Федеральное государственное бюджетное образовательное

учреждение высшего образования

Московский государственный университет имени М.В. Ломоносова

Факультет вычислительной математики и кибернетики

**УТВЕРЖДАЮ**

декан факультета вычислительной математики и кибернетики

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_/И.А. Соколов /**

**«\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_20\_\_\_г.**

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ**

**Наименование дисциплины:**

**Элементы криптографического анализа**

**Уровень высшего образования:**

**бакалавриат**

**Направление подготовки / специальность:**

**01.03.02 «Прикладная математика и информатика» (3++)**

**Направленность (профиль):**

**Математические методы обработки информации и принятия решений**

**Форма обучения:**

**очная**

**Москва 2023**

Рабочая программа дисциплины (модуля) разработана в соответствии с самостоятельно установленным МГУ образовательным стандартом (ОС МГУ) для реализуемых основных профессиональных образовательных программ высшего образования по направлению подготовки 01.03.02, 01.04.02 "Прикладная математика и информатика" программы бакалавриата Утвержден приказом МГУ от 30 августа 2019 года № 1041 (в редакции приказов МГУ от 11 сентября 2019 года № 1109, от 10 июня 2021 года № 609, от 7 октября 2021 года № 1048, от 21 декабря 2021 года № 1404, от 2 ноября 2022 года № 1299)

**1.** Дисциплина относится к вариативной части ОПОП ВО.

**2.** Входные требования для освоения дисциплины (модуля): учащиеся должны владеть знаниями по математическому анализу, теории вероятностей и математической статистике, дискретной математики в объеме, соответствующем программам первого и второго года обучения основных образовательных программ бакалавриата по укрупненным группам направлений и специальностей 01.00.00 «Математика и механика», 02.00.00 «Компьютерные и информационные науки».

**3.** Результаты обучения по дисциплине (модулю), соотнесенные с требуемыми компетенциями выпускников*.*

Компетенции выпускников, частично формируемые при реализации дисциплины (модуля):

* **ОПК-2.Б** Способность применять и модифицировать математические модели, а также интерпретировать полученные математические результаты при решения задач в области профессиональной деятельности
* **ОПК-3.Б** Способность решать задачи в области прикладной математики и информатики с использованием современных информационных технологий, учитывая основные требования информационной безопасности
* **ПК-2.Б** Способность понимать и применять в научно-исследовательской деятельности современный математический аппара**т**

Планируемые результаты обучения по дисциплине (модулю):

**Знать:**

1. основные виды шифров;
2. основные методы анализа криптоалгоритмов;
3. основные факты по системам с открытым ключом;
4. основные криптопротоколы.

**Уметь:**

1. применять на практике полученные знания к исследованию простых шифров;
2. строить и изучать математические модели криптоалгоритмов;
3. решать основные задачи по применению криптографических алгоритмов в защите информации.

**Владеть:**

1. навыками употребления отечественной терминологии в области криптографии для выражения количественных и качественных требований по защите информации;
2. навыками использования математического аппарата в проведении исследований;
3. навыками пользования библиотеками прикладных программ для ЭВМ для решения прикладных задач.)

**4.** Формат обучения: занятия проводятся с использованием меловой или маркерной доски, интерактивные материалы демонстрируются с помощью ноутбука и проектора.

**5.** Объем дисциплины (модуля) составляет 2 з.е., в том числе 36 академических часа, отведенных на контактную работу обучающихся с преподавателем, 36 академических часов на самостоятельную работу обучающихся.

**6.** Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием отведенного на них количества академических часов и виды учебных занятий.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Наименование и краткое содержание разделов и тем дисциплины (модуля),**  **Форма промежуточной аттестации по дисциплине (модулю)** | **Всего**  **(часы**) | В том числе | | | |
| **Контактная работа  (работа во взаимодействии с преподавателем)**  **Виды контактной работы, часы** | | | **Самостоятельная работа обучающегося,**  **часы** |
| Занятия лекционного типа\* | Занятия семинарского типа\* | **Всего** |  |
| 1. Основные понятия криптографии (определение и примеры шифров (алгоритмы DES, ГОСТ 3412-2015, гаммирования, предположения об исходных условиях криптоанализа , понятия теоретическая и практическая стойкость шифров). | **5** | 4 | 0 | **4** | **1** |
| 1. Текущий контроль успеваемости: контрольная работа № 1 | **2** | 0 | 0 | **0** | **2** |
| 1. Универсальные методы криптоанализа. Метод тотального опробования ключей. Математическое ожидание числа опробований при случайном и равновероятном выборе ключа. Неравновероятный выбор ключей и его учет при переборе ключей. Распараллеливание при тотальном переборе ключей. Метод “вирусов”. “Китайская лотерея”. | **5** | 4 | 0 | **4** | **1** |
| 1. Методы анализа шифралгоритмов, реализующих линейные преобразования. Методы анализа, сводящиеся к решению линейных систем уравнений. Сложность решения линейных систем методом Гаусса. | **5** | 4 | 0 | **4** | **1** |
| 1. Метод “встреча посередине”. Оценка сложности метода. Условия, когда метод дает оценку числа опробований, равную корню из числа всех ключей. Метод криптоанализа “разделяй и побеждай”. Оценка сложности метода. Атака с помощью метода “разделяй и побеждай” на двойной DES. Условия, при которых сокращение вариантов опробования ключей при использовании данного метода оценивается корнем из числа всех ключей. | **5** | 4 | 0 | **4** | **1** |
| 1. Методы криптоанализа при неравновероятной гамме. Расстояние единственности, 1 и 2 теоремы Шеннона. Методы криптоанализа при повторе гаммы. Оценка времени ожидания перекрытия гаммы. | **5** | 4 | 0 | **4** | **1** |
| 1. Корреляционный метод криптоанализа. Статистические модели. | **4** | 2 | 0 | **2** | **2** |
| 1. Текущий контроль успеваемости: контрольная работа № 2. | **2** | 0 | 0 | **0** | **2** |
| 1. Линейный криптоанализ блочных шифров. Метод Мацуи для анализа DES. Дифференциальный криптоанализ блочных шифров. | **5** | 4 | 0 | **4** | **1** |
| 1. Текущий контроль успеваемости: контрольная работа № 3. | **3** | 0 | 0 | **0** | **3** |
| 1. Метод коллизий при анализе функций хэширования. Оценка трудоемкости метода. | **3** | 2 | 0 | **2** | **1** |
| 1. Анализ схем шифрования, использующих многократно один блочный шифр. Атака на тройной DES с помощью линейного криптоанализа. Техника атаки на тройной DES, основанная на задаче о днях рождения. | **5** | 4 | 0 | **4** | **1** |
| 1. Методы анализа систем с открытым ключом. Схема RSA. Атаки на RSA. Система Диффи и Хелмана. Атаки на систему Диффи и Хелмана. Криптопротоколы. Схема шифрования ElGamal. Подпись ElGamal. Схемы идентификации и распределения ключей. | **5** | 4 | 0 | **4** | **1** |
| Промежуточная аттестация: устный экзамен | **18** | 0 | 0 | **0** | **18** |
| **Итого** | **72** | **36** | **0** | **36** | **36** |

7. Фонд оценочных средств (ФОС) для оценивания результатов обучения по дисциплине (модулю)

7.1. Типовые контрольные задания или иные материалы для проведения текущего контроля успеваемости.

|  |
| --- |
| Контрольная работа № 1 |
| Вариант 1 |
| 1. Дешифровать шифр простой замены, найти ключ и открытый текст:  18 32 33 64 33 23 61 18 76 94 18 61 33 64 94 13 39 35 85 94 32 13 32 01 39 13 18 76 61 97 32 33 39 94 01 39 61 39 94 61 35 85 94 64 13 76 32 01 39 65 18 58 61 97 76 19 76 76 61 18 61 64 13 39 13 38 73 33 94 91 61 23 33 73 33 33 32 61 13 39 13 15 33 97 01 76 94 64 13 23 01 27 76 32 01 11 97 33 64 61 27 35 85 94 39 01 32 94 33 91 45 01 39 61 85 33 15 65 97 13 23 39 13 35 18 13 94 09 18 33 23 58 61 91 39 01 32 33 18 35 85 94 81 23 09 17 33 18 01 73 39 33 97 33 18 76 32 13 35 32 13 97 01 94 48 32 11 33 94 19 91 45 85 33 94 33 97 65 35 85 94 48 94 33 18 33 23 58 61 91 39 01 32 01 01 73 39 33 97 45 91 23 13 73 33 85 33 23 65 48 39 33 85 64 33 28 01 18 13 23 01 91 33 32 33 91 33 32 76 23 38 15 09 97 01 35 85 94 13 33 94 81 23 09 17 33 18 33 76 94 13 23 01 76 09 97 39 33 73 33 48 01 76 23 61 39 39 45 61 01 65 91 61 15 01 94 61 23 09 39 45 61 76 18 01 15 61 94 61 23 09 76 94 18 13 01 11 76 65 56 61 76 94 18 33 18 13 39 01 19 94 48 32 01 33 85 13 64 13 23 23 61 23 09 39 45 11 97 01 64 13 11 91 45 23 33 15 33 76 94 33 18 61 64 39 33 01 35 18 61 76 94 39 33 35 85 94 48 94 33 94 13 32 33 18 45 61 76 65 56 61 76 94 18 65 38 94 35 85 94 01 94 33 97 65 01 97 61 23 01 76 09 39 13 73 23 19 15 39 45 61 15 33 32 13 35 13 94 61 23 09 76 94 18 13 35 85 94 94 13 32 39 13 35 45 18 13 61 97 45 61 85 61 64 61 76 61 23 61 39 42 45  2. Дешифровать шифр вертикальной перестановки, найти ключ и открытый текст:  **МНТОЮ НСЧЛА ЕОАГН АВЕЖИ АММГЕ ЕУСЕА НИУСЩ АТЕНЛ НОЬЯМ ВТЛНН ЛЛНОО КОРУР ДПОКР РМЯЕЧ ССМОА ЛИНЕГ МААРГ СНТЕП ЕДЕГА ИНРОН ЫММЕЕ ХАУЦО ТОРОЦ ШАЯСИ** |
| Контрольная работа № 2 |
| Вариант 1 |
| 1. Провести полный расчет корреляционного метода 2. Применяя корреляционный метод найти начальное заполнение линейного регистра сдвига.   **схема.jpg**  **z** = 0010110000101011101010001111110 |
| Контрольная работа № 3 |
| Вариант 1 |
| 1. Построить редуцированный в 4 раза алгоритм DES без начальной и конечной перестановок (по аналогии с полным алгоритмом):  число раундов 4, входной блок - 16 бит, длина ключа – 12 бит; блок шифртекста – 16 бит;  функция усложнения: функция расширения (по аналогии с функцией расширения полного DES), 2 S-бокса (S-бокс: 6 бит вход, 4 бит выход, включает 4 самостоятельно придуманные перестановки), перестановка (также самостоятельно придуманная);  алгоритм генерации подключей строить не надо.  2. Построить линейный статаналог каждого из 2-х S-боксов.  3. Построить линейный статаналог одного раунда редуцированного DES  4. Построить линейный статаналог 4-х раундового редуцированного DES. |

**Вопросы к экзамену**.

1. Определение шифра, понятие стойкости, предположения об исходных условиях криптоанализа однонаправленные функции, криптосистемы с открытым ключом, функции хэширования.
2. Классические шифры. Шифры гаммирования и колонной замены, современные системы шифрования (симметрические и асимметрические). Алгоритмы DES, ГОСТ 3412-2015, гаммирования.
3. Метод тотального опробования ключей. Математическое ожидание числа опробований при случайном и равновероятном выборе ключа. Неравновероятный выбор ключей и его учет при переборе ключей. Распараллеливание при тотальном переборе ключей. Метод “вирусов”. “Китайская лотерея”.
4. Методы анализа шифралгоритмов, реализующих линейные преобразования.
5. Методы анализа, сводящиеся к решению линейных систем уравнений. Сложность решения линейных систем методом Гаусса.
6. Метод “встреча по середине”. Оценка сложности метода. Условия, когда метод дает оценку числа опробований, равную корню из числа всех ключей.
7. Метод криптоанализа “разделяй и побеждай”. Оценка сложности метода. Атака с помощью метода “разделяй и побеждай” на двойной DES. Условия, при которых сокращение вариантов опробования ключей при использовании данного метода оценивается корнем из числа всех ключей.
8. Методы криптоанализа при неравновероятной гамме. Расстояние единственности, 1 и 2 теоремы Шеннона.
9. Методы криптоанализа при повторе гаммы. Оценка времени ожидания перекрытия гаммы.
10. Корреляционный метод криптоанализа. Статистические модели.
11. Линейный криптоанализ блочных шифров. Метод Мацуи для анализа DES.
12. Дифференциальный криптоанализ блочных шифров.
13. Метод коллизий при анализе функций хэширования. Оценка трудоемкости метода.
14. Анализ схем шифрования, использующих многократно один блочный шифр.
15. Атака на тройной DES с помощью линейного криптоанализа. Техника атаки на тройной DES, основанная на задаче о днях рождения.
16. Методы анализа генераторов псевдослучайных чисел.
17. Схема RSA. Атаки на RSA. Система Диффи и Хелмана. Атаки на систему Диффи и Хелмана.
18. Схема шифрования ElGamal. Подпись ElGamal. Схемы идентификации и распределения ключей.

**Экзаменационный билет** состоит из двух вопросов и задачи, например

1. Метод тотального опробования ключей. Математическое ожидание числа опробований при случайном и равновероятном выборе ключа.
2. Методы криптоанализа при неравновероятной гамме. 1 теорема Шеннона.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ШКАЛА И КРИТЕРИИ ОЦЕНИВАНИЯ результатов обучения (РО) по дисциплине (модулю)** | | | | |
| Оценка  РО и соответствующие виды оценочных средств | 2 | 3 | 4 | 5 |
| **Знания**  *Экзамен* | Отсутствие знаний | Фрагментарные знания | Общие, но не структурированные знания | Сформированные систематические знания |
| **Умения**  *Контрольная работа* | Отсутствие умений | В целом успешное, но не систематическое умение | В целом успешное, но содержащее отдельные пробелы умение (допускает неточности непринципиального характера) | Успешное и систематическое умение |
| **Навыки  (владения, опыт деятельности)**  *Экзамен* | Отсутствие навыков (владений, опыта) | Наличие отдельных навыков (наличие фрагментарного опыта) | В целом, сформированные навыки (владения), но используемые не в активной форме | Сформированные навыки (владения), применяемые при решении задач |

|  |  |
| --- | --- |
| **Соответствие результатов обучения и компетенций, в развитии которых участвует дисциплина (модуль)** | |
| Результаты обучения | Компетенция, с частичным формированием которой связано достижение результата обучения |
| **Знать:**   1. основные виды шифров; 2. основные методы анализа криптоалгоритмов; 3. основные факты по системам с открытым ключом; 4. основные криптопротоколы.   **Уметь:**   1. применять на практике полученные знания к исследованию простых шифров; 2. строить и изучать математические модели криптоалгоритмов; 3. решать основные задачи по применению криптографических алгоритмов в защите информации.   **Владеть:**   1. навыками использования основных методов криптоанализа; | ОПК-2.Б |
| **Знать:**   1. методологию криптоанализа основных типов шифров; 2. основы теории оценки стойкости шифров; 3. классификацию методов оценки стойкости шифров;   **Уметь:**   1. применять методы оценки стойкости шифров;   **Владеть:**   1. навыками применения методов анализа простых шифров; | ОПК-3.Б |
| **Владеть:**   1. навыками использования криптографии в практических задачах; | ПК-2.Б |

8. Ресурсное обеспечение:

Основная литература:

1. Грушо А.А., Применко Э.А., Тимонина Е.Е. Теоретические основы компьютерной безопасности. Учебное пособие. М.: Академия, 2009.
2. Лапонина О.Р. Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия. Курс лекций. Учебное пособие. М.: Интернет Ун-т Информ. Технологий, 2005.
3. Столлингс В. Криптография и защита сетей. Принципы и практика, 2-е издание. М.: издательский дом «Вильямс», 2001.
4. Шеннон К. Работы по теории информатики и кибернетики. М.: Иностранная литература, 1963.

Дополнительная литература:

1. Menzes A., van Oorschot P., Vanstone S. Hadbook of Applied Cryptography, CRC Press, 1997.

Информационные справочные системы: <https://www.schneier.com/academic/>

Материально-техническое обеспечение: аудитория с партами, меловой или маркерной доской.

9. Язык преподавания - русский.

10. Преподаватели: профессор факультета ВМК МГУ, д.ф.-м.н., проф. А.А. Грушо,

доцент факультета ВМК МГУ, д.т.н., проф. Е.Е. Тимонина.

11. Авторы программы: профессора факультета ВМК МГУ Е.Е. Тимонина, А.А. Грушо.