Внешний курс

Криптография

Солдатов А. Е

9 мая 2025

Российский университет дружбы народов, Москва, Россия

НКАбд-04-23

Докладчик

- 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?**)).

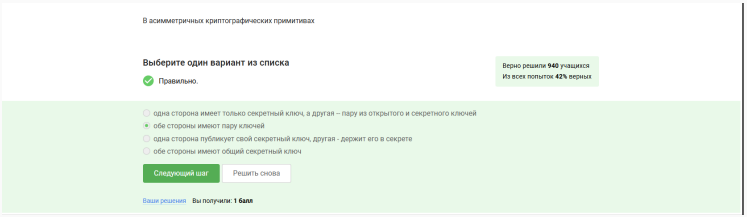

Рис. 1: Асимметричный примитив

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

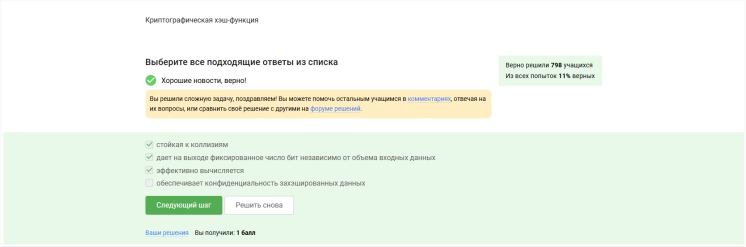

Рис. 2: Хэш-функция

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

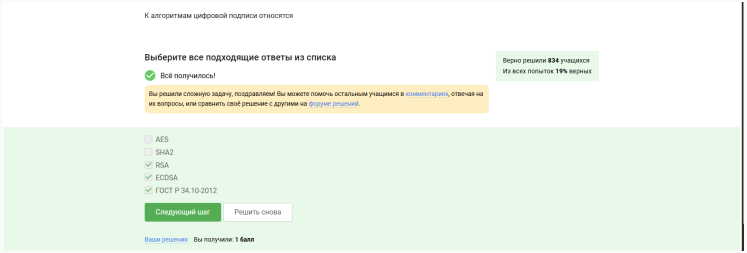

Рис. 3: Примеры

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

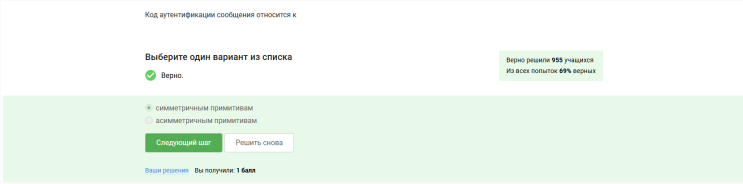

Рис. 4: Код аутентификации

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

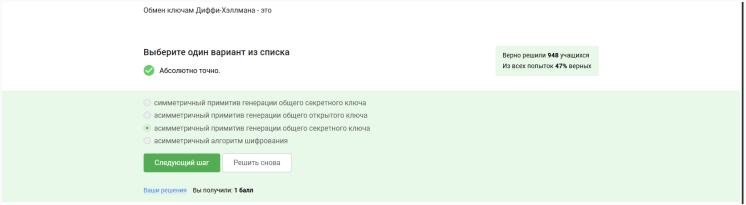

Рис. 5: Обмен ключами Диффи-Хэллмана

Выполнение блока 2 (Цифровая подпись)

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

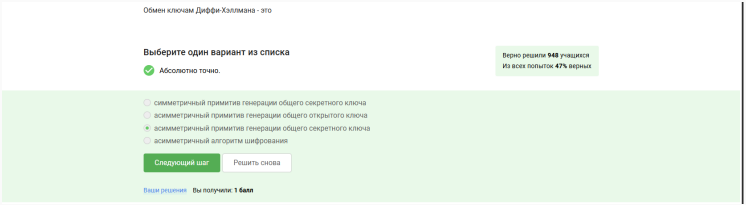

Рис. 6: Эл. циф. подпись

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

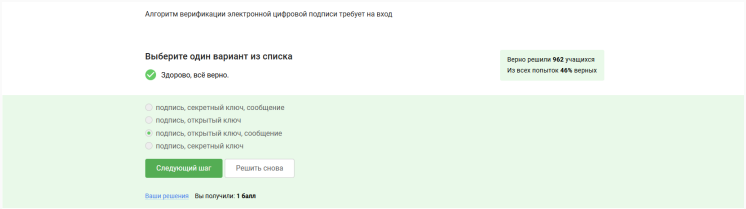

Рис. 7: Что требует алгоритм

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

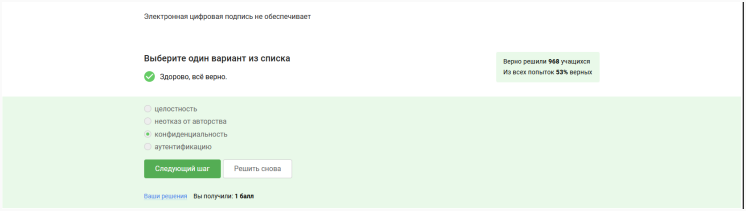

Рис. 8: Что не обеспечивает эл. циф. подпись

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

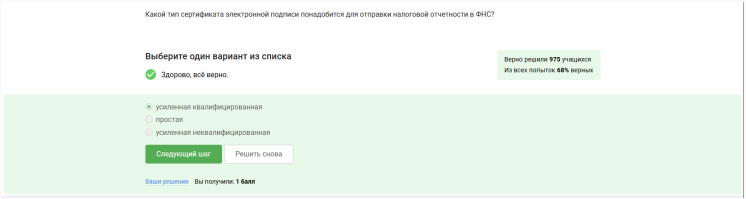

Рис. 9: Отчетность ФНС

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

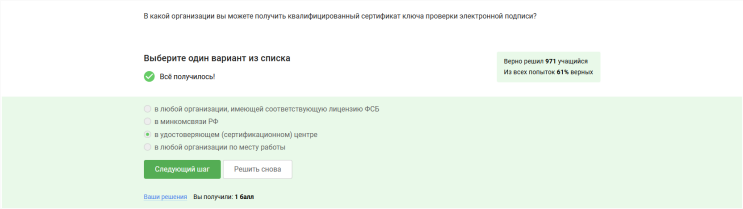

Рис. 10: Удостоверяющий центр

Выполнение блока 3 (Электронные платежа)

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

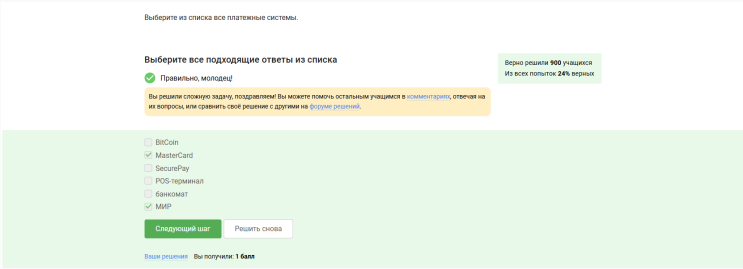

Рис. 11: Платежные системы

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

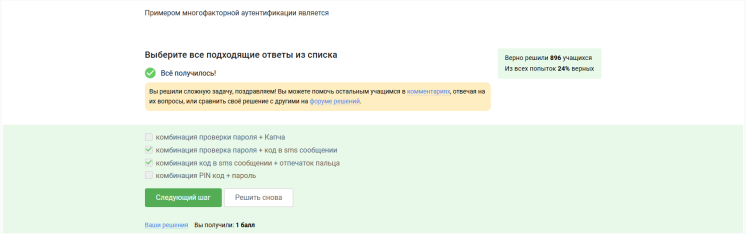

Рис. 12: Многофакторная аутентификация

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

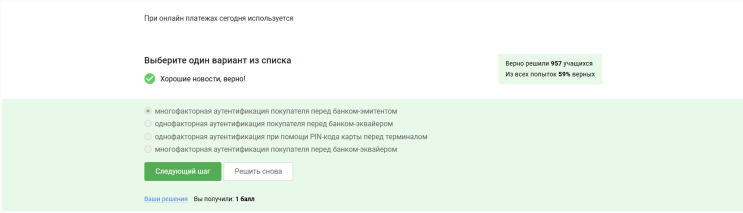

Рис. 13: Онлайн платежи

Выполнение блока 4 (Блокчейн)

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

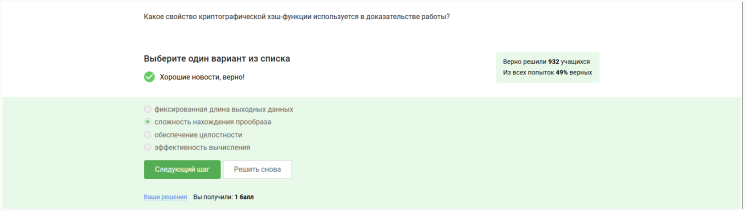

Рис. 14: Сложность нахождения прообраза

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

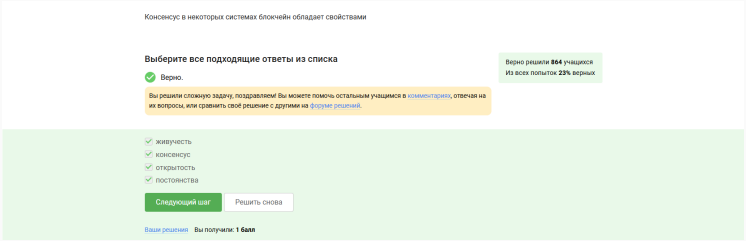

Рис. 15: Консенсус

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

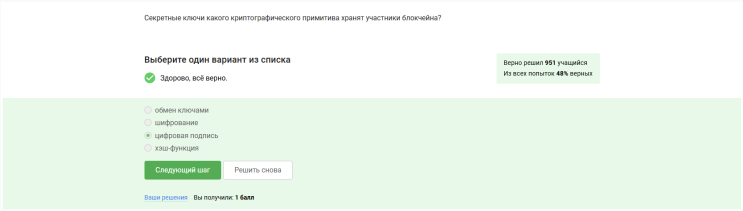

Рис. 16: Что хранят участники блокчейна

Выводы

Выводы

Получил полезные знания и прошел тесты по теме криптография