

Курс по основам кибербезопасности

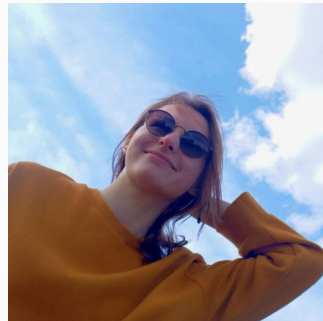
Этап 3

Ведьмина Александра Сергеевна

Российский университет дружбы народов, Москва, Россия

Информация

- Ведьмина Александра Сергеевна
- студентка
- Российский университет дружбы народов
- 1132236003@rudn.ru
- <https://asvedjmina.github.io/ru/>



Цель работы

Выполнить задания третьей части курса по кибербезопасности.

Выполнение лабораторной работы

Два ключа - исходя из определения ассимитричного шифрования.

В ассиметричных криптографических примитивах

Выберите один вариант из списка

☒ Правильно, молодец!

- ☒ обе стороны имеют пару ключей
- ☐ одна сторона публикует свой секретный ключ, другая - держит его в секрете
- ☐ одна сторона имеет только секретный ключ, а другая – пару из открытого и секретного ключей
- ☐ обе стороны имеют общий секретный ключ

По свойствам хэш-функции.

Криптографическая хэш-функция

Выберите все подходящие ответы из списка



Верно. Так держать!

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](#).



стойкая к коллизиям



эффективно вычисляется

Алгоритмы:

К алгоритмам цифровой подписи относятся

Выберите все подходящие ответы из списка



Отлично!

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](#).

- ☐ AES
- ☐ SHA2
- ☒ RSA
- ☒ ECDSA
- ☒ ГОСТ Р 34.10-2012

Следующий шаг

Решить снова

Так как для шифровки и дешифровки используется один и тот же ключ.

Вы прошли больше 80% курса, оставьте отзыв

Код аутентификации сообщения относится к

Выберите один вариант из списка



Правильно.

- ☒ симметричным примитивам
- ☐ асимметричным примитивам

Следующий шаг

Решить снова

По определению этого алгоритма.

Вы прошли больше 80% курса, оставьте отзыв

Обмен ключам Диффи-Хэллмана - это

Выберите один вариант из списка



Хорошие новости, верно!

- ☐ симметричный примитив генерации общего секретного ключа
- ☐ асимметричный примитив генерации общего открытого ключа
- ☒ асимметричный примитив генерации общего секретного ключа
- ☐ асимметричный алгоритм шифрования

Следующий шаг

Решить снова

Потому что используется асимметричное шифрование.

Вы прошли больше 80% курса, оставьте отзыв

Протокол электронной цифровой подписи относится к

Выберите один вариант из списка



Правильно.

- ☐ протоколам с симметричным ключом
- ☒ протоколам с публичным (или открытым) ключом

Следующий шаг

Решить снова

Подписанное сообщение проверяется открытым ключом.

Вы прошли больше 80% курса, оставьте отзыв

Алгоритм верификации электронной цифровой подписи требует на вход

Выберите один вариант из списка



Хорошие новости, верно!

- ☐ подпись, открытый ключ
- ☐ подпись, секретный ключ
- ☐ подпись, секретный ключ, сообщение
- ☒ подпись, открытый ключ, сообщение

Следующий шаг

Решить снова

Она наоборот гарантирует, что можно определить, кто подписал.

Вы прошли больше 80% курса, оставьте отзыв

Электронная цифровая подпись не обеспечивает

Выберите один вариант из списка

☒ Правильно, молодец!

☐ неотказ от авторства

☒ конфиденциальность

☐ аутентификацию

☐ целостность

Следующий шаг

Решить снова

Так как в налоговую нужны юридически значимые документы.

Вы прошли больше 80% курса, оставьте отзыв

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

Выберите один вариант из списка

☒ Всё правильно.

- ☐ усиленная неквалифицированная
- ☒ усиленная квалифицированная
- ☐ простая

Следующий шаг

Решить снова

В сертифицированном центре.

Вы прошли больше 80% курса, оставьте отзыв

В какой организации вы можете получить квалифицированный сертификат ключа проверки электрон

Выберите один вариант из списка



Отлично!

- ☐ в любой организации, имеющей соответствующую лицензию ФСБ
- ☐ в минкомсвязи РФ
- ☒ в удостоверяющем (сертификационном) центре
- ☐ в любой организации по месту работы

Следующий шаг

Решить снова

МИР и Mastercard всем известны.

Выберите из списка все платежные системы.

Выберите все подходящие ответы из списка



Хорошая работа.

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](#).

- ☐ BitCoin
- ☒ MasterCard
- ☐ SecurePay
- ☐ POS-терминал
- ☐ банкомат
- ☒ МИР

Отметила верные методы.

Примером многофакторной аутентификации является

Выберите все подходящие ответы из списка



Здорово, всё верно.

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](#).

- ☐ комбинация проверки пароля + Капча
- ☒ комбинация проверка пароля + код в sms сообщении
- ☒ комбинация код в sms сообщении + отпечаток пальца
- ☐ комбинация PIN код + пароль

Следующий шаг

Решить снова

Используется многофакторная аутентификация.

При онлайн платежах сегодня используется

Выберите один вариант из списка



Прекрасный ответ.

- ☒ 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

Следующий шаг

Решить снова

Прообраз действительно сложно найти, поэтому она надёжна.

Какое свойство криптографической хэш-функции используется в доказательстве работы?

Выберите один вариант из списка



Всё правильно.

- ☐ фиксированная длина выходных данных
- ☒ сложность нахождения прообраза
- ☐ обеспечение целостности
- ☐ эффективность вычисления

Следующий шаг

Решить снова

По свойствам консенсуса.

Консенсус в некоторых системах блокчейн обладает свойствами

Выберите все подходящие ответы из списка



Верно. Так держать!

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](#).

- ☒ постоянства
- ☒ консенсус
- ☒ открытость
- ☒ живучесть

Следующий шаг

Решить снова

Они хранят цифровые подписи.

Секретные ключи какого криптографического примитива хранят участники блокчейна?

Выберите один вариант из списка



Правильно.

- ☐ обмен ключами
- ☐ шифрование
- ☒ цифровая подпись
- ☐ хэш-функция

Следующий шаг

Решить снова

Выполнение лабораторной работы

Ура, я завершила курс!

The screenshot shows a web browser window with the Stepik website. The browser's address bar displays the URL: `stepik.org/lesson/666230/step/6/lesson-end?unit=664219`. The browser's toolbar includes icons for Google, Gmail, and various social media and utility services like VK, Zoom, and Telegram. The Stepik website interface is in Russian. On the left, a sidebar lists course topics under the heading 'Основы кибербезопасности'. The main content area shows a progress bar for '4.4 Блокчейн' and a large white modal window in the center. The modal window contains a congratulatory message, a course completion certificate, and social media sharing options. The background of the website is dark grey.

stepik.org/lesson/666230/step/6/lesson-end?unit=664219

Google Gmail Мой диск – Go... Карты YouTube VK Zoom Авиабилеты Уведомления Яндекс Maps Telegram Rutube Youtube-os plvideo

stepik

Основы кибербезопасности
Прогресс по курсу: 53/53

2. Безопасность в сети

2.1. Как работает интернет

2.2. Персонализация сети

2.3. Браузер TOR. Анонимы

2.4. Беспроводные сети Wi-Fi

3. Защита ПК/телефона

3.1. Шифрование диска

3.2. Пароли

3.3. Фейдинг

3.4. Вирусы. Примеры

3.5. Безопасность мессенджеров

4. Криптография на практике

4.1. Введение в криптографию

4.2. Цифровая подпись

4.3. Электронные платежи

4.4. Блокчейн

4.4 Блокчейн 6 из 6 шагов пройдено 3 из 3 баллов получено

Вы прошли

Секретные к

Выберите

Правила

обмен кодами

шифрование

цифровая подпись

хэш-функции

Следующий шаг

Ваше решение: Вы получили: 1 балл

Шаг 6

11 Комментариев Решения

Самые популярные

Поздравляем!
Вы завершили курс «Основы кибербезопасности».

Вы набрали 53 балла из 53, изучив 98% материалов курса.
Сертификат в нём не выдаётся, но вы можете поделиться своим результатом в соцсетях.

Всего решено 951 учеником
Из всех попыток 48% верных

Оставить отзыв Нет, спасибо

Оставить отзыв Найти новый курс

<https://stepik.org/course/111512>

Выводы

Все задания третьей части выполнены. Курс завершён.