Внешний курс. Блок 3: Криптография на практике

Дисцеплина: Основы информационной безопасности

Неустроева Ирина Николаевна

Содержание

Список иллюстраций

Список таблиц

1 Цель работы

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

2 Выполнение заданий блока “Основы Кибербезопасности”

2.1 Введение в криптографию

В асимметричной криптографии у каждой из старон есть пара ключей: открытый и секретный ключ (рис. 2.1).

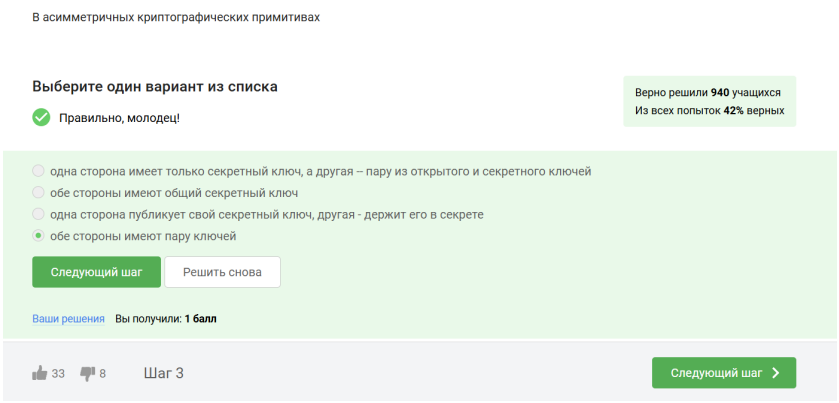

Рис. 2.1: Вопрос 4.1.1

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. (рис. 2.2).

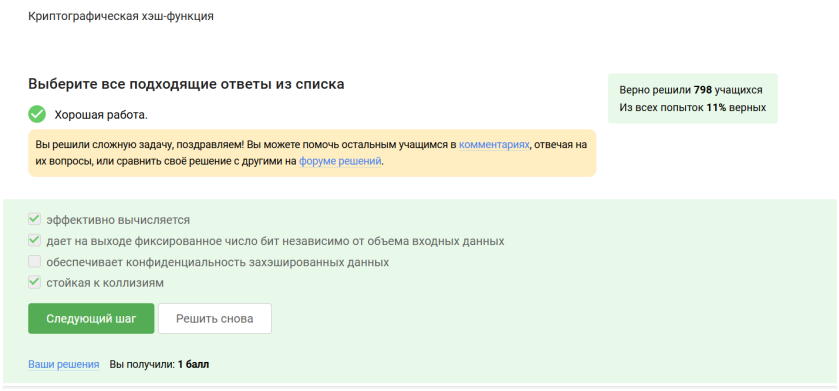

Рис. 2.2: Вопрос 4.1.2

Отмечены алгоритмы цифровой подписи (рис. 2.3).

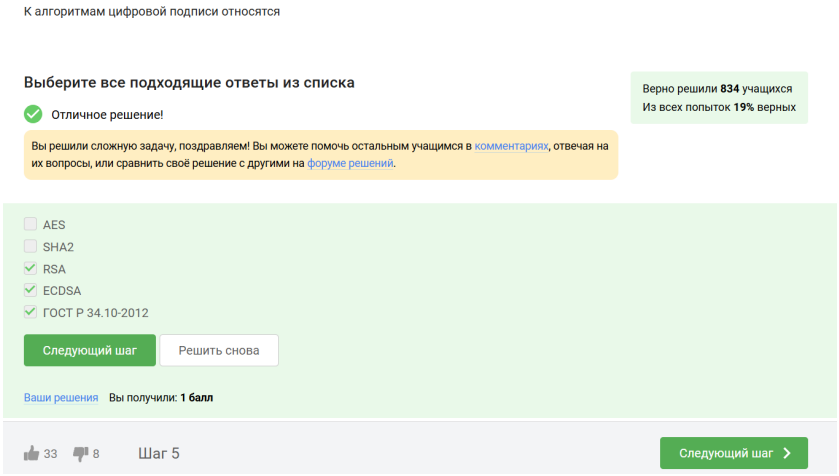

Рис. 2.3: Вопрос 4.1.3

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.(рис. 2.4).

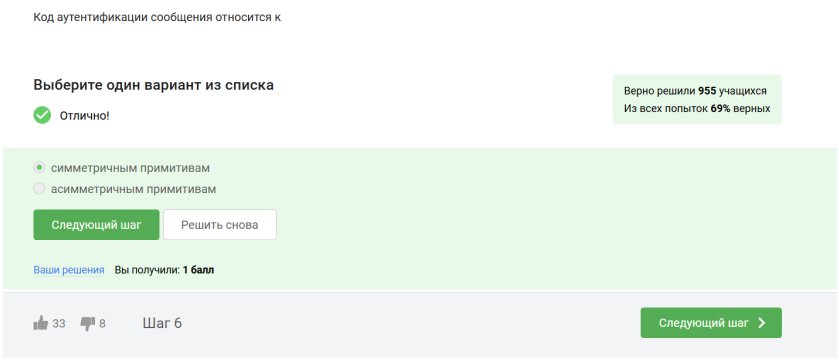

Рис. 2.4: Вопрос 4.1.4

Чтобы ответить на данный вопрос использую определение Диффи-Хэллмана (рис. 2.5).

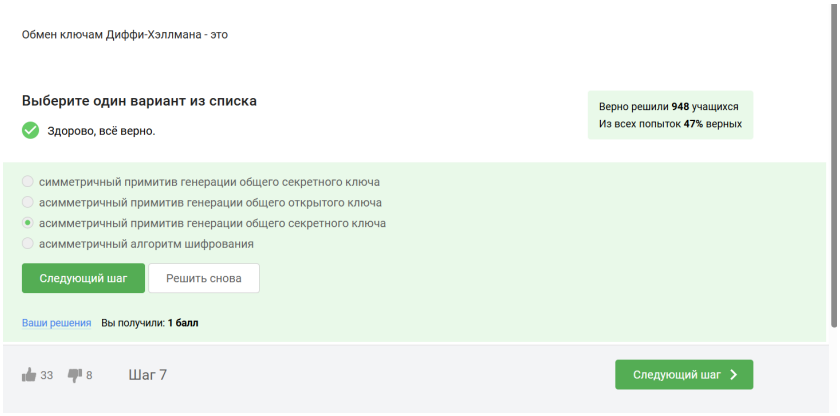

Рис. 2.5: Вопрос 4.1.5

2.2 Цифровая подпись

По определению цифровой подписи протокол ЭЦП относиться к протоколам с публичным ключом (рис. 2.6).

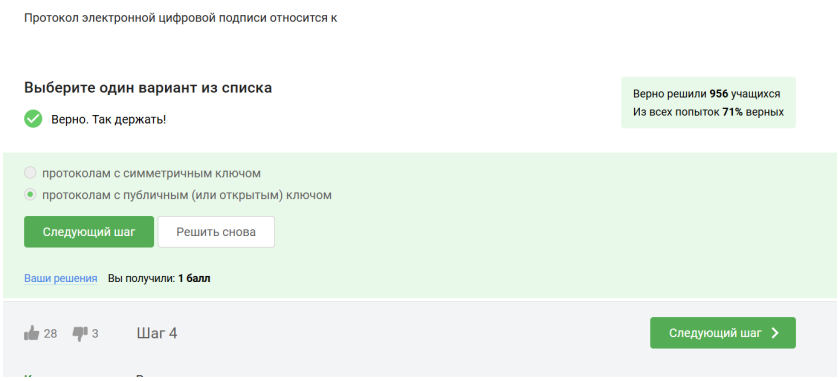

Рис. 2.6: Вопрос 4.2.1

Каждая машина процедуру верификации, которая берет на вход само обновление, подпись и открытый ключ разработчика (рис. 2.7).

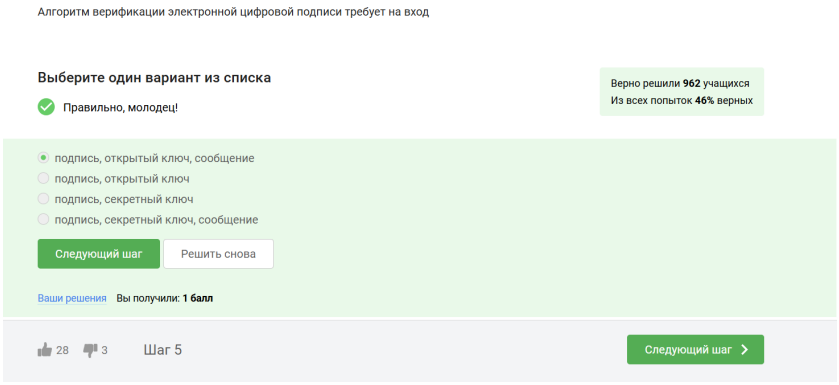

Рис. 2.7: Вопрос 4.2.2

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.(рис. 2.8).

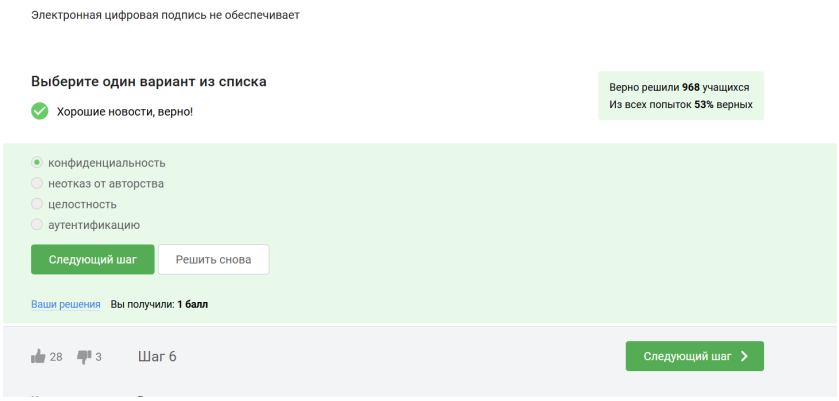

Рис. 2.8: Вопрос 4.2.3

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. (рис. 2.9).

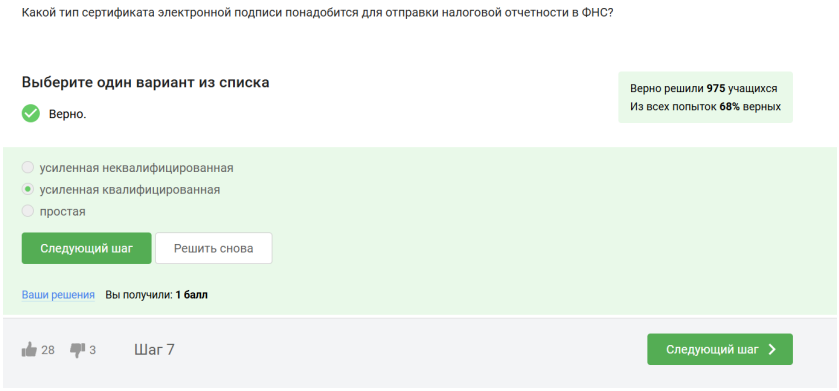

Рис. 2.9: Вопрос 4.2.4

Сертификат подписывается с помощью электронной подписи уже доверенной стороной, удостоверяющим центром. (рис. 2.10).

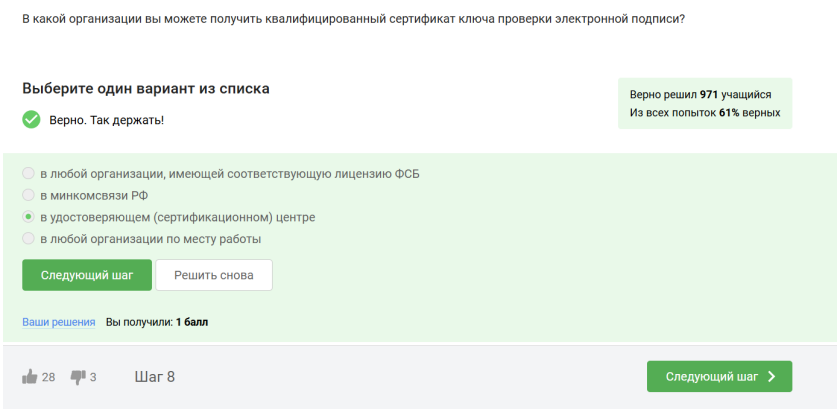

Рис. 2.10: Вопрос 4.2.5

2.3 Электронные платежи

На данный момент существуют такие платежные системы, как: Visa, MasterCard, МИР (рис. 2.11).

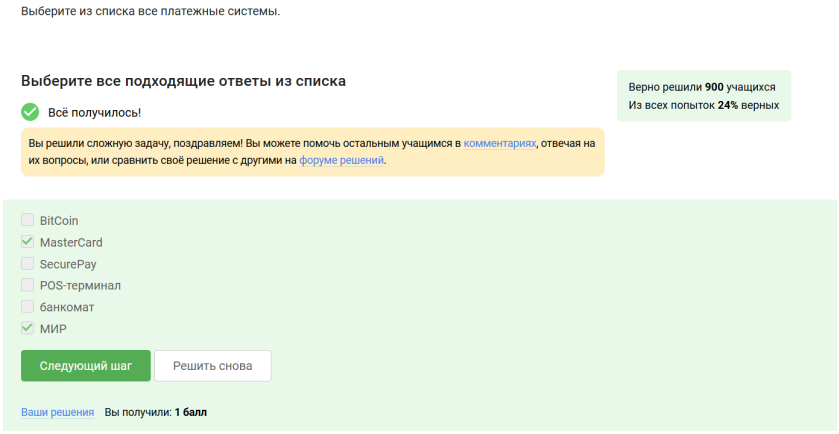

Рис. 2.11: Вопрос 4.3.1

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 код 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. (рис. 2.12).

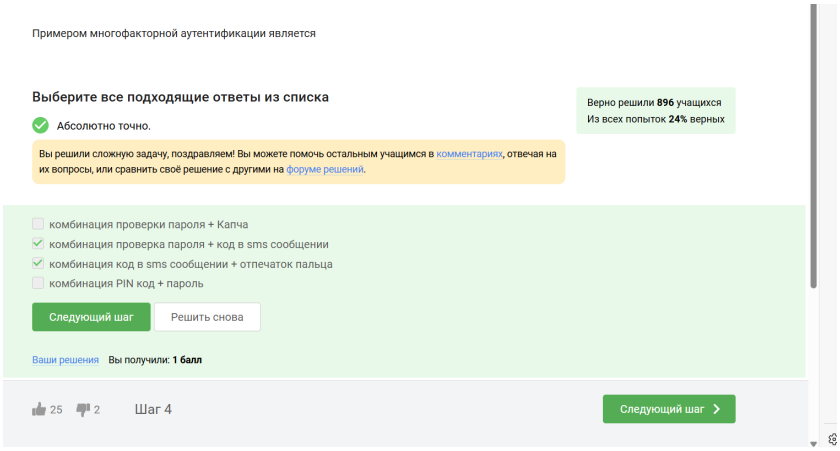

Рис. 2.12: Вопрос 4.3.2

При онлайн платежах используется многофакторная аутентификация банком-эмитентом (выпустившим карту), чтобы удостовериться, что транзакцию совершает именно владелец карты или счета, а не злоумышленник(рис. 2.13).

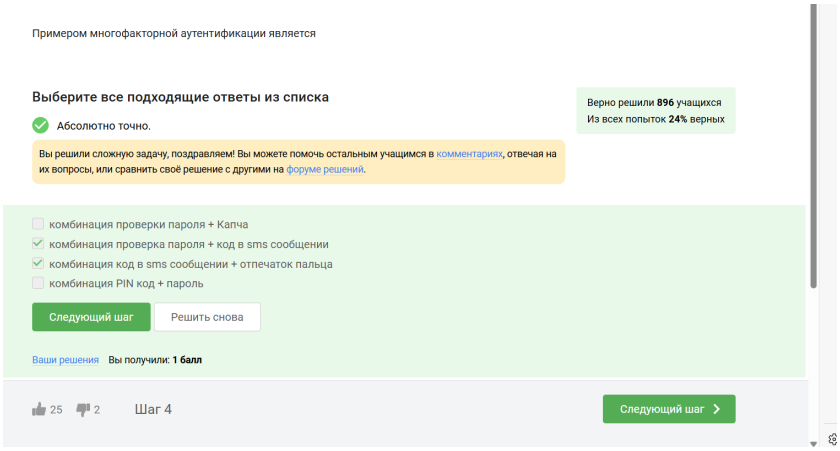

Рис. 2.13: Вопрос 4.3.3

2.4 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.(рис. 2.14).

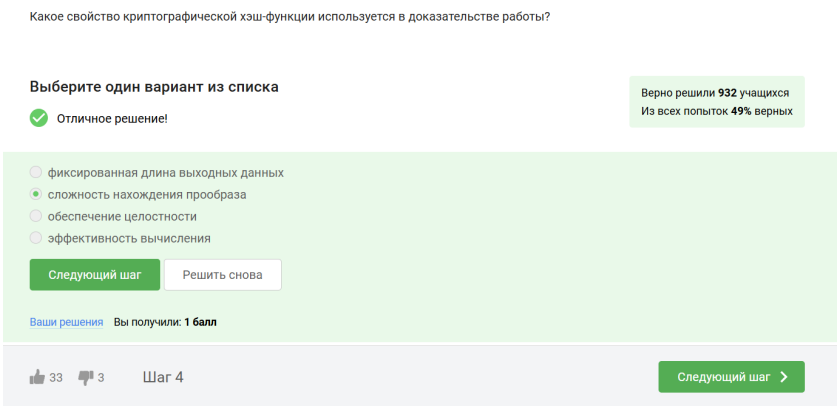

Рис. 2.14: Вопрос 4.4.1

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. (рис. 2.15).

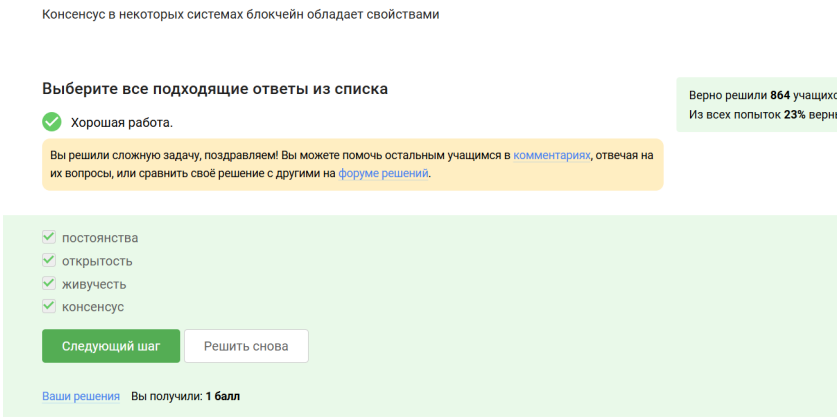

Рис. 2.15: Вопрос 4.4.2

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 аутентичность транзакций в блокчейне. (рис. 2.16).

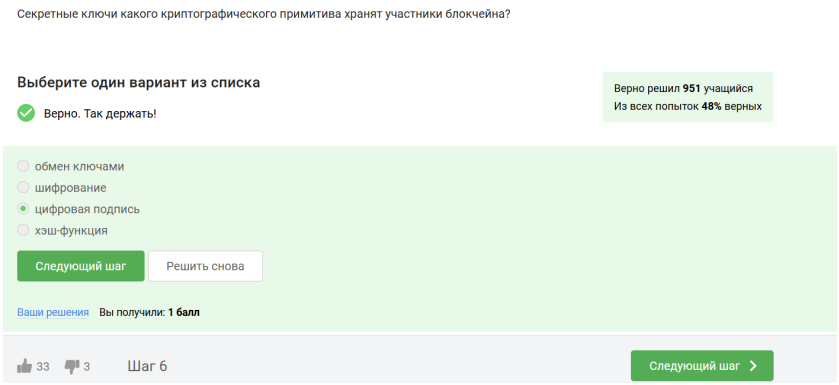

Рис. 2.16: Вопрос 4.4.3

3 Выводы

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