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:**

**Кода аутентификации и хэш-функции**

**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 подискретной математике, алгебре, теории вероятностей и математической статистике, и специальными курсамив объеме, соответствующем программе третьего 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):

* **СПК-КАХФ-1.Б.**Способность применять знания об основных подходах к криптоанализу кодов аутентификации и хэш-функций, иметь представление о современных стандартах и методах синтеза кодов аутентификации и хэш-функций, иметь навык работы со статьями по теме курса, а также уметь использовать ЭВМ для решения прикладных задач.

Планируемые результаты обучения по дисциплине (модулю):

**Знать:**

1. основные конструкции кодов аутентификации;
2. основные методы криптоанализа кодов аутентификации;
3. основные конструкции хэш-функций;
4. основные методы криптоанализа хэш-функций.

**Уметь:**

1. применять на практике полученные знания к исследованию различных кодов аутентификации и хэш-функций;
2. строить и изучать математические модели криптоалгоритмов, используемых в их криптоанализе;
3. решать основные задачи по применению криптографическихалгоритмов в защите информации;
4. понимать и применять на практике математические методы для решения различных задач криптографического анализа;
5. находить, анализировать и обрабатывать научно-техническую информацию;
6. извлекать полезную научно-техническую информацию из электронных библиотек, реферативных журналов;
7. демонстрировать способность к анализу и синтезу;
8. демонстрировать способность к письменному и устному общению на русском языке.

**Владеть:**

1. навыками употребления отечественной терминологии в области криптографии для выражения количественных и качественных требований по защите информации;
2. использования математического аппарата в проведении исследований;
3. 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. Вопросы синтеза хэш-функций, основные конструкции хэш-функций. | **9** | 9 |  | **9** | **0** |
| 1. Текущий контроль успеваемости: практическое задание №1. | **6** | 0 |  | **0** | **6** |
| 1. Основные методы криптоанализа хэш-функций. | **9** | 9 |  | **9** | **0** |
| 1. Текущий контроль успеваемости: практическое задание №2. | **6** | 0 |  | **0** | **6** |
| 1. Вопросы синтеза кодов аутентификации, основные конструкции кодов аутентификации. | **9** | 9 |  | **9** | **0** |
| 1. Текущий контроль успеваемости: практическое задание №3. | **6** | 0 |  | **0** | **6** |
| 1. Основные методы анализа кодов аутентификации. | **9** | 9 |  | **9** | **0** |
| 1. Текущий контроль успеваемости: практическое задание №4. | **6** | 0 |  | **0** | **6** |
| Аттестация: экзамен | **12** | 0 |  | **0** | **12** |
| **Итого** | **72** | 36 |  | **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.

Практическое задание № 1

Реализовать на одном из языков программированияC, C++, Pythonалгоритм нахождения прообраза итерационной хэш-функции MD2.

Практическое задание № 2

Выявитьсреди функций сжатия вида , где , , нестойкие к атакам: прямая, перестановочная, направленная вперед, направленная назад, неподвижные точки.

Практическое задание №3

Реализовать на одном из языков программирования C, C++, Pythonалгоритм нахождения коллизии функции сжатия ГОСТ Р 34.11-94.

Практическое задание № 4

Применить знания, полученные в области кодов аутентификации для решенияряда задач.

Пример задач:

1. Построить атаку на код аутентификации, который задается как , где , , *F* – псевдослучайная функция.
2. Построить атаку на CBC-MACв случае, когда алгоритм выдает, помимо итогового, каждый промежуточный код, но проверяющий верифицирует только итоговый.

Примеры самостоятельных работ.

1. a. Подделать подпись RSA (то есть по заданному открытому ключу *e* построить валидную пару сообщение-подпись без знания секретного ключа *d*). Возможна ли данная атака при замене сообщения на ?

b. Для алгоритма RSAпо двум известным парамсообщение-подписьпостроить новую валидную пару. Возможна ли данная атака при замене сообщения на ?

1. Применить парадокс днейрождений, моделируемый однородной схемой размещения шаров по ящикам, для поиска коллизий хэш-функции.
2. Для итерационной хэш-функции*h*, функция сжатия которой имеет вид где блоковая переменная, переменная сцепления, *V* — константа, некоторый блочный шифр, причем предложить атаку, реализующую одну из стандартных угроз (нахождение коллизий, прообраза, второго прообраза) для *h* быстрее, чем общие атаки.
3. Используя свойство комплементарности, построить коллизию итерационной хэш-функции
4. Применить ро-метод Полларда для поиска коллизии хэш-функции с функцией сжатия и начальным значением
5. Привести пример ортогонального массива .
6. Построить атаку на CBC-MAC без завершающего преобразования.
7. Построить пример нестойкой схемы AEAD, построенной по принципу E&M.

7.2. Типовые контрольные задания или иные материалы для проведения промежуточной аттестации.

Вопросы к экзамену.

1. Определение хэш-функции, криптографические требования к хэш-функциям. Основные приложения криптографических хэш-функций, вывод криптографических требований к хэш-функциям из требований стойкости этих приложений.
2. Правила дополнения исходного сообщения.Итерационная (последовательная) структура.
3. Структура Меркла-Дамгарда, структура HAIFA (HAshIterativeFrAmework), древовидная структура, структура типа «губка».
4. Задача о днях рождения. Однородная и неоднородная схемы размещения шаров по ящикам. Оценки вероятности попадания двух и более шаров в один ящик для однородной схемы.
5. Угадывание прообраза. Поиск коллизий, моделируемый однородной и неоднородной (атака Ювала) схемами размещения шаров по ящикам. Оценка вероятности успеха этих атак. Уточненное определение криптографической хэш-функции.
6. Атака типа «встреча посередине», атака корректировкой блока, использование неподвижных точек. Необходимые условия на функцию сжатия.
7. Атаки на функции сжатия на базе блочного алгоритма шифрования DES. Использование свойства комплементарности ключей, наличия слабых и полуслабых ключей, коллизий ключей и неподвижных точек блочного шифра.
8. Функции сжатия вида , где , , . Выявление нестойких функций сжатия к атакам: прямая, перестановочная, направленная вперед, направленная назад, неподвижные точки.
9. Схема Фейстеля. Утверждение о композиции схем Фейстеля и обратимости. Шифр , выражение блочного шифра ГОСТ 28147-89 через . Построение симметричных неподвижных точек шифра ГОСТ 28147-89 с линейными ограничениями на ключ.
10. Описание процедуры MD-усиления, структуры и функции сжатия для хэш-функции ГОСТ Р 34.11-94. Применение направленной назад атаки к упрощенному варианту хэш-функции ГОСТ Р 34.11-94.
11. Формулировка обобщенной задачи о днях рождения (GBP). Оценка трудоемкости алгоритма Вагнера для решения GBP на примере 4 списков (с выводом). Оценка трудоемкости алгоритма Вагнера в общем случае (без вывода).
12. Сведение задачи поиска коллизий для функции сжатия ГОСТ Р 34.11-94 к поиску неподвижных точек блочного шифра ГОСТ 28147-89, оценка трудоемкости. Построение мультиколлизии из простых коллизий функции сжатия. Мультиколлизии для хэш-функции ГОСТ Р 34.11-94 без контрольной суммы. Применение алгоритма Вагнера для GBP к построению коллизий полной хэш-функции ГОСТ Р 34.11-94. Оценка трудоемкости метода.
13. Понятие о дифференциальном криптанализе.Пример применения методов дифференциального криптоанализа для поиска коллизий у хэш-функции N-hash.
14. Ро-метод Полларда для построения коллизий хэш-функций. Задача поиска коллизий двух хэш-функций и ее решение.
15. Описание процедуры MD-усиления, итерационной структуры и функции сжатия для хэш-функции ГОСТ Р 34.11-2012 (Стрибог-256 и Стрибог-512).
16. Определение кода аутентификации (теоретико-информационный подход). Требования к кодам аутентификации. Атаки имитации и подмены. Вероятности успешной имитации и подмены, их свойства. Оптимальные коды аутентификации.
17. Определение ортогонального массива . Лемма о простейших свойствах ортогональных массивов. Теорема о связи параметров ортогонального массива . Пример ортогонального массива . Теорема о связи параметров ортогонального массива . Пример ортогонального массива .
18. Теорема Стинсона о связи ортогональных массивов с оптимальными кодами аутентификации. Теорем Стинсона о связи ортогональных массивов с оптимальными кодами аутентификации.
19. Понятия псевдослучайной функции (PRF) и псевдослучайной подстановки (PRP). Определения стойких PRF и PRP. Примеры стойких PRP с практической точки зрения. Формулировка переключающей леммы. Контрпример к переключающей лемме в случае, когда область определения (область значений) функции мала.
20. Задача обеспечения целостности сообщения. Определение кода аутентификации сообщения (теоретико-сложностной подход). Модели угроз и их связи. Атака с выбором сообщения, осуществляющая универсальную подделку, экзистенциальную подделку, селективную подделку. Понятие стойкого кода аутентификации сообщения.
21. Формулировка теоремы о связи стойких PRF и стойких кодов аутентификации, идея доказательства. Контрпример к теореме в случае, когда область значений функции мала. Формулировка леммы об усечении множества значений стойкой PRF. Следствие из леммы для кодов аутентификации на основе PRF.
22. Конструкция кодов аутентификации CBC-MAC. Обоснование необходимости завершающего преобразования в CBC-MAC. Конструкция кодов аутентификации NMAC. Обоснование необходимости завершающего преобразования в NMAC. Формулировка теоремы о связи стойкости конструкций CBC-MAC и NMAC со стойкостью базовых функций PRP и PRF соответственно. Точность оценок из теоремы. Следствия для количества подписанных сообщений на одном ключе (примеры AES и 3DES). Рандомизированная конструкция CBC-MAC.
23. Конструкция кода аутентификации PMAC (параллелизуемый MAC). Формулировка теоремы о связи стойкости PMAC со стойкостью базовой PRF. Свойство быстрого обновления PMAC при изменении одного блока сообщения. Одноразовый код аутентификации сообщения, определение его стойкости. Пример одноразового кода аутентификации сообщения на основе полиномов. Конструкция кода аутентификации сообщения Картера-Вегмана на базе одноразового кода аутентификации сообщения и PRF. Формулировка теоремы о стойкости конструкции Картера-Вегмана.
24. Неудачный пример построения кода аутентификации сообщения на базе бесключевой хэш-функции. Конструкция кода аутентификации HMAC. Дополняющие правила при вычислении кода аутентификации длинного сообщения. Конструкция кода аутентификации CMAC.
25. Особенности реализации операции сравнения в библиотеке Keyczarcryptolibrary. Использование данной особенности в атаке на основе времени вычисления кода аутентификации сообщения. Два способа защиты от этой атаки.
26. Схемы обеспечения конфиденциальности и целостности (AEAD). Определение, основные использующиеся модели. Типы AEAD-схем:E&M, MtE, EtM,их стойкость.Определение схемы AEAD с одноразовым кодом. КонструкцииCCM и GCM.

Типовые задачи для экзамена.

1. Построить оптимальный код аутентификации с параметрами
2. Проверить криптографические свойства хэш-функции CRC-N.
3. Построить коллизию для упрощенной версии хэш-функции ГОСТ Р 34.11-94, у которой в дополняющем правиле отсутствует добавление блока с длиной исходного сообщения.
4. Построить атаку на код аутентификации, который задается как , где , , F – псевдослучайная функция, а означает представление числа *x*в виде -битной строки.

Экзаменационный билет состоит из одного вопросаи одной задачи по разным частям курса, например

1. Атака типа «встреча посередине», атака корректировкой блока, использование неподвижных точек. Необходимые условия на функцию сжатия.
2. Построить оптимальный код аутентификации с параметрами

или

1. Определение кода аутентификации (теоретико-информационный подход). Требования к кодам аутентификации. Атаки имитации и подмены. Вероятности успешной имитации и подмены, их свойства. Оптимальные коды аутентификации.
2. Проверить криптографические свойства хэш-функции CRC-N.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **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**  *Самостоятельные работы, практические задания* | 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 конструкции кодов аутентификации; 2. основные методы криптоанализа кодов аутентификации; 3. основные конструкции хэш-функций; 4. основные методы криптоанализа хэш-функций.   **Уметь:**   1. применять на практике полученные знания к исследованию различных кодов аутентификации и хэш-функций; 2. строить и изучать математические модели криптоалгоритмов, используемых в их криптоанализе; 3. решать основные задачи по применению криптографическихалгоритмов в защите информации; 4. понимать и применять на практике математические методы для решения различных задач криптографического анализа; 5. находить, анализировать и обрабатывать научно-техническую информацию; 6. извлекать полезную научно-техническую информацию из электронных библиотек, реферативных журналов; 7. демонстрировать способность к анализу и синтезу; 8. демонстрировать способность к письменному и устному общению на русском языке.   **Владеть:**   1. навыками употребления отечественной терминологии в области криптографии для выражения количественных и качественных требований по защите информации; 2. использования математического аппарата в проведении исследований; 3. пользования библиотеками прикладных программ для ЭВМ для решения прикладных задач. | СПК-КАХФ-1.Б |

8. Ресурсное обеспечение:

Основная литература:

1. Денисов А.М., Разгулин А.В. Обыкновенные дифференциальные уравнения. М.: Макс-ПРЕСС, 2009.
2. PreneelB. Analysis and Design of Cryptographic Hash Functions, PhD Thesis, 1993.
3. Государственный стандарт Союза ССР, Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования ГОСТ 28147-89, Москва: ИПК Издательство стандартов, 1990.
4. Государственный стандарт Российской Федерации, Информационная технология. Криптографическая защита информации. Функция хэширования, Москва: Госстандарт России, 1994.
5. MendelF., PramstallerN., RechbergerC., KontakM., SzmidtJ.Cryptanalysis of the GOST Hash Function, CRYPTO 2008, LNCS 5157, Springer, 2008, pp. 162-178.
6. WagnerD.A Generalized Birthday Problem, CRYPTO 2002, LNCS 2442, Springer, 2002, pp. 288-304.
7. JouxA.Multicollisions in Iterated Hash Functions. Application to Cascaded Constructions, Advances in Cryptology - CRYPTO 2004, Springer, 2004, pp. 306-315.
8. Национальный стандарт Российской Федерации, Информационная технология. Криптографическая защита информации. Функция хэширования, Москва: Госстандарт России, 2012.
9. БыковС. И. Предельные теоремы для рандомизированных разделимых статистик и их приложения. Дис. … кандидата физ.-мат.наук, М.: МИЭМ, 1991.
10. КолчинВ. Ф., СевастьяновБ. А., ЧистяковВ. П. Случайные размещения. М.: Наука, 1976.
11. BihamE., Dunkelman O. A Framework for Iterative Hash Functions – HAIFA, Cryptology ePrint Archive,<https://eprint.iacr.org/2007/278>.
12. Bertoni G., Daemen J., Peeters M., Van Assche G. Duplexing the Sponge: Single-Pass Authenticated Encryption and Other Applications, Areas in Cryptography, 2012, pp. 320-337.
13. Merkle. R.C. Secrecy, authentication, and public key systems. Stanford Ph.D. thesis, 1979, pp. 13-15.
14. Becker G. Merkle Signature Schemes, Merkle Trees and Their Cryptanalysis. Ruhr-UniversitätBochumPh.D. thesis, 2011, pp. 12-16.
15. FIPS 46, DataEncryptionStandart, FederalInformationProcessingStandard, NationalBureauofStandarts, U.S. DepartmentofCommerce, Washington D.C., January 1977 (revisedas FIPS 46-1:1988; FIPS 46-2:1993).
16. CrépeauC., BreauP.-W.CryptographyandDataSecurity, CourseinMcGillUniversity,<http://crypto.cs.mcgill.ca/~crepeau/CS547/BOOK/Theory10.pdf>.
17. BellareM., RogawayP. Introduction to modern cryptography, Lecture Notes, 2008.
18. BoneD. Review: PRPs and PRFs, Introduction to Cryptography, Course on coursera.com,<https://class.coursera.org/crypto-preview/lecture>.
19. BoneD. Message Authentication Codes, Introduction to Cryptography, Course on coursera.com,<https://class.coursera.org/crypto-preview/lecture>.
20. Bone D. MACs Based On PRFs, Introduction to Cryptography, Course on coursera.com,<https://class.coursera.org/crypto-preview/lecture>.
21. Bone D. CBC-MAC and NMAC, Introduction to Cryptography, Course on coursera.com,<https://class.coursera.org/crypto-preview/lecture>.
22. Bone D. MAC padding, Introduction to Cryptography, Course on coursera.com,<https://class.coursera.org/crypto-preview/lecture>.
23. Bone D. PMAC and the Carter-Wegman MAC, Introduction to Cryptography, Course on coursera.com,<https://class.coursera.org/crypto-preview/lecture>.
24. Bone D. HMAC, Introduction to Cryptography, Course on coursera.com,<https://class.coursera.org/crypto-preview/lecture>.
25. Bone D. Timing attacks on MAC verification, Introduction to Cryptography, Course on coursera.com,<https://class.coursera.org/crypto-preview/lecture>.

Дополнительнаялитература:

1. MenezesA. J., van OorschotP.C., VanstoneS. A. Handbook of applied cryptography(Discrete Mathematics and Its Applications), 5th edition, CRC Press, 2001.
2. ЧеремушкинА. В. Криптографические протоколы. Основные свойства и уязвимости, М: Издательский центр "Академия", 2009.
3. BakhtiariS., Safavi-NainiR., PieprzykJ. Cryptographic HashFunctions: A Survey, Technical Report 95-09, Department of ComputerScience, University of Wollongong, 1995.
4. StinsonD. R.Cryptography: Theory and Practice(Discrete Mathematics and Its Applications), 3d edition,Chapman and Hall/CRCPress, 2006.
5. Katz J., Lindell Y. Introduction to Modern Cryptography 2nd edition,Chapman and Hall/CRC Press, 2014.

Информационныесправочныесистемы: https://google.ru/

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

9. Язык преподавания - русский.

10. Преподаватели: В.В. Высоцкая.

11. Авторы программы: доцент факультета ВМК МГУ И.В. Чижов, В.В. Высоцкая.