

Прохождение внешнего курса

Криптография на практике

Софич Андрей Геннадьевич

Содержание

1	Цель работы	1
2	Выполнение лабораторной работы.....	1
3	Выводы	5

Список иллюстраций

Рис. 1: Задание 1	2
Рис. 2: Задание 2	2
Рис. 3: Задание 3	2
Рис. 4: Задание 4	2
Рис. 5: Задание 5	3
Рис. 6: Задание 6	3
Рис. 7: Задание 7	3
Рис. 8: Задание 8	3
Рис. 9: Задание 9	3
Рис. 10: Задание 10	4
Рис. 11: Задание 11	4
Рис. 12: Задание 12	4
Рис. 13: Задание 13	4
Рис. 14: Задание 14	5
Рис. 15: Задание 15	5
Рис. 16: Задание 15	5

Список таблиц

Элементы списка иллюстраций не найдены.

1 Цель работы

Проработать задания, которые касаются криптографии

2 Выполнение лабораторной работы

Ассиметричные криптографические примитивы (рис. 1).

В асимметричных криптографических примитивах

Выберите один вариант из списка

Верно решили 940 учащихся
Из всех попыток 42% верных

☒ Правильно.

☐ одна сторона имеет только секретный ключ, а другая - пару из открытого и секретного ключей

☒ обе стороны имеют пару ключей

☐ одна сторона публикует свой секретный ключ, другая - держит его в секрете

☐ обе стороны имеют общий секретный ключ

Следующий шаг Решить снова

Ваше решение Вы получили: 1 балл

Рис. 1: Задание 1

Хэш-функция (рис. 2).

Криптографическая хэш-функция

Выберите все подходящие ответы из списка

Верно решили 798 учащихся
Из всех попыток 11% верных

☒ Хорошие новости, верно!

Вы решили сложную задачу, поздравляем! Вы можете помочь остальным учащимся в комментариях, отвечая на их вопросы, или сравнить своё решение с другими на [форуме решений](#).

☒ стойкая к коллизиям

☒ даёт на выходе фиксированное число бит независимо от объёма входных данных

☒ эффективно вычисляется

☐ обеспечивает конфиденциальность зашифрованных данных

Следующий шаг Решить снова

Ваше решение Вы получили: 1 балл

Рис. 2: Задание 2

Алгоритмы цифровой подписи (рис. 3).

К алгоритмам цифровой подписи относятся

Выберите все подходящие ответы из списка

Верно решили 834 учащихся
Из всех попыток 69% верных

☒ Все получилось!

Вы решили сложную задачу, поздравляем! Вы можете помочь остальным учащимся в комментариях, отвечая на их вопросы, или сравнить своё решение с другими на [форуме решений](#).

☐ AES

☐ SHA2

☒ RSA

☒ ECDSA

☒ ГОСТ Р 34.10-2012

Следующий шаг Решить снова

Ваше решение Вы получили: 1 балл

Рис. 3: Задание 3

Код аутентификации сообщения (рис. 4).

Код аутентификации сообщения относится к

Выберите один вариант из списка

Верно решили 955 учащихся
Из всех попыток 69% верных

☒ Верно.

☒ симметричным примитивам

☐ асимметричным примитивам

Следующий шаг Решить снова

Ваше решение Вы получили: 1 балл

Рис. 4: Задание 4

Обмен ключами Диффи-Хэлмана (рис. 5).

Обмен ключами Диффи-Хеллмана - это

Выберите один вариант из списка

☒ Абсолютно точно.

Верно решили 948 учащихся
Из всех попыток 47% верных

☐ симметричный primitive генерации общего секретного ключа

☐ асимметричный primitive генерации общего открытого ключа

☒ асимметричный primitive генерации общего секретного ключа

☐ асимметричный алгоритм шифрования

Следующий шаг Решить снова

Ваше решение Вы получили: 1 балл

Рис. 5: Задание 5

Протокол электронной цифровой подписи (рис. 6).

Протокол электронной цифровой подписи относится к

Выберите один вариант из списка

☒ Хорошие новости, верней!

Верно решили 956 учащихся
Из всех попыток 71% верных

☐ протоколам с симметричным ключом

☒ протоколам с публичным (или открытым) ключом

Следующий шаг Решить снова

Ваше решение Вы получили: 1 балл

Рис. 6: Задание 6

Алгоритм верификации электронной цифровой подписи (рис. 7).

Алгоритм верификации электронной цифровой подписи требует на вход

Выберите один вариант из списка

☒ Здорово, всё верно.

Верно решили 962 учащихся
Из всех попыток 48% верных

☐ подпись, секретный ключ, сообщение

☐ подпись, открытый ключ

☒ подпись, открытый ключ, сообщение

☐ подпись, секретный ключ

Следующий шаг Решить снова

Ваше решение Вы получили: 1 балл

Рис. 7: Задание 7

Подпись(рис. 8).

Электронная цифровая подпись не обеспечивает

Выберите один вариант из списка

☒ Здорово, всё верно.

Верно решили 968 учащихся
Из всех попыток 53% верных

☐ целостность

☐ неотрека от авторства

☒ конфиденциальность

☐ аутентификацию

Следующий шаг Решить снова

Ваше решение Вы получили: 1 балл

Рис. 8: Задание 8

Тип сертификата электронной подписи в ФНС (рис. 9).

Какой тип сертификата электронной подписи понадобится для отправки налоговой отчетности в ФНС?

Выберите один вариант из списка

☒ Здорово, всё верно.

Верно решили 975 учащихся
Из всех попыток 68% верных

☒ усиленная квалифицированная

☐ простая

☐ усиленная неквалифицированная

Следующий шаг Решить снова

Ваше решение Вы получили: 1 балл

Рис. 9: Задание 9

Организация (рис. 10).

В какой организации вы можете получить квалифицированный сертификат ключа проверки электронной подписи?

Выберите один вариант из списка

✓ Все получилось!

Верно решил 971 учащийся
из всех попыток 61% верных

☐ в любой организации, имеющей соответствующую лицензию ФСБ
☐ в министерстве РФ
☒ в удостоверяющем (сертификационном) центре
☐ в любой организации по месту работы

Следующий шаг Решить снова

Ваши решения Вы получили: 1 балл

Рис. 10: Задание 10

Платежные системы (рис. 11).

Выберите из списка все платежные системы.

Выберите все подходящие ответы из списка

✓ Правильно, молодец!

Верно решил 900 учащийся
из всех попыток 24% верных

Вы решили сложную задачу, поздравляем! Вы можете помочь остальным учащимся в комментариях, отвечая на их вопросы, или сравнить своё решение с другими на [форуме решений](#).

☐ ВiSnet
☒ MasterCard
☐ SecurePay
☐ POS-терминал
☐ банкомат
☒ МИР

Следующий шаг Решить снова

Ваши решения Вы получили: 1 балл

Рис. 11: Задание 11

Многофакторная аутентификация (рис. 12).

Примером многофакторной аутентификации является

Выберите все подходящие ответы из списка

✓ Все получилось!

Верно решил 896 учащийся
из всех попыток 24% верных

Вы решили сложную задачу, поздравляем! Вы можете помочь остальным учащимся в комментариях, отвечая на их вопросы, или сравнить своё решение с другими на [форуме решений](#).

☐ комбинация проверки пароля + Кaptcha
☒ комбинация проверки пароля + код в sms сообщении
☒ комбинация код в sms сообщении + отпечаток пальца
☐ комбинация PIN код + пароль

Следующий шаг Решить снова

Ваши решения Вы получили: 1 балл

Рис. 12: Задание 12

Онлайн платежи сегодня (рис. 13).

При онлайн платежах сегодня используется

Выберите один вариант из списка

✓ Хорошие новости, верно!

Верно решил 957 учащийся
из всех попыток 59% верных

☒ многофакторная аутентификация покупателя перед банком-эквайером
☐ однофакторная аутентификация покупателя перед банком-эквайером
☐ однофакторная аутентификация при помощи PIN-кода карты перед терминалом
☐ многофакторная аутентификация покупателя перед банком-эквайером

Следующий шаг Решить снова

Ваши решения Вы получили: 1 балл

Рис. 13: Задание 13

Свойство криптографической хэш-функции (рис. 14).

Какое свойство криптографической хэш-функции используется в доказательстве работы?

Выберите один вариант из списка

☒ Хорошие новости, верно!

Верно решили 932 учащихся
Из всех попыток 49% верных

☐ фиксированная длина выходных данных
☒ сложность нахождения прообраза
☐ обеспечение целостности
☐ эффективность вычисления

Следующий шаг Решить снова

Ваше решение Вы получили: 1 балл

Рис. 14: Задание 14

Свойства консенсуса в системах блокчейн (рис. 15).

Консенсус в некоторых системах блокчейн обладает свойствами

Выберите все подходящие ответы из списка

☒ Верно.

Вы решили сложную задачу, поздравляем! Вы можете помочь остальным учащимся в [квизах](#), отвечая на их вопросы, или сравнить своё решение с другими на [форуме решений](#).

Верно решили 864 учащихся
Из всех попыток 23% верных

☒ живучесть
☒ консенсус
☒ открытость
☒ устойчивость

Следующий шаг Решить снова

Ваше решение Вы получили: 1 балл

Рис. 15: Задание 15

Секретные ключи (рис. 15).

Секретные ключи какого криптографического примитива хранят участники блокчейна?

Выберите один вариант из списка

☒ Здорово, всё верно.

Верно решили 951 учащийся
Из всех попыток 48% верных

☐ обмен ключами
☐ шифрование
☒ цифровая подпись
☐ хэш-функция

Следующий шаг Решить снова

Ваше решение Вы получили: 1 балл

Рис. 16: Задание 15

3 Выводы

Проделаны задания, связанные с криптографией