Отчет по третьему этапу внешнего курса

Дисциплина: основы информационнной безопасности

Казазаев Даниил Михайлович

Содержание

1	Цель работы	4
2	Этап первый	5
3	Выполнение первого этапа внешнего курса. 3.1 Введине в криптографиюВведине в криптографию	6
4	Цифровая подпись	11
5	Электронные платежи	15
6	Блокчейн	19
7	Вывод	22

Список иллюстраций

3.1	Первый вопрос	6
3.2	Второй вопрос	7
3.3	Третий вопрос	8
3.4	Четвертый вопрос	9
3.5	Пятый вопрос	10
4.1	Первый вопрос	11
4.2	Второй вопрос	12
4.3	Третий вопрос	13
4.4	Четвертый вопрос	14
	Пятый вопрос	14
5.1	Первый вопрос	16
5.2	Второй вопрос	17
5.3	Третий вопрос	18
6.1	Первый вопрос	19
6.2	Второй вопрос	20
6.3	Третий вопрос	21

1 Цель работы

Внешний кур состоит из трех этапов.

2 Этап первый

Первый этап курса состоит из 4 частей:

- 1. Введине в криптографию
- 2. Цифровая подпись
- 3. Электронные платежи
- 4. Блокчейн

3 Выполнение первого этапа внешнего курса.

3.1 Введине в криптографиюВведине в криптографию

В ассиметричных криптографических примитивах обестороны имеют пару ключей. (рис. 3.1)

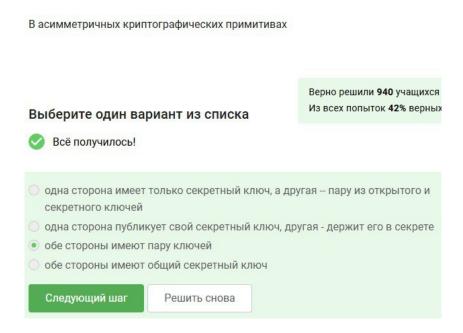


Рис. 3.1: Первый вопрос

Хещ-функция стойкая к колизиям, дает определенное кол-во бит вне зависимости от объема входных данных и эффективно вычисляется. (рис. 3.2)

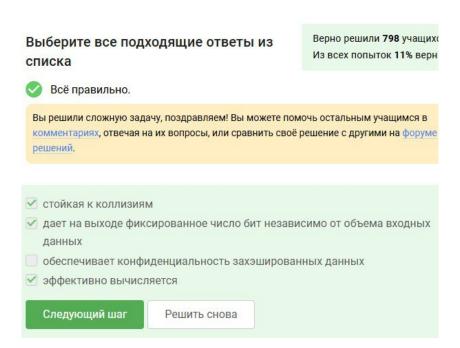


Рис. 3.2: Второй вопрос

RSA, ECDSA и ГОСТ стандарт(кузнечик) - алгоритмы цифровой подписи. (рис. 3.3)

Выберите все подходящие ответы из списка

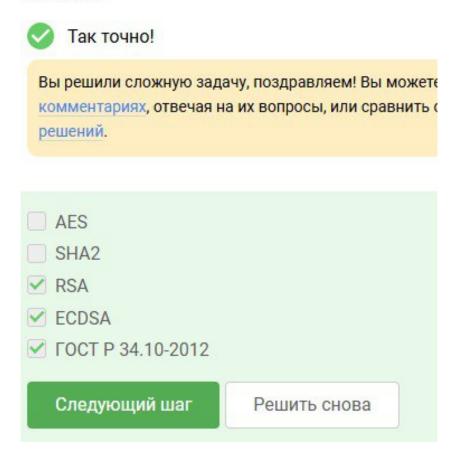


Рис. 3.3: Третий вопрос

Код аунтификации сообщения отеосится к симмитричным примитивам. (рис. 3.4)

Код аутентификации сообщения относится к

Выберите один вариант из списка Верно. Так держать! симметричным примитивам асимметричным примитивам Следующий шаг Решить снова ваши решения вы получили: 1 балл

Рис. 3.4: Четвертый вопрос

Обмен ключами Диффи-Хэллмана - ассиметрический примитив генерации обзего секретного ключа. (рис. 3.5)

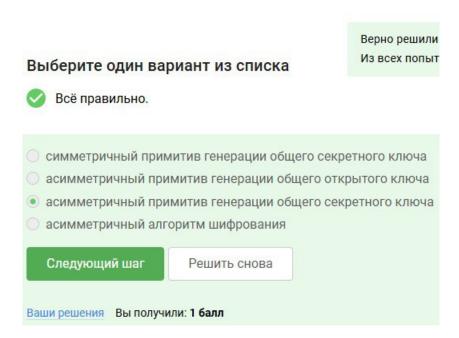
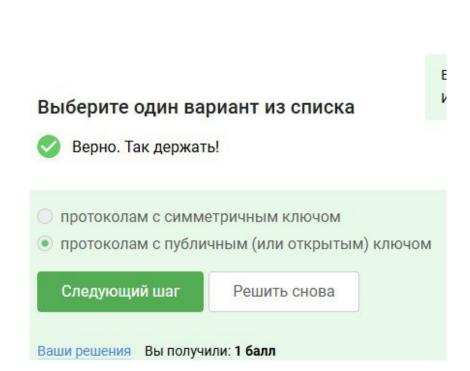


Рис. 3.5: Пятый вопрос

4 Цифровая подпись

Протоколы цифровой подписи с публичным ключом.(рис. 4.1)



Протокол электронной цифровой подписи относится к

Рис. 4.1: Первый вопрос

Алгоритм верификации требует на вход: подпись, открытый ключ, сообщение.(рис. 4.2)

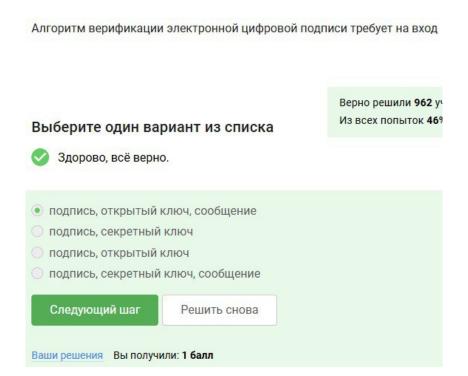


Рис. 4.2: Второй вопрос

Электронная подпись не обеспечивает конфиденциальность.(рис. 4.3)

Выберите один вариант из списка Здорово, всё верно. конфиденциальность целостность неотказ от авторства аутентификацию Следующий шаг Решить снова Ваши решения Вы получили: 1 балл

Рис. 4.3: Третий вопрос

Для отправки налоговой отчетности необходим сертификат с усилненной квалификацией. (рис. 4.4)

Какой тип сертификата электронной подписи понадобится для отправки налоговой отчетности в ФНС?

Верно решили 975 у Из всех попыток 68 отлично!

Усиленная неквалифицированная
усиленная квалифицированная
простая

Рис. 4.4: Четвертый вопрос

Решить снова

Следующий шаг

Квалифицированный сертификат можно получить в удостоверяющем центре.(рис. 4.5)

В какой организации вы можете получить квалифицированный сертификат ключа проверки электронной подписи?

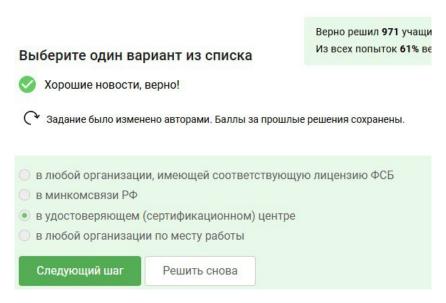


Рис. 4.5: Пятый вопрос

5 Электронные платежи

МИР, MasterCard - платежные системы. (рис. 5.1)

Выберите из списка все платежные системы.

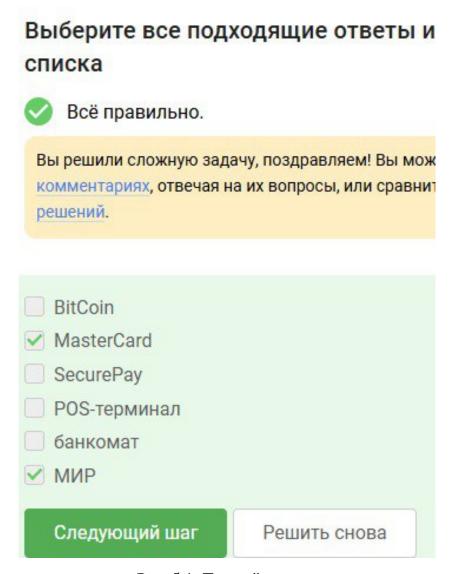


Рис. 5.1: Первый вопрос

Отмеченные варианты ответов являются примером многофакторной аутентификации. (рис. 5.2)

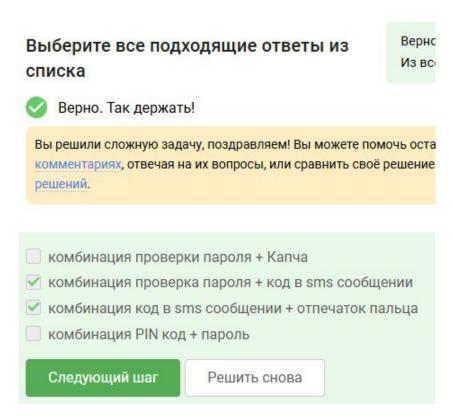


Рис. 5.2: Второй вопрос

Сегодня при онлайн платежах используется многофакторная аутентификация покупателя перед банком-эмитентом. (рис. 5.3)

Верно решили 957 учаш Из всех попыток 59% все Отличное решение!

многофакторная аутентификация покупателя перед банком-эмитентом однофакторная аутентификация покупателя перед банком-эквайером однофакторная аутентификация при помощи PIN-кода карты перед терминалом
многофакторная аутентификация покупателя перед банком-эквайером однофакторная аутентификация покупателя перед банком-эквайером

При онлайн платежах сегодня используется

Рис. 5.3: Третий вопрос

6 Блокчейн

В доказательстве работы криптографической хеш-функции используется сложность нахождения прообраза. (рис. 6.1)

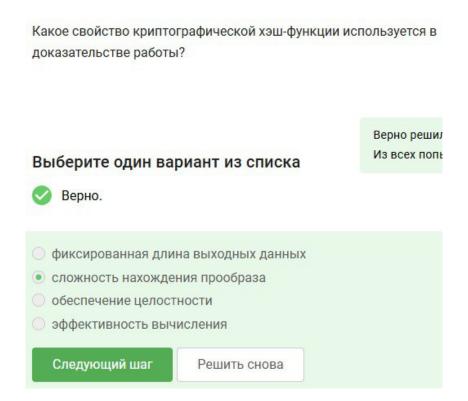


Рис. 6.1: Первый вопрос

Все ответы являются верными для консенсуса некоторых блокчейн систем. (рис. 6.2)

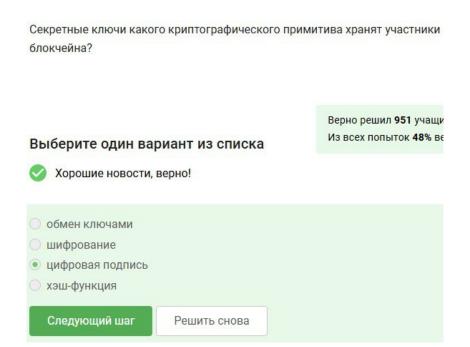


Рис. 6.2: Второй вопрос

Участники криптографического примитива хранят при себе только цифровую подпись. (рис. 6.3)

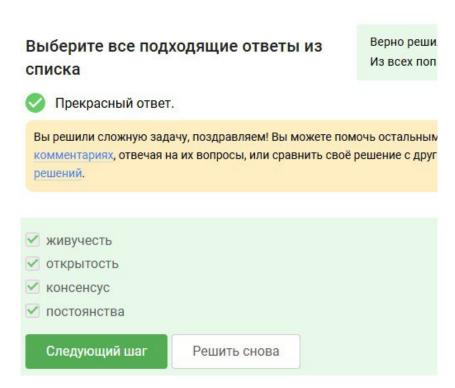


Рис. 6.3: Третий вопрос

7 Вывод

Выполнен третий этап внешнего курса