НСД). Классы и виды НСД.
3. Политика безопасности в компьютерных системах. Понятие политики безопасности и её основные базовые представления. Оценка защищенности
4. Идентификация пользователей КС-субъектов доступа к данным. Задача идентификации пользователя. Понятие протокола идентификации. Понятие идентифицирующей информации
5. Средства и методы ограничения доступа к файлам. Основные подходы к защите данных от НСД. Способы фиксации фактов доступа. Журналы доступа.
6. Доступ к данным со стороны процесса. Особенности защиты данных от изменения. Надежность систем ограничения доступа. Подход на основе формирования хэш-функции, требования к построению и способы реализации.
7. Программно-аппаратные средства шифрования. Построение программно-аппаратных комплексов шифрования. Проектирование модулей криптопреобразований на основе сигнальных процессоров.
8. Методы и средства ограничения доступа к компонентам ЭВМ. Компоненты ПЭВМ. Классификация защищаемых компонент ПЭВМ: отчуждаемые и неотчуждаемые компоненты ПЭВМ.
9. Защита программ от несанкционированного копирования. Подходы к задаче защиты от копирования. Привязка ПО к аппаратному окружению и физическим носителям как единственное средство защиты от копирования ПО.
10. Хранения ключевой информации. Пароли и ключи. Секретная информация, используемая для контроля доступа: ключи и пароли.
11. Управление криптографическими ключами. Генерация ключей. Распределение ключей.
12. Протокол аутентификации распределения ключей для симметричных криптосистем. Основные понятия и определения, типы криптографических протоколов, примеры.
13. Протокол для ассиметричных криптосистем с использованием сертификатов открытых ключей.

14. Организация хранения ключей (с примерами реализации). Магнитные диски прямого доступа. Магнитные и интеллектуальные. Средство TouchMemory.

15. Защита программ от изучения. Изучение и обратное проектирование ПО. Цели и задачи изучения работы ПО. Способы изучения ПО: статическое и динамическое изучение.

III. Список использованных источников

Основная:

1. Дискретная математика для программистов Хаггарти Р. Изд. Техносфера. М: 2012, 400 с.
2. CryptoSchool. Joachim von zur Gathen. Springer; 1st ed. 2015 edition.888 pages;
3. Goutam Paul , Subhamoy Maitra. Publisher.RC4 Stream Cipher and Its Variants (Discrete Mathematics and Its Applications). : CRC Press; 1st edition 2019. 311 pages.
4. С.А. Абрамов Элементы компьютерной алгебры линейных обыкновенных дифференциальных, разностных и q-разностных операторов М: МЦМНО 2012 126с.
5. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черёмушкин А.В. Основы криптографии. М.: Гелиос АРВ, 2002. 2-е изд.
6. Кнут Д. Искусство программирования. Т. 2. Получисленные алгоритмы. Вильямс: М. – СПб. – Киев, 2000. 3-е издание.
7. Michael E. Whitman, Herbert J. Mattord. Principles of Information Security. Cengage Learning; 6th edition, 2017, 656 pages
8. Richard E. Smith Elementary Information Security. Jones & Bartlett Learning; 3rd edition, 2019. 708 pages
9. David Kim (Author), Michael G. Solomon. Fundamentals of Information Systems Security. Jones & Bartlett Learning; 3rd edition,2016. 548 pages
10. Е.В. Вострецова, Основы информационной безопасности, Екатеринбург, 2019 г., 208с.
11. Ш.Парасрам, А.Замм, Т.Хериянто, Ш.Али, "Kali Linux. Тестирование на проникновение и безопасность", Питер, 2020 г., 448 с.
12. Alan Grid, "Cybersecurity. Learn Information Technology Security: How To Protect Your Electronic Data From Hacker Attacks While You Are Browsing The Internet With Your Smart Devices, Pc Or Television", Via Etenea LTD, 2020, 126 p.
13. Яворски Питер, «Ловушка для багов. Полевое руководство по веб-хакингу», Питер, 2020., 272 с.
14. Шелухин О.И., Сакалема Д.Ж., Филинова А.С., "Обнаружение вторжений в компьютерные сети (сетевые аномалии)", 2018 г., 220 с.
15. В. Ф. Шаньгин, "Информационная безопасность и защита информации", ДМК Пресс, 2017 г., 702 с.
16. А. А. Бирюков, "Информационная безопасность. Защита и нападение", ДМК Пресс, 2017г., 434 с.

Дополнительная:

1. Michael E. Whitman, Herbert J. Mattord. Principles of Information Security.Cengage Learning; 6th edition, 2017, 656 pages

2. Richard E. Smith Elementary Information Security. Jones & Bartlett Learning; 3rd edition, 2019. 708 pages

3. 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 – 784 с.

4. Анохин М.И., Варновский Н.П., Сидельников В.М., Ященко В.В. Криптография в банковском деле. М.: МИФИ, 1997.

5. Brij Gupta, Gregorio Martinez Perez, Dharma P. Agrawal, Deepak Gupta. Handbook Of Computer Networks And Cyber Security: Principles And Paradigms. Springer, 2020 – p. 957.

6. Aboul Ella Hassanien, Mohamed Elhoseny. Cybersecurity and Secure Information Systems: hallenges and Solutions in Smart Environments. Advanced Sciences and Technologies for Security Applications. Springer International Publishing, 1st ed., 2019 – p. 320.

7. Виноградов И.М. Основы теории чисел. М.: Наука, 1972.

8. Столлингс В. Криптография и защита сетей: принципы и практика, 2-е изд. – М.: Вильямс, 2001. – 672 с.

9. Kutub Thakur, Al-Sakib Khan Pathan. Cybersecurity Fundamentals: A Real-World Perspective. CRC Press. 2020 – p. 305

10. RC4 Stream Cipher and Its Variants (Discrete Mathematics and Its Applications). Goutam Paul , Subhamoy Maitra. Publisher : CRC Press; 1st edition 2019. 311 pages

11. С.А.Абрамов Элементы компьютерной алгебры линейных обыкновенных дифференциальных, разностных и q-разностных операторов М: МЦМНО 2012 126с.

12. Нечаев В.И. Элементы криптографии (Основы теории защиты информации) / Под ред. В.А. Садовничего. – М.: Высшая школа, 1999. – 109 с.

13. 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 – 784 с.