

Внешний курс. Блок 3: Криптография на практике

Основы информационной безопасности

Закиров Нурислам Дамирович

Содержание

1	Цель работы	5
2	Выполнение блока 3: Криптография на практике	6
2.1	Введение в криптографию	6
2.2	Цифровая подпись	8
2.3	Электронные платежи	10
2.4	Блокчейн	11
3	Выводы	13

Список иллюстраций

2.1	Вопрос 4.1.1	6
2.2	Вопрос 4.1.2	6
2.3	Вопрос 4.1.3	7
2.4	Вопрос 4.1.4	7
2.5	Вопрос 4.1.5	8
2.6	Вопрос 4.2.1	8
2.7	Вопрос 4.2.2	9
2.8	Вопрос 4.2.3	9
2.9	Вопрос 4.2.4	9
2.10	Вопрос 4.2.5	10
2.11	Вопрос 4.3.1	10
2.12	Вопрос 4.3.2	10
2.13	Вопрос 4.3.3	11
2.14	Вопрос 4.4.1	11
2.15	Вопрос 4.4.2	12
2.16	Вопрос 4.4.3	12

Список таблиц

1 Цель работы

Пройти третий блок курса “Основы кибербезопасности”

2 Выполнение блока 3: Криптография на практике

2.1 Введение в криптографию

Для ответа на вопрос используется определение асимметричного шифрования с двумя ключами (рис. 2.1).

4.1 Введение в криптографию 3 из 7 шагов пройдено 1 из 5 баллов получено

Вы прошли больше 80% курса, оставьте отзыв [Оставить отзыв](#) [Нет, спасибо](#)

В асимметричных криптографических примитивах

Выберите один вариант из списка

☒ Абсолютно 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

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

☒ обе стороны имеют пару ключей

[Следующий шаг](#) [Решить снова](#)

Рис. 2.1: Вопрос 4.1.1

Отмечены основные условия для криптографической хэш-функции (рис. 2.2).

4.1 Введение в криптографию 4 из 7 шагов пройдено 2 из 5 баллов получено

Вы прошли больше 80% курса, оставьте отзыв [Оставить отзыв](#) [Нет, спасибо](#)

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 свои решения с другими на [форуме решений](#).

Верно решили 798 учащихся
Из всех попыток 11% верных

☒ стойкая к коллизиям

☒ эффективно вычисляется

☐ обеспечивает конфиденциальность зашифрованных данных

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

[Следующий шаг](#) [Решить снова](#)

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

Рис. 2.2: Вопрос 4.1.2

Отмечены алгоритмы цифровой подписи (рис. 2.3).

4.1 Введение в криптографию 5 из 7 шагов пройдено 3 из 5 баллов получено

Вы прошли больше 80% курса, оставьте отзыв [Оставить отзыв](#) Нет, спасибо

К алгоритмам цифровой подписи относятся

Выберите все подходящие ответы из списка

✓ Хорошая работа.

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 834 учащихся
Из всех попыток 19% верных

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

[Следующий шаг](#) [Решить снова](#)

[Ваши решения](#) Вы получили: 1 балл

Рис. 2.3: Вопрос 4.1.3

В информационной безопасности аутентификация сообщения или аутентификация источника данных-это свойство, которое гарантирует, что сообщение не было изменено во время передачи (целостность данных) и что принимающая сторона может проверить источник сообщения (рис. 2.4)

4.1 Введение в криптографию 6 из 7 шагов пройдено 4 из 5 баллов получено

Вы прошли больше 80% курса, оставьте отзыв [Оставить отзыв](#) Нет, спасибо

Код аутентификации сообщения относится к

Выберите один вариант из списка

✓ Хорошая работа.

Верно решили 955 учащихся
Из всех попыток 69% верных

- ☐ асимметричным примитивам
- ☒ симметричным примитивам

[Следующий шаг](#) [Решить снова](#)

[Ваши решения](#) Вы получили: ...

Рис. 2.4: Вопрос 4.1.4

Определение обмена ключами Диффи-Хэллмана. (рис. 2.5).

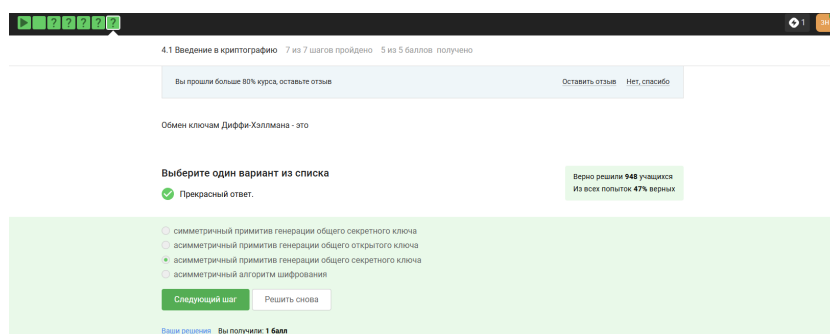


Рис. 2.5: Вопрос 4.1.5

2.2 Цифровая подпись

По определению цифровой подписи протокол ЭЦП относится к протоколам с публичным ключом (рис. 2.6).

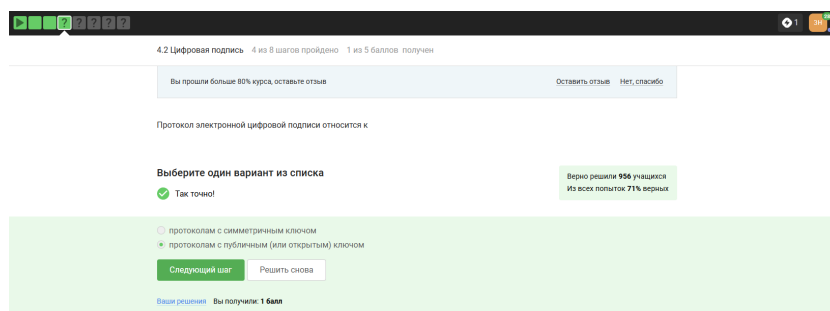


Рис. 2.6: Вопрос 4.2.1

Алгоритм верификации электронной подписи состоит в следующем. На первом этапе получатель сообщения строит собственный вариант хэш-функции подписанного документа. На втором этапе происходит расшифровка хэш-функции, содержащейся в сообщении с помощью открытого ключа отправителя. На третьем этапе производится сравнение двух хэш-функций. Их совпадение гарантирует одновременно подлинность содержимого документа и его авторства (рис. 2.7).

4.2 Цифровая подпись 5 из 8 шагов пройдено 2 из 5 баллов получено

Вы прошли больше 80% курса, оставляйте отзыв Оставить отзыв Нет, спасибо

Алгоритм верификации электронной цифровой подписи требует на вход

Выберите один вариант из списка

✓ Хорошие новости, верно!

Верно решили 942 учащихся
Из всех попыток 46% верных

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

Следующий шаг Решить снова

Ваши решения Вы получили: 1 балл

Рис. 2.7: Вопрос 4.2.2

Электронная подпись обеспечивает все указанное, кроме конфиденциальности (рис. 2.8).

4.2 Цифровая подпись 6 из 8 шагов пройдено 3 из 5 баллов получено

Вы прошли больше 80% курса, оставляйте отзыв Оставить отзыв Нет, спасибо

Электронная цифровая подпись не обеспечивает

Выберите один вариант из списка

✓ Верно. Так держите!

Верно решили 948 учащихся
Из всех попыток 53% верных

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

Следующий шаг Решить снова

Ваши решения Вы получили: 1 балл

Рис. 2.8: Вопрос 4.2.3

Для отправки налоговой отчетности в ФНС используется усиленная квалифицированная электронная подпись (рис. 2.9).

4.2 Цифровая подпись 7 из 8 шагов пройдено 4 из 5 баллов получено

Вы прошли больше 80% курса, оставляйте отзыв Оставить отзыв Нет, спасибо

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

- ☐ простая
- ☒ усиленная квалифицированная
- ☐ усиленная неквалифицированная

Следующий шаг Решить снова

Ваши решения Вы получили: ...

Рис. 2.9: Вопрос 4.2.4

Верный ответ укзaan на изображении (рис. 2.10).

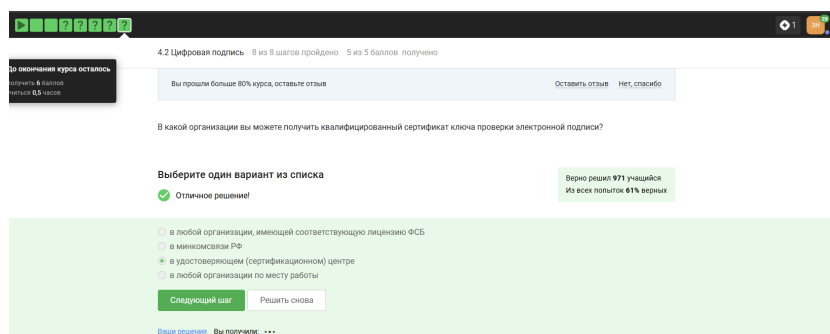


Рис. 2.10: Вопрос 4.2.5

2.3 Электронные платежи

Известные платежные системы – Visa, MasterCard, МИР (рис. 2.11).

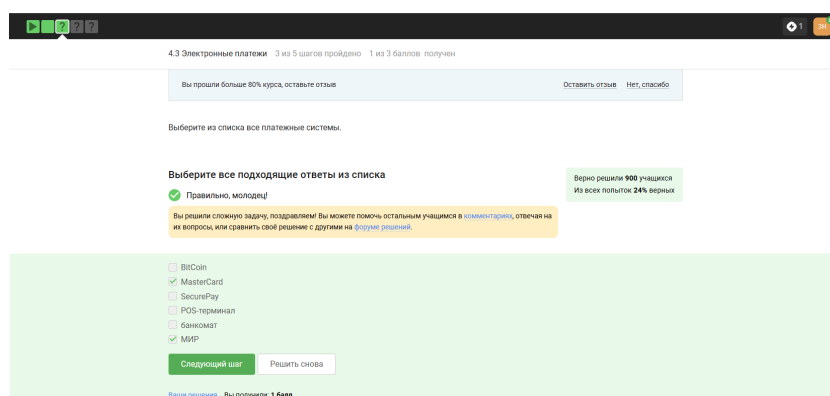


Рис. 2.11: Вопрос 4.3.1

Верный ответ на изображении (рис. 2.12).

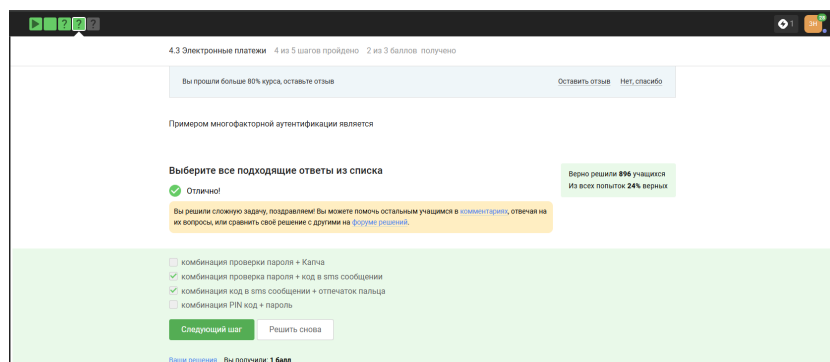


Рис. 2.12: Вопрос 4.3.2

При онлайн платежах используется многофакторная аутентификация (рис. 2.13).

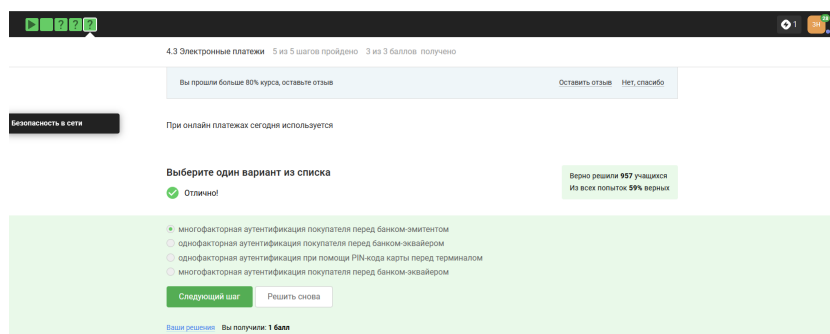


Рис. 2.13: Вопрос 4.3.3

2.4 Блокчейн

Proof-of-Work, или PoW, (доказательство выполнения работы) — это алгоритм достижения консенсуса в блокчейне; он используется для подтверждения транзакций и создания новых блоков. С помощью PoW майнеры конкурируют друг с другом за завершение транзакций в сети и за вознаграждение. Пользователи сети отправляют друг другу цифровые токены, после чего все транзакции собираются в блоки и записываются в распределенный реестр, то есть в блокчейн. (рис. 2.14).

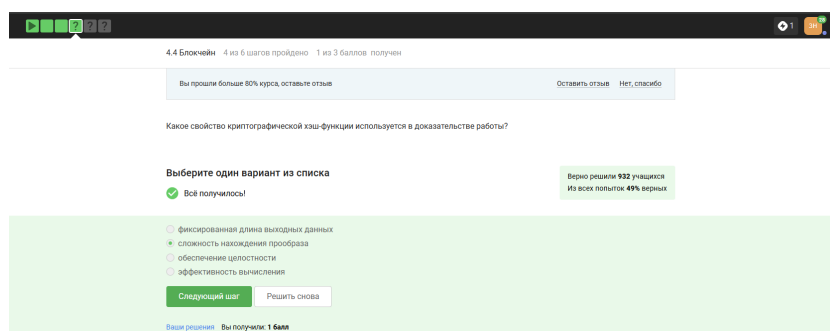


Рис. 2.14: Вопрос 4.4.1

Консенсус блокчейна — это процедура, в ходе которой участники сети достигают согласия о текущем состоянии данных в сети. Благодаря этому алгоритмы

консенсуса устанавливают надежность и доверие к самой сети. (рис. 2.15).

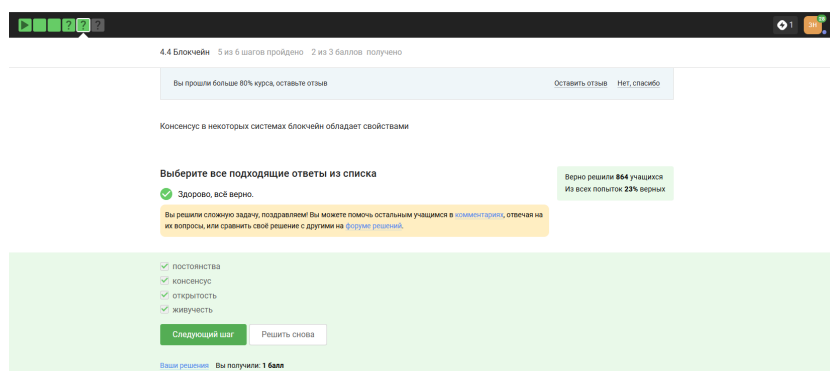


Рис. 2.15: Вопрос 4.4.2

Ответ - цифровая подпись (рис. 2.16).

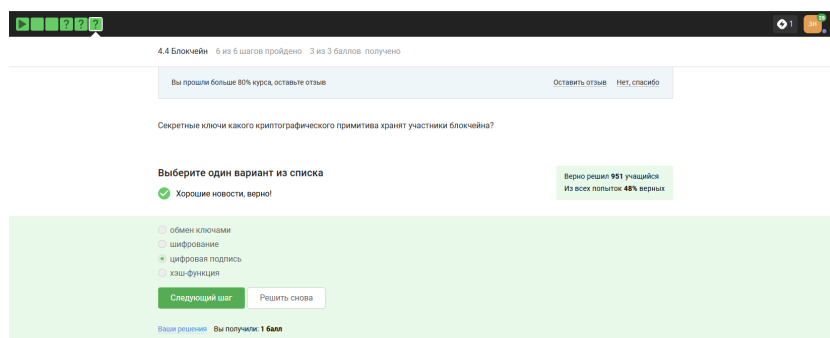


Рис. 2.16: Вопрос 4.4.3

3 Выводы

Я прошел третий блок, соответственно завершив прохождение всего внешнего курса по основам кибербезопасности.