

Этап3

НКАбд-01-23

Улитина Мария Максимовна

Содержание

1	Выполнение второго этапа внешнего курса	5
2	Выводы	13

Список иллюстраций

1.1	ключи	5
1.2	хэш-функция	6
1.3	функция	6
1.4	код	7
1.5	ключи	7
1.6	подпись	8
1.7	алгоритм	8
1.8	подпись	9
1.9	подпись	9
1.10	организация	10
1.11	платежные системы	10
1.12	примеры	11
1.13	мфа	11
1.14	хэш-функция	12
1.15	консенсус	12

Список таблиц

1 Выполнение второго этапа внешнего курса

Имеют пару ключей (рис. 1.1).

В асимметричных криптографических примитивах

Выберите один вариант из списка

✔ Отлично!

- ☒ обе стороны имеют пару ключей
- ☐ 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 общий секретный ключ

Следующий шаг

Решить снова

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

Рис. 1.1: ключи

Свойства хэш-функции(рис. 1.2).

Криптографическая хэш-функция

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](#).

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

Следующий шаг

Решить снова

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

Рис. 1.2: хэш-функция

Алгоритмы цифровой функции (рис. 1.3).

К алгоритмам цифровой подписи относятся

Выберите все подходящие ответы из списка

☒ 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](#).

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

Следующий шаг

Решить снова

Рис. 1.3: функция

Код аутентификации (рис. 1.4).

Код аутентификации сообщения относится к

Выберите один вариант из списка

☒ Всё правильно.

- ☐ асимметричным примитивам
- ☒ симметричным примитивам

Следующий шаг

Решить снова

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

Рис. 1.4: код

Ключи Диффи-хеллмана(рис. 1.5).

Обмен ключам Диффи-Хэллмана - это

Выберите один вариант из списка

☒ Верно.

- ☐ 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**

Рис. 1.5: ключи

Электронная цифровая подпись(рис. 1.6).

Протокол электронной цифровой подписи относится к

Выберите один вариант из списка

☒ Хорошая работа.

- ☐ протоколам с симметричным ключом
- ☒ протоколам с публичным (или открытым) ключом

Следующий шаг

Решить снова

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

Рис. 1.6: подпись

Алгоритм верификации (рис. 1.7).

Алгоритм верификации электронной цифровой подписи требует на вход

Выберите один вариант из списка

☒ Абсолютно точно.

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

Следующий шаг

Решить снова

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

Рис. 1.7: алгоритм

Не обеспечивает конфиденциальность(рис. 1.8).

Электронная цифровая подпись не обеспечивает

Выберите один вариант из списка

☒ Хорошая работа.

A screenshot of a quiz interface. At the top, there is a green checkmark icon followed by the text 'Хорошая работа.' Below this, there is a light green box containing four radio button options: 'конфиденциальность', 'аутентификацию', 'целостность', and 'неотказ от авторства'. The first option is selected. Below the options are two buttons: 'Следующий шаг' (green) and 'Решить снова' (white). At the bottom of the green box, it says 'Ваши решения' in blue and 'Вы получили: 1 балл' in black.

Рис. 1.8: подпись

Усиленная квалифицированная(рис. 1.9).

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

Выберите один вариант из списка

☒ Отлично!

Верн
Из в

A screenshot of a quiz interface. At the top, there is a green checkmark icon followed by the text 'Отлично!'. Below this, there is a light green box containing three radio button options: 'усиленная квалифицированная', 'простая', and 'усиленная неквалифицированная'. The first option is selected. Below the options are two buttons: 'Следующий шаг' (green) and 'Решить снова' (white). At the bottom of the green box, it says 'Ваши решения' in blue and 'Вы получили: 1 балл' in black.

Рис. 1.9: подпись

Организация(рис. 1.10).

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

Выберите один вариант из списка

☒ Верно. Так держать!

Верно решил 971 учащихся
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. 1.10: организация

Платежные системы МИР и Мастер Кард(рис. 1.11).

Выберите из списка все платежные системы.

Выберите все подходящие ответы из списка

☒ Всё правильно.

Вы решили сложную задачу, поздравляем! Вы можете помочь остальным ученикам с их вопросами, или сравнить своё решение с другими на [форуме решений](#).

- ☐ BitCoin
- ☒ MasterCard
- ☐ SecurePay
- ☐ POS-терминал
- ☐ банкомат
- ☒ МИР

Следующий шаг

Решить снова

Рис. 1.11: платежные системы

МФ аутентификация(рис. 1.12).

Примером многофакторной аутентификации является

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](#).

- ☐ 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. 1.12: примеры

Где используется мфа(рис. 1.13).

При онлайн платежах сегодня используется

Выберите один вариант из списка

☒ Всё получилось!

- ☒ 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. 1.13: мфа

Сложность нахождения прообраза (рис. 1.14).

Какое свойство криптографической хэш-функции используется в доказательстве работы?

Выберите один вариант из списка

✓ Верно.

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

Следующий шаг

Решить снова

[Ваши решения](#) Вы получили: 1 балл

Рис. 1.14: хэш-функция

консенсус(рис. 1.15).

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
- ☒ постоянства
- ☒ живучесть
- ☒ открытость

Следующий шаг

Решить снова

[Ваши решения](#) Вы получили: 1 балл

Рис. 1.15: консенсус

2 Выводы

Выполнен третий этап.