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»

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 «Криптографические протоколы» 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. 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 2. 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 доверенно-

го 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 3. 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 использованием 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 4. 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 : учебное пособие для вузов. – СПб. : Лань, 2022. 544 с.

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