Отчёт по Внешнему Курсу - Этап 3

Основы информационной безопасности

Чистов Даниил Максимович

Содержание

Список иллюстраций

1 Цель работы

Пройти внешний курс - Этап 3

2 Выполнение лабораторной работы

В лекционных материалах было сказано, что в протоколы прикладного уровня включён HTTPS (рис. 2.1).

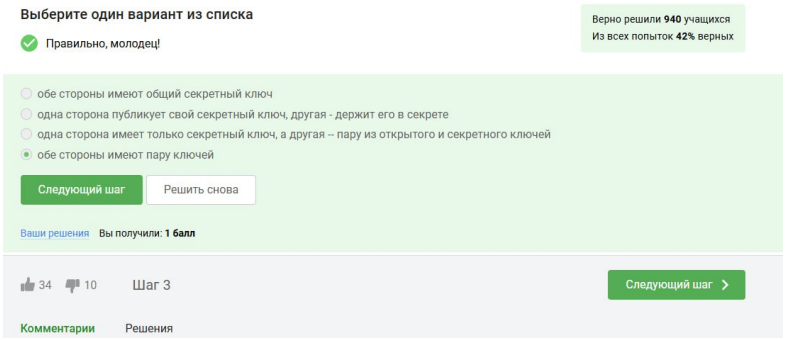

Рис. 2.1: Задание 001

Обе стороны имеют публичный ключ и секретный ключ, одна сторона открывает публичный ключ, а другая использует его для шифрования, но только владелец секретного ключа его расшифровывает (рис. 2.2).

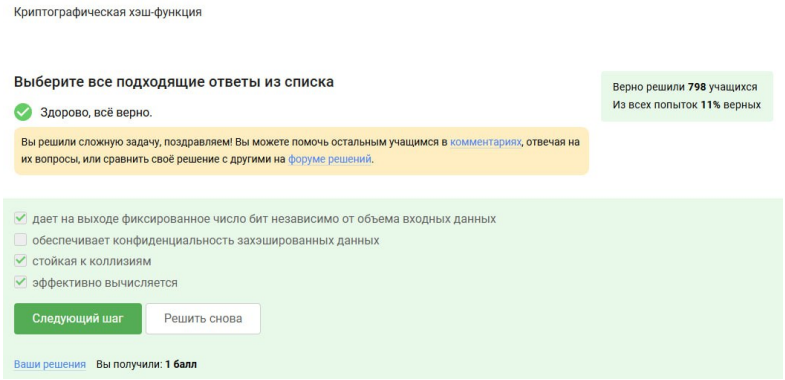

Рис. 2.2: Задание 002

Всё подходит, но очевидно, что хэш-функция не обеспечивает конфиденциальность (рис. 2.3).

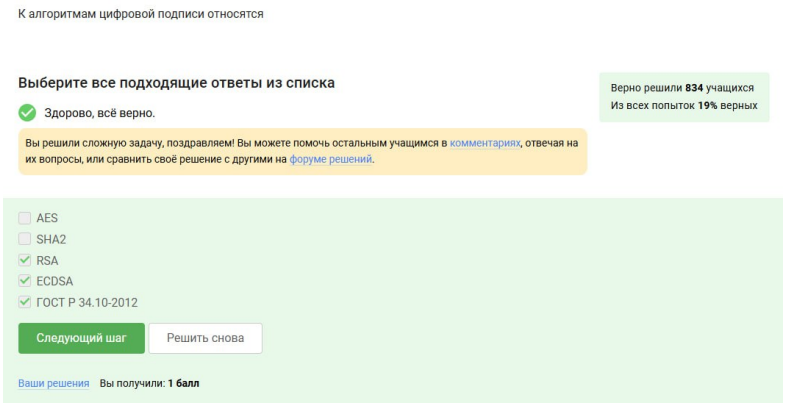

Рис. 2.3: Задание 003

Первые два ответа - никак не относятся к цифровой подписи, это алгоритм симметричного шифрования (AES) и хэш-функция (рис. 2.4).

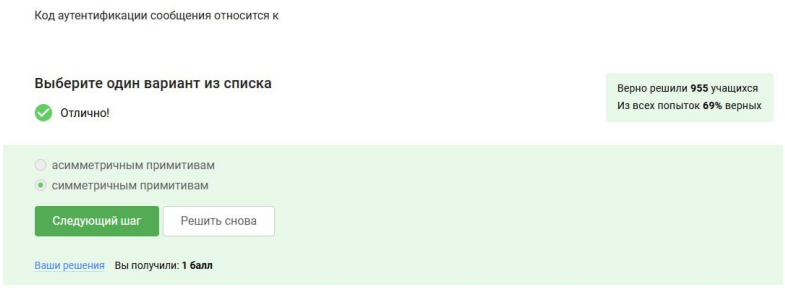

Рис. 2.4: Задание 004

Т.к. обе стороны по сути проверяются по одному ключу, следовательно это симметричная криптография (рис. 2.5).

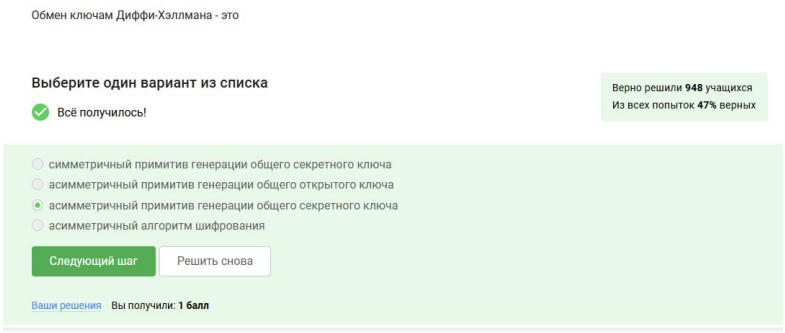

Рис. 2.5: Задание 005

Асимметричный, т.к. у каждой стороны и свой секретная и открытая часть, и он устанавливает ключ, но не шифрует (рис. 2.6).

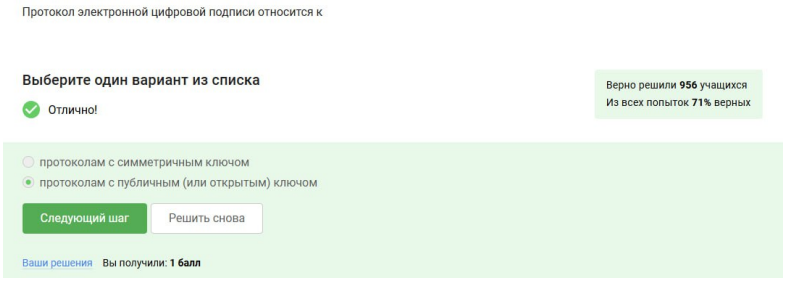

Рис. 2.6: Задание 006

Т.к. для подписей используется асимметричная криптография, следовательно это публичный протокол (рис. 2.7).

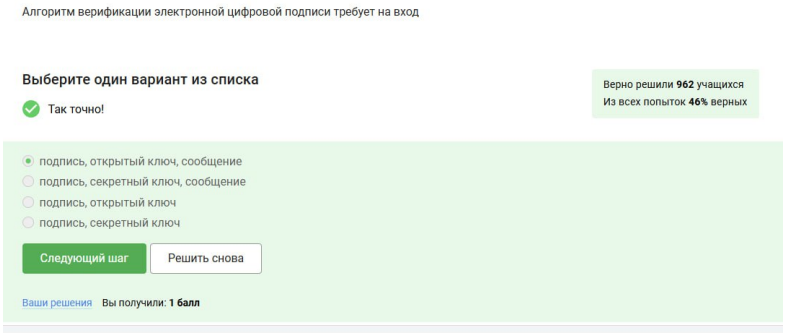

Рис. 2.7: Задание 007

Открытый ключ используется для расшифровки подписи, подпись это зашифрованный хэш, ну и сам хэш (рис. 2.8).

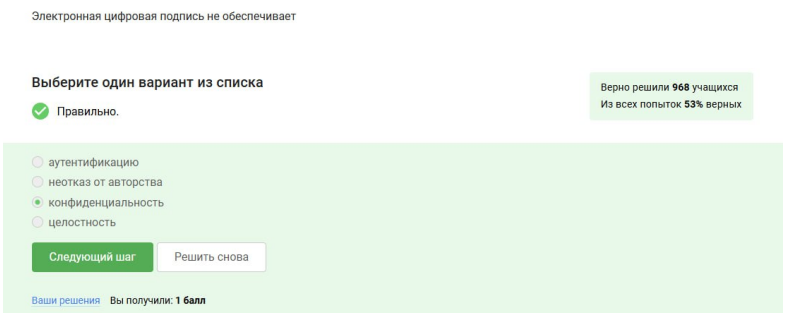

Рис. 2.8: Задание 008

Конфиденциальность не обеспечивается, т.к. сообщение не шифруется (рис. 2.9).

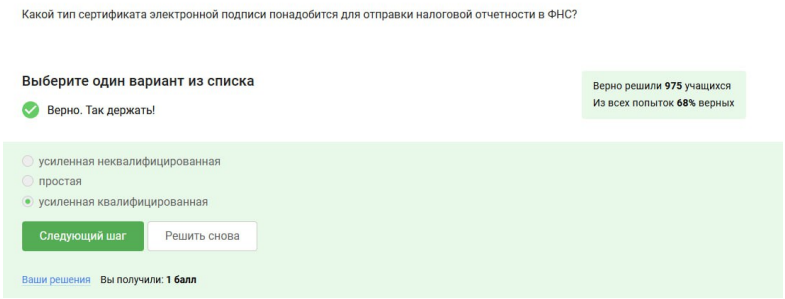

Рис. 2.9: Задание 009

Она создаётся с использование сертифицированных средств криптозащиты, а также имеет юридическую силу, что важно при работе с государством (рис. 2.10).

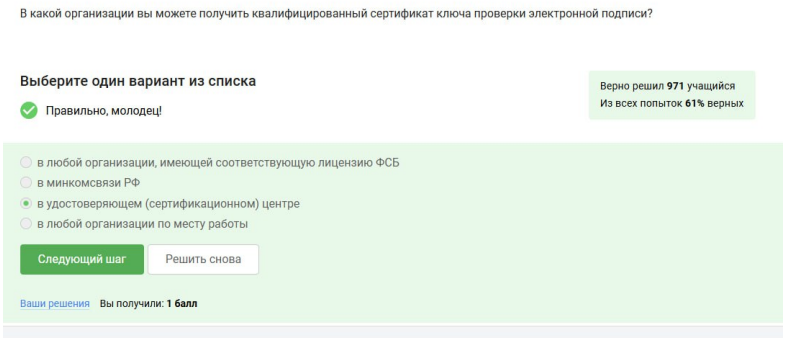

Рис. 2.10: Задание 010

Такие центры именно для этого и созданы, когда речь идёт о безопасности - это наилучший вариант, чем позволять выдавать сертификаты каждой желающей организации (рис. 2.11).

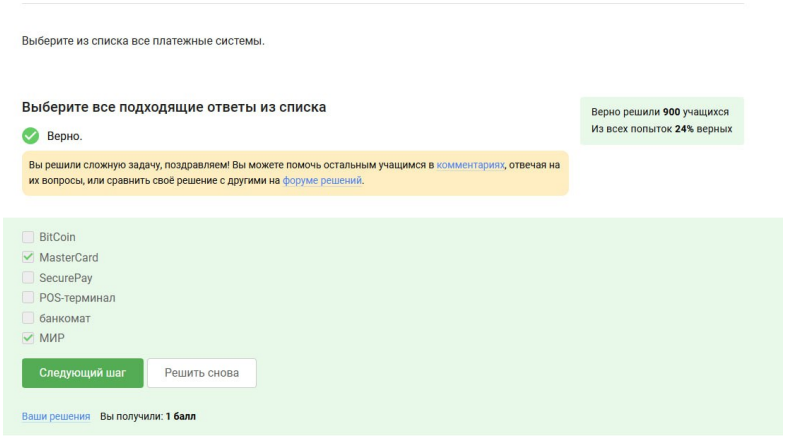

Рис. 2.11: Задание 011

SecurePay не считается, т.к. это электронная платёжная система, по сути и Bitcoin по этому не считается (рис. 2.12).

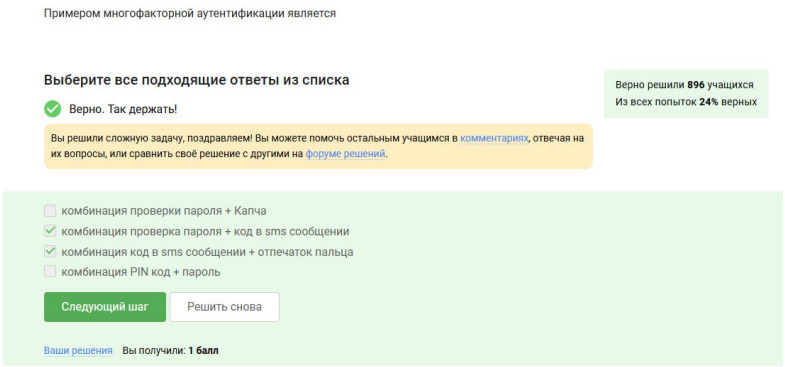

Рис. 2.12: Задание 012

Капча лишь может предотвратить (и то не всегда) автоматизированную атаку, а PIN-код + пароль тоже можно подобрать и не нужно иметь доступ к чему-нибудь стороннему (например, телефону) (рис. 2.13).

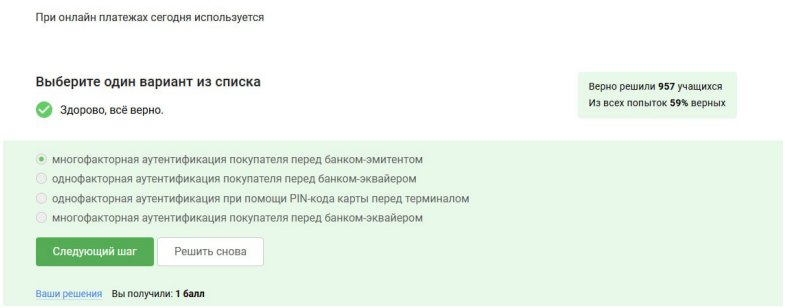

Рис. 2.13: Задание 013

Банк-эмитент - тот, кто выпустил карту, следовательно он несёт ответственность за аутентификацию пользователя, также используется многофакторная аутентификация - что-то, что знает пользователь + что-то, что этот пользователь имеет (телефон) (рис. 2.14).

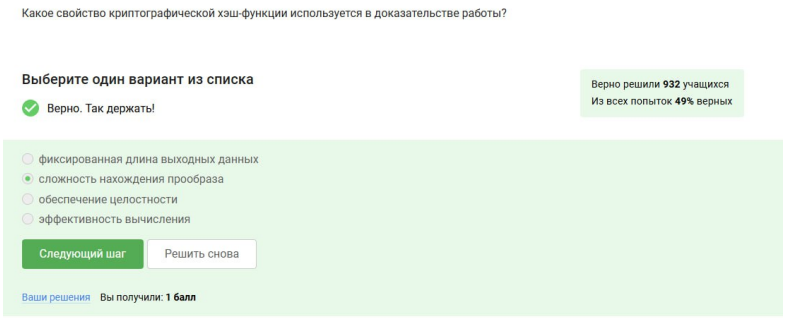

Рис. 2.14: Задание 014

При нахождении потребуется очень много вычислений, переборов - оттого и сложность, однако проверка результата будет быстрой (рис. 2.15).

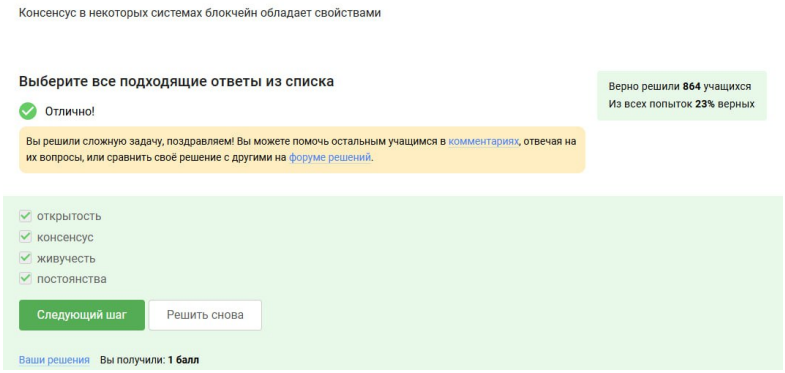

Рис. 2.15: Задание 015

Подходят все варианты (рис. 2.16).

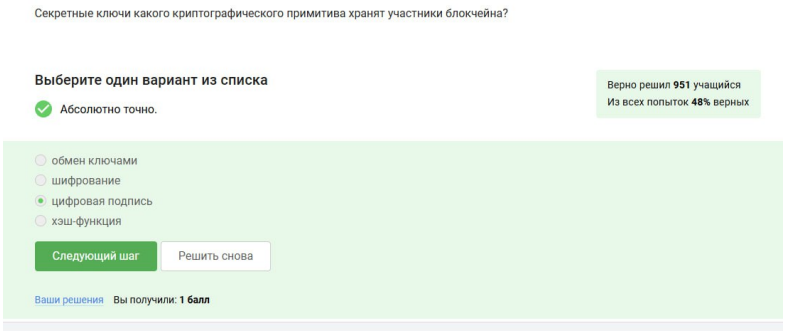

Рис. 2.16: Задание 016

Курс успешно пройден (рис. 2.17).

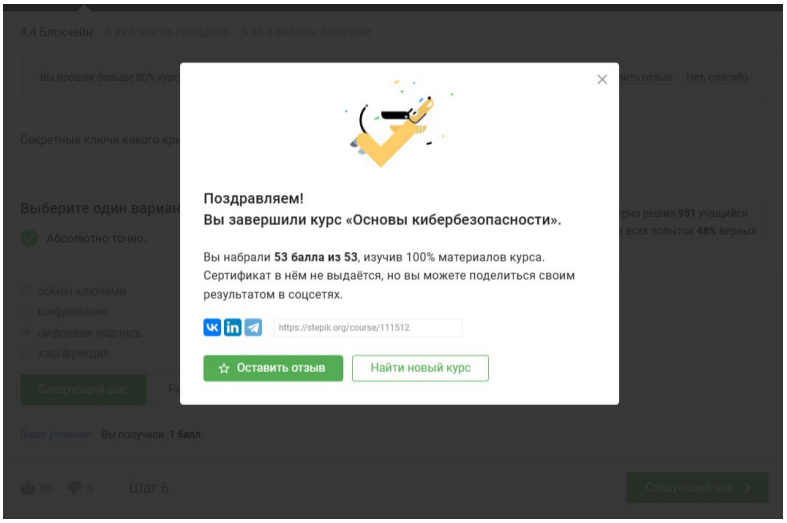

Рис. 2.17: Курс успешно пройден

3 Выводы

Этап 3 пройден успешно на максимальный балл.

4 Список литературы

Курс “Основы Кибербезопасности” на платформе Stepik