Внешний курс раздел 3

Криптография на практике

Александр Андреевич Шуплецов

Содержание

Список иллюстраций

Список таблиц

1 Цель работы

Изучить основы криптографии.

2 Выполнение работы

1. В асимметричных криптографических примитивах обе стороны имеют пару ключей - публичный и секретный.

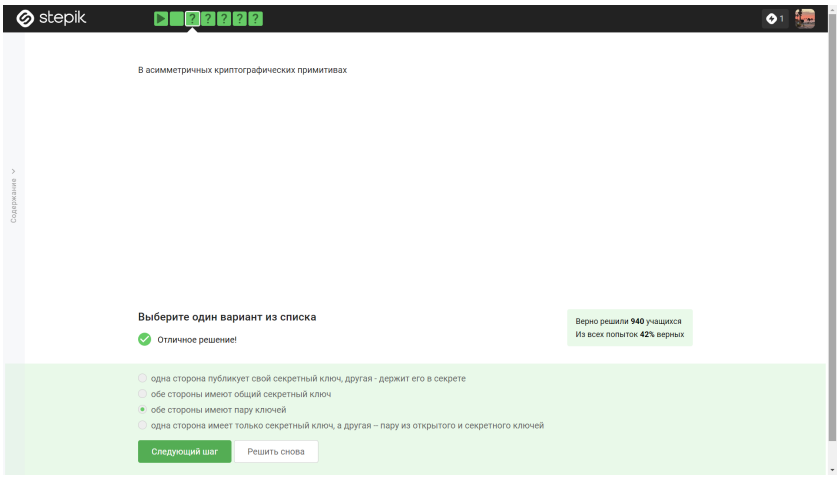

Рис. 2.1: первое задание

2. Криптографическая хэш-функция, в отличие от обычной хэш-функции, не обеспечивает конфиденциальность захэшированных данных, но она стойкая к коллизиям, эффективно вычисляется, дает на выходе фиксированное число бит независимо от объема входных данных.

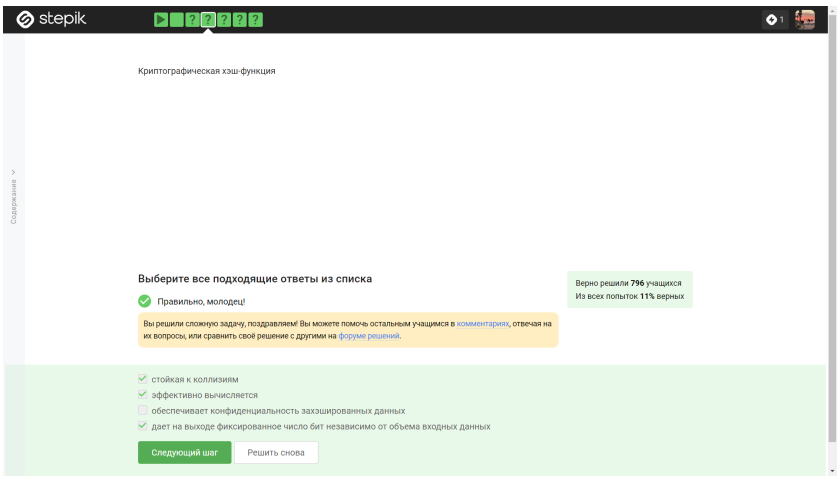

Рис. 2.2: второе задание

3. К алгоритмам цифровой подписи относятся зарубежные RSA и ECDSA, российский ГОСТ Р 34.10-2012.

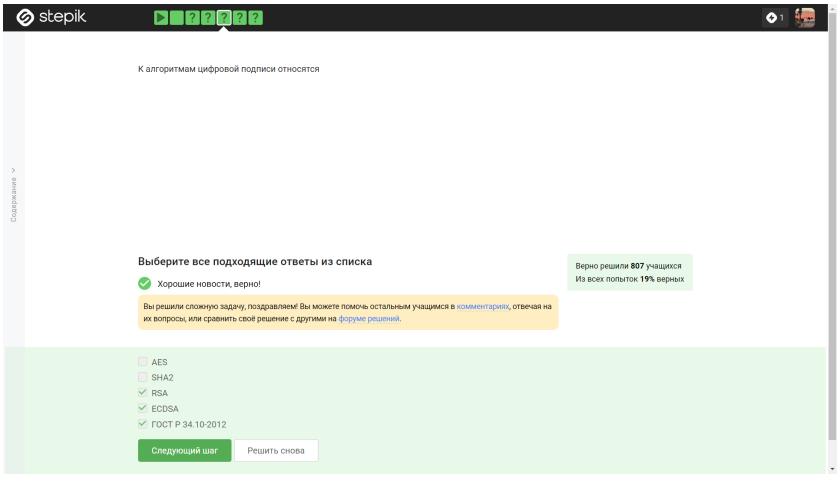

Рис. 2.3: третье задание

4. Код аутентификации сообщения относится к симметричным примитивам.

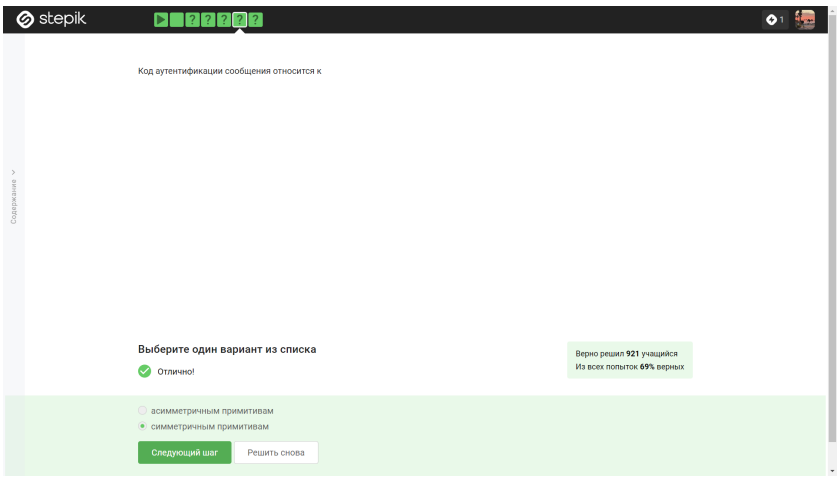

Рис. 2.4: четвертое задание

5. Обмен ключами Диффи-Хэллмана - это асимметричный примитив генерации общего секретного ключа.

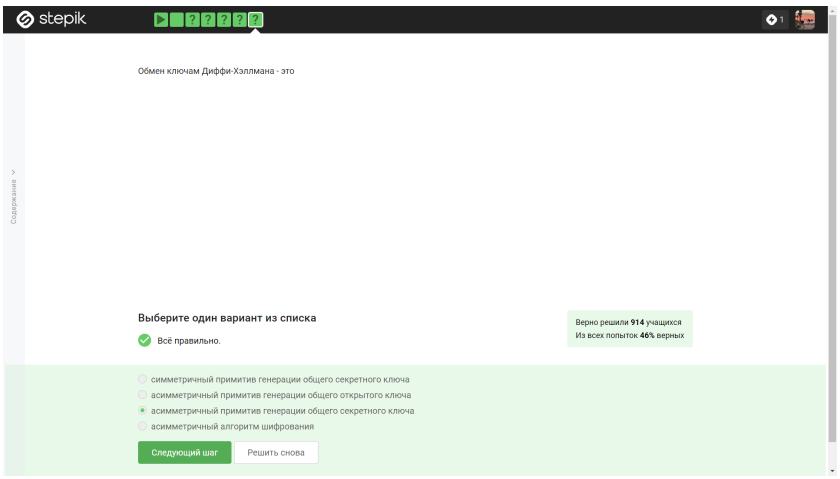

Рис. 2.5: пятое задание

6. Протокол электронной цифровой подписи относится к протоколам с публичным ключом.

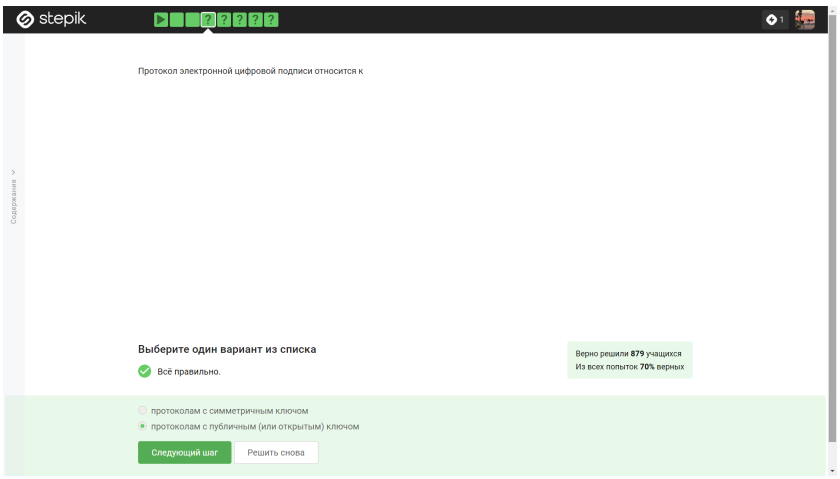

Рис. 2.6: шестое задание

7. Алгоритм верификации электронной цифровой подписи требует на вход подпись, открытый ключ, сообщение.

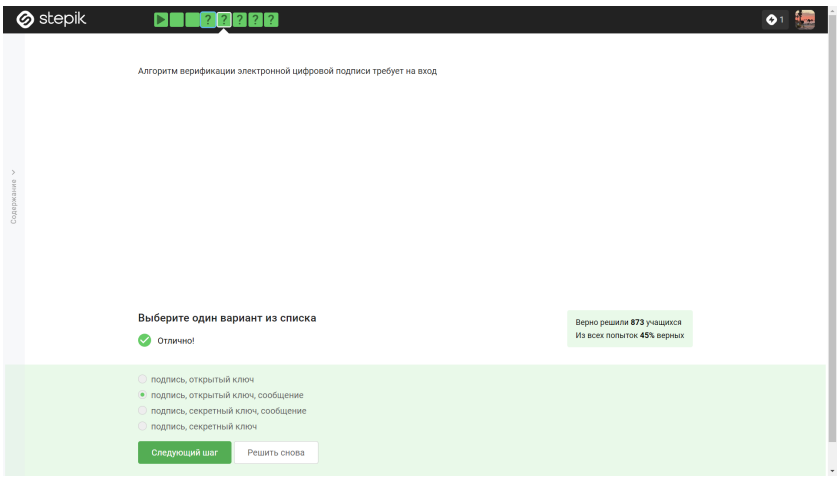

Рис. 2.7: седьмое задание

8. Электронная цифровая подпись не обеспечивает конфиденциальность.

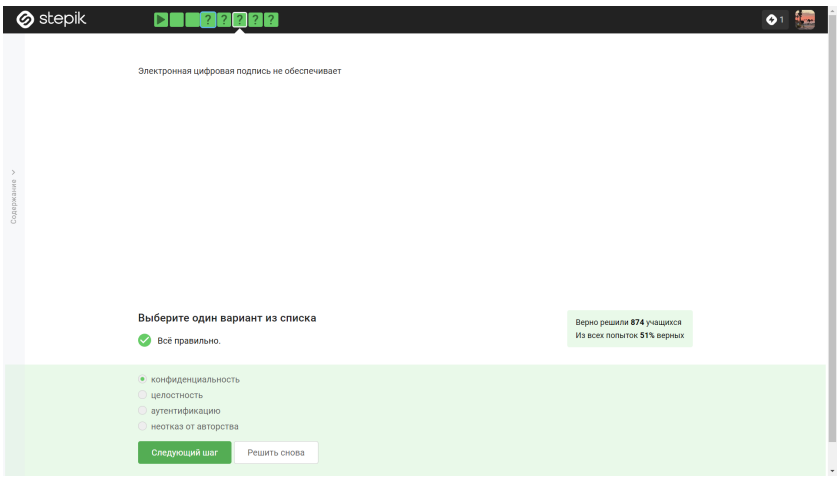

Рис. 2.8: восьмое задание

9. Для отправки налоговой отчетности в ФНС понадобится самый сильный тип сертификата электронной подписи - усиленная квалификационная.

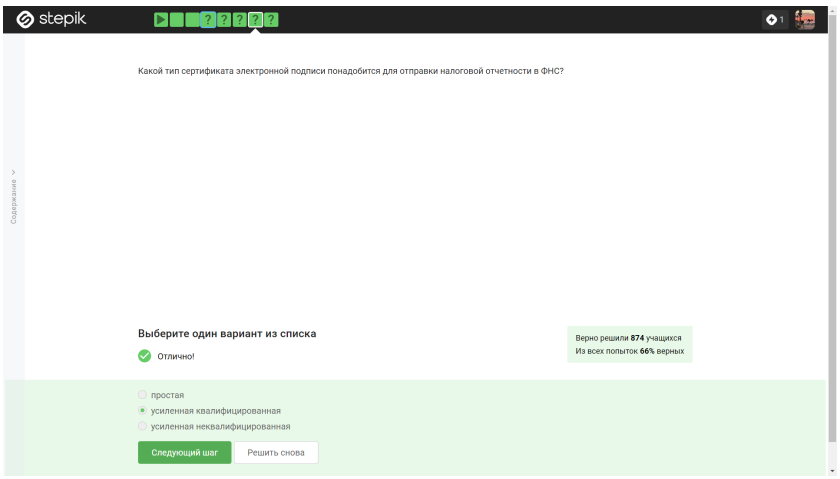

Рис. 2.9: девятое задание

10. Квалифицированный сертификат ключа проверки электронной подписи можно получить в удостоверяющем (сертификационном) центре.

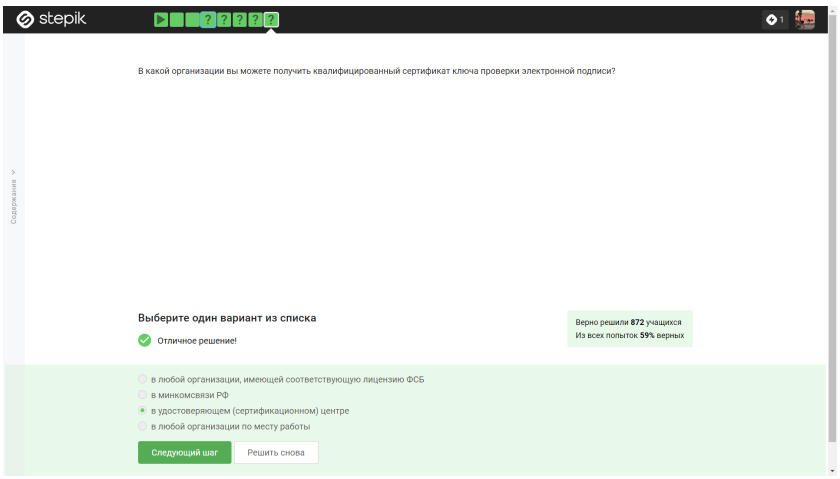

Рис. 2.10: десятое задание

11. MasterCard и МИР являются платежными системами в предоставленном в задании списке.

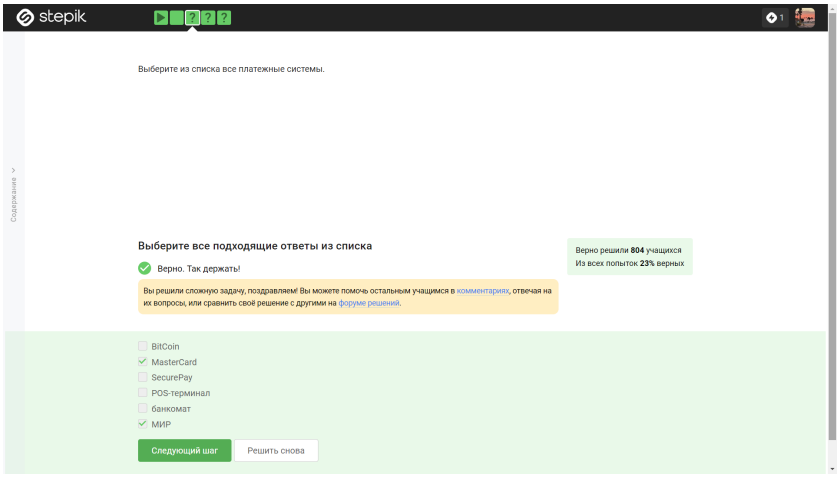

Рис. 2.11: одиннадцатое задание

12. Примерами многофакторной аутентификации являются комбинация проверка пароля + код в sms сообщении, комбинация код в sms сообщении + отпечаток пальца, капча с паролем и пароль с пин кодом не являются примерами многофакторной аутентификации.

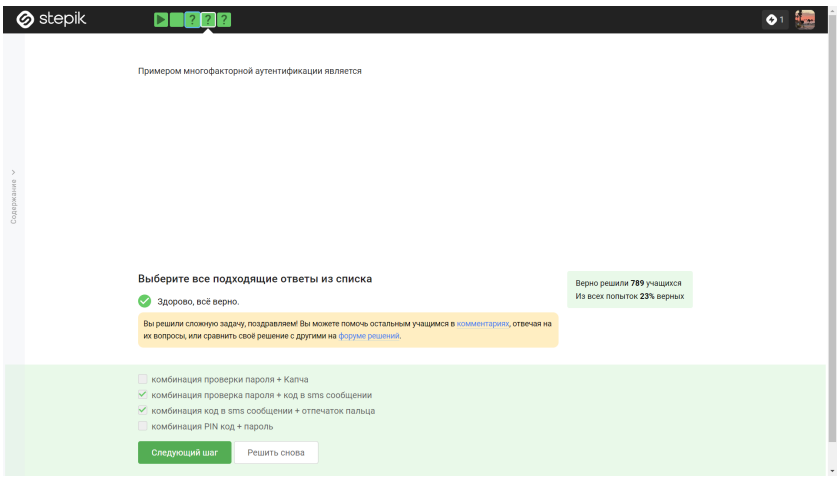

Рис. 2.12: двенадцатое задание

13. При онлайн платежах сегодня используется многофакторная аутентификация покупателя перед банком-эмитентом - банком, на счете которого покупатель хранит денежные средства.

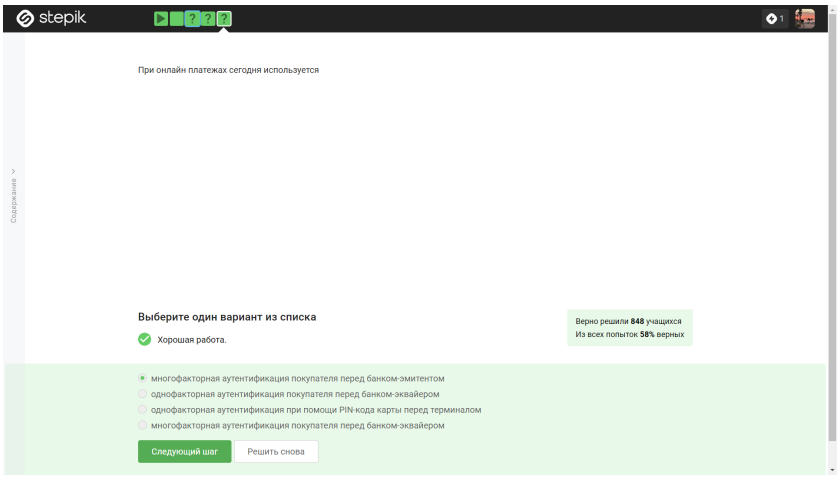

Рис. 2.13: тринадцатое задание

14. Сложность нахождения прообраза как свойство криптографической хэш-функции используется в доказательстве работы майнера.

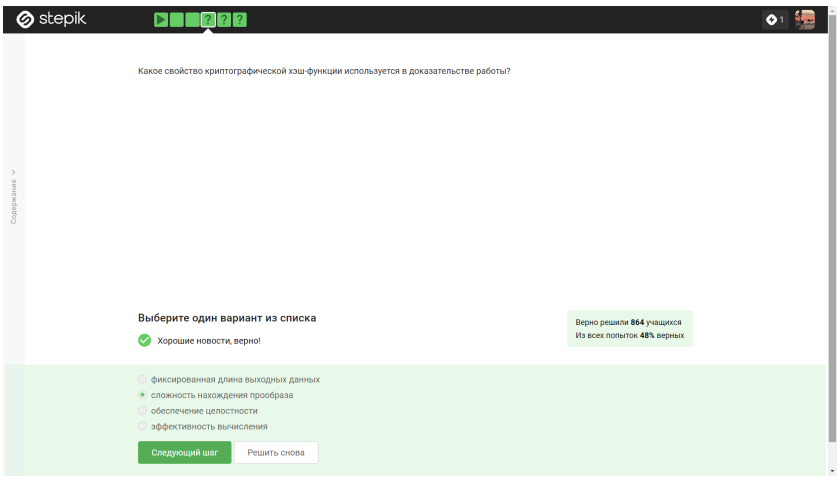

Рис. 2.14: четырнадцатое задание

15. Консенсус в некоторых системах блокчейн обладает свойствами: открытость, живучесть, постоянство.

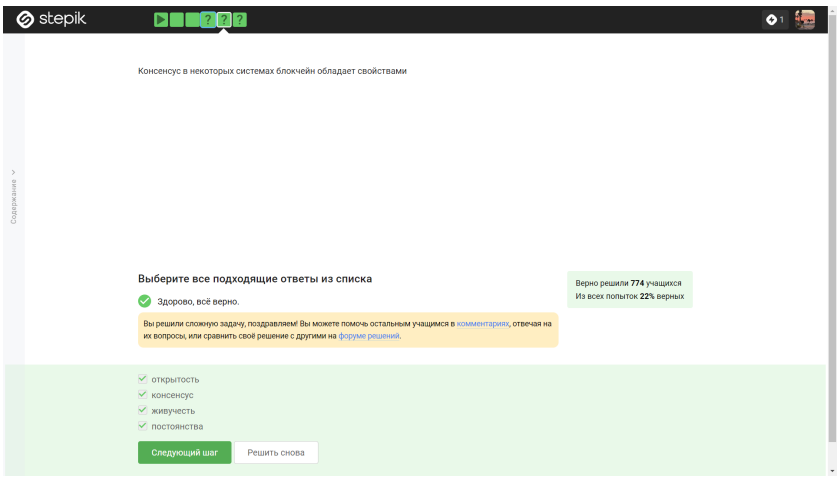

Рис. 2.15: пятнадцатое задание

16. Цифровая подпись используется в качестве криптографического примитива в блокчейне.

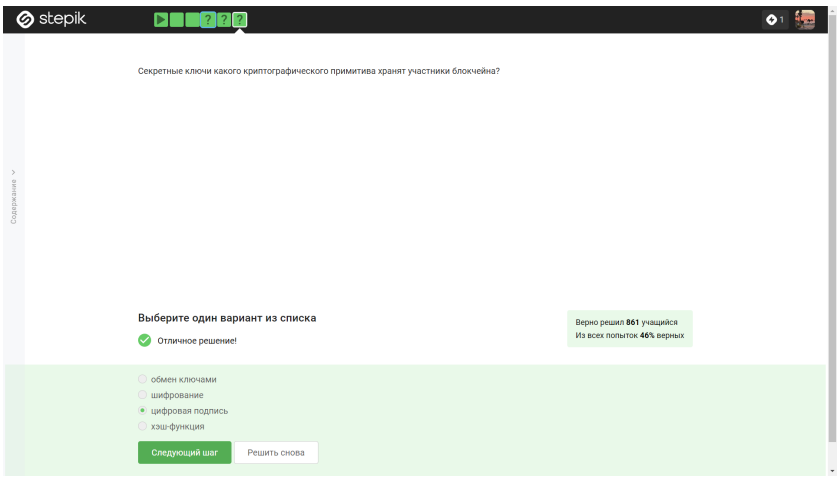

Рис. 2.16: шестнадцатое задание

3 Выводы

Я изучил основы криптографии.

4 Список литературы

Конспекты к лекциям курса “Основы кибербезопасности”.