

Внешний курс

Криптография

Солдатов А. Е

9 мая 2025

Российский университет дружбы народов, Москва, Россия

НКАбд-04-23

- Солдатов Алексей Евгеньевич
- Студент
- НКАбд-04-23
- Российский университет дружбы народов
- 1132236009@pfur.ru



Выполнение блока 1 (Введение в криптографию)

После просмотра видеоматериала приступил к выполнению заданий

В видеолекции было рассказано, что в асимметричных примитивах обе стороны имеют пару ключей (рис. 1 (fig:001?)).

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: Асимметричный примитив

В видеолекции было рассказано о свойствах криптографической хэш-функции (рис. 2 (fig:002?)).

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

Следующий шаг Решить снова

[Ваши решения](#) Вы получили: 1 балл

Рис. 2: Хэш-функция

В видеолекции было рассказано, что относится к алгоритмам цифровой подписи (рис. 3 (fig:003?)).

К алгоритмам цифровой подписи относятся

Выберите все подходящие ответы из списка

Верно решили 834 учащихся
Из всех попыток 19% верных

✓ 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](#).

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

[Виды решений](#) Вы получили: 1 балл

Следующий шаг Решить снова

Рис. 3: Примеры

В видеолекции было сказано, что код аутентификации сообщения относится к симметричным примитивам (рис. 4 (**fig:004?**)).

Код аутентификации сообщения относится к

Выберите один вариант из списка

✓ Верно.

Верно решили 955 учащихся
Из всех попыток 69% верных

☒ симметричным примитивам
☐ асимметричным примитивам

Следующий шаг Решить снова

[Взгляните на решение](#) Вы получили: 1 балл

Рис. 4: Код аутентификации

В видеолекции было рассказано, что такое обмен ключами Диффи-Хэллмана (рис. 5 (fig:005?)).

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](#)

[Ваше решение](#) Вы получили 1 балл

Рис. 5: Обмен ключами Диффи-Хэллмана

Выполнение блока 2 (Цифровая подпись)

В видеолекции было сказано, что протокол электронной цифровой подписи относится к протоколам с публичным ключом (рис. 6 (fig:006?)).

Обмен ключом Диффи-Хеллмана - 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](#)

[Ваше решение](#) Вы получили 1 балл

Рис. 6: Эл. циф. подпись

В видеолекции было рассказано что требует алгоритм верификации эл. цифр. подписи (рис. 7 (**fig:007?**)).

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: Что требует алгоритм

В видеолекции было рассказано что обеспечивает эл. циф. подпись, следовательно можно было понять, чего она не обеспечивает (рис. 7 (fig:007?)).

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: Что не обеспечивает эл. циф. подпись

В видеолекции было рассказано, какой тип сертификата эл. циф. подписи понадобится для отправки в налоговую (рис. 9 (**fig:009?**)).

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](#)

[Ваши решения](#) Вы получили: 1 балл

Рис. 9: Отчетность ФНС

В видеолекции было сказано, в какой организации можно получить квалифицированный сертификат ключа проверки эл. подписи (рис. 10 (fig:010?)).

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

Выберите один вариант из списка

✓ Всё получилось!

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: Удостоверяющий центр

Выполнение блока 3 (Электронные платежи)

В видеолекции было рассказано о некоторых из платежных систем (рис. 11 (fig:011?)).

Выберите из списка все платежные системы.

Выберите все подходящие ответы из списка

Верно решили 900 учащихся
Из всех попыток 24% верных

✔ Правильно, молодец!

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](#)

[Ваше решение](#) Вы получили: 1 балл

Рис. 11: Платежные системы

В видеолекции было рассказано, что является примером многофакторной аутентификации (рис. 12 (**fig:012?**)).

Примером многофакторной аутентификации является

Выберите все подходящие ответы из списка

✓ Всё получилось!

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

Вы решили словную 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: Многофакторная аутентификация

В видеолекции было рассказано, что используется при онлайн платежах (рис. 13 (fig:013?)).

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: Онлайн платежи

Выполнение блока 4 (Блокчейн)

В видеолекции было рассказано, какое свойство криптографической хэш-функции используется в доказательстве работы (рис. 14 (**fig:014?**)).

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

[Ваши решения](#) Вы получили: 1 балл

Рис. 14: Сложность нахождения прообраза

В видеолекции было рассказано, какими свойствами обладает консенсус (рис. 15 (fig:015?)).

Консенсус в некоторых системах блокчейн обладает свойствами

Выберите все подходящие ответы из списка

☒ Верно.

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 свое решение с другими на [форуме решений](#).

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

[Следующий шаг](#) [Решить снова](#)

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

Рис. 15: Консенсус

В видеолекции было сказано, что участники блокчейна хранят цифровые подписи (рис. 16 (fig:016?)).

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](#)

[Ваше решение](#) Вы получили: 1 балл

Рис. 16: Что хранят участники блокчейна

Выводы

Получил полезные знания и прошел тесты по теме криптография