Отчёт по прохождению внешнего курса №3

Основы Кибербезопасности

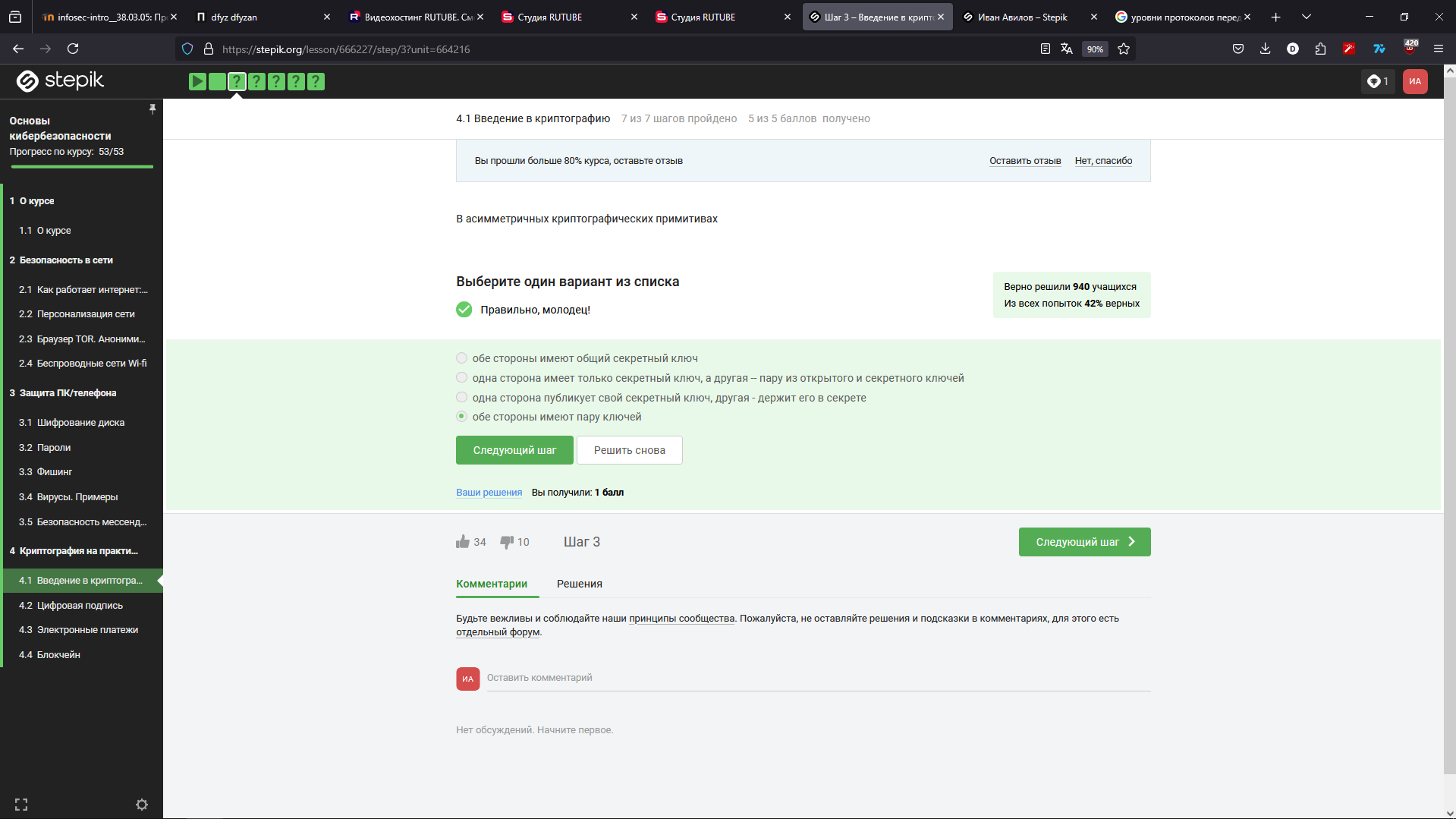
Авилов Иван Олегович"

Содержание"

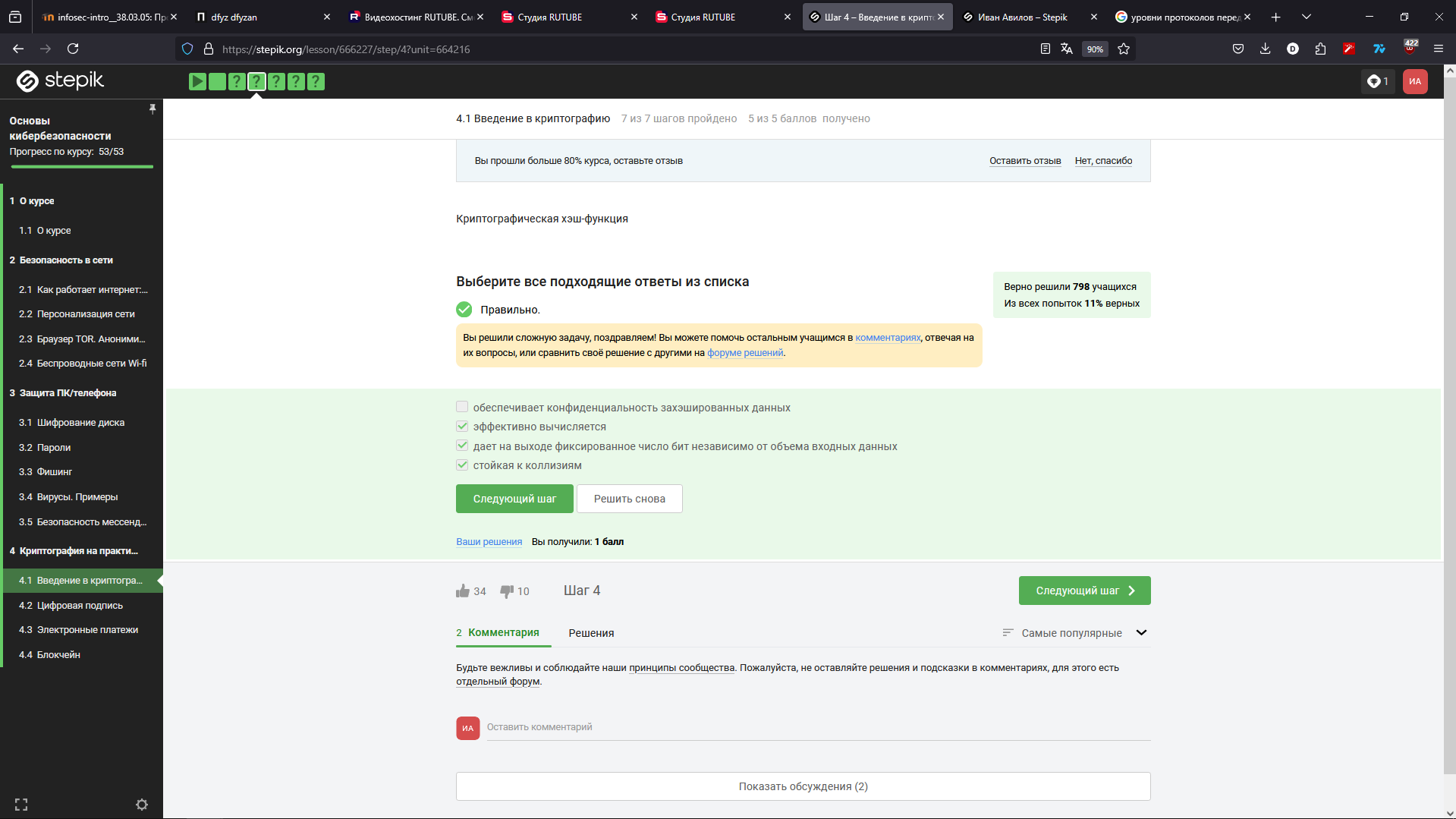
Список иллюстраций

Список таблиц

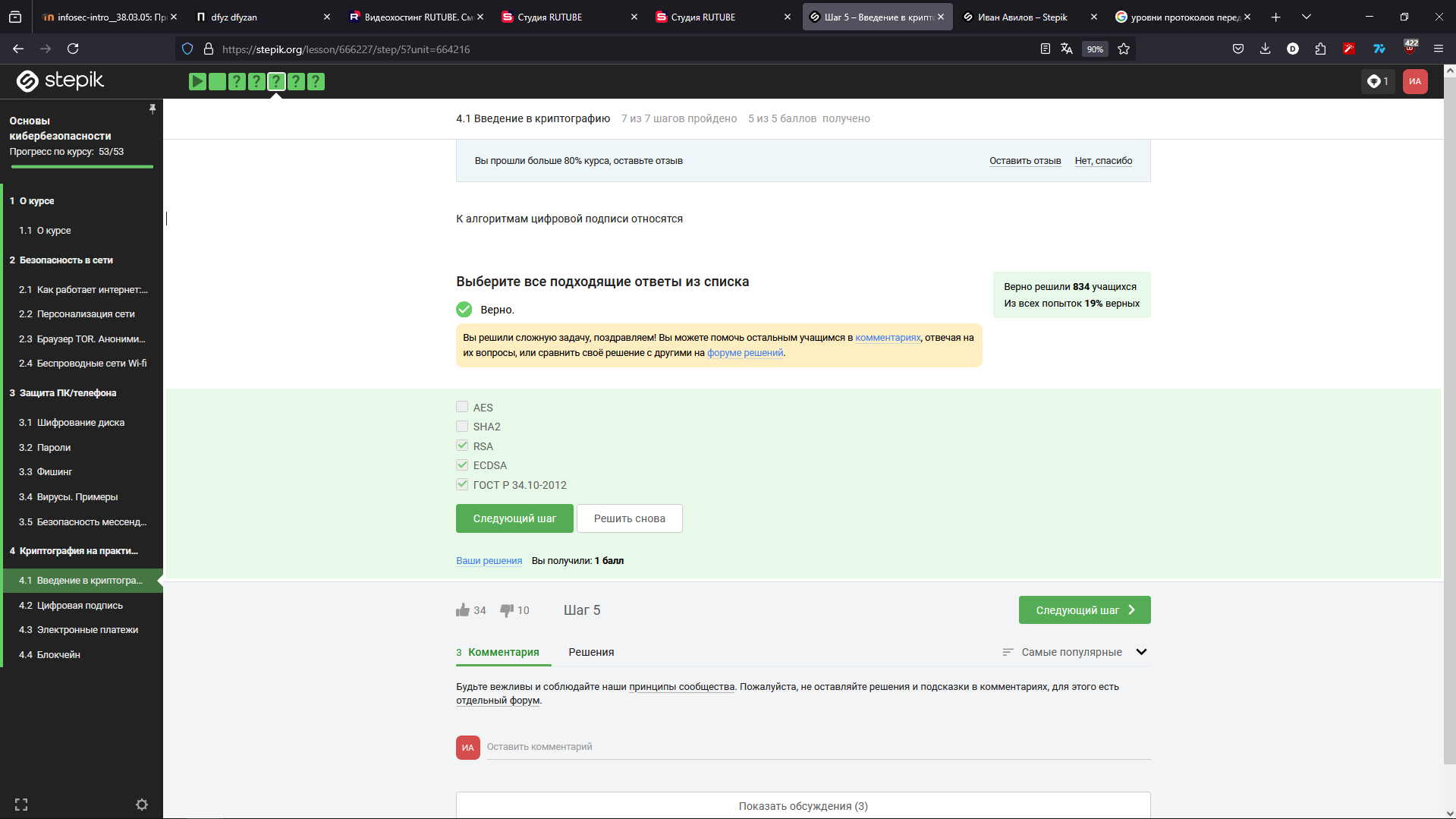
# Задание



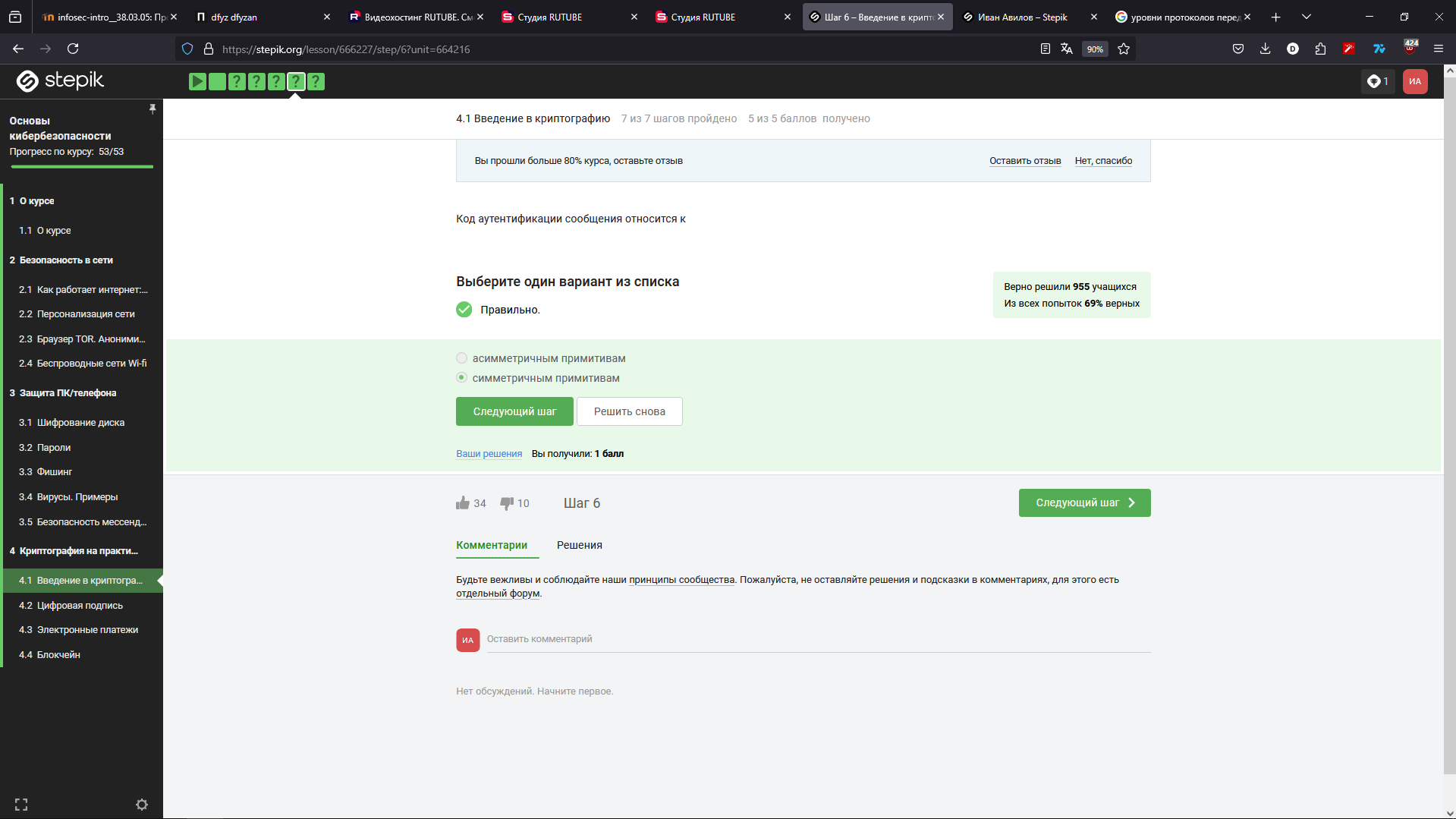
Правильный ответ - последний



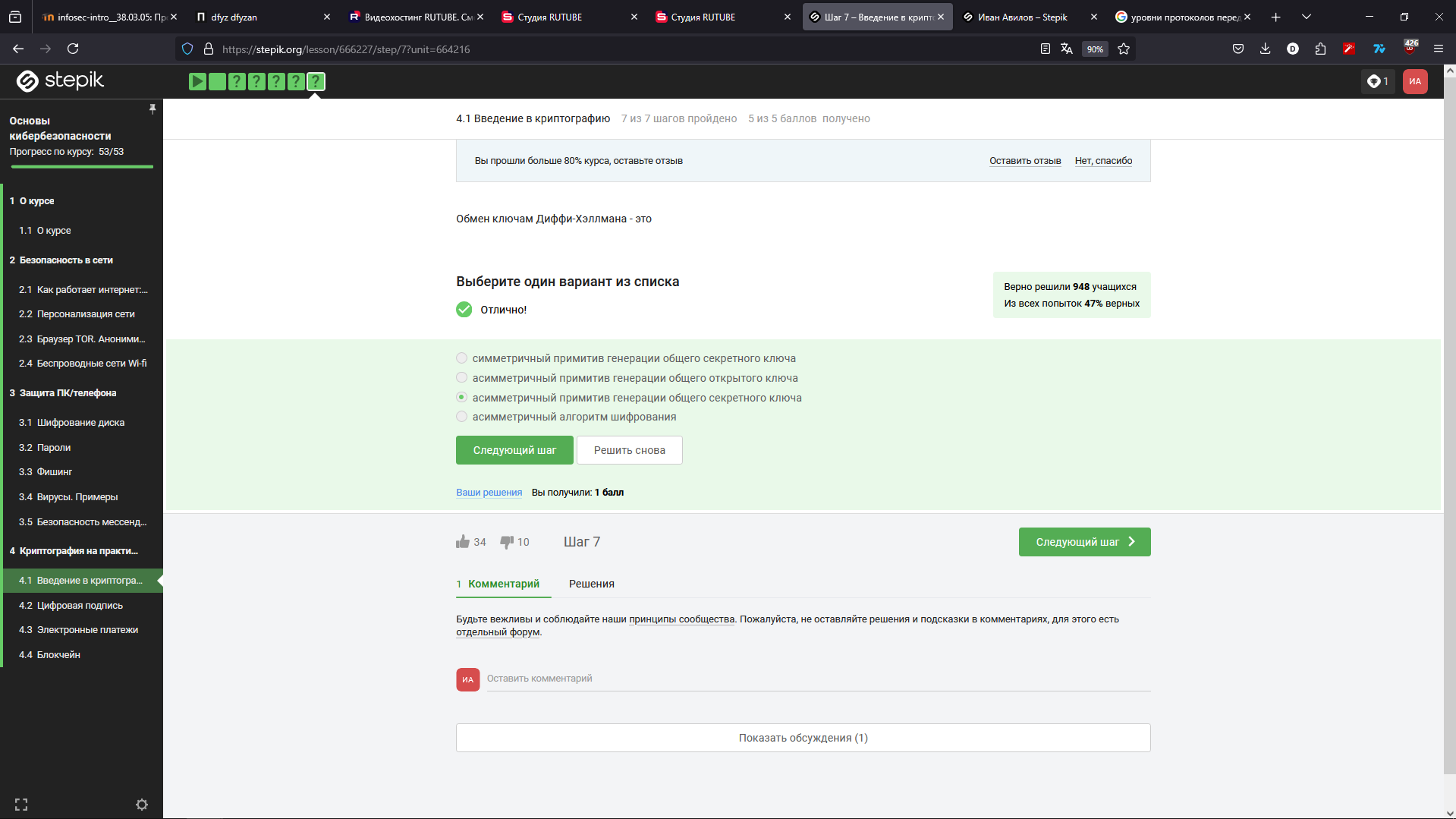
Хэш-функция должна быть быстрой, иметь одинаковую длину выхода и быть максимально стойкой к коллизиям



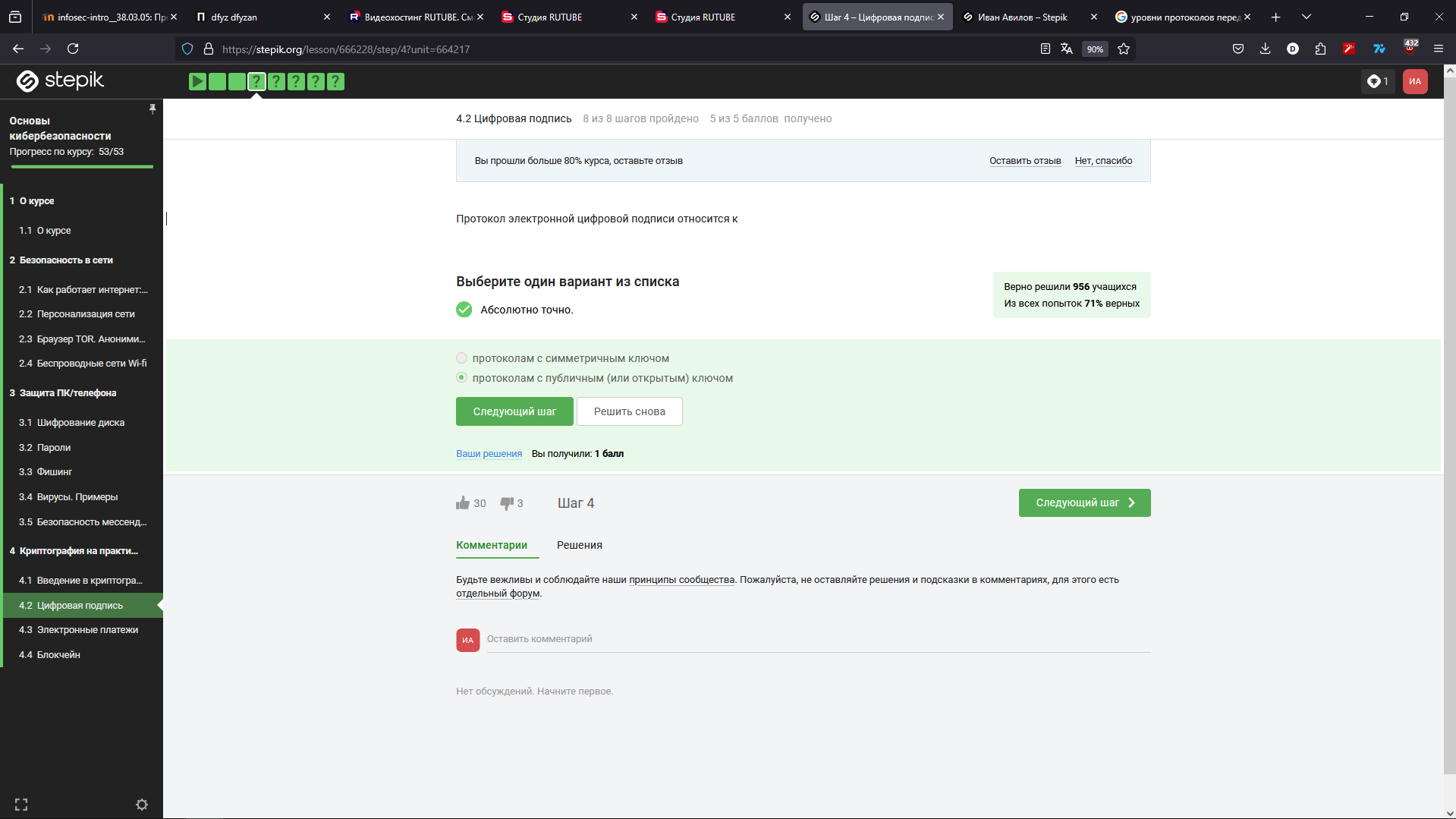
AES и SHA2 - хэш-функции, а не алгоритмы цифровой подписи



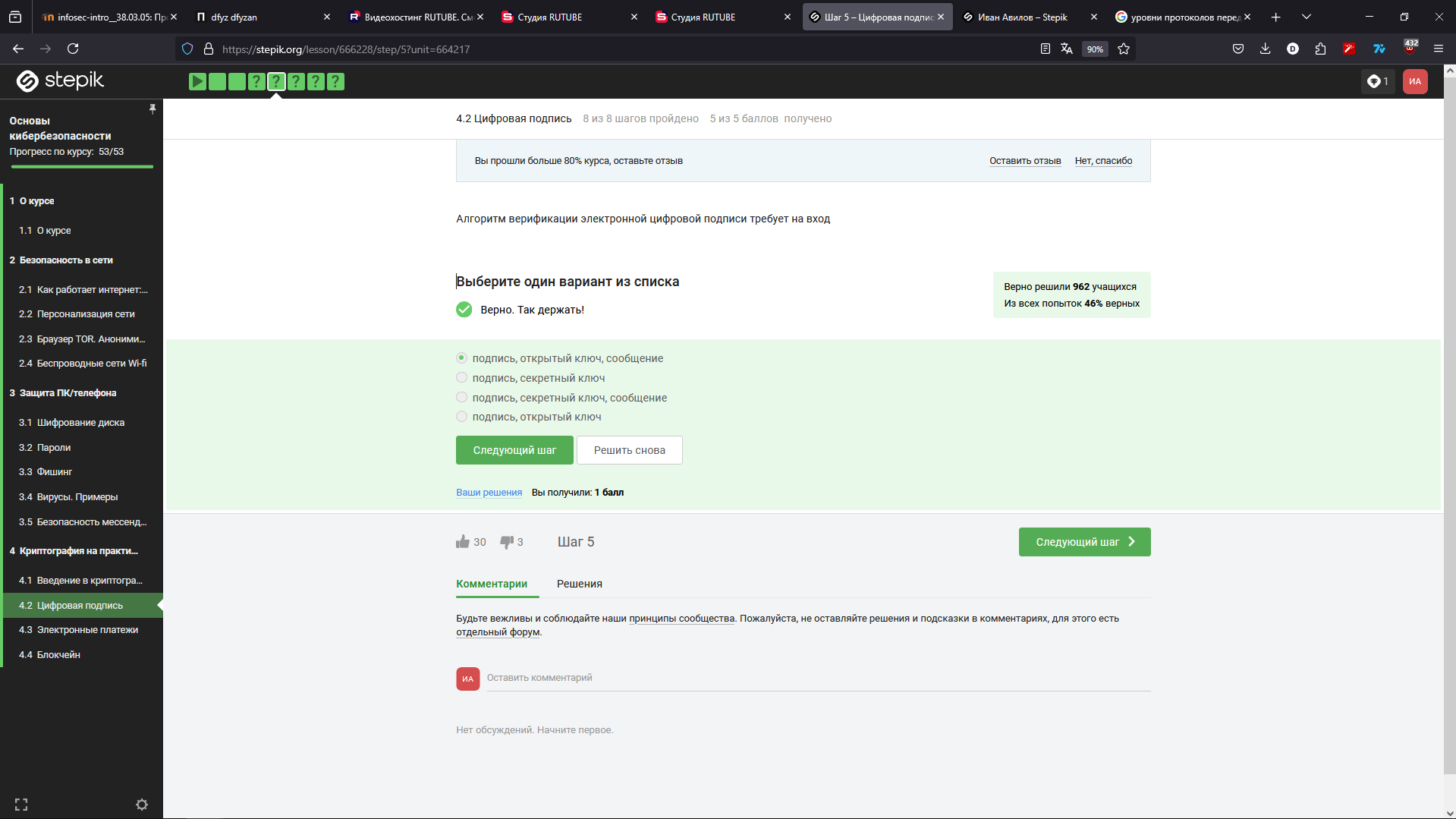
Код аутентификации сообщения является симметричным примитивом



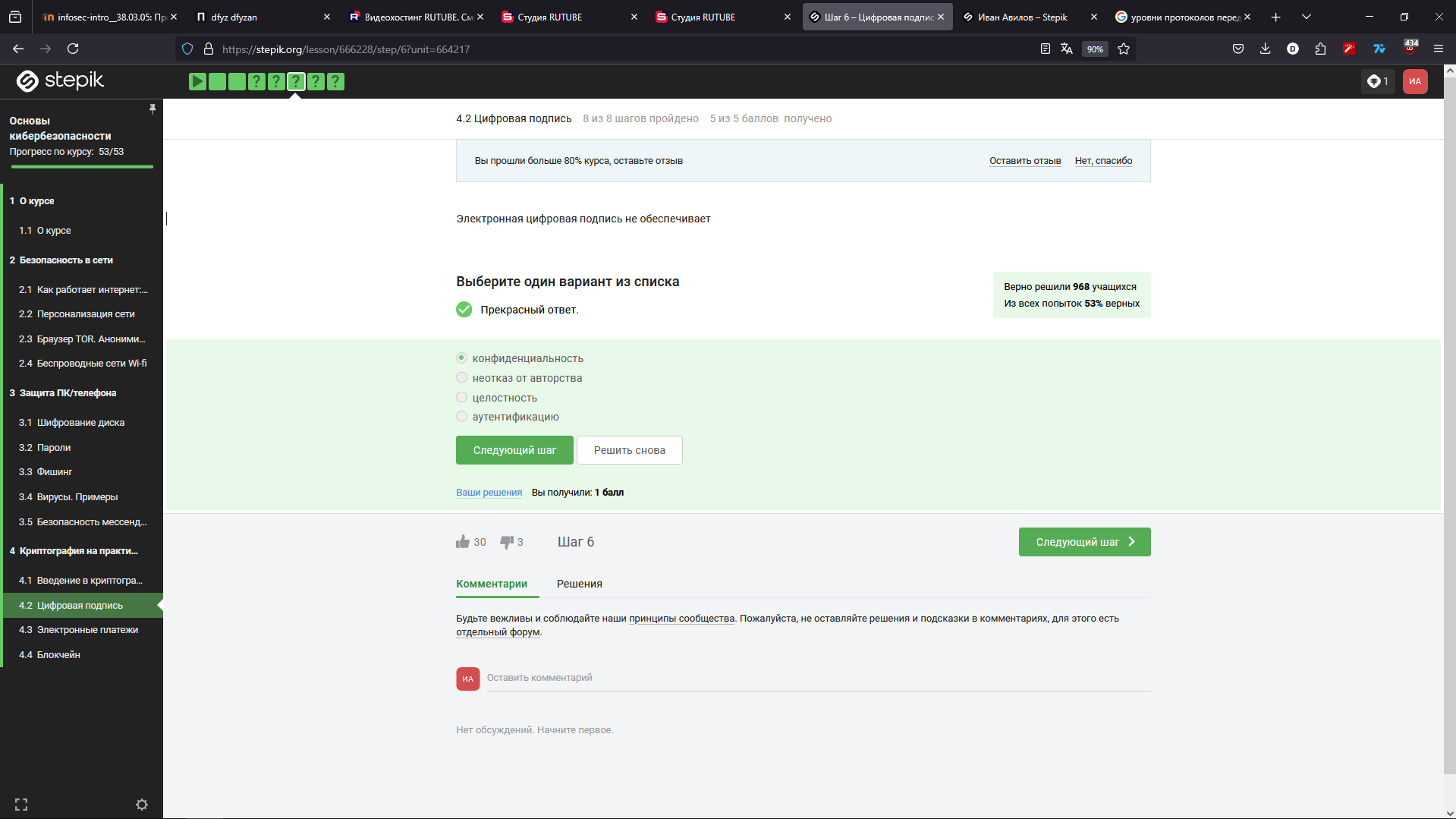
Правильный ответ - асимметричный примитив генерации общего секретного ключа



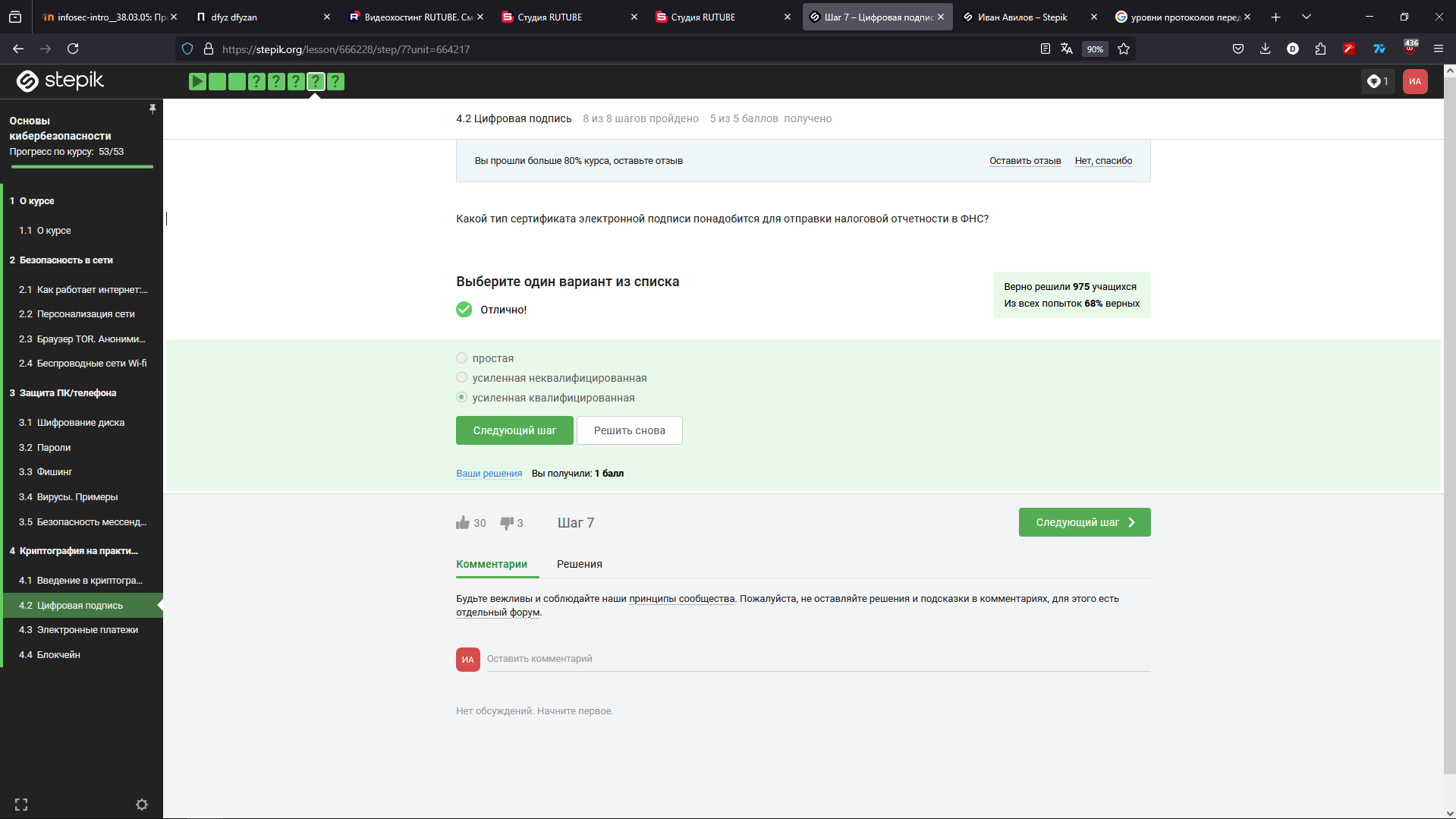
Для проверки подписи используется открытый ключ



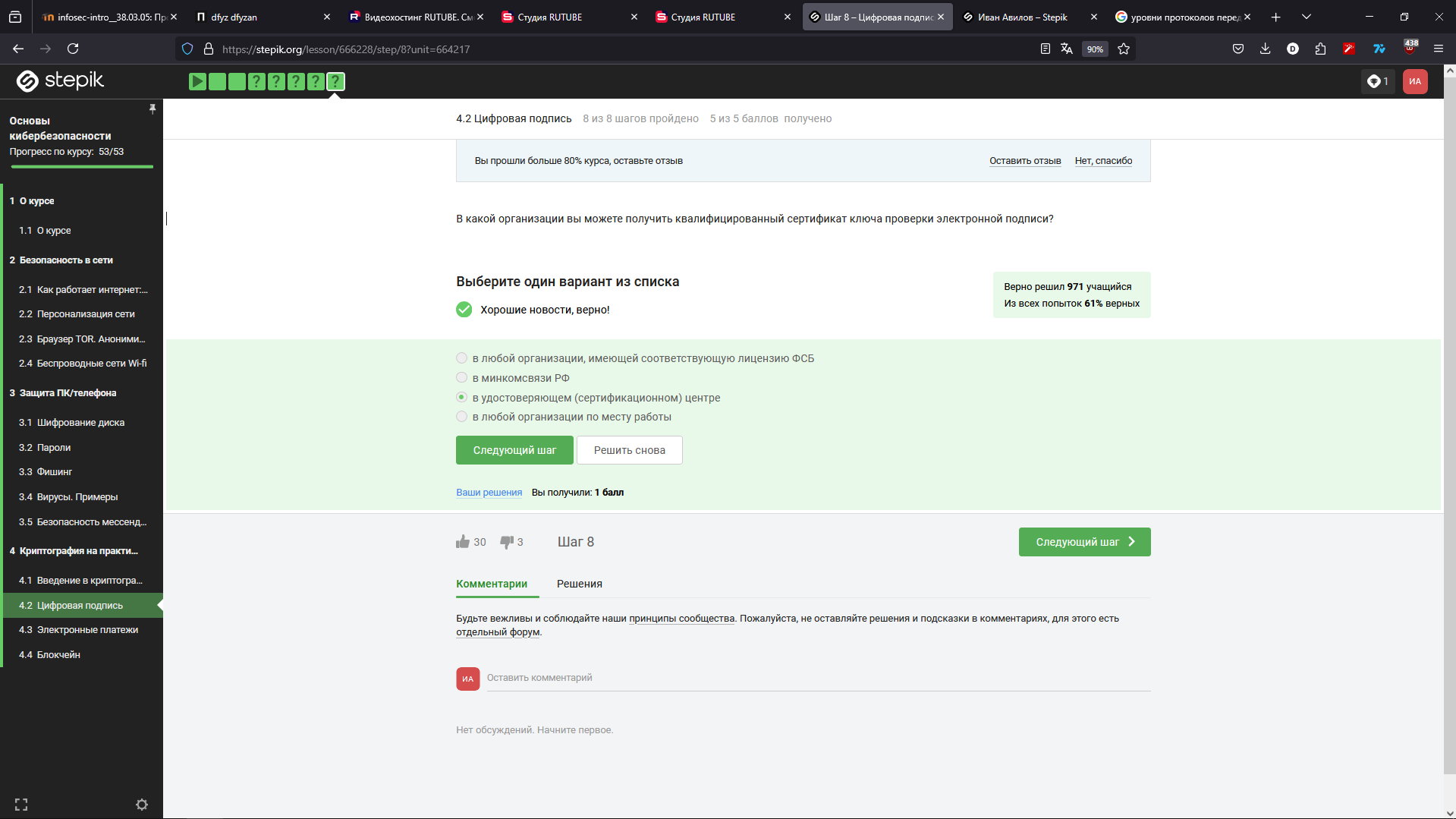
Необходимы подпись, открытый ключ и само сообщение



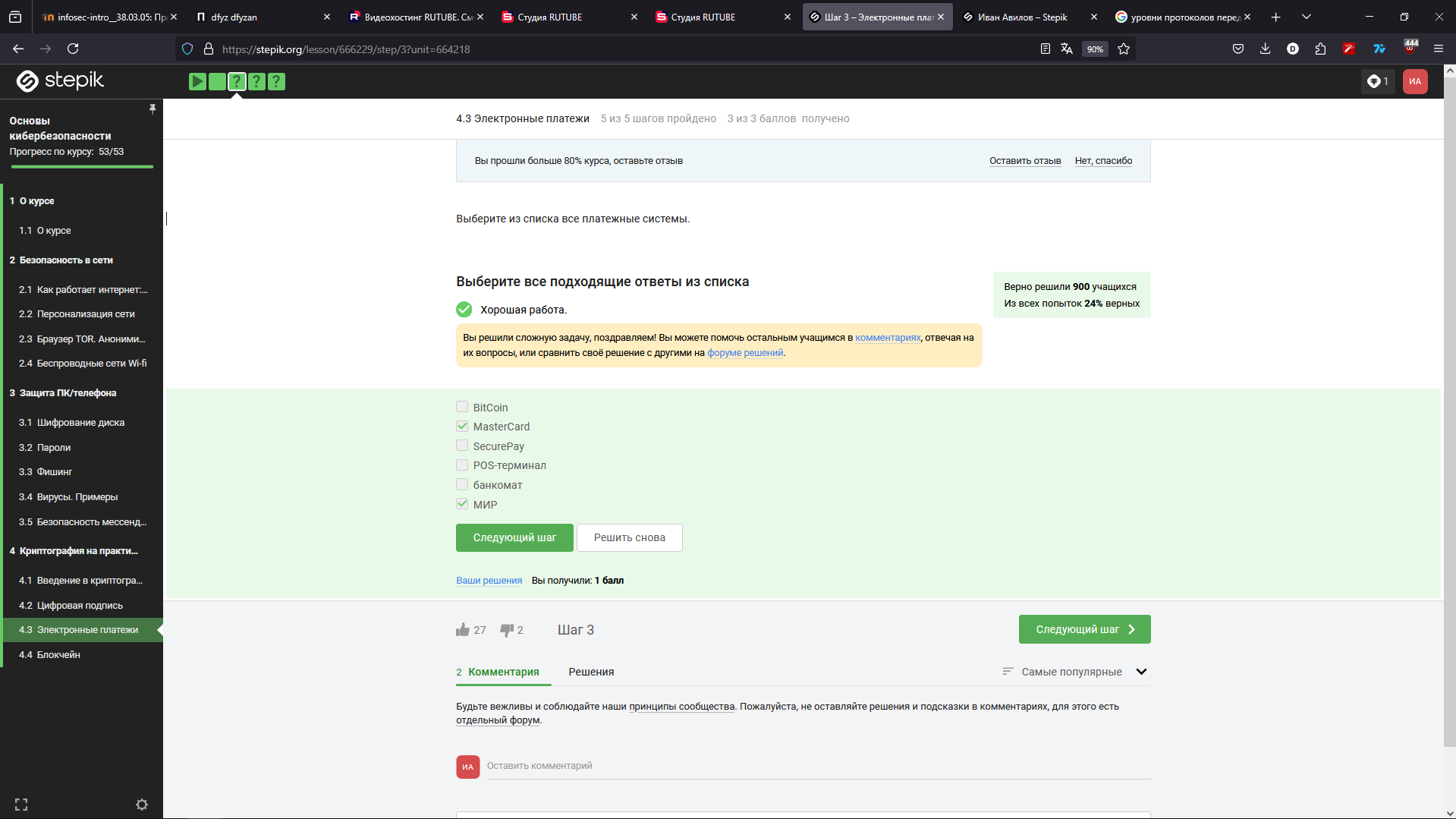
Конфиденциальность не обеспечивается цифровой подписью



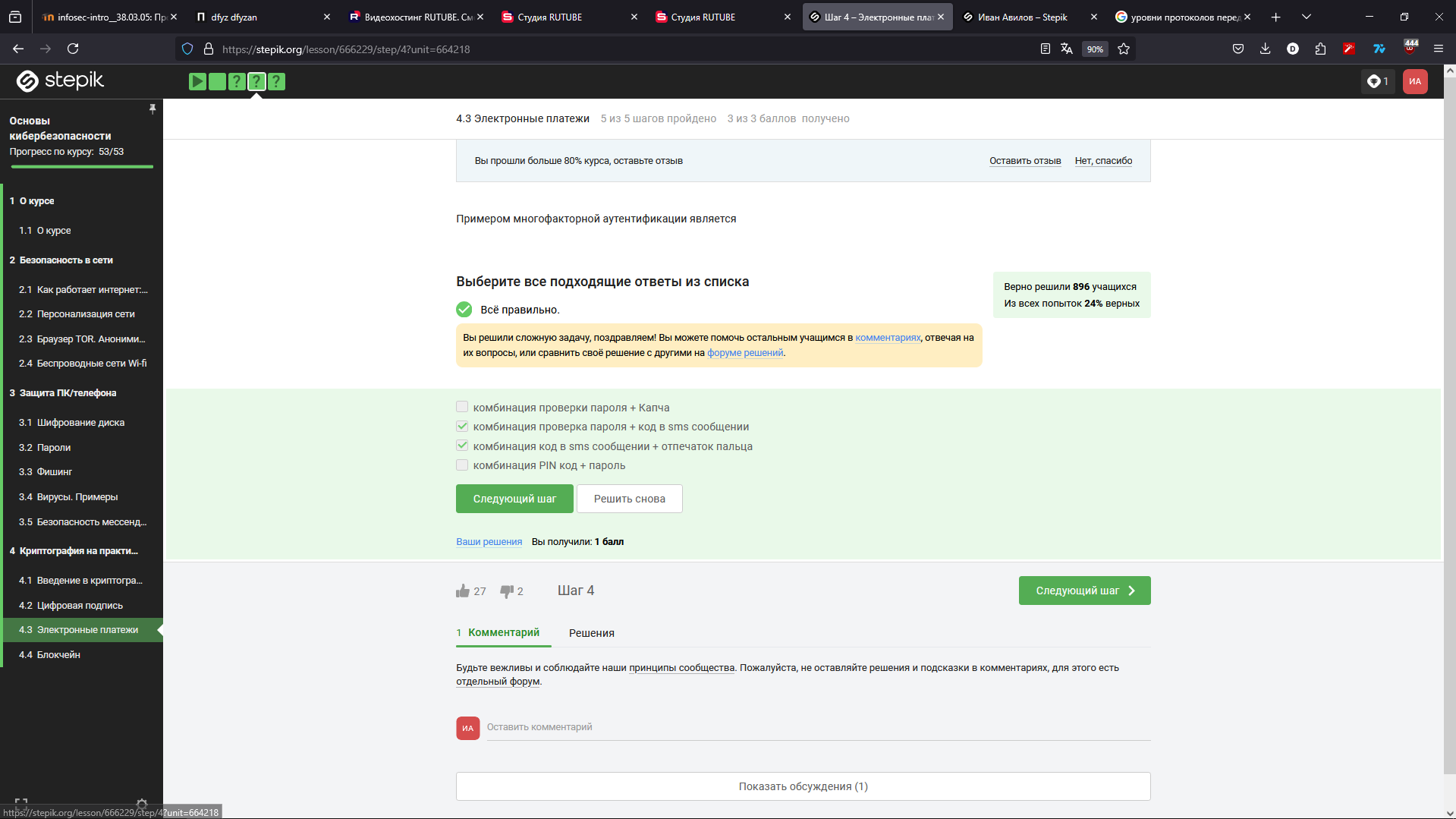
Для подачи налоговой отчётности необходима усиленная квалифицированная подпись



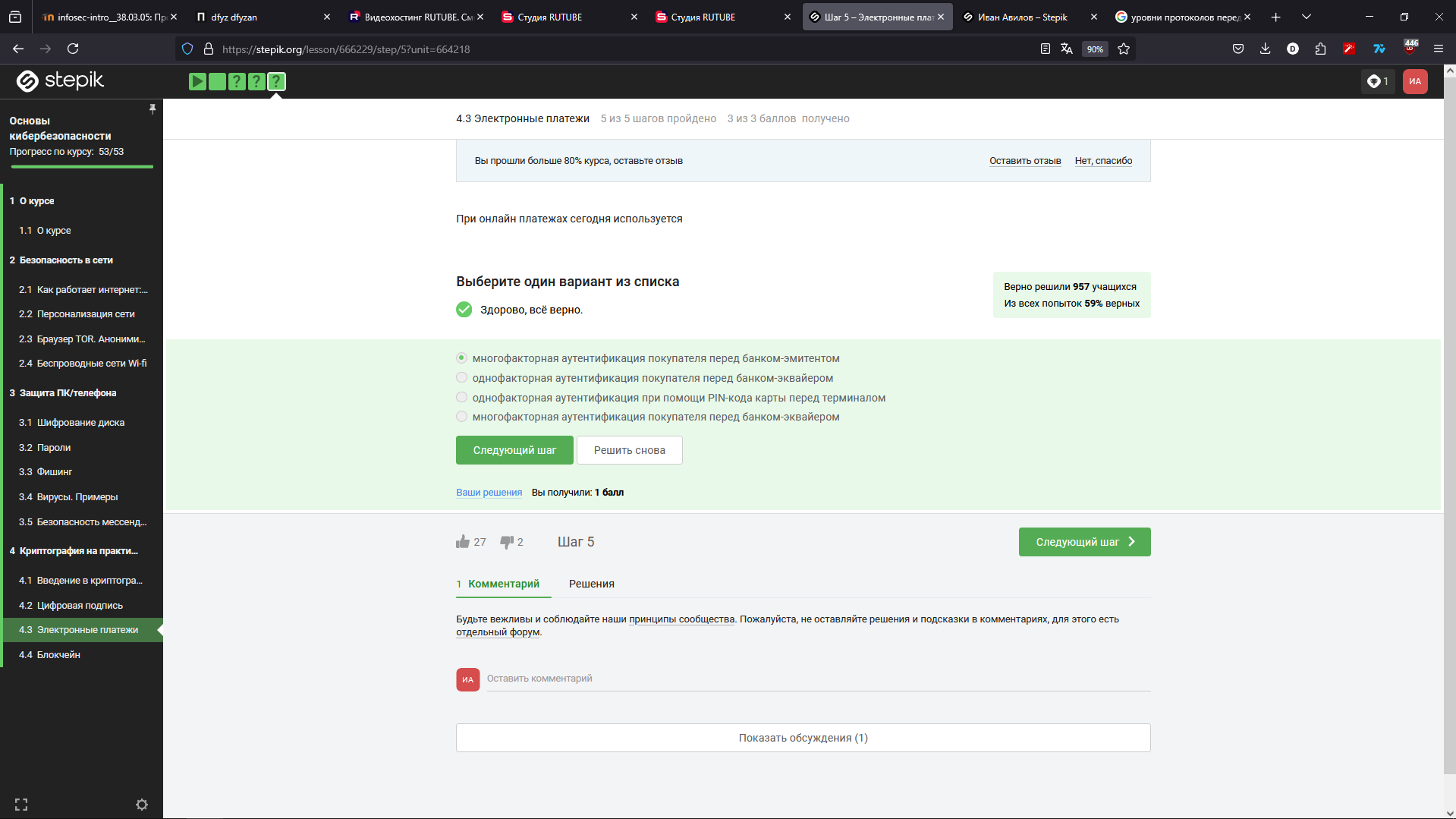
Такую подпись можно получить в специальном удостоверяющем центре



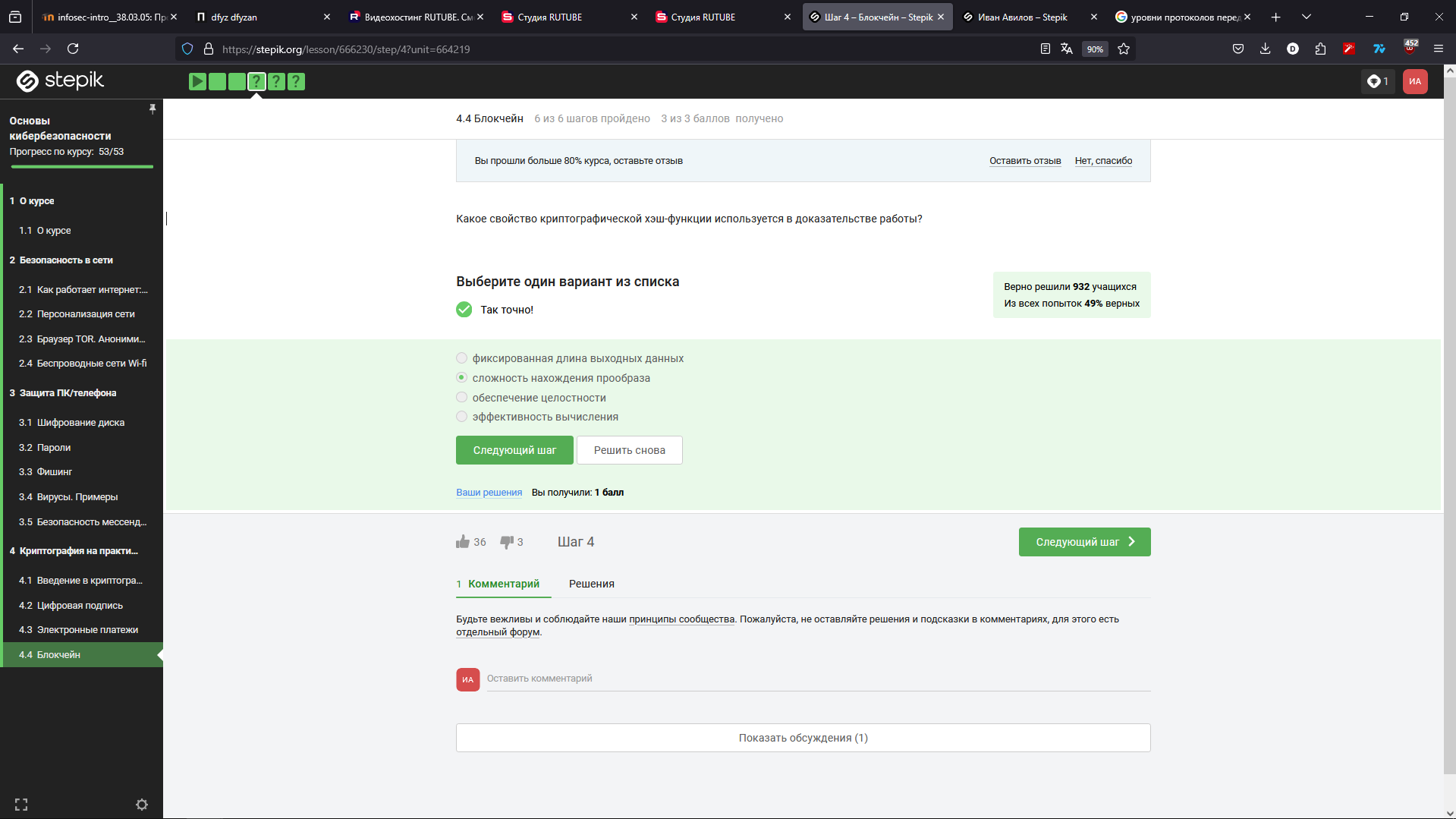
Платёжная система - система, обеспечивающая передачу данных между разными участниками платежа



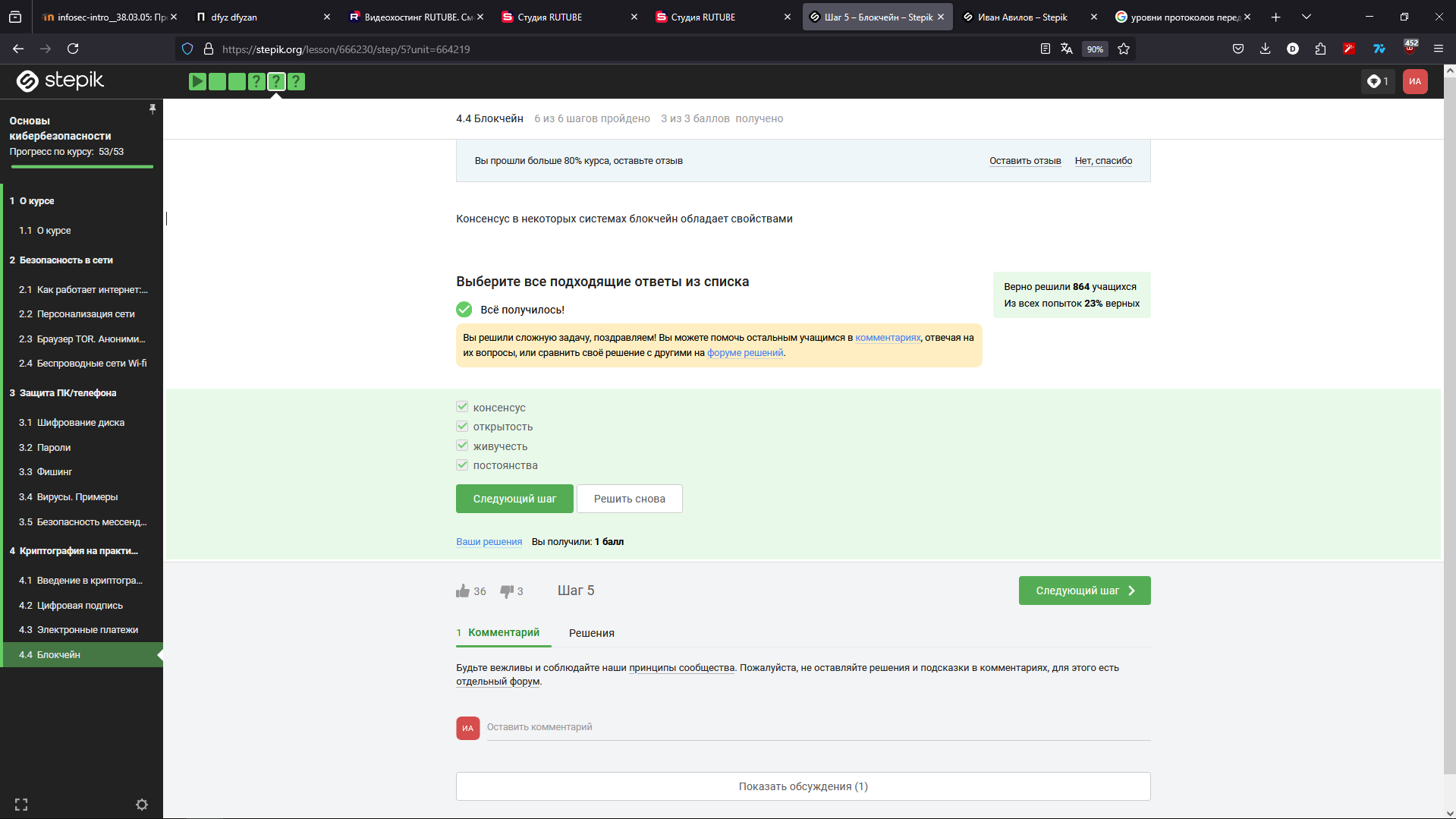
Многофакторная аутентификация - аутентификация, использующая несколько РАЗЛИЧНЫХ факторов



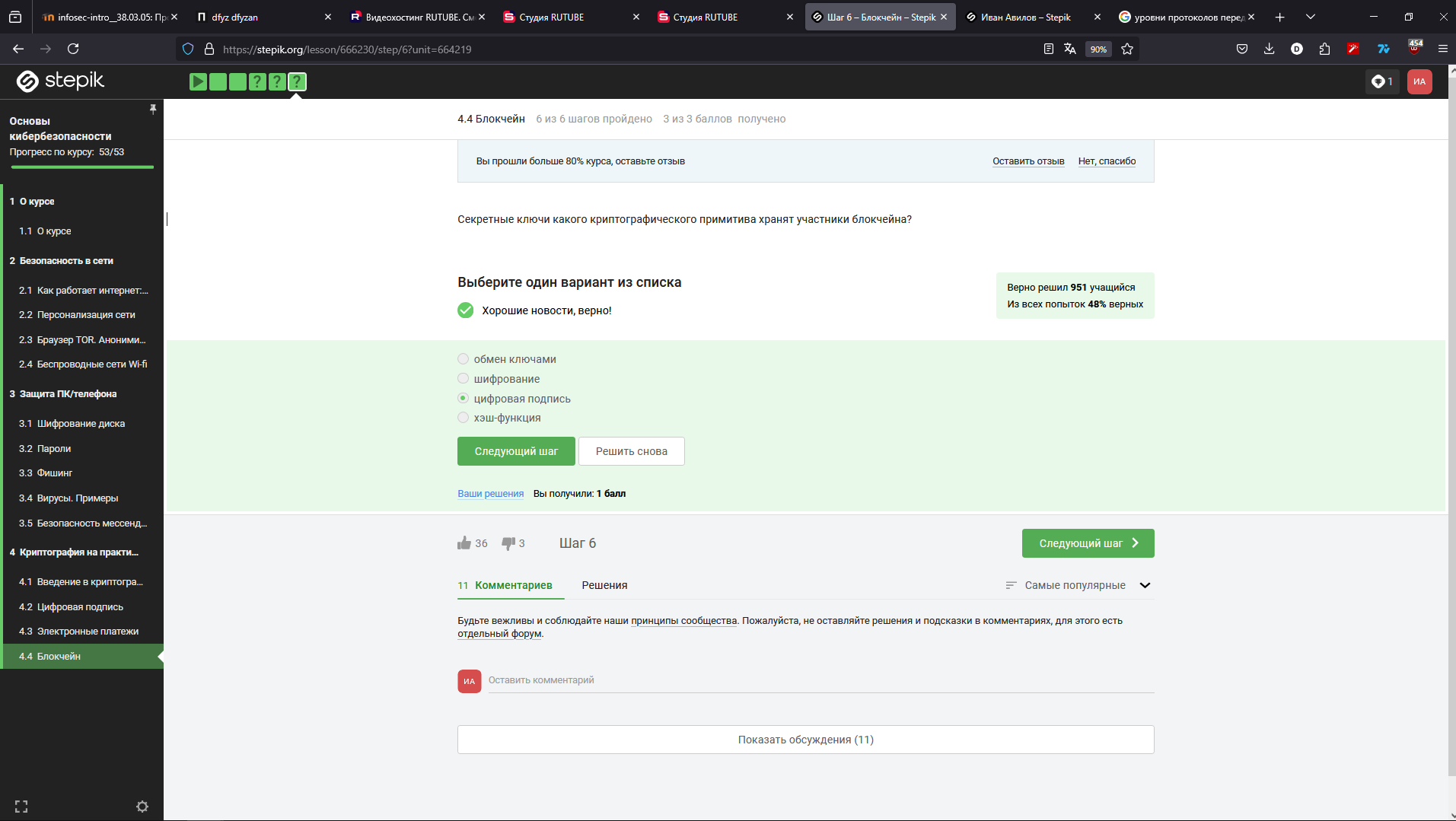
При онлайн платеже вы подтверждаете личность банку, выпустившему вашу карту (эмитенту)



Proof-of-work требует высокую сложность нахождения прообраза



Он обладает всеми свойствами



Цифровая подпись необходима для проверки