МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«УЛЬЯНОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

ФАКУЛЬТЕТ МАТЕМАТИКИ, ИНФОРМАЦИОННЫХ
И АВИАЦИОННЫХ ТЕХНОЛОГИЙ
КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ТЕОРИИ УПРАВЛЕНИЯ

Рацеев С.М.

Методические указания для самостоятельной работы студентов по дисциплине «Методы и средства криптографической защиты информации»

для студентов специальностей
10.05.01 «Компьютерная безопасность» и
10.05.03 «Информационная безопасность автоматизированных систем»

Ульяновск
2022

Рацеев С.М. Методические указания для самостоятельной работы студентов по дисциплине «Методы и средства криптографической защиты информации» для студентов специальностей 10.05.01 «Компьютерная безопасность» и 10.05.03 «Информационная безопасность автоматизированных систем». – Ульяновск: УлГУ, 2022.

Методические указания рекомендованы к введению в образовательный процесс решением Ученого Совета ФМИАТ УлГУ (протокол № 3/22 от 19.04.2022 г.).

Тема 1. Шифры замены и перестановки

Основные вопросы темы:

Шифр простой замены. Шифр сдвига. Методы взлома данного шифра. Аффинный шифр и методы его взлома. Преобразование биграмм аффинным шифром. Шифр замены с конечным ключом. Шифр Виженера. Криптоанализ шифра Виженера. Многопетлевые подстановки. Аффинный блочный шифр. Шифр Холла. Криптоанализ аффинного блочного шифра. Табличное гаммирование. Модульное гаммирование. Шифр Вернама. Шифр пропорциональной замены (шифр омофонов). Маршрутные перестановки. Криптоанализ шифров.

Рекомендации по изучению темы:

Все вопросы изложены в главе 5 учебного пособия [2].

Контрольные вопросы:

1. Одноалфавитные шифры замены: шифр простой замены, шифр сдвига. Методы взлома данных шифров. 2. Одноалфавитные шифры замены: аффинный шифр, преобразование биграмм аффинным шифром. Мето-ды взлома данных шифров. 3. Многоалфавитные шифры замены. Шифр Виженера. Криптоанализ шифра Виженера. 4. Многоалфавитные шифры замены: многопетлевые подстановки, аффинный блочный шифр, шифр Хил-ла. Криптоанализ аффинного блочного шифра. 5. Многоалфавитные шифры замены: табличное гаммирование, модульное гаммирование. Шифр Вернама. 6. Многоалфавитные шифры замены. Шифр пропорциональной замены (шифр омофонов).

Задачи для самостоятельной работы:

1. Пусть $A = B = \{\text{а}, \text{б}, \text{в}, \text{г}, \text{д}, \text{е}, \text{ж}, \text{з}, \text{и}, \text{й}\}$. Зашифровать слово «забег» следующими шифрами: шифр простой замены, шифр сдвига.

2. Найти обратный к 27 по модулю 44.

3. В первом задании применить аффинный шифр.

4. В первом задании применить шифр Виженера.

5. Зашифровать слово «звезда» аффинным блочным шифром на ключе

$$A = \begin{pmatrix} 3 & 5 \\ 7 & 4 \end{pmatrix}, \quad B = \begin{pmatrix} 6 \\ 8 \end{pmatrix}.$$

Тема 2. Математические модели открытых текстов.

Основные вопросы темы:

Детерминированная модель открытого текста. Вероятностная модель независимых символов алфавита. Вероятностная модель независимых биграмм. Вероятностная модель марковски зависимых символов. Критерии распознавания открытых текстов. Критерий на основе проверки гипотезы с использованием леммы Неймана-Пирсона. Критерий на основе запретных m-грамм.

Рекомендации по изучению темы:

Все вопросы изложены в главе 4 учебного пособия [2].

Контрольные вопросы:

1. Детерминированная модель открытого текста. 2. Вероятностные модели открытого текста: модель независимых символов алфавита, модель независимых биграмм, модель марковски зависимых букв.

Тема 3. Математическая модель шифров

Основные вопросы темы:

Формальные модели шифров. Алгебраическая модель шифра. Вероятностная модель шифра. Математические модели некоторых шифров. Математическая модель шифра простой замены. Математическая модель шифра сдвига. Математическая модель шифра перестановки. Математическая модель аффинного шифра. Математическая модель шифра Хилла.

Рекомендации по изучению темы:

Все вопросы изложены в параграфах 6.1, 6.2 учебного пособия [2].

Контрольные вопросы:

1. Алгебраическая и вероятностная модели шифров. 2. Математическая модель некоторых шифров: шифр простой замены, шифр сдвига, аффинный шифр. 3. Математическая модель некоторых шифров: шифр замены с конечным ключом, шифр Виженера, шифр перестановки.

Задачи для самостоятельной работы:

1. Пусть Σ_B — шифр, определенный множествами

$$X = \{x_1, x_2\}, \quad K = \{k_1, k_2, k_3\}, \quad Y = \{y_1, y_2, y_3\},$$

матрицей зашифрования

$K \diagdown X$	x_1	x_2
k_1	y_1	y_2
k_2	y_2	y_3
k_3	y_3	y_2

и распределениями вероятностей $P(X)$, $P(K)$

X	x_1	x_2
$P(X)$	1/3	2/3

K	k_1	k_2	k_3
$P(K)$	1/7	2/7	4/7

Найти распределения вероятностей $P(Y)$, $P(Y|X)$.

Тема 4. Совершенные шифры.

Основные вопросы темы:

Определение совершенного по Шеннону шифра. Эквивалентные условия. Необходимые условия совершенного по Шеннону шифра. Достаточное условие совершенного по Шеннону шифра. Теорема Шеннона. Критерий совершенных шифров в классе шифров с равномерным распределением вероятностей на множестве ключей. Пример совершенного неэндоморфного шифра с равномерным распределением на множестве ключей. Пример совершенного эндоморфного шифра с неравномерным распределением на множестве ключей. $(k|y)$-совершенные шифры: определение, эквивалентные условия. Необходимые и достаточные условия

$(k|y)$-совершенных шифров. Необходимые и достаточные условия одновременно совершенных и $(k|y)$-совершенных шифров. Математические модели шифра замены с ограниченным и неограниченным ключом. Шифрвеличины и шифробозначения. Опорный шифр шифра замены. Степень опорного шифра. Случайный и детерминированный генераторы ключевого потока. Шифр замены с неограниченным ключом. Шифр замены с ограниченным ключом. Совершенные шифры замены. Определение совершенного шифра замены, эквивалентные условия. Несовершенность в общем случае шифра замены с ограниченным ключом. Достаточные условия совершенного шифра замены с неограниченным ключом. Критерий совершенности шифра замены с неограниченным ключом в классе эндоморфных шифров. Критерий совершенности шифра замены с неограниченным ключом в классе шифров с равномерным распределением на множестве ключей.

Рекомендации по изучению темы:

Все вопросы изложены в параграфах 6.4-6.8 учебного пособия [2].

Контрольные вопросы:

1. Определение совершенного по Шеннону шифра. Эквивалентные условия. Необходимые условия совершенного по Шеннону шифра. 2. Достаточное условие совершенного по Шеннону шифра. Теорема Шеннона. 3. Критерий совершенных шифров в классе шифров с равномерным распределением вероятностей на множестве ключей. 4. $(k|y)$-совершенные шифры: определение, эквивалентные условия. 5. Необходимые и достаточные условия $(k|y)$-совершенных шифров. Необходимые и достаточные условия одновременно совершенных и $(k|y)$-совершенных шифров. 6. Шифрвеличины и шифробозначения. Опорный шифр шифра замены. Степень опорного шифра. Случайный и детерминированный генераторы ключевого потока. 7. Шифр замены с неограниченным ключом. Шифр замены с ограниченным ключом. 8. Совершенные шифры замены. Определение совершенного шифра замены, эквивалентные условия. Несовершенность в общем случае шифра замены с ограниченным ключом. 9. Достаточные условия совершенного шифра замены с неограниченным ключом. 10. Критерий совершенности шифра замены с неограниченным ключом в классе эндоморфных шифров. 11. Критерий совершенности шифра замены с неограниченным ключом в классе шифров с равномерным распределением на множестве ключей.

Задачи для самостоятельной работы:

1. Построить пример совершенного неэндоморфного шифра с равномерным распределением на множестве ключей.

2. Построить пример совершенного эндоморфного шифра с неравномерным распределением на множестве ключей.

3. Построить пример совершенного неэндоморфного шифра с неравномерным распределением на множестве ключей.

4. Построить примеры совершенных шифров с условиями $|X| = |Y| = |K|$, $|X| < |Y| = |K|$, $|X| = |Y| < |K|$, $|X| < |Y| < |K|$.

5. Построить примеры (k|y)-совершенных шифров с условиями $|X| = |Y| >$

$|K|$, $|X| = |Y| = |K|$, $|X| = |Y| < |K|$.

6. Построить примеры одновременно совершенного и $(k|y)$-совершенного шифра с условиями $|X| = |Y| = |K|$, $|X| = |Y| < |K|$.

Тема 5. Вопросы имитостойкости шифров.

Основные вопросы темы:

Подмена шифрованного сообщения. Имитация шифрованного сообщения. Имитостойкость шифра. Нижние оценки вероятности имитации и подмены сообщения.

Рекомендации по изучению темы:

Все вопросы изложены в параграфах 6.9-6.11 учебного пособия [2].

Контрольные вопросы:

1. Понятие имитации сообщений. Определение вероятности P_{im}. Нижняя оценка для вероятности имитации сообщения. Критерий достижимости нижней оценки. 2. Понятие подмены сообщений. Определение вероятности P_{podm}. Нижняя оценка для вероятности подмены сообщения. Критерий достижимости нижней оценки. 3. Совершенные имитостойкие шифры замены с неограниченным ключом.

Задачи для самостоятельной работы:

1. Построить примеры шифров с достижимой нижней оценкой имитации сообщений.

2. Построить примеры шифров с достижимой нижней оценкой подмены сообщений.

Тема 6. Шифры, не распространяющие искажений.

Основные вопросы темы:

Шифры, не распространяющие искажений типа замены знаков. Метрика Хэмминга на открытых и шифрованных текстах. Определение шифра, не распространяющего искажений типа замены знаков. Эквивалентные условия шифра, не распространяющего искажений типа замены знаков. Понятие изометрии. Теорема А.А.Маркова. Шифры, не распространяющие искажений типа пропуска (вставки) знаков. Определение шифра, не распространяющего искажений типа пропуска знаков. Эквивалентные условия шифра, не распространяющего искажений типа пропуска знаков. Критерий шифра, не распространяющего искажений типа пропуска знаков, в классе эндоморфных шифров.

Рекомендации по изучению темы:

Все вопросы изложены в главе 7 учебного пособия [2].

Контрольные вопросы:

1. Шифры, не распространяющие искажений типа замены знаков: определение, эквивалентные условия. 2. Понятие изометрии. Свойства изометрий. 3. Теорема А.А.Маркова. Примеры шифров, не распространяющих искажения типа замены знаков. 4. Шифры, не распространяющие искажений типа пропуска знаков: основные понятия. 5. Критерий для шифров, не распространяющеих искажений типа пропуска знаков, в классе эндоморфных шифров. 6. Шифры, не распространяю-

щие искажений типа вставки знаков.

Тема 7. Пороговые схемы разделения секрета.

Основные вопросы темы:

Понятие (n, t)-пороговой схемы разделения секрета. Пример (n, n)-пороговой схемы. Схема разделения секрета на основе решения СЛАУ. Схема разделения секрета Шамира. Проверяемая схема разделения секрета Фельдмана-Шамира. Совершенная проверяемая схема разделения секрета Педерсона-Шамира. Схемы разделения секрета на основе n-разрядных равновесных двоичных кодов.

Рекомендации по изучению темы:

Все вопросы изложены в параграфе 13.1 учебного пособия [2].

Контрольные вопросы:

1. Понятие (n, t)-пороговой схемы разделения секрета. Пример (n, n)-пороговой схемы. Схема разделения секрета на основе решения СЛАУ. 2. Схема разделения секрета Шамира. 3. Проверяемая схема разделения секрета Фельдмана-Шамира. 4. Совершенная проверяемая схема разделения секрета Педерсона-Шамира. 5. Схемы разделения секрета на основе n-разрядных равновесных двоичных кодов.

Задачи для самостоятельной работы:

1. Найти многочлен Лагранжа степени 2 над кольцом вычетов по модулю 7, проходящий через следующие точки: $(1, 4), (3, 2), (6, 3)$.

2. Восстановить значение секрета s в схеме Шамира с порогом 3 над кольцом вычетов по модулю 13, если доли трех участников, пытающихся восстановить секрет, равны: $(2, 5), (4, 7), (7, 5)$.

Тема 8. Схемы разделения секрета с произвольной структурой доступа.

Основные вопросы темы:

Схемы разделения секрета для произвольных структур доступа: основные понятия. Схема Бенало-Лейхтера. Схема Ито-Саито-Нишизеки.

Рекомендации по изучению темы:

Все вопросы изложены в параграфе 13.2 учебного пособия [2].

Контрольные вопросы:

1. Схемы разделения секрета для произвольных структур доступа: основные понятия. 2. Схема Бенало-Лейхтера. 3. Схема Ито-Саито-Нишизеки.

Задачи для самостоятельной работы:

Схема Ито-Саито-Нишизеки. Пусть $P = \{1, 2, 3, 4, 5\}$ — участники разделения секрета s, (R, Z) — структура доступа на P, которая задается множеством минимальных правомочных коалиций $R_{min} = \{\{1, 2, 3, 4\}, \{3, 5\}, \{4, 5\}\}$. Найти множество максимальных непровомочных коалиций Z_{max} (выписать в лексикографическом порядке), кумулятивный массив C, а также разделить секрет $s = 5$ (выписать доли секрета для каждого участника).

Тема 9. Симметричные блочные шифры.

Основные вопросы темы:

Итеративные блочные шифры. Понятие раундовой функции, раундового ключа. Условия, обеспечивающие обратимость итеративного блочного шифра. Построение цикловой функции. Входное и выходное отображения. Слабые ключи итеративного блочного шифра. Определение шифра Фейстеля. Функция усложнения шифра Фейстеля. Условия, обеспечивающие обратимость шифра Фейстеля. Режимы использования блочных шифров. Режим электронной кодовой книги. Режим сцепления блоков. Режим гаммирования с обратной связью по шифртексту. Режим гаммирования. Режим выработки имитовставки. Свойства данных режимов. Примеры итеративных блочных шифров. Шифры "Магма" и "Кузнечик" из ГОСТ Р 34.12-2015.

Рекомендации по изучению темы:

Все вопросы изложены в главе 8 учебного пособия [2].

Контрольные вопросы:

1. Итеративные блочные шифры. Обратимость итеративного блочного шифра. 2. Шифры Фейстеля и их обратимость. 3. Построение раундовой функции. Входное и выходное отображения. 4. Режимы использования симметричных блочных шифров. 5. Шифр Магма из ГОСТ Р 34.12-2015.

Тема 10. Шифрование с открытым ключом.

Основные вопросы темы:

Задачи, приводящие к криптографии с открытым ключом. Понятие односторонней функции. Быстрое (бинарное) возведение в степень. Система Диффи-Хеллмана. Способы выбора образующего элемента. Криптосистема без передачи ключа (шифр Месси-Омуры). Шифр Эль-Гамаля. Ограничения на параметры системы. Шифр RSA. Понятие односторонней функции с «лазейкой». Описание шифра RSA. Ограничения на параметры системы. Рюкзачные системы. Описание «проблемы рюкзака». Система Меркла-Хеллмана на основе супервозрастающей последовательности.

Рекомендации по изучению темы:

Все вопросы изложены в главе 9 учебного пособия [2].

Контрольные вопросы:

1. Алгоритм быстрого возведения в степень. Схема Диффи-Хеллмана. 2. Криптосистема Месси-Омуры. Вероятностный шифр Эль-Гамаля. 3. Шифр RSA. Рюкзачные криптосистемы, система Меркла-Хеллмана.

Задачи для самостоятельной работы:

1. Вычислить, используя быстрые алгоритмы возведения в степень, $2^{11} \pmod{10}$, $3^{7} \pmod{10}$, $4^{71} \pmod{14}$, $3^{68} \pmod{100}$.

2. Используя теоремы Эйлера и Ферма, вычислить значения $3^{102} \pmod{11}$, $5^{40} \pmod{17}$, $3^{50} \pmod{21}$, $5^{34} \pmod{24}$.

3. Найти все допустимые варианты параметра g в системе Диффи-Хеллмана при $p = 29$.

4. Шифр Месси-Омуры. Пусть a_1, a_2 — пара секретных ключей абонента A, b_1, b_2 — пара секретных ключей абонента B, p — простое число, m — передаваемое

сообщение от A к B. Известно, что $p = 17$, $a_1 = 3$, $b_1 = 5$, $m = 6$. Найти a_2, b_2, m_1, m_2, m_3, m_4.

5. Шифр Эль-Гамаля. Пусть x, y — соответственно секретный и открытый ключи абонента A, p — простое число, g — первообразный корень по модулю p (параметры шифрсистемы), m — передаваемое сообщение абоненту A, k — случайное число. Известно, что $p = 13$, $g = 2$, $x = 5$, $k = 3$, $m = 10$. Найти y и шифрованное сообщение (c_1, c_2), передаваемое абоненту A.

6. Шифр RSA. Пусть e, d — соответственно секретный и открытый ключи абонента A, p, q — простые числа абонента A, m — передаваемое сообщение абоненту A. Известно, что $p = 5$, $q = 11$, $e = 3$, $m = 8$. Найти d и шифрованное сообщение y, передаваемое абоненту A.

Тема 11. Криптографические хеш-функции.

Основные вопросы темы:

Определение хеш-функции. Примеры хеш-функций. Целесообразность использования хеш-функций. Основные требования, которым должна удовлетворять хеш-функция. Зависимость данных требований друг от друга. Парадокс дней рождений. Построение хеш-функций. Примеры криптографических хеш-функций. Коды аутентификации. Основные понятия. Имитация и подмена для кода аутентификации. Нижние границы вероятностей имитации и подмены. Критерий достижимости нижних оценок. Оптимальные коды аутентификации. Ортогональные таблицы. Математическая модель кода аутентификации с неограниченным ключом. Примеры оптимальных кодов аутентификации с неограниченным ключом.

Рекомендации по изучению темы:

Все вопросы изложены в главах 10, 11 учебного пособия [2].

Контрольные вопросы:

1. Хеш-функции. Требования, предъявляемые к хеш-функциям. 2. Криптографические хеш-функции. Способы построения криптографических хеш-функций. 3. Понятие имитации и подмены кода аутентификации. Определение вероятностей Рим, Рподм. 4. Нижние оценки для вероятности имитации и подмены кода аутентификации. Критерий достижимости нижних оценок. 5. Оптимальные коды аутентификации. Достаточные условия оптимального кода аутентификации.

Тема 12. Электронная подпись.

Основные вопросы темы:

Общие положения. Задачи, решаемые с помощью электронных подписей. Надежность электронной подписи. Электронная подпись на основе шифрсистем с открытыми ключами. Электронные подписи на основе симметричных криптосистем. Примеры электронных подписей. Подпись Фиата-Шамира. Подпись Эль-Гамаля. Подпись RSA. Подпись Шнорра. Одноразовые электронные подписи.

Рекомендации по изучению темы:

Все вопросы изложены в главе 12 учебного пособия [2].

Контрольные вопросы:

1. Определение электронной подписи, основные свойства. Электронная подпись RSA. 2. Электронная подпись Фиата-Шамира, Эль-Гамаля, Шнорра.

Задачи для самостоятельной работы:

Во всех алгоритмах электронной подписи нужна хеш-функция. Поэтому в следующих заданиях она есть, только в упрощенном виде (для выполнения заданий в ручном режиме). Алгоритм хеш-функции $h = h(M)$ одинаковый для всех заданий. Двоичный вид сообщения M разбивается справа налево по три бита (элементы кольца по модулю 8). Затем полученные значения складываются по модулю 8. Полученное значение — свертка сообщения M.

Пример. Пусть $M = 10$ — сообщение, $r = 6$ — некоторый параметр. Предположим, что нужно найти свертку $h(M, r)$ указанным выше алгоритмом. Приводим M и r в двоичный вид: $M = (1010)_2$, $r = (110)_2$. Теперь склеиваем их: $(1010110)_2$. Если длина сообщения не делится на 3 (нужно разбить по 3 бита), то к началу сообщения M, r добавляем нужное число нулей. Получим $(001010110)_2 = (001|010|110)_2$ — разбиение по три бита. Каждые три бита – число: 1, 2, 6. Эти числа нужно сложить по модулю 8: $1 + 2 + 6 \equiv 1 (\mathrm{mod}\ 8)$. Это значит, что свертка сообщения M, r равна $h = 1 = (001)_2$. Заметим, что по определению алгоритма h все свертки будут иметь длину 3.

Если нужно найти $h(M)$, то все аналогично, только для сообщения M. Также заметим, что при приведении к двоичному виду учитываются только значащие биты: $5 = (101)_2$, но не $(0101)_2$, так как результат хеширования может быть неверным, хотя оба варианта представления верны. Нули в начало добавляются только для приведения к нужной длине.

1. Подпись Фиата-Шамира. Пусть p, q — простые числа, $n = pq$, a_1, a_2, a_3 — секретные ключи абонента A, b_1, b_2, b_3 — открытые ключи абонента A, M — подписываемое сообщение, k — случайное число. Известно, что $p = 3$, $q = 5$, $n = 15$, $a_1 = 7$, $a_2 = 8$, $a_3 = 14$, $k = 13$, $M = 19$. Найти b_1, b_2, b_3, подписать сообщение M подписью абонента A и проверить подпись.

2. Подпись Эль-Гамаля. Пусть p — простое число, g — первообразный корень по модулю p, x, y — соответственно секретный и открытый ключи абонента A, M — подписываемое сообщение, k — случайное число. Известно, что $p = 11$, $g = 2$, $x = 5$, $k = 3$, $M = 21$. Найти y, подписать сообщение M подписью абонента A и проверить подпись.

3. Подпись Шнорра. Пусть p — простое число, q — простой делитель числа $p - 1$, g — элемент из кольца вычетов по модулю p (имеющий порядок q), x, y — соответственно секретный и открытый ключ абонента A, M — подписываемое сообщение, k — случайное число. Известно, что $p = 13$, $q = 3$, $g = 3$, $x = 2$, $M = 11$, $k = 2$. Найти y, подписать сообщение M подписью абонента A и проверить подпись.

Литература

[1] Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии. М.: Гелиос АРВ, 2005. 480 с.

[2] Рацеев С. М. Математические методы защиты информации : учебное пособие для вузов. – СПб. : Лань, 2022. 544 с.

[3] Черемушкин А.В. Криптографические протоколы. Основные свойства и уязвимости. М.: Академия, 2009. 272 с.