

Внешний курс. Блок 3: Криптография на практике

Неустроева И.Н.

Российский университет дружбы народов, Москва, Россия

Информация

- Неустроева Ирина Николаевна
- студентка группы НБИ 02-23
- Российский университет дружбы народов

- Кулябов Дмитрий Сергеевич
- д.ф.-м.н., профессор
- профессор кафедры прикладной информатики и теории вероятностей
- Российский университет дружбы народов

Вводная часть

Выполнить контрольные задания третьего блока “Криптография на практи” внешнего курса “Основы кибербезопасности”.

Интернет-ресурсы

Основная часть

Выполнение заданий блока “Основы Кибербезопасности”

В асимметричной криптографии у каждой из сторон есть пара ключей: открытый и секретный ключ

В асимметричных криптографических примитивах

Выберите один вариант из списка

☒ Правильно, молодец!

Верно решили **940** учащихся
Из всех попыток **42%** верных

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

Следующий шаг

Решить снова

[Ваши решения](#) Вы получили: **1 балл**

Выполнение заданий блока “Основы Кибербезопасности”

Криптографическая хэш-функция обладает важным свойством стойкости к коллизиям, что означает, что крайне сложно найти два разных входа, которые дают одинаковый хэш. Она принимает произвольный объем данных и выдает фиксированную строку заданной длины (например, n). Обычно функция сжимает данные, преобразуя большой набор информации в небольшое значение

Криптографическая хэш-функция

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](#).

Верно решили **798** учащихся
Из всех попыток **11%** верных

☒ эффективно вычисляется

Выполнение заданий блока “Основы Кибербезопасности”

Отмечены алгоритмы цифровой подписи

К алгоритмам цифровой подписи относятся

Выберите все подходящие ответы из списка

☒ Отличное решение!

Верно решили **834** учащихся
Из всех попыток **19%** 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](#).

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

Следующий шаг

Решить снова

[Ваши решения](#) Вы получили: **1 балл**

Выполнение заданий блока “Основы Кибербезопасности”

Код аутентификации сообщения (MAC) относится к симметричным примитивам, поскольку для его генерации и проверки используется общий секретный ключ, известный только отправителю и получателю, что обеспечивает целостность и аутентичность данных

Код аутентификации сообщения относится к

Выберите один вариант из списка



Отлично!

Верно решили **955** учащихся
Из всех попыток **69%** верных

- ☒ симметричным примитивам
- ☐ асимметричным примитивам

Следующий шаг

Решить снова

[Ваши решения](#) Вы получили: **1 балл**

Выполнение заданий блока “Основы Кибербезопасности”

Чтобы ответить на данный вопрос использую определение Диффи-Хэллмана

Обмен ключам Диффи-Хэллмана - это

Выберите один вариант из списка

☒ Здорово, всё верно.

Верно решили **948** учащихся
Из всех попыток **47%** верных

- ☐ 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

[Ваши решения](#) Вы получили: **1 балл**

👍 33 👎 8

Шаг 7

Следующий шаг >

10/21

Выполнение заданий блока Цифровая подпись

По определению цифровой подписи протокол ЭЦП относится к протоколам с публичным ключом

Протокол электронной цифровой подписи относится к

Выберите один вариант из списка

☒ Верно. Так держать!



Верно решили **956** учащихся
Из всех попыток **71%** верных

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

Следующий шаг

Решить снова

[Ваши решения](#) Вы получили: **1 балл**

 28  3

Шаг 4

Следующий шаг >

Выполнение заданий блока Цифровая подпись

Каждая машина процедуру верификации, которая берет на вход само обновление, подпись и открытый ключ разработчика

Алгоритм верификации электронной цифровой подписи требует на вход

Выберите один вариант из списка



Правильно, молодец!

Верно решили **962** учащихся
Из всех попыток **46%** верных

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

Следующий шаг

Решить снова

[Ваши решения](#) Вы получили: **1 балл**

Выполнение заданий блока Цифровая подпись

Цифровая подпись обеспечивает три ключевых функции:

1. Целостность сообщения — изменения в сообщении приводят к некорректной проверке подписи.
2. Аутентификация — позволяет установить, что подпись принадлежит конкретному владельцу.
3. Неотказ от авторства — подписавший не может отказаться от своей подписи.

Однако, если секретный ключ украден, безопасность подписи подрывается, и она не обеспечивает конфиденциальности

Выполнение заданий блока Цифровая подпись

Усиленная квалифицированная подпись (УКЭП) имеет юридическую силу и равнозначна рукописной подписи. Для её получения необходимо обратиться в аккредитованный сертификационный центр с паспортом и другими данными.

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

Выберите один вариант из списка

☒ Верно.

Верно решили **975** учащихся
Из всех попыток **68%** верных

- ☐ усиленная неквалифицированная
- ☒ усиленная квалифицированная
- ☐ простая

Следующий шаг

Решить снова

Выполнение заданий блока Цифровая подпись

Сертификат подписывается с помощью электронной подписи уже доверенной стороной, удостоверяющим центром.

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

Выберите один вариант из списка

☒ Верно. Так держать!

Верно решил **971** учащийся
Из всех попыток **61%** верных

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

Следующий шаг

Решить снова


[Ваши решения](#) Вы получили: **1 балл**

Выполнение заданий блока Электронные платежи

На данный момент существуют такие платежные системы, как: Visa, MasterCard, МИР

Выберите из списка все платежные системы.

Выберите все подходящие ответы из списка

 Всё получилось!

Верно решили **900** учащихся
Из всех попыток **24%** 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](#).

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

Следующий шаг

Решить снова

Выполнение заданий блока Электронные платежи

Основные категории вещей, которые мы можем использовать для доказательства своей идентичности:

1. Знание: Это что-то, что я знаю, например, пароль, PIN-код или секретный код для онлайн-платежей.
2. Владение: В онлайн-платежах используется второй фактор — это то, чем я владею, например, телефон, на который приходит код для подтверждения.
3. Свойства: Биометрические данные, такие как отпечаток пальца или сетчатка глаза, служат третьим фактором аутентификации.
4. Локация: Четвертый фактор аутентификации — это место, откуда осуществляется доступ, что также может быть учтено при проверке идентичности.

Выполнение заданий блока Блокчейн

Proof-of-Work (PoW) — это способ, который используется в блокчейне для подтверждения транзакций и создания новых блоков. В этом процессе майнеры (люди, которые занимаются добычей криптовалюты) соревнуются друг с другом за завершение транзакций в сети и за вознаграждение

Когда люди отправляют друг другу цифровые деньги, эти транзакции собираются в блоки и добавляются в общую базу данных, называемую блокчейном. Чтобы сделать сеть безопасной и защитить её от мошенничества, PoW требует много вычислительных ресурсов. Это значит, что для успешного участия в процессе нужно много мощных компьютеров

Какое свойство криптографической хэш-функции используется в доказательстве работы?

Выберите один вариант из списка



Отличное решение!

Верно решили **932** учащихся
Из всех попыток **49%** верных

Выполнение заданий блока Блокчейн

В основе любого блокчейна, включая биткоин, лежит консенсус — публичная структура данных (ledger), содержащая историю всех транзакций. Консенсус обеспечивает четыре ключевых свойства:

1. **Постоянство:** Добавленные данные не могут быть удалены.
2. **Согласованность:** Все участники видят и согласны с одними и теми же данными, за исключением последних изменений.
3. **Живучесть:** Возможность добавления новых транзакций в любое время.
4. **Открытость:** Любой желающий может стать участником блокчейна.

Эти свойства обеспечивают надежность и безопасность системы.

Выполнение заданий блока Блокчейн

В блокчейне у каждого из трех участников есть секретный ключ, который они используют для подтверждения транзакций. Этот секретный ключ позволяет создавать цифровую подпись, которая служит доказательством того, что транзакция была инициирована конкретным участником. Цифровая подпись основана на паре ключей — секретном и открытом. Секретный ключ используется для подписания транзакции, а открытый ключ позволяет другим участникам проверить подлинность этой подписи. Таким образом, цифровая подпись обеспечивает безопасность и аутентичность транзакций в блокчейне.

Секретные ключи какого криптографического примитива хранят участники блокчейна?

Выберите один вариант из списка

☒ Верно. Так держать!

Верно решил **951** учащийся
Из всех попыток **48%** верных

В результате 3 этапа я узнала много нового о криптографии, цифровых подписях и технологиях блокчейна. Выяснила, как обеспечивается безопасность транзакций.

...