

Внешний курс. Блок 3: Криптография на практике

Основы информационной безопасности

Дворкина Ева Владимировна

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	11
2.4	Блокчейн	12
3	Выводы	14

Список иллюстраций

2.1	Вопрос 4.1.1	6
2.2	Вопрос 4.1.2	7
2.3	Вопрос 4.1.3	7
2.4	Вопрос 4.1.4	8
2.5	Вопрос 4.1.5	8
2.6	Вопрос 4.2.1	9
2.7	Вопрос 4.2.2	9
2.8	Вопрос 4.2.3	10
2.9	Вопрос 4.2.4	10
2.10	Вопрос 4.2.5	10
2.11	Вопрос 4.3.1	11
2.12	Вопрос 4.3.2	11
2.13	Вопрос 4.3.3	12
2.14	Вопрос 4.4.1	12
2.15	Вопрос 4.4.2	13
2.16	Вопрос 4.4.3	13

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).

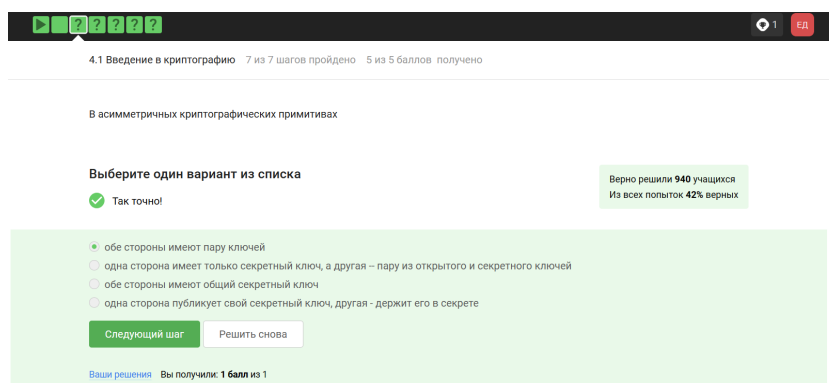


Рис. 2.1: Вопрос 4.1.1

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

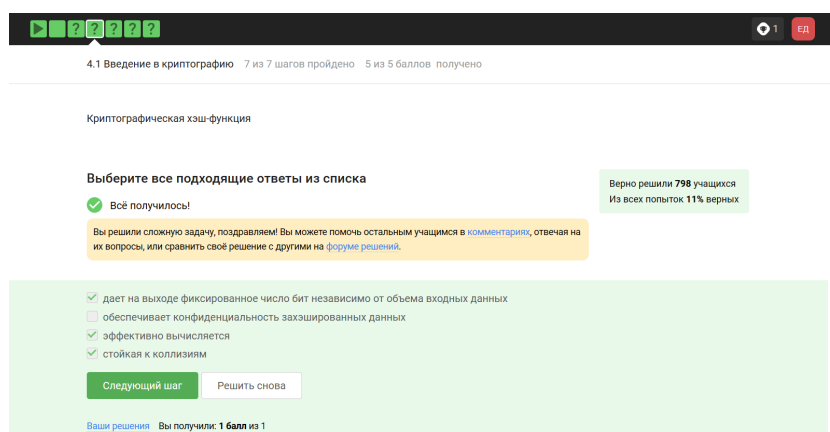


Рис. 2.2: Вопрос 4.1.2

Отмечены алгоритмы цифровой подписи (рис. 2.3).

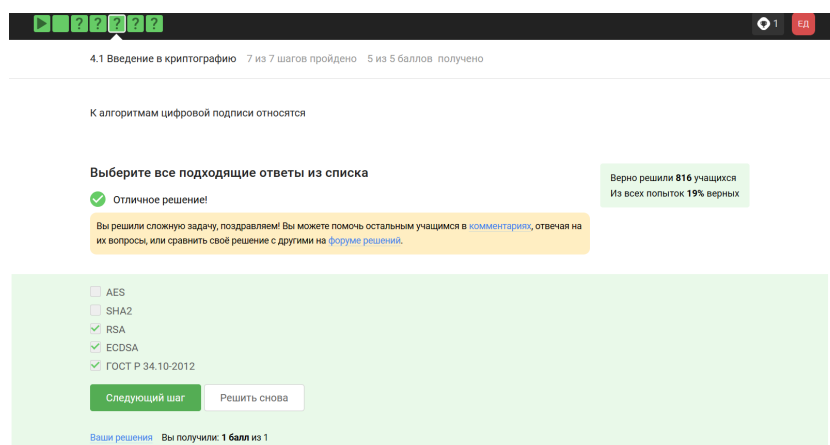


Рис. 2.3: Вопрос 4.1.3

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 7 из 7 шагов пройдено 5 из 5 баллов получено

Код аутентификации сообщения относится к

Выберите один вариант из списка

✓ Хорошая работа.

Верно решили 930 учащихся
Из всех попыток 69% верных

☐ асимметричным примитивам

☒ симметричным примитивам

Следующий шаг Решить снова

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

Рис. 2.4: Вопрос 4.1.4

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

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

Обмен ключам Диффи-Хэллмана - это

Выберите один вариант из списка

✓ Хорошая работа.

Верно решили 923 учащихся
Из всех попыток 46% 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 из 1

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).

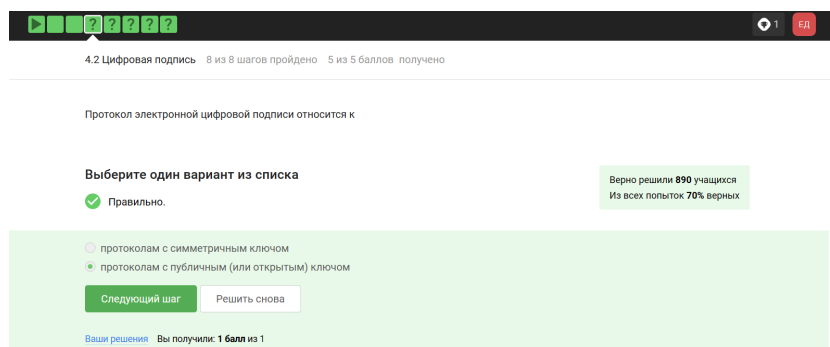


Рис. 2.6: Вопрос 4.2.1

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).

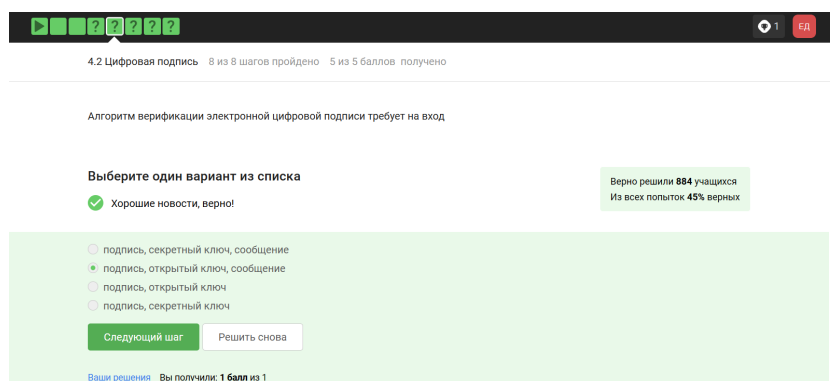


Рис. 2.7: Вопрос 4.2.2

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

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

Электронная цифровая подпись не обеспечивает

Выберите один вариант из списка

☒ Абсолютно точно.

Верно решили 885 учащихся
Из всех попыток 51% верных

☐ целостность
☐ конфиденциальность
☐ аутентификацию
☐ отказ от авторства

Следующий шаг Решить снова

Ваши решения Вы получили: 1 балл из 1

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 8 из 8 шагов пройдено 5 из 5 баллов получено

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

Выберите один вариант из списка

☒ Отлично!

Верно решили 885 учащихся
Из всех попыток 67% верных

☒ усиленная квалифицированная
☐ усиленная неквалифицированная
☐ простая

Следующий шаг Решить снова

Ваши решения Вы получили: 1 балл из 1

Рис. 2.9: Вопрос 4.2.4

Верный ответ указан на изображении (рис. 2.10).

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

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

Выберите один вариант из списка

☒ Отлично!

Верно решили 883 учащихся
Из всех попыток 60% 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 из 1

Рис. 2.10: Вопрос 4.2.5

2.3 Электронные платежи

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

The screenshot shows a quiz interface for the topic "4.3 Электронные платежи". The progress bar indicates "5 из 5 шагов пройдено" and "3 из 3 баллов получено". The question asks to select all applicable payment systems from a list. The correct answer is "Здорово, всё верно." (Great, everything is correct). A green box on the right states "Верно решили 814 учащихся" (Correctly solved by 814 students) and "Из всех попыток 23% верных" (23% correct of all attempts). The list of payment systems includes Bitcoin, MasterCard, SecurePay, POS-терминал, банкомат, and МИР. The correct answers are MasterCard and МИР. The interface includes buttons for "Следующий шаг" (Next step) and "Решить снова" (Solve again), and a feedback message: "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."

Рис. 2.11: Вопрос 4.3.1

Верный ответ на изображении (рис. 2.12).

The screenshot shows a quiz interface for the topic "4.3 Электронные платежи". The progress bar indicates "5 из 5 шагов пройдено" and "3 из 3 баллов получено". The question asks for an example of multifactor authentication. The correct answer is "Отлично!" (Excellent!). A green box on the right states "Верно решили 800 учащихся" (Correctly solved by 800 students) and "Из всех попыток 23% верных" (23% correct of all attempts). The list of options includes: "комбинация проверки пароля + Калча", "комбинация проверки пароля + код в sms сообщении", "комбинация код в sms сообщении + отпечаток пальца", and "комбинация PIN код + пароль". The correct answers are "комбинация проверки пароля + код в sms сообщении" and "комбинация код в sms сообщении + отпечаток пальца". The interface includes buttons for "Следующий шаг" (Next step) and "Решить снова" (Solve again), and a feedback message: "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."

Рис. 2.12: Вопрос 4.3.2

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

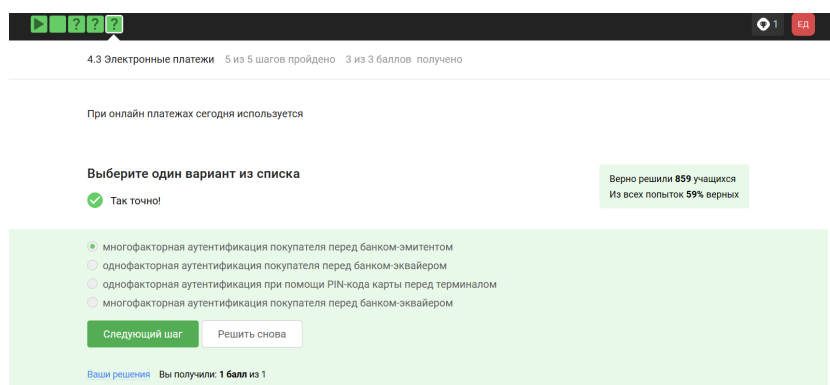


Рис. 2.13: Вопрос 4.3.3

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).

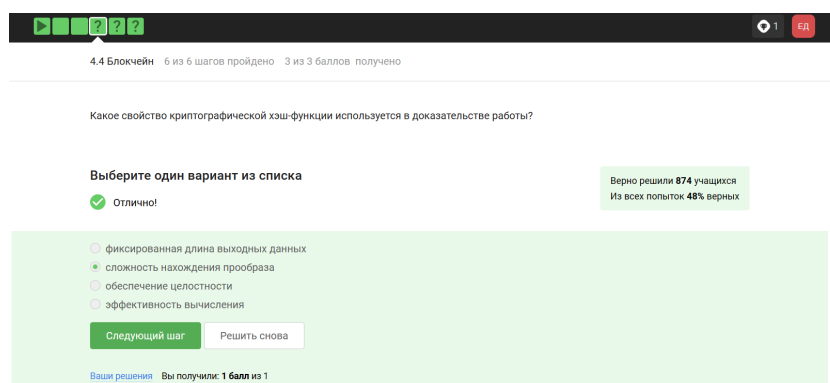


Рис. 2.14: Вопрос 4.4.1

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).

4.4 Блокчейн 6 из 6 шагов пройдено 3 из 3 баллов получено

Консенсус в некоторых системах блокчейн обладает свойствами

Выберите все подходящие ответы из списка

☒ Правильно.

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](#).

Верно решили 785 учащихся
Из всех попыток 22% верных

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

[Следующий шаг](#) [Решить снова](#)

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

Рис. 2.15: Вопрос 4.4.2

Ответ - цифровая подпись (рис. 2.16).

4.4 Блокчейн 6 из 6 шагов пройдено 3 из 3 баллов получено

Секретные ключи какого криптографического примитива хранят участники блокчейна?

Выберите один вариант из списка

☒ Хорошая работа.

Верно решили 872 учащихся
Из всех попыток 46% верных

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

[Следующий шаг](#) [Решить снова](#)

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

Рис. 2.16: Вопрос 4.4.3

3 Выводы

Я прошла третий блок