Внешний курс. Блок 3. Криптография на практике

Основы информационной безопасности

Мурашов И. В., НКАбд-03-23 17 мая 2025

Российский университет дружбы народов, Москва, Россия

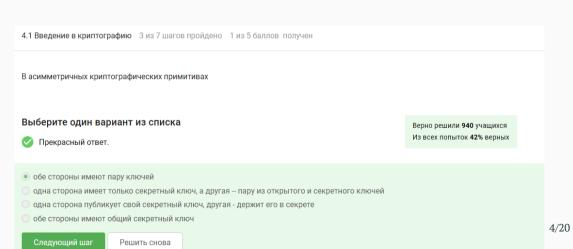
Докладчик

- Мурашов Иван Вячеславович
- Студент, 2 курс, группа НКАбд-03-23
- Российский университет дружбы народов
- 1132236018@rudn.ru
- https://neve7mind.github.io

Цель работы

Выполнение контрольных заданий 3го блока внешнего курса "Основы Кибербезопасности".

Асимметричные криптографические системы подразумевают под собой то, что пара ключей есть у обоих сторон.



Отмечены основные условия для криптографической хэш-функции.

4.1 Введение в криптографию 4 из 7 шагов пройдено 2 из 5 баллов получено				
Криптографическая хэш-функция				
Выберите все подходящие ответы из списка	Верно решили 798 учащихся			
Хорошая работа.	Из всех попыток 11% верных			
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.				
 ✓ дает на выходе фиксированное число бит независимо от объема входных данных ✓ эффективно вычисляется ✓ стойкая к коллизиям □ обеспечивает конфиденциальность захэшированных данных 				
Следующий шаг Решить снова				

Отмечены алгоритмы цифровой подписи.

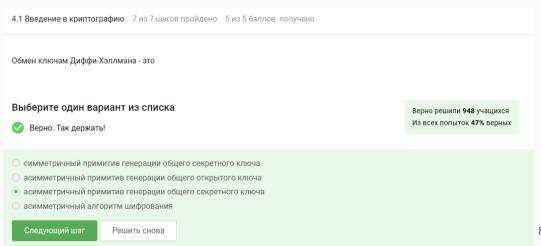
4.1 Введение в криптографию 5 из 7 шагов пройдено 3 из 5 баллов получено К алгоритмам цифровой подписи относятся Выберите все подходящие ответы из списка Верно решили 834 учащихся Из всех попыток 19% верных Хорошие новости, верно! Вы решили сложную задачу, поздравляем! Вы можете помочь остальным учащимся в комментариях, отвечая на их вопросы, или сравнить своё решение с другими на форуме решений. AES SHA2 ✓ RSA ✓ ECDSA ✓ FOCT P 34.10-2012

симметричным примитивам

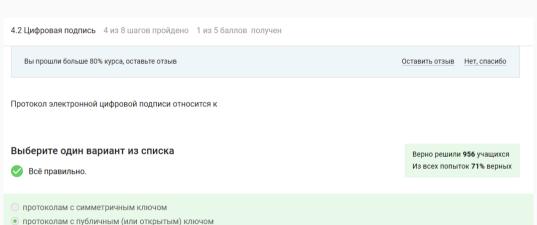
В информационной безопасности аутентификация сообщения или аутентификация источника данных-это свойство, которое гарантирует, что сообщение не было изменено во время передачи (целостность данных) и что принимающая сторона может проверить источник сообщения.



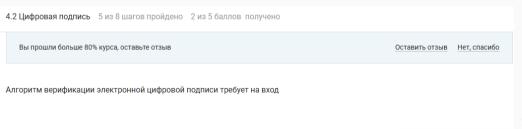
Определение обмена ключами Диффи-Хэллмана.



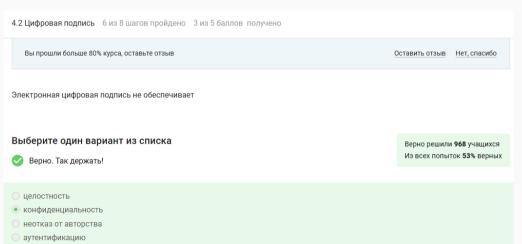
По определению цифровой подписи протокол ЭЦП относится к протоколам с публичным ключом.



лгоритм 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.

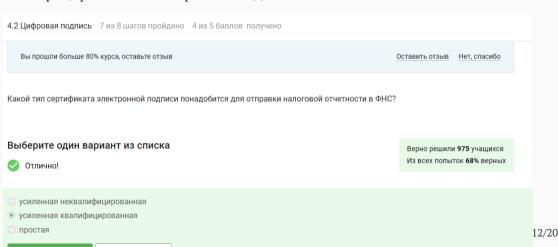


Электронная подпись обеспечивает все указанное, кроме конфиденциальности.



D-----

Для отправки налоговой отчетности в ФНС используется усиленная квалифицированная электронная подпись.

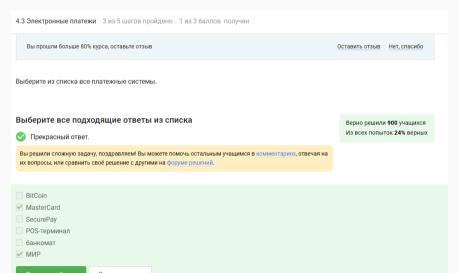


Верный ответ укзаан на изображении.

4.2 Цифровая подпись 8 из 8 шагов пройдено 5 из 5 баллов получено				
Вы прошли больше 80% курса, оставьте отзыв	Оставить отзыв Нет, спасибо			
В какой организации вы можете получить квалифицированный сертификат ключа проверки электронной подписи?				
Выберите один вариант из списка Верно.	Верно решил 971 учащийся 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				

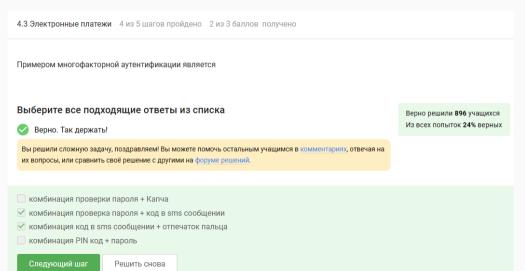
Электронные платежи

Известные платежные системы - Visa, MasterCard, МИР.



Электронные платежи

Верный ответ на изображении.



Электронные платежи

При онлайн платежах используется многофакторная аутентификация.

4.3 Электронные плате	жи 5 из 5 шагов про	йдено 3 из 3 баллов получено	
При онлайн платежах с	сегодня используется		
Выберите один ва Всё правильно.	риант из списка		Верно решили 957 учащихся Из всех попыток 59 % верных
однофакторная ауте однофакторная ауте	ентификация покупате ентификация при поме	теля перед банком-эмитентом еля перед банком-эквайером ощи PIN-кода карты перед терминало теля перед банком-эквайером	м
Следующий шаг	Решить снова		

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.

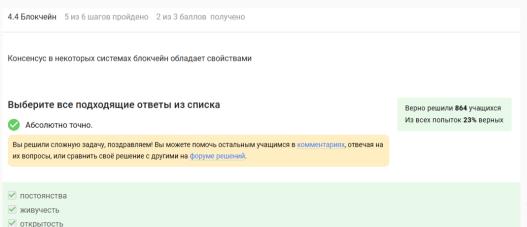


Какое свойство криптографической хэш-функции используется в доказательстве работы?

Выберите один вариант из списка

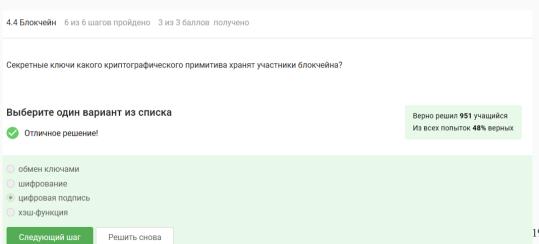
Блокчейн

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 самоу сети.



Блокчейн

Ответ - цифровая подпись.



Выводы

Был пройден третий блок курса "Основы кибербезопасности", мной были изучены такие понятия как цифровая подпись, электронные платежи и блокчейн.