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 «Криптографические протоколы и стандарты»

для студентов специальности
10.05.03 «Информационная безопасность автоматизированных систем»

Ульяновск
2019

Рацеев С.М. Методические указания для самостоятельной работы студентов по дисциплине «Криптографические протоколы и стандарты» для студентов специальности 10.05.03 «Информационная безопасность автоматизированных систем». – Ульяновск: УлГУ, 2019.

Методические указания рекомендованы к введению в образовательный процесс решением Ученого Совета ФМИАТ УлГУ (протокол № 2/19 от 19 марта 2019г.).

Тема 1. 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 2. 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. Ко-

ды 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 3. 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:

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.

Тема 4. Протоколы аутентификации, использующие технику «запрос-ответ»

Основные вопросы темы:

Протоколы аутентификации, использующие пароли (слабая аутентификация). Протоколы аутентификации, использующие технику «запрос-ответ»: «запрос-ответ» с использованием симметричных алгоритмов шифрования. Протоколы аутентификации, использующие технику «запрос-ответ»: «запрос-ответ» с использованием асимметричных алгоритмов шифрования.

Рекомендации по изучению темы:

Все вопросы изложены в параграфах 14.1, 14.2 учебного пособия [2].

Контрольные вопросы:

1. Протоколы аутентификации, использующие пароли (слабая аутентификация). 2. Протоколы аутентификации, использующие технику «запрос-ответ»: «запрос-ответ» с использованием симметричных алгоритмов шифрования. 3. Протоколы аутентификации, использующие технику «запрос-ответ»: «запрос-ответ» с использованием асимметричных алгоритмов шифрования и электронной подписи.

Тема 5. Протоколы аутентификации с нулевым разглашением

Основные вопросы темы:

Протокол аутентификации Фиата-Шамира. Протокол Фейга-Фиата-Шамира. Итеративный протокол аутентификации Фиата-Шамира без доверенного центра. Трехпроходный протокол аутентификации Фиата-Шамира без доверенного центра. Протокол аутентификации Шнорра. Итеративный и трехпроходный модифицированный протокол Шнорра. Модификация протокола Шнорра на эллиптических кривых. Итеративный и трехпроходный модифицированный протокол Шнорра на эллиптических кривых. Протокол аутентификации Окамото. Модификация протокола Окамото на эллиптических кривых. Протокол аутентификации Гиллоу-Куискатр (GQ). Протокол аутентификации с нулевым разглашением на основе доказательства изоморфизма графов. Пятипроходный протокол аутентификации на основе изоморфизма графов с использованием эллиптических кривых. Протокол аутентификации с нулевым разглашением на основе асимметричных шифров. Протокола аутентификации с нулевым разглашением на основе шифра RSA. Протокола аутентификации с нулевым разглашением на основе шифра Эль-Гамаля. Модификация протокола аутентификации с нулевым разглашением на основе шифра Эль-Гамаля с использованием эллиптических кривых. Модификация протокола аутентификации с нулевым разглашением на основе системы Диффи-Хеллмана с использованием эллиптических кривых.

Рекомендации по изучению темы:

Все вопросы изложены в параграфе 14.3 учебного пособия [2].

Контрольные вопросы:

1. Протокол аутентификации Фиата-Шамира. 2. Протокол Фейга-Фиата-Шамира.

3. Итеративный протокол аутентификации Фиата-Шамира без доверенного центра. 4. Трехпроходный протокол аутентификации Фиата-Шамира без доверенного центра. 5. Протокол аутентификации Шнорра. 6. Итеративный и трехпроходный модифицированный протокол Шнорра. 7. Модификация протокола Шнорра на эллиптических кривых. 8. Итеративный и трехпроходный модифицированный протокол Шнорра на эллиптических кривых. 9. Протокол аутентификации Окамото. 10. Модификация протокола Окамото на эллиптических кривых. 11. Протокол аутентификации Гиллоу-Куискатр (GQ). 12. Протокол аутентификации с нулевым разглашением на основе доказательства изоморфизма графов. 13. Пятипроходный протокол аутентификации на основе изоморфизма графов с использованием эллиптических кривых. 14. Протокол аутентификации с нулевым разглашением на основе асимметричных шифров. 15. Протокола аутентификации с нулевым разглашением на основе шифра RSA. 16. Протокола аутентификации с нулевым разглашением на основе шифра Эль-Гамаля. 17. Модификация протокола аутентификации с нулевым разглашением на основе шифра Эль-Гамаля с использованием эллиптических кривых. 18. Модификация протокола аутентификации с нулевым разглашением на основе системы Диффи-Хеллмана с использованием эллиптических кривых.

Задачи для самостоятельной работы:

1. Протокол Фиата-Шамира. Пусть $n = p \cdot q$ — параметр протокола, x, y — соответственно секретный и открытый ключи доказывающего абонента A, k — случайный параметр из первого шага протокола, a — запрос из второго шага протокола. Найти y и привести все вычисления на четырех шагах протокола (найти r, s, проверить соответствующее сравнение), если известно, что $p = 3, q = 7, a = 1, x = 13, k = 17$. $(y = 1, r = 16, s = 11)$.

2. Протокол 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, k — случайное число из первого шага протокола. Известно, что $p = 13, q = 3, g = 3, a = 1, x = 2, k = 2$. Найти y и привести все вычисления на четырех шагах протокола (найти r, s, проверить соответствующее сравнение). $(y = 3, r = 9, s = 1)$.

3. Протокол GQ. Пусть $n = p \cdot q$ — параметр протокола, x, y — соответственно секретный и открытый ключи доказывающего абонента A, k — случайный параметр из первого шага протокола, a — запрос из второго шага протокола. Найти y и привести все вычисления на четырех шагах протокола (найти r, s, проверить соответствующее сравнение), если известно, что $p = 3, q = 5, a = 1, x = 7, e = 3, k = 4$. $(y = 7, r = 4, s = 13)$.

Тема 6. Протоколы с нулевым разглашением

Основные вопросы темы:

Протокол подбрасывания монеты по телефону. Протокол типа “подбрасывание монеты по телефону” с использованием эллиптических кривых. Протоколы привязки к биту. Протокол привязки к биту на основе протокола Шнорра с ис-

пользованием эллиптических кривых.

Рекомендации по изучению темы:

Все вопросы изложены в главе 15 учебного пособия [2].

Контрольные вопросы:

1. Протокол подбрасывания монеты по телефону. 2. Протокол типа “подбрасывание монеты по телефону” с использованием эллиптических кривых. 3. Протоколы привязки к биту. 4. Протокол привязки к биту на основе протокола Шнорра с использованием эллиптических кривых.

Тема 7. Протоколы передачи ключей

Основные вопросы темы:

Передача ключей с использованием симметричного шифрования: двусторонние протоко-лы. Передача ключей с использованием симметричного шифрования: трехсторонние протоколы. Протокол Kerberos. Передача ключей с использованием асимметричного шифрования. Открытое распределение ключей. Протоколы MTI. Модификация семейства про-токолов MTI на эллиптических кривых. Предварительное распределение ключей. Схема Блома.

Рекомендации по изучению темы:

Все вопросы изложены в главе 16 учебного пособия [2].

Контрольные вопросы:

1. Передача ключей с использованием симметричного шифрования: двусторонние протоколы. 2. Передача ключей с использованием симметричного шифрования: трехсторонние протоколы. Протокол Kerberos. 3. Передача ключей с использованием асимметричного шифрования. 4. Открытое распределение ключей. Протоколы MTI. 5. Модификация семейства протоколов MTI на эллиптических кривых. 6. Предварительное распределение ключей. Схема Блома.

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 [Электронный ресурс]: Электронное учеб. пособие. – Ульяновск: УлГУ, 2018. 1 CD-R. № гос. регистрации – 0321901084.

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