Внешний курс. Этап 3

Криптография на практике

Буллер Т.А.

13 мая 2025

Российский университет дружбы народов, Москва, Россия

Информация

Докладчик

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

Вводная часть

Объект и предмет исследования

- Криптографические примитивы
- Блокчейн-системы

Цели и задачи

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

Выполнение контрольных заданий

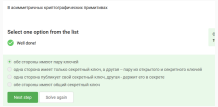

Рис. 1: Задание 1

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.

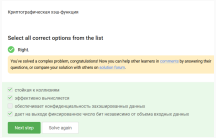

Рис. 2: Задание 2

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.

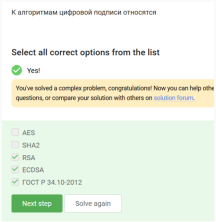

Рис. 3: Задание 3

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

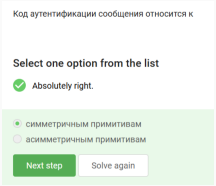

Рис. 4: Задание 4

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

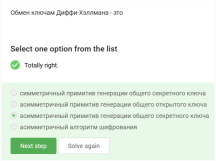

Рис. 5: Задание 5

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

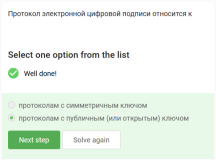

Рис. 6: Задание 6

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

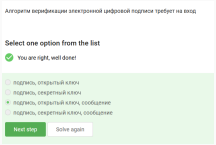

Рис. 7: Задание 7

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

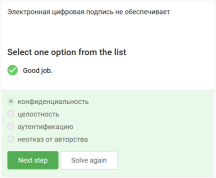

Рис. 8: Задание 8

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

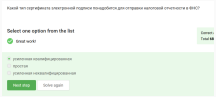

Рис. 9: Задание 9

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

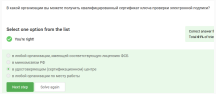

Рис. 10: Задание 10

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

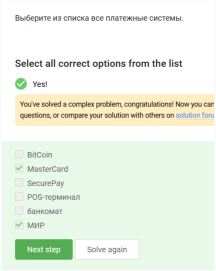

Рис. 11: Задание 11

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

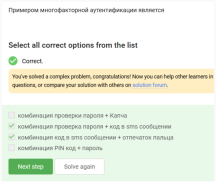

Рис. 12: Задание 12

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

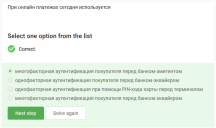

Рис. 13: Задание 13

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.

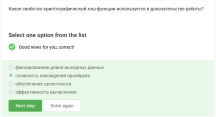

Рис. 14: Задание 14

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

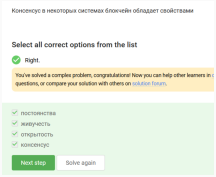

Рис. 15: Задание 15

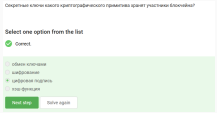

Рис. 16: Задание 16

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

Выводы

Выводы

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