

Внешний курс. Этап 3

Криптография на практике

Буллер Т.А.

13 мая 2025

Российский университет дружбы народов, Москва, Россия

Информация

- Буллер Татьяна Александровна
- студент направления Бизнес-информатика
- Российский университет дружбы народов

Вводная часть

- Криптографические примитивы
- Блокчейн-системы

- Получение и закрепление на практике знаний о криптографических примитивах и областях их применения.

Выполнение контрольных заданий

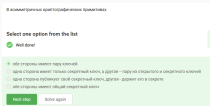


Рис. 1: Задание 1

В ассиметричных примитивах обе стороны имеют пару ключей: секретный (частный) и открытый. Секретный ключ не публикуется ни в коем случае, общий ключ стороны имеют в симметричных примитивах.

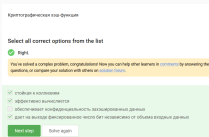


Рис. 2: Задание 2

Хорошая хэш-функция должна выдавать стойкие к коллизиям результаты, что, однако, не всегда соответствует правде на практике. На выходе, вне зависимости от объема входных данных, она дает фиксированное число бит, но не обеспечивает конфиденциальность данных.

К алгоритмам цифровой подписи относятся

Select all correct options from the list

✔ Yes!

You've solved a complex problem, congratulations! Now you can help other questions, or compare your solution with others on [solution forum](#).

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

Next step Solve again

Рис. 3: Задание 3

Из представленных в списке AES - алгоритм симметричного шифрования, SHA2 - хэш-функция. Остальные как раз являются алгоритмами, применимыми для создания цифровой подписи.

Код аутентификации сообщения относится к

Select one option from the list

✓ Absolutely right.

☒ симметричным примитивам

☐ асимметричным примитивам

Next step Solve again

Рис. 4: Задание 4

Код аутентификации сообщения - симметричный примитив, представляющий собой общий для сторон секретный ключ.

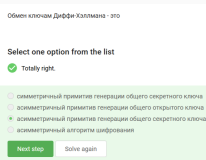


Рис. 5: Задание 5

Алгоритм обмена ключами DH - асимметричный алгоритм генерации общего секретного ключа, где стороны получают общий ключ из собственного секрета и открытого ключа на основе общего секрета, переданного другой стороной.

Протокол электронной цифровой подписи относится к

Select one option from the list

✔ Well done!

☐ протоколом с симметричным ключом

☒ протоколом с публичным (или открытым) ключом

Next step Solve again

Рис. 6: Задание 6

Протоколы ЭЦП относятся к протоколам с открытым ключом, где секретный ключ используется для непосредственно подписания документа, открытый - для проверки подлинности подписи.

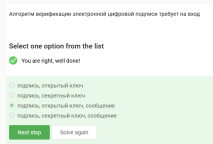


Рис. 7: Задание 7

Алгоритм верификации требует на вход подпись, сообщение, которое было ею подписано, и открытый ключ.

Электронная цифровая подпись не обеспечивает

Select one option from the list

✔ Good job.

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

Next step Solve again

Рис. 8: Задание 8

ЭЦП не обеспечивает конфиденциальности, скорее, наоборот - она обеспечивает подтверждение личности отправителя документа.

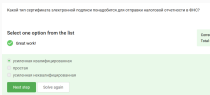


Рис. 9: Задание 9

Для отправки налоговой отчетности ЭЦП должна быть подтверждена, поэтому подойдет только усиленная квалифицированная подпись.



Рис. 10: Задание 10

Квалифицированный сертификат проверки можно получить только в специализированных сертификационных центрах. Минкомсвязи непосредственно этим не занимаются.

Выберите из списка все платежные системы.

Select all correct options from the list

✔ Yes!

You've solved a complex problem, congratulations! Now you can questions, or compare your solution with others on [solution foru](#)

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

Next step Solve again

Рис. 11: Задание 11

Платежными системы из перечисленных являются только МИР и мастеркард. Биткоин - криптовалюта, ПОС-терминал и банкомат - технические средства проведения банковских операций.

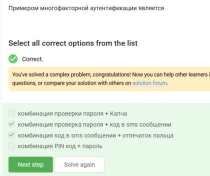


Рис. 12: Задание 12

Многофакторная аутентификация сочетает “то, что я знаю” и “то, что у меня есть”.
Комбинации ПИН + пароль и пароль + капча не удовлетворяют этому критерию.

При онлайн-платежах сегодня используется

Select one option from the list

☒ Correct.

- ☒ многофакторная аутентификация покупок перед банком-эмитентом
- ☐ одофакторная аутентификация покупок перед банком-эмитентом
- ☐ одофакторная аутентификация при покупке РН-кода карты перед терминалом
- ☐ многофакторная аутентификация покупок перед банком-эмитентом

[Next step](#) [Solve again](#)

Рис. 13: Задание 13

При онлайн-платежах используется многофакторная аутентификация перед банком-эмитентом, так как только он обладает данными о конкретном плательщике и обязан удостовериться, что платеж проводится легитимным клиентом.

Какие свойства криптографической функции используются в доказательстве работы?

Select one option from the list

☒ Good news for you, correct

- ☐ Фиксированная длина выходных данных
- ☒ сложность нахождения прообраза
- ☐ обеспечение целостности
- ☐ обратимость вычисления

[Next step](#) [Go back](#)

Рис. 14: Задание 14

В доказательстве работы используется свойство сложности нахождения прообраза (нарочно не придумаешь), остальные не обеспечивают доказательства как такового.

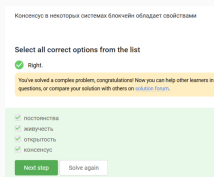


Рис. 15: Задание 15

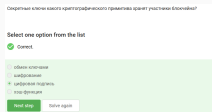


Рис. 16: Задание 16

Участники блокчейна хранят секретные ключи цифровой подписи. Обмен ключами и шифрование осуществляются независимо от них.

Выводы

Получены и закреплены на практике знания о криптографических примитивах и областях их применения.