Внешний курс. Блок 3: Криптография на практике

Неустроева И.Н.

Российский университет дружбы народов, Москва, Россия

Информация

Докладчик

- Неустроева Ирина Николаевна
- студентка группы НБИ 02-23
- Российский университет дружбы народов

Преподаватель

- Кулябов Дмитрий Сергеевич
- д.ф.-м.н., профессор
- профессор кафедры прикладной информатики и теории вероятностей
- Российский университет дружбы народов

Вводная часть

Цели и задачи

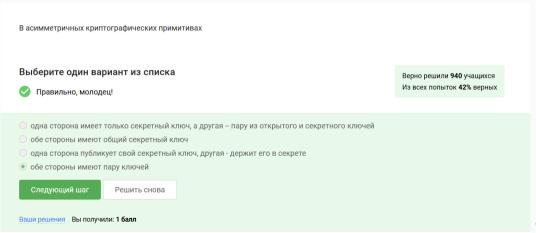
Выполненить контрольные задания третьего блока "Криптография на практи" внешнего курса "Основы кибербезопасности".

Материалы и методы

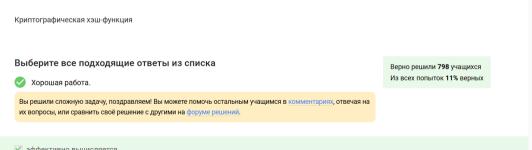
Интернет-ресурсы

Основная часть

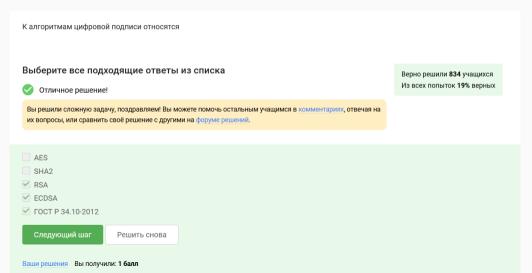
В асимметричной криптографии у каждой из старон есть пара ключей: открытый и секретный ключ



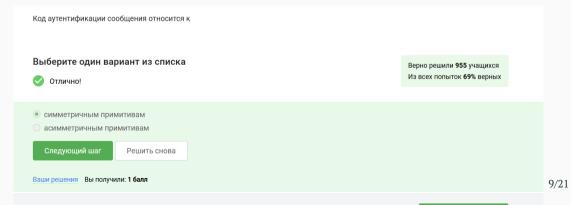
Криптографическая хэш-функция обладает важным свойством стойкости к коллизиям, что означает, что крайне сложно найти два разных входа, которые дают одинаковый хэш. Она принимает произвольный объем данных и выдает фиксированную строку заданной длины (например, n). Обычно функция сжимает данные, преобразуя большой набор информации в небольшое значение



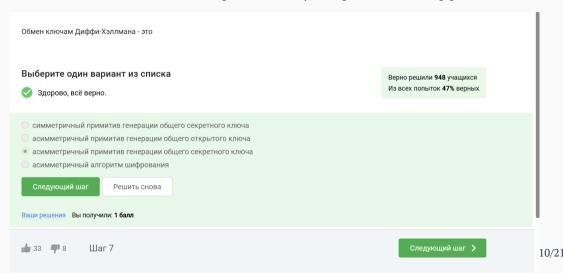
Отмечены алгоритмы цифровой подписи



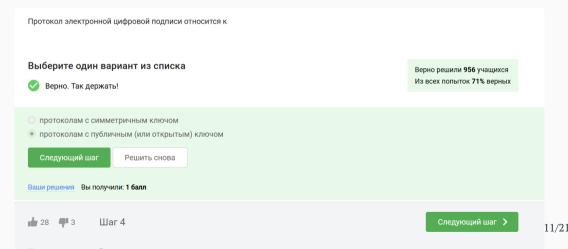
Код аутентификации сообщения (MAC) относится к симметричным примитивам, поскольку для его генерации и проверки используется общий секретный ключ, известный только отправителю и получателю, что обеспечивает целостность и аутентичность данных



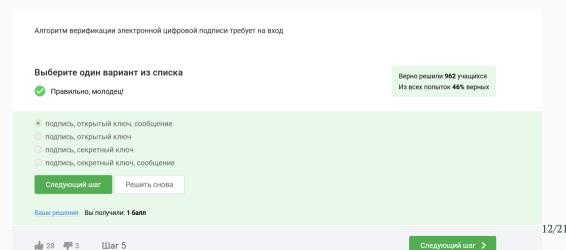
Чтобы ответить на данный вопрос использую определение Диффи-Хэллмана



По определению цифровой подписи протокол ЭЦП относиться к протоколам с публичным ключом



Каждая машина процедуру верификации, которая берет на вход само обновление, подпись и открытый ключ разработчика



Цифровая подпись обеспечивает три ключевых функции:

- 1. Целостность сообщения изменения в сообщении приводят к некорректной проверке подписи.
- 2. Аутентификация позволяет установить, что подпись принадлежит конкретному владельцу.
- 3. Неотказ от авторства подписавший не может отказаться от своей подписи.

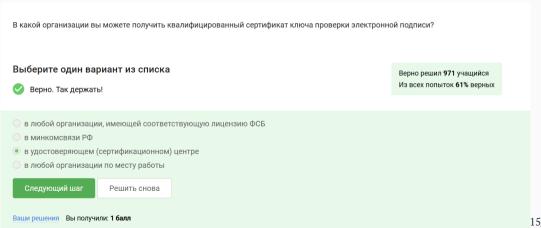
Однако, если секретный ключ украден, безопасность подписи подрывается, и она не обеспечивает конфиденциальности

Ваши решения Вы получили: 1 балл

Усиленная квалифицированная подпись (УКЭП) имеет юридическую силу и равнозначна рукописной подписи. Для её получения необходимо обратиться в аккредитованный сертификационный центр с паспортом и другими данными.

Какой тип сертификата электронной подписи понадобится для отправки налоговой отчетности в ФНС?		
Выберите один вариант из списка Верно.	Верно решили 975 учащихся Из всех попыток 68% верных	
усиленная неквалифицированная усиленная квалифицированная простая		
Следующий шаг		14/2

Сертификат подписывается с помощью электронной подписи уже доверенной стороной, удостоверяющим центром.



Выполнение заданий блока Электронные платежи

На данный момент существуют такие платежные системы, как: Visa, MasterCard, MИР

Выберите все подходящие ответы из списка Верно решили 900 учащихся Из всех попыток 24% 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. ВіtCoin МаsterCard	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. ВitCoin	Зыберите из списка все платежные системы.	
их вопросы, или сравнить своё решение с другими на форуме решений. ВitCoin MasterCard	их вопросы, или сравнить своё решение с другими на форуме решений. ВitCoin ✓ MasterCard SecurePay РOS-терминал		
✓ MasterCard	✓ MasterCard SecurePay РОS-терминал		
	РОS-терминал	✓ MasterCard	

Выполнение заданий блока Электронные платежи

Основные категории вещей, которые мы можем использовать для доказательства своей идентичности:

- 1. Знание: Это что-то, что я знаю, например, пароль, PIN-код или секретный кол для онлайн-платежей.
- 2. Владение: В онлайн-платежах используется второй фактор это то, чем я владею, например, телефон, на который приходит код для подтверждения.
- 3. Свойства: Биометрические данные, такие как отпечаток пальца или сетчатка глаза, служат третьим фактором аутентификации.
- 4. Локация: Четвертый фактор аутентификации это место, откуда осуществляется доступ, что также может быть учтено при проверке идентичности.

17/21

Выполнение заданий блока Блокчейн

Proof-of-Work (PoW) — это способ, который используется в блокчейне для подтверждения транзакций и создания новых блоков. В этом процессе майнеры (люди, которые занимаются добычей криптовалюты) соревнуются друг с другом за завершение транзакций в сети и за вознаграждение

Когда люди отправляют друг другу цифровые деньги, эти транзакции собираются в блоки и добавляются в общую базу данных, называемую блокчейном. Чтобы сделать сеть безопасной и защитить её от мошенничества, PoW требует много вычислительных ресурсов. Это значит, что для успешного участия в процессе нужно много мощных компьютеров

Какое свойство криптографической хэш-функции используется в доказательстве работы?

Выберите один вариант из списка



Выполнение заданий блока Блокчейн

В основе любого блокчейна, включая биткоин, лежит консенсус — публичная структура данных (ledger), содержащая историю всех транзакций. Консенсус обеспечивает четыре ключевых свойства:

- 1. Постоянство: Добавленные данные не могут быть удалены.
- 2. Согласованность: Все участники видят и согласны с одними и теми же данными, за исключением последних изменений.
- 3. Живучесть: Возможность добавления новых транзакций в любое время.
- 4. Открытость: Любой желающий может стать участником блокчейна.

Эти свойства обеспечивают надежность и безопасность системы.

Выполнение заданий блока Блокчейн

В блокчейне у каждого из трех участников есть секретный ключ, который они используют для подтверждения транзакций. Этот секретный ключ позволяет создавать цифровую подпись, которая служит доказательством того, что транзакция была инициирована конкретным участником. Цифровая подпись основана на паре ключей — секретном и открытом. Секретный ключ используется для подписания транзакции, а открытый ключ позволяет другим участникам проверить подлинность этой подписи. Таким образом, цифровая подпись обеспечивает безопасность и аvтентичность транзакций в блокчейне.

Секретные ключи какого криптографического примитива хранят участники блокчейна?

Выберите один вариант из списка



Вывод

В результате 3 этапа я узнала много нового о криптографии, цифровых подписях и технологиях бкокчейна. Выяснила, как обеспечивается безопасность транзакций.

:::