

Внешний курс. Блок 3: Криптография на практике

Дисциплина: Основы информационной безопасности

Неустроева Ирина Николаевна

Содержание

1	Цель работы	5
2	Выполнение заданий блока “Основы Кибербезопасности”	6
2.1	Введение в криптографию	6
2.2	Цифровая подпись	8
2.3	Электронные платежи	11
2.4	Блокчейн	13
3	Выводы	16

Список иллюстраций

2.1	Вопрос 4.1.1	6
2.2	Вопрос 4.1.2	7
2.3	Вопрос 4.1.3	7
2.4	Вопрос 4.1.4	8
2.5	Вопрос 4.1.5	8
2.6	Вопрос 4.2.1	9
2.7	Вопрос 4.2.2	9
2.8	Вопрос 4.2.3	10
2.9	Вопрос 4.2.4	10
2.10	Вопрос 4.2.5	11
2.11	Вопрос 4.3.1	11
2.12	Вопрос 4.3.2	12
2.13	Вопрос 4.3.3	13
2.14	Вопрос 4.4.1	14
2.15	Вопрос 4.4.2	14
2.16	Вопрос 4.4.3	15

Список таблиц

1 Цель работы

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

2 Выполнение заданий блока “Основы Кибербезопасности”

2.1 Введение в криптографию

В асимметричной криптографии у каждой из сторон есть пара ключей: открытый и секретный ключ (рис. 2.1).

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

👍 33 🗳 8 Шаг 3 Следующий шаг >

Рис. 2.1: Вопрос 4.1.1

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. (рис. 2.2).

Криптографическая хэш-функция

Выберите все подходящие ответы из списка

Верно решили 798 учащихся
Из всех попыток 11% верных

✓ Хорошая работа.

Вы решили сложную задачу, поздравляем! Вы можете помочь остальным учащимся в [комментариях](#), отвечая на их вопросы, или сравнить свое решение с другими на [форуме решений](#).

☒ эффективно вычисляется
☒ дает на выходе фиксированное число бит независимо от объема входных данных
☐ обеспечивает конфиденциальность захешированных данных
☒ стойкая к коллизиям

Следующий шаг Решить снова

[Ваши решения](#) Вы получили: 1 балл

Рис. 2.2: Вопрос 4.1.2

Отмечены алгоритмы цифровой подписи (рис. 2.3).

К алгоритмам цифровой подписи относятся

Выберите все подходящие ответы из списка

Верно решили 834 учащихся
Из всех попыток 19% верных

✓ Отличное решение!

Вы решили сложную задачу, поздравляем! Вы можете помочь остальным учащимся в [комментариях](#), отвечая на их вопросы, или сравнить свое 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

👍 33 👎 8 Шаг 5
 Следующий шаг >

Рис. 2.3: Вопрос 4.1.3

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.(рис. 2.4).

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

👍 33 🗣 8 Шаг 6
 Следующий шаг >

Рис. 2.4: Вопрос 4.1.4

Чтобы ответить на данный вопрос использую определение Диффи-Хэллмана (рис. 2.5).

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 >

Рис. 2.5: Вопрос 4.1.5

2.2 Цифровая подпись

По определению цифровой подписи протокол ЭЦП относиться к протоколам с публичным ключом (рис. 2.6).

Протокол электронной цифровой подписи относится к

Выберите один вариант из списка

✓ Верно. Так держаты!

Верно решили 956 учащихся
Из всех попыток 71% верных

☐ протоколом с симметричным ключом

☒ протоколом с публичным (или открытым) ключом

Следующий шаг Решить снова

Ваши решения Вы получили: 1 балл

28 3 Шаг 4 Следующий шаг >

Рис. 2.6: Вопрос 4.2.1

Каждая машина процедуру верификации, которая берет на вход само обновление, подпись и открытый ключ разработчика (рис. 2.7).

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

28 3 Шаг 5 Следующий шаг >

Рис. 2.7: Вопрос 4.2.2

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.(рис. 2.8).

Электронная цифровая подпись не обеспечивает

Выберите один вариант из списка

✓ Хорошие новости, верно!

Верно решили 968 учащихся
Из всех попыток 53% верных

- ☒ конфиденциальность
- ☐ неотказ от авторства
- ☐ целостность
- ☐ аутентификацию

Следующий шаг Решить снова

Ваши решения Вы получили: 1 балл

👍 28 👎 3 Шаг 6

Следующий шаг >

Рис. 2.8: Вопрос 4.2.3

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. (рис. 2.9).

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

Ваши решения Вы получили: 1 балл

👍 28 👎 3 Шаг 7

Следующий шаг >

Рис. 2.9: Вопрос 4.2.4

Сертификат подписывается с помощью электронной подписи уже доверенной стороной, удостоверяющим центром. (рис. 2.10).

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

28 3 Шаг 8 Следующий шаг >

Рис. 2.10: Вопрос 4.2.5

2.3 Электронные платежи

На данный момент существуют такие платежные системы, как: Visa, MasterCard, МИР (рис. 2.11).

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

[Ваши решения](#) Вы получили: 1 балл

Рис. 2.11: Вопрос 4.3.1

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. (рис. 2.12).

Примером многофакторной аутентификации является

Выберите все подходящие ответы из списка

✓ Абсолютно точно.

Верно решили 896 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](#).

- ☐ 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

[Ваши решения](#) Вы получили: 1 балл

👍 25 🗨 2 Шаг 4 Следующий шаг >

Рис. 2.12: Вопрос 4.3.2

При онлайн платежах используется многофакторная аутентификация банком-эмитентом (выпустившим карту), чтобы удостовериться, что транзакцию совершает именно владелец карты или счета, а не злоумышленник(рис. 2.13).

Примером многофакторной аутентификации является

Выберите все подходящие ответы из списка

Верно решили 896 учащихся
Из всех попыток 24% верных

Абсолютно точно.

Вы решили сложную задачу, поздравляем! Вы можете помочь остальным учащимся в [комментарии](#), 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

Ваши решения Вы получили: 1 балл

👍 25 🗳 2 Шаг 4 Следующий шаг >

Рис. 2.13: Вопрос 4.3.3

2.4 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.(рис. 2.14).

Какое свойство криптографической хэш-функции используется в доказательстве работы?

Выберите один вариант из списка

Верно решили 932 учащихся
Из всех попыток 49% верных

✓ Отличное решение!

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

Следующий шаг Решить снова

Ваши решения Вы получили: 1 балл

👍 33 🗣 3 Шаг 4 Следующий шаг >

Рис. 2.14: Вопрос 4.4.1

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. (рис. 2.15).

Консенсус в некоторых системах блокчейн обладает свойствами

Выберите все подходящие ответы из списка

Верно решили 864 учащихся
Из всех попыток 23% верных

✓ 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](#).

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

Следующий шаг Решить снова

Ваши решения Вы получили: 1 балл

Рис. 2.15: Вопрос 4.4.2

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. (рис. 2.16).

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

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

Следующий шаг Решить снова

Ваши решения Вы получили: 1 балл

👍 33 🗳️ 3 Шаг 6 Следующий шаг >

Рис. 2.16: Вопрос 4.4.3

3 Выводы

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