Отчёт прохождения внешнего курса

Безопасность в сети

Криптография на практике

Содержание

Список иллюстраций

Список таблиц

1 Цель работы

Провести контроль усвоения теоритического материала раздела “Криптография на практике”

2 Выполнение контрольных заданий

В асимметричной криптографии, также известной как криптография с открытым ключом, каждая сторона обладает парой ключей: открытым и закрытым (или секретным). Открытый ключ доступен для общего использования, в то время как закрытый ключ хранится конфиденциально у владельца. К протоколам асимметричной криптографии относятся электронно-цифровая подпись и протокол генерации общего ключа. Последний позволяет установить общий секретный ключ без необходимости физического взаимодействия между сторонами.(рис. 2.1).

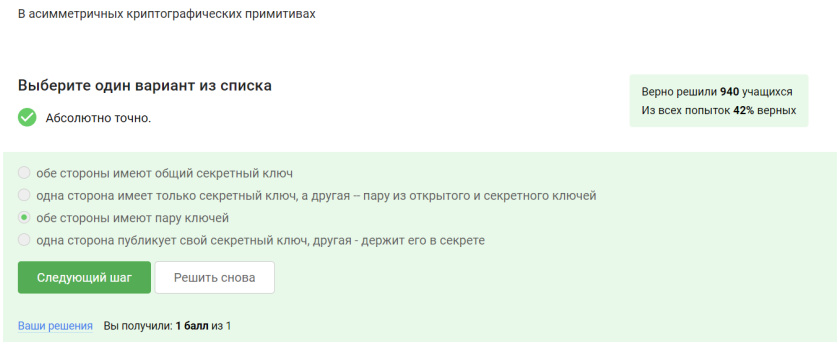

Рис. 2.1: Задание 1

Криптографическая хэш-функция, эффективно вычисляется, дает на выходе фиксированное число бит независимо от объема входных данных, но главное она стойкая к колизиям. Это значит что двое разных входных данных не могут дать один выходной(рис. 2.2).

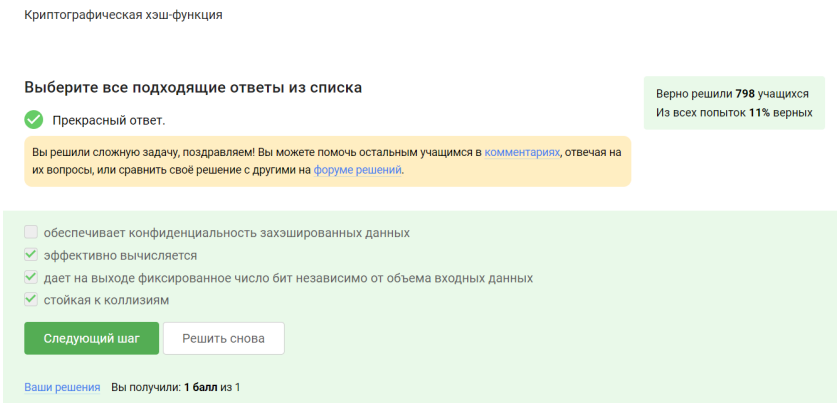

Рис. 2.2: Задание 2

К ним относятся именно RSA, ECDSA, ГОСТ Р 34.10-2012, остальные отношения не имеют(рис. 2.3).

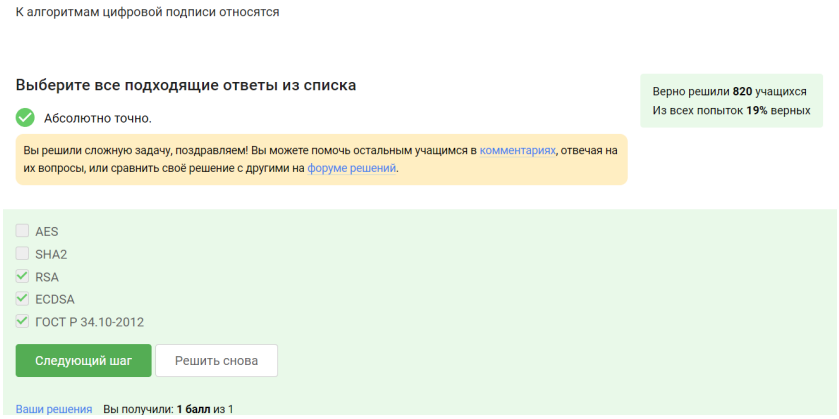

Рис. 2.3: Задание 3

Этот процесс также является симметричным и использует ключ (который должен быть отличным от ключа, использованного для шифрования) и само сообщение для создания кода аутентификации. Этот примитив можно представить как симметричный аналог подписи. Обычно код аутентификации сообщения создается с использованием хэш-функции или симметричного шифрования.(рис. 2.4).

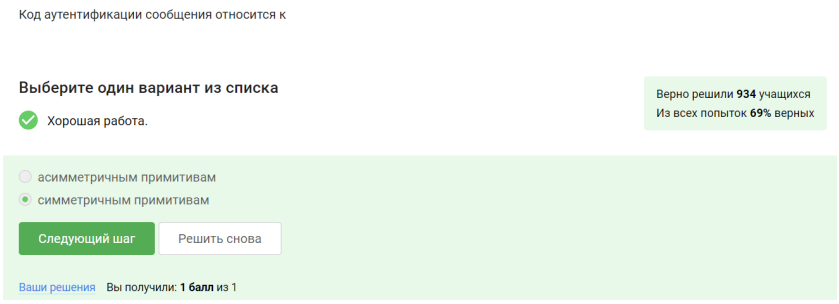

Рис. 2.4: Задание 4

Обмен ключам Диффи-Хэллмана - это асимметричный примитив генерации общего секретного ключа(рис. 2.5).

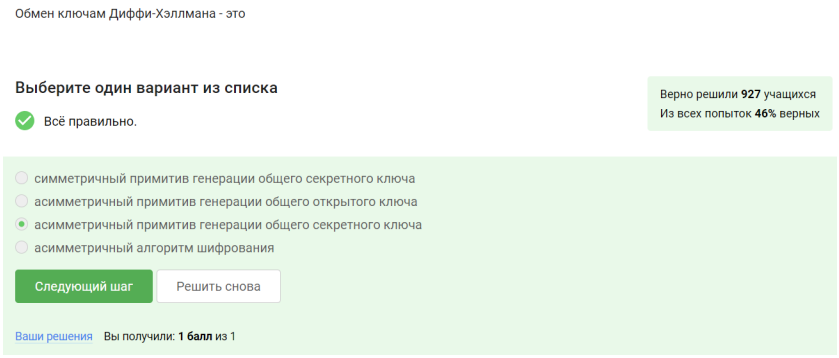

Рис. 2.5: Задание 5

Конечно же к протоколам с публичным(открытым ключом)(рис. 2.6).

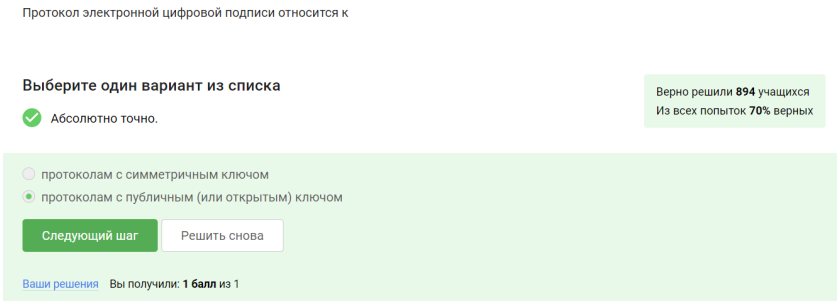

Рис. 2.6: Задание 6

НАм в первую очередь нужна сама подпись, потом открытый ключ(никак не секретный) и потом также сообщение. ТОлько так пройдёт верификация (рис. 2.7).

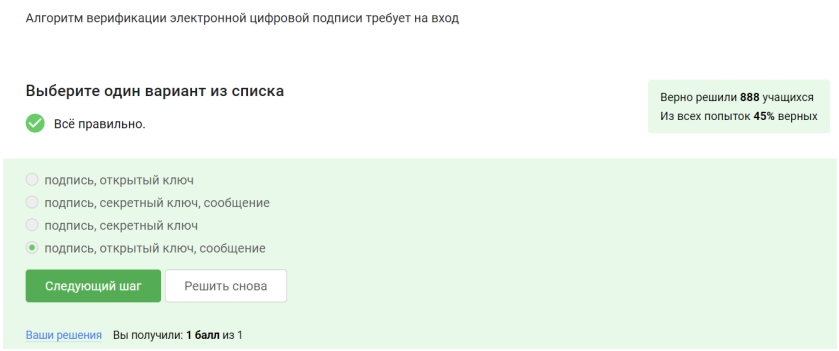

Рис. 2.7: Задание 7

Конечно конфиденциальность. Это же подпись. ОНа указывает на человека, которому принадлежит(рис. 2.8).

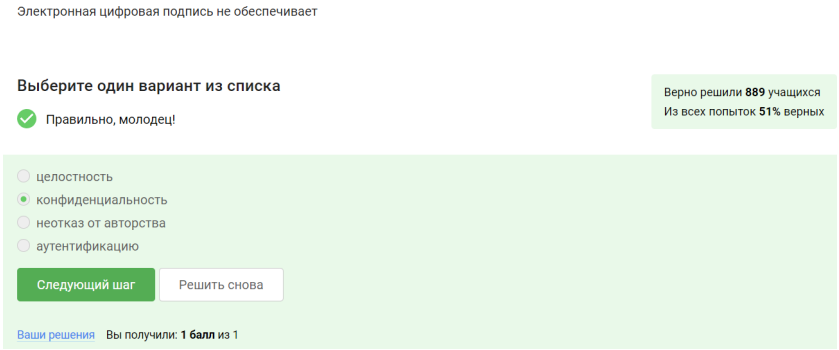

Рис. 2.8: Задание 8

Только усиленная квалифицированная. Это касается серьёзных документов. Никакая другая не подойдёт (рис. 2.9).

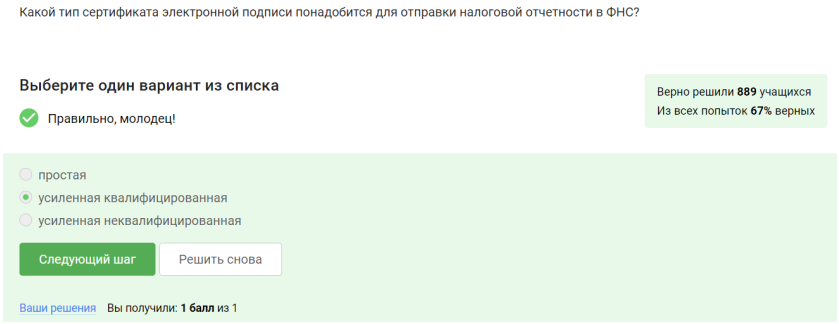

Рис. 2.9: Задание 9

Только в удостоверяющем, сертификационном центре. Иные организации таких полномочий не имеют.(рис. 2.10).

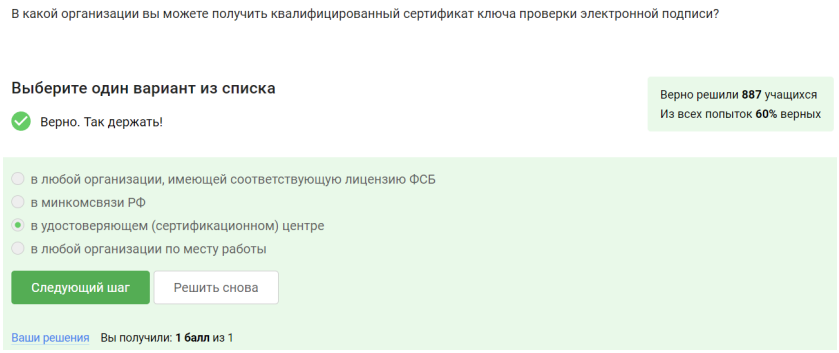

Рис. 2.10: Задание 10

Мастеркарт и мир. Биткоин это валюта, банкомат - усстройство, выдающее и принимающе деньги.(рис. 2.11).

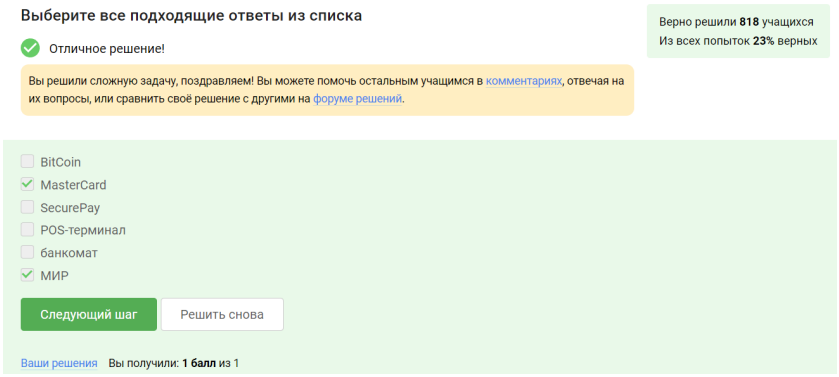

Рис. 2.11: Задание 11

Нам нужны доказательства из разных категорий. Минимум две. В эти категории входят наша биометрия, то что мы знаем(пароль) и то что имеем (наприер телефон). Пароль и капча таковыми не являются, капча это вообще защита от автоматических атак, ну и пин код с паролем тоже из одной категории(рис. 2.12).

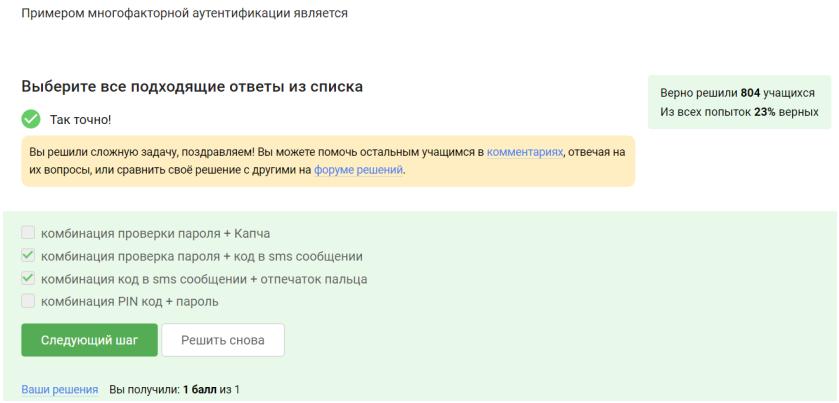

Рис. 2.12: Задание 12

При онлайн платежах сегодня используется многофакторная аутентификация покупателя перед банком-эмитентом(рис. 2.13).

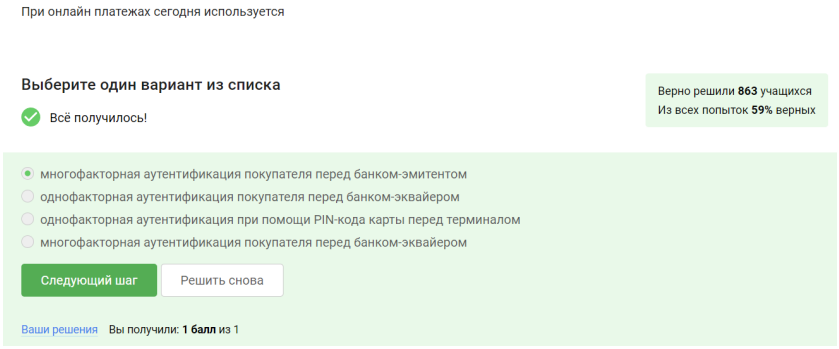

Рис. 2.13: Задание 13

СЛожность нахождения прообраза конечно же. Это очень важное свойствр(рис. 2.14).

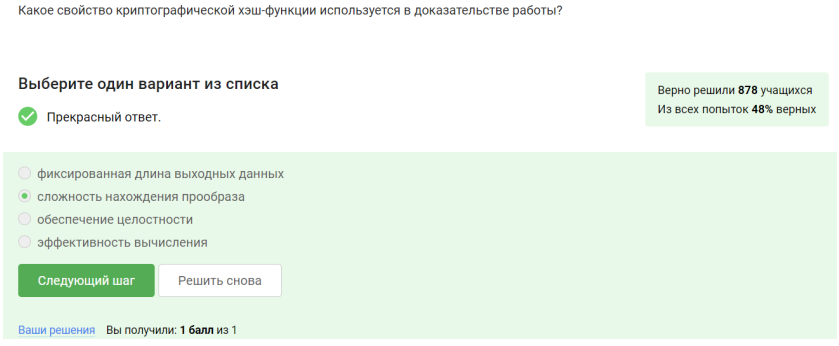

Рис. 2.14: Задание 14

Снова задание с подвохом. ЗДесь подходят все варианты. Об этом говорилось в лекции(рис. 2.15).

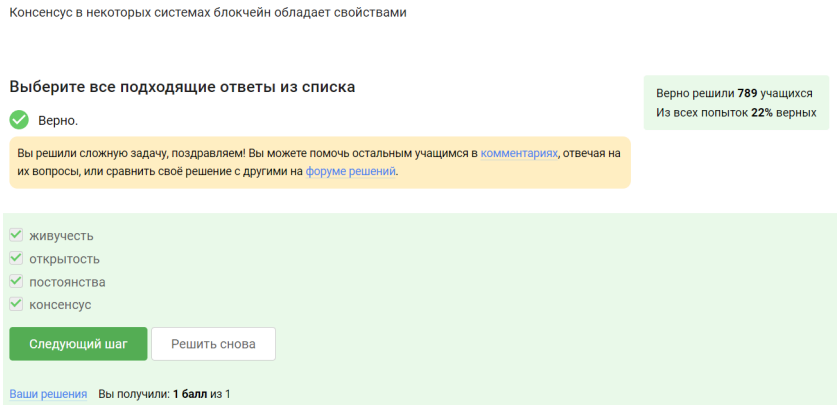

Рис. 2.15: Задание 15

(рис. 2.16).

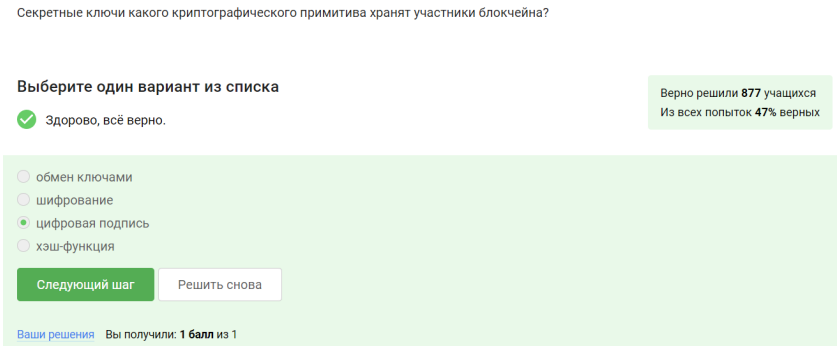

Рис. 2.16: Задание 16

3 Выводы

Мы успешно прошли контроль усвоения теоритического материала раздела “Криптография на практике”

Список литературы