

Прохождение внешнего курса

Криптография на практике

Софич А.С

04 мая 2025

Российский университет дружбы народов, Москва, Россия

НКАбд-04-23

- Софич Андрей Геннадьевич
- Студент
- НКАбд-04-23
- Российский университет дружбы народов
- 1132237371@pfur.ru



Проработать задания, которые касаются криптографии

Выполнение лабораторной работы

Ассиметричные криптографические примитивы

В асимметричных криптографических примитивах

Выберите один вариант из списка

☒ Правильно.

Верно решили **940** учащихся
Из всех попыток **42%** верных

- ☐ 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

[Ваши решения](#) Вы получили: **1 балл**

Рис. 1: Задание 1

Криптографическая хэш-функция

Выберите все подходящие ответы из списка

☒ 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

☒ дает на выходе фиксированное число бит независимо от объема входных данных

☒ эффективно вычисляется

☐ обеспечивает конфиденциальность захешированных данных

[Следующий шаг](#) [Решить снова](#)

[Ваши решения](#) Вы получили: **1 балл**

Верно решили **798** учащихся
Из всех попыток **11%** верных

Рис. 2: Задание 2

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

Следующий шаг

Решить снова

[Ваши решения](#) Вы получили: **1 балл**

Рис. 3: Задание 3

Код аутентификации сообщения относится к

Выберите один вариант из списка

☒ Верно.

☐ симметричным примитивам

☐ асимметричным примитивам

[Ваши решения](#) Вы получили: **1 балл**

Верно решили **955** учащихся
Из всех попыток **69%** верных

Следующий шаг

Решить снова

Рис. 4: Задание 4

Обмен ключам Диффи-Хэллмана - 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 относится к

Выберите один вариант из списка

☒ Хорошие новости, верно!

☐ протоколам с симметричным ключом

☒ протоколам с публичным (или открытым) ключом

[Ваша история](#) [Ваша статистика](#)

[Следующий шаг](#) [Решить снова](#)

[Ваша статистика](#) Вы получили: **1 балл**

Верно решили **956** учащихся
Из всех попыток **71%** верных

Рис. 6: Задание 6

Алгоритм верификации электронной цифровой подписи

Алгоритм верификации электронной цифровой подписи требует на вход

Выберите один вариант из списка

☒ Здорово, всё верно.

Верно решили **962** учащихся
Из всех попыток **46%** верных

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

[Следующий шаг](#) [Решить снова](#)

[Ваши решения](#) Вы получили: **1 балл**

Рис. 7: Задание 7

Электронная цифровая подпись не обеспечивает

Выберите один вариант из списка

☒ Здорово, всё верно.

Верно решили **968** учащихся
Из всех попыток **53%** верных

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

Следующий шаг

Решить снова

[Ваши решения](#) Вы получили: **1 балл**

Рис. 8: Задание 8

Тип сертификата электронной подписи в ФНС

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

Выберите один вариант из списка

☒ Здорово, всё верно.

☐ усиленная квалифицированная

☐ простая

☐ усиленная неквалифицированная

[Следующий шаг](#) [Решить снова](#)

[Ваши решения](#) Вы получили: **1 балл**

Верно решили **975** учащихся
Из всех попыток **68%** верных

Рис. 9: Задание 9

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

Выберите один вариант из списка

☒ Всё получилось!

Верно решил **971** учащихся
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

Выберите из списка все платежные системы.

Выберите все подходящие ответы из списка

✔ Правильно, молодец!

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

Примером многофакторной аутентификации является

Выберите все подходящие ответы из списка

✓ Всё 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](#).

Верно решили **896** учащихся
Из всех попыток **24%** верных

- ☐ 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

При онлайн платежах сегодня используется

Выберите один вариант из списка

☒ Хорошие новости, верно!

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

Какое свойство криптографической хэш-функции используется в доказательстве работы?

Выберите один вариант из списка

☒ Хорошие новости, верно!

☐ фиксированная длина выходных данных

☒ сложность нахождения прообраза

☐ обеспечение целостности

☐ эффективность вычисления

[Следующий шаг](#) [Решить снова](#)

[Ваши решения](#) Вы получили: **1 балл**

Верно решили **932** учащихся
Из всех попыток **49%** верных

Рис. 14: Задание 14

Свойства консенсуса в системах блокчейн

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 [комментариях](#), отвечая на их вопросы, или сравнить своё решение с другими на [форуме решений](#).

☒ живучесть
☒ консенсус
☒ открытость
☒ постоянства

[Следующий шаг](#) [Решить снова](#)

[Ваши решения](#) Вы получили: **1 балл**

Верно решили **864** учащихся
Из всех попыток **23%** верных

Рис. 15: Задание 15

Секретные ключи какого криптографического примитива хранят участники блокчейна?

Выберите один вариант из списка

☒ Здорово, всё верно.

Верно решил **951** учащихся
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 15

Проделаны задания, связанные с криптографией