

Прохождение внешнего курса

Криптография на практике

Селиванов Вячеслав Алексеевич

Содержание

1	Цель работы.....	1
2	Выполнение лабораторной работы.....	1
3	Выводы	7

Список иллюстраций

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

Список таблиц

No table of figures entries found.

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

☒ Так точно!

Верно решили 940 учащихся
Из всех попыток 42% верных

- ☐ обе стороны имеют общий секретный ключ
- ☐ одна сторона публикует свой секретный ключ, другая - держит его в секрете
- ☒ обе стороны имеют пару ключей
- ☐ одна сторона имеет только секретный ключ, а другая - пару из открытого и секретного ключей

Следующий шаг

Решить снова

[Ваши решения](#) Вы получили: 1 балл

Рис. 1: Задание 1

Хэш-функция (рис. 2).

Криптографическая хэш-функция

Выберите все подходящие ответы из списка

☒ Правильно, молодец!

Верно решили 798 учащихся
Из всех попыток 11% 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](#).

- ☒ эффективно вычисляется
- ☒ дает на выходе фиксированное число бит независимо от объема входных данных
- ☒ стойкая к коллизиям
- ☐ обеспечивает конфиденциальность зашифрованных данных

Следующий шаг

Решить снова

Рис. 2: Задание 2

Алгоритмы цифровой подписи (рис. 3).

К алгоритмам цифровой подписи относятся

Выберите все подходящие ответы из списка

☒ Всё получилось!

Верно решили 834 учащихся
Из всех попыток 19% 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](#).

- ☐ AES
- ☐ SHA2
- ☒ RSA
- ☒ ECDSA
- ☒ ГОСТ Р 34.10-2012

Рис. 3: Задание 3

Код аутентификации сообщения (рис. 4).

Код аутентификации сообщения относится к

Выберите один вариант из списка

✓ Правильно.

Верно решили 955 учащихся
Из всех попыток 69% верных

- ☒ симметричным примитивам
☐ асимметричным примитивам

Следующий шаг

Решить снова

[Ваши решения](#) Вы получили: 1 балл

Рис. 4: Задание 4

Обмен ключами Диффи-Хэлмана (рис. 5).

Обмен ключам Диффи-Хэлмана - это

Выберите один вариант из списка

✓ Абсолютно точно.

Верно решили 948 учащихся
Из всех попыток 47% верных

- ☐ симметричный примитив генерации общего секретного ключа
☐ асимметричный примитив генерации общего открытого ключа
☒ асимметричный примитив генерации общего секретного ключа
☐ асимметричный алгоритм шифрования

Следующий шаг

Решить снова

[Ваши решения](#) 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

✓ Отлично!

Верно решили 956 учащихся
Из всех попыток 71% верных

- ☐ протоколам с симметричным ключом
☒ протоколам с публичным (или открытым) ключом

Следующий шаг

Решить снова

[Ваши решения](#) 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

✔ Отлично!

Верно решили 962 учащихся
Из всех попыток 46% верных

- ☒ подпись, открытый ключ, сообщение
- ☐ подпись, секретный ключ, сообщение
- ☐ подпись, секретный ключ
- ☐ подпись, открытый ключ

Следующий шаг

Решить снова

[Ваши решения](#) Вы получили: 1 балл

Рис. 7: Задание 7

Подпись(рис. 8).

Электронная цифровая подпись не обеспечивает

Выберите один вариант из списка

✔ Отлично!

Верно решили 968 учащихся
Из всех попыток 53% верных

- ☐ аутентификацию
- ☐ целостность
- ☒ конфиденциальность
- ☐ отказ от авторства

Следующий шаг

Решить снова

[Ваши решения](#) 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

✔ Отлично!

Верно решили 975 учащихся
Из всех попыток 68% верных

- ☒ усиленная квалифицированная
- ☐ усиленная неквалифицированная
- ☐ простая

Следующий шаг

Решить снова

[Ваши решения](#) 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

☒ Здорово, всё верно.

Верно решил 971 учащийся
Из всех попыток 61% верных

- ☐ в любой организации, имеющей соответствующую лицензию ФСБ
- ☐ в минкомсвязи 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

☒ Всё получилось!

Верно решили 900 учащихся
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](#).

- ☐ BitCoin
- ☒ 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

☒ Правильно.

Верно решили 896 учащихся
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 + Капча
- ☒ комбинация проверка 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

☒ Правильно.

Верно решили 957 учащихся
Из всех попыток 59% верных

- ☒ многофакторная аутентификация покупателя перед банком-эмитентом
- ☐ 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

☒ Отличное решение!

Верно решили 932 учащихся
Из всех попыток 49% верных

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

Следующий шаг

Решить снова

[Ваши решения](#) 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

☒ Всё получилось!

Верно решили 864 учащихся
Из всех попыток 23% 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](#).

- ☒ консенсус
- ☒ открытость
- ☒ живучесть
- ☒ постоянства

Следующий шаг

Решить снова

Рис. 15: Задание 15

Секретные ключи (рис. 16).

Секретные ключи какого криптографического примитива хранят участники блокчейна?

Выберите один вариант из списка

✓ Всё получилось!

Верно решил 951 учащийся
Из всех попыток 48% верных

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

Следующий шаг

Решить снова

[Ваши решения](#) Вы получили: 1 балл

Рис. 16: Задание 16

3 Выводы

Проделаны задания, связанные с криптографией