

Внешний курс

Отчёт по разделу 3

Аскеров Александр Эдуардович

Содержание

1	Пункт 4.1	4
2	Пункт 4.2	7
3	Пункт 4.3	10
4	Пункт 4.4	12
5	Курс завершён	14

Список иллюстраций

1.1	Ключи в асимметричных криптографических примитивах	4
1.2	Свойства криптографической хэш-функции	4
1.3	Алгоритмы цифровой подписи	5
1.4	Код аутентификации сообщения	5
1.5	Обмен ключами Диффи-Хэллмана	6
2.1	Протокол электронной цифровой подписи	7
2.2	Алгоритм верификации электронной цифровой подписи	8
2.3	Характеристики электронной цифровой подписи	8
2.4	Типы сертификата электронной цифровой подписи	9
2.5	Организации по выдаче квалифицированного сертификата ключа проверки электронной подписи	9
3.1	Платёжные системы	10
3.2	Многофакторная аутентификация	10
3.3	Онлайн платежи	11
4.1	Криптографическая хэш-функция	12
4.2	Системы блокчейн	12
4.3	Секретные ключи	13
5.1	Результат завершённого курса	14

1 Пункт 4.1

Укажем, какие ключи имеют стороны в асимметричных криптографических примитивах.

В асимметричных криптографических примитивах

Выберите один вариант из списка

✓ Хорошая работа.

- ☐ одна сторона имеет только секретный ключ, а другая – пару из открытого и секретного ключей
- ☒ обе стороны имеют пару ключей
- ☐ обе стороны имеют общий секретный ключ
- ☐ одна сторона публикует свой секретный ключ, другая - держит его в секрете

Рис. 1.1: Ключи в асимметричных криптографических примитивах

Выберем, свойства криптографической хэш-функции.

Криптографическая хэш-функция

Выберите все подходящие ответы из списка

✓ Верно. Так держать!

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](#).

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

Рис. 1.2: Свойства криптографической хэш-функции

Выберем алгоритмы цифровой подписи.

К алгоритмам цифровой подписи относятся

Выберите все подходящие ответы из списка

✓ Прекрасный ответ.

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

Рис. 1.3: Алгоритмы цифровой подписи

Выберем, к чему относится код аутентификации сообщения.

Код аутентификации сообщения относится к

Выберите один вариант из списка

✓ Всё правильно.

- ☐ асимметричным примитивам
- ☒ симметричным примитивам

Рис. 1.4: Код аутентификации сообщения

Дадим определение обмену ключами Диффи-Хэллмана.

Обмен ключам Диффи-Хэллмана - это

Выберите один вариант из списка

☒ Всё правильно.

- ☐ симметричный примитив генерации общего секретного ключа
- ☐ асимметричный примитив генерации общего открытого ключа
- ☒ асимметричный примитив генерации общего секретного ключа
- ☐ асимметричный алгоритм шифрования

Рис. 1.5: Обмен ключами Диффи-Хэллмана

2 Пункт 4.2

Выберем, к чему относится протокол электронной цифровой подписи.

Протокол электронной цифровой подписи относится к

Выберите один вариант из списка



Отличное решение!



протоколам с симметричным ключом



протоколам с публичным (или открытым) ключом

Рис. 2.1: Протокол электронной цифровой подписи

Выберем, что требует на вход алгоритм верификации электронной цифровой подписи.

Алгоритм верификации электронной цифровой подписи требует на вход

Выберите один вариант из списка

☒ Прекрасный ответ.

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

Рис. 2.2: Алгоритм верификации электронной цифровой подписи

Укажем, что не обеспечивает электронная цифровая подпись.

Электронная цифровая подпись не обеспечивает

Выберите один вариант из списка

☒ Абсолютно точно.

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

Рис. 2.3: Характеристики электронной цифровой подписи

Выберем тип сертификата электронной цифровой подписи для отправки налоговой отчётности в ФНС.

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

Выберите один вариант из списка

Верно решили **904** учащихся
Из всех попыток **67%** верных

☒ Отлично!

☐ простая

☐ усиленная неквалифицированная

☒ усиленная квалифицированная

Рис. 2.4: Типы сертификата электронной цифровой подписи

Выберем, в какой организации можно получить квалифицированный сертификат ключа проверки электронной подписи.

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

Выберите один вариант из списка

Верно решили **902** учащихся
Из всех попыток **60%** верных

☒ Хорошая работа.

☐ в любой организации, имеющей соответствующую лицензию ФСБ

☐ в минкомсвязи РФ

☒ в удостоверяющем (сертификационном) центре

☐ в любой организации по месту работы

Рис. 2.5: Организации по выдаче квалифицированного сертификата ключа проверки электронной подписи

3 Пункт 4.3

Выберем все платёжные системы в списке.

Выберите из списка все платёжные системы.

Выберите все подходящие ответы из списка

✓ Всё правильно.

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

Рис. 3.1: Платёжные системы

Выберем из списка примеры многофакторной аутентификации.

Примером многофакторной аутентификации является

Выберите все подходящие ответы из списка

✓ Отличное решение!

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](#).

- ☐ комбинация проверки пароля + Капча
- ☒ комбинация проверка пароля + код в sms сообщении
- ☒ комбинация код в sms сообщении + отпечаток пальца
- ☐ комбинация PIN код + пароль

Рис. 3.2: Многофакторная аутентификация

Мы выбрали те варианты, в которых используются факторы разных категорий аутентификации.

Выберем, что используется при онлайн платежах.

При онлайн платежах сегодня используется

Выберите один вариант из списка

☒ Правильно, молодец!

- ☒ 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

Рис. 3.3: Онлайн платежи

4 Пункт 4.4

Выберем, какое свойство криптографической хэш-функции используется в доказательстве работы.

Какое свойство криптографической хэш-функции используется в доказательстве работы?

Выберите один вариант из списка

✓ Прекрасный ответ.

- ☐ фиксированная длина выходных данных
- ☒ сложность нахождения прообраза
- ☐ обеспечение целостности
- ☐ эффективность вычисления

Рис. 4.1: Криптографическая хэш-функция

Выберем, какими свойствами обладает консенсус в некоторых 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](#).

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

Рис. 4.2: Системы блокчейн

Выберем, секретные ключи какого криптографического примитива хранят участники блокчейна.

Секретные ключи какого криптографического примитива хранят участники блокчейна?

Выберите один вариант из списка

☒ Хорошая работа.

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

Рис. 4.3: Секретные ключи

5 Курс завершён

Курс завершён.

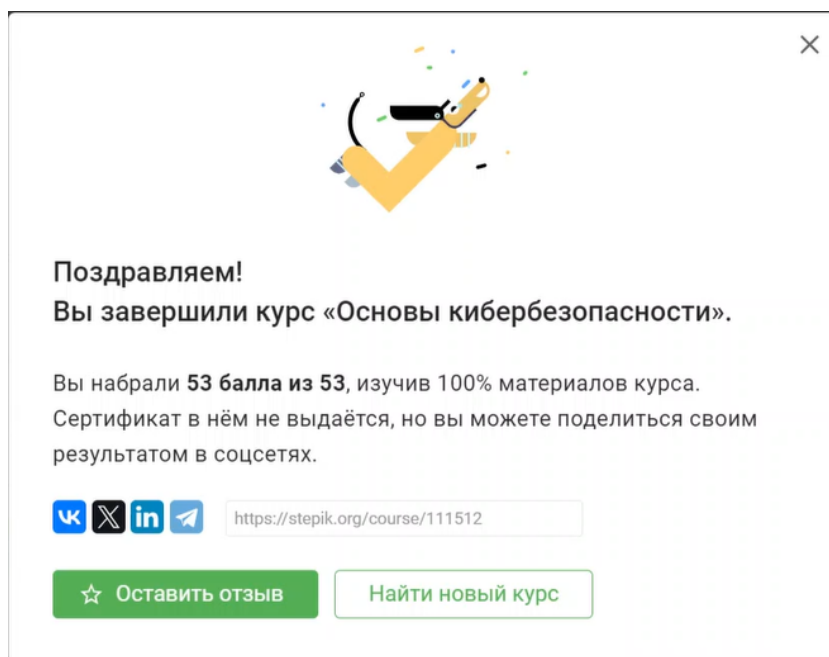


Рис. 5.1: Результат завершённого курса