# Прохождение внешнего курса

# Криптография на практике Селиванов Вячеслав Алексеевич

#### Содержание

1 Це	ель работы	1
2 Вь	ыполнение лабораторной работы	1
3 Вь	ыводы	7
Спи	исок иллюстраций	
Рис. 1:	I: Задание 1	2
Рис. 2:	2: Задание 2	2
	3: Задание 3	
	l: Задание 4	
Рис. 5:	5: Задание 5	3
	S: Задание 6	
Рис. 7:	7: Задание 7	4
	3: Задание 8	
Рис. 9:	9: Задание 9	4
	l0: Задание 10	
	1: Задание 11	
	l2: Задание 12	
	l3: Задание 13	
	4: Задание 14	
	!5: Задание 15	
	I6: Задание 16	

#### Список таблиц

No table of figures entries found.

### 1 Цель работы

Проработать задания, которые касаются криптографии

#### 2 Выполнение лабораторной работы

Ассимитричные криптографические примитивы (рис. 1).

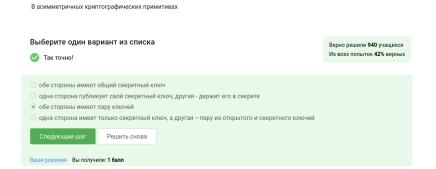


Рис. 1: Задание 1

Хэш-функция (рис. 2).

Криптографическая хэш-функция	
Выберите все подходящие ответы из списка	Верно решили <b>798</b> учащихся
	Из всех попыток 11% 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.	
<ul> <li>         ✓ эффективно вычисляется         ✓ дает на выходе фиксированное число бит независимо от объема входных данных         ✓ стойкая к коллизиям         ○ обеспечивает конфиденциальность захэшированных данных     </li> </ul>	
Следующий шаг Решить снова	

Рис. 2: Задание 2

Алгоритмы цифровой подписи (рис. 3).

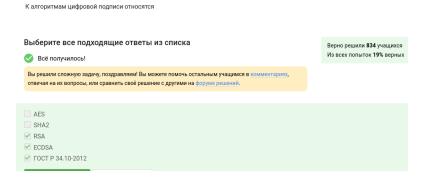


Рис. 3: Задание 3

Код аунтетификации сообщения (рис. 4).



Рис. 4: Задание 4

Обмен ключами Диффи-Хэлмана (рис. 5).

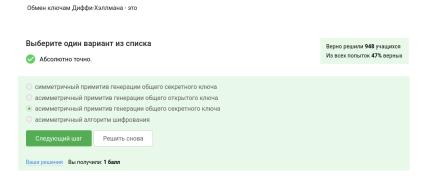


Рис. 5: Задание 5

Протокол электронной цифровой подписи (рис. 6).

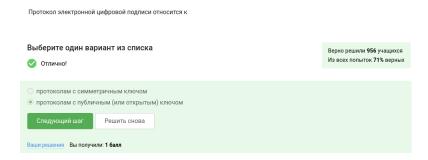


Рис. 6: Задание 6

Алгоритм верификации электронной цифровой подписи (рис. 7).

Алгоритм верификации электронной цифровой подписи требует на вход



Рис. 7: Задание 7

Подпись(рис. 8).

Электронная цифровая подпись не обеспечивает

Выберите один вариант из списка

№ Отлично!

Верно решили 968 учащихся
Из всех попыток 53% верных

аутентификацию
целостность

конфиденциальность
неотказ от авторства

Следующий шаг

Решить снова

Рис. 8: Задание 8

Ваши решения Вы получили: 1 балл

Тип сертификата электронной подписи в ФНС (рис. 9).

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

Выберите один вариант из списка

✓ Отлично!

Верно решили 975 учащихся
Из всех попыток 68% верных

усиленная квалифицированная
усиленная неквалифицированная
простая

Следующий шаг Решить снова

Ваши решения Вы получили: 1 балл

Рис. 9: Задание 9

Организация (рис. 10).

Выберите один вариант из списка

№ 3дорово, всё верно.

В рлюбой организации, имеющей соответствующую лицензию ФСБ

в минкомсвязи РФ

в удостоверяющем (сертификационном) центре

в любой организации по месту работы

Следующий шаг

Решить снова

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

Рис. 10: Задание 10

Ваши решения Вы получили: 1 балл

Платежные системы (рис. 11).

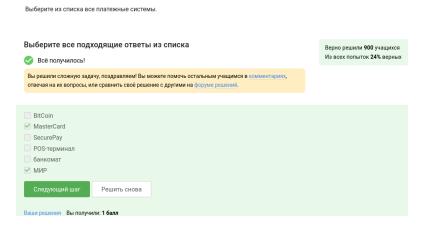


Рис. 11: Задание 11

Многофакторная аунтетификация (рис. 12).

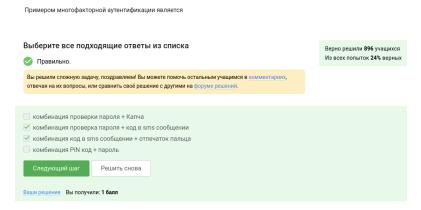


Рис. 12: Задание 12

Онлайн платежи сегодня (рис. 13).

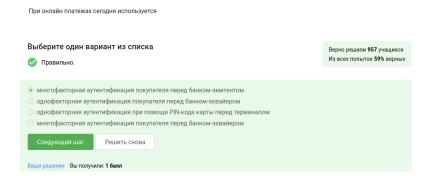


Рис. 13: Задание 13

Свойство криптографичской хэш-функции (рис. 14).

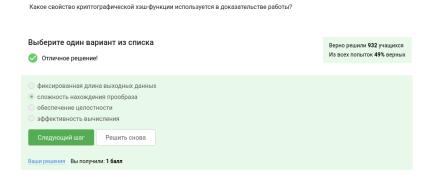


Рис. 14: Задание 14

Свойства консенсуса в системах блокчейн (рис. 15).

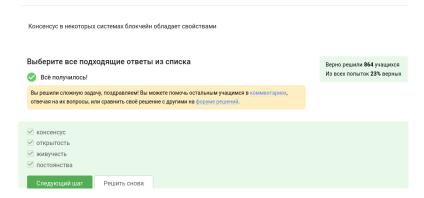


Рис. 15: Задание 15

Секретные ключи (рис. 16).

Выберите один вариант из списка

Верно решил 951 учащийся

Всё получилось!

Всё получилось!

обмен ключами
шифрован подпись

хэш-функция

Следующий шаг

Решить снова

Выши решения Вы получили: 1 балл

Рис. 16: Задание 16

## 3 Выводы

Проделаны задания, связаные с криптографией