

Внешний курс. Этап 3

Криптография на практике

Татьяна Александровна Буллер

Содержание

| | | |
|----------|---------------------------------------|-----------|
| 1 | Цель работы | 5 |
| 2 | Выполнение контрольных заданий | 6 |
| 2.1 | Введение в криптографию | 6 |
| 2.2 | Цифровая подпись | 10 |
| 2.3 | Электронные платежи | 13 |
| 2.4 | Блокчейн | 15 |
| 3 | Выводы | 17 |

Список таблиц

Список иллюстраций

| | | |
|------|----------------------|----|
| 2.1 | Задание 1 | 6 |
| 2.2 | Задание 2 | 7 |
| 2.3 | Задание 3 | 8 |
| 2.4 | Задание 4 | 9 |
| 2.5 | Задание 5 | 9 |
| 2.6 | Задание 6 | 10 |
| 2.7 | Задание 7 | 11 |
| 2.8 | Задание 8 | 11 |
| 2.9 | Задание 9 | 12 |
| 2.10 | Задание 10 | 12 |
| 2.11 | Задание 11 | 13 |
| 2.12 | Задание 12 | 14 |
| 2.13 | Задание 13 | 14 |
| 2.14 | Задание 14 | 15 |
| 2.15 | Задание 15 | 16 |
| 2.16 | Задание 16 | 16 |

1 Цель работы

Получение и закрепление на практике знаний о криптографических примитивах и областях их применения.

2 Выполнение контрольных заданий

2.1 Введение в криптографию

В асимметричных криптографических примитивах

Select one option from the list

✓ Well done!

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

Next step Solve again

Рис. 2.1: Задание 1

В асимметричных примитивах обе стороны имеют пару ключей: секретный (частный) и открытый. Секретный ключ не публикуется ни в коем случае, общий ключ стороны имеют в симметричных примитивах.

Select all correct options from the list

✓ Right.

You've solved a complex problem, congratulations! Now you can help other learners in [comments](#) by answering their questions, or compare your solution with others on [solution forum](#).

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

Next step

Solve again

Рис. 2.2: Задание 2

Хорошая хэш-функция должна выдавать стойкие к коллизиям результаты, что, однако, не всегда соответствует правде на практике. На выходе, вне зависимости от объема входных данных, она дает фиксированное число бит, но не обеспечивает конфиденциальность данных.

К алгоритмам цифровой подписи относятся

Select all correct options from the list

✓ Yes!

You've solved a complex problem, congratulations! Now you can help other questions, or compare your solution with others on [solution forum](#).

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

Next step

Solve again

Рис. 2.3: Задание 3

Из представленных в списке AES - алгоритм симметричного шифрования, SHA2 - хэш-функция. Остальные как раз являются алгоритмами, применимыми для создания цифровой подписи.

Код аутентификации сообщения относится к

Select one option from the list

✓ Absolutely right.

☒ симметричным примитивам

☐ асимметричным примитивам

Next step Solve again

Рис. 2.4: Задание 4

Код аутентификации сообщения - симметричный примитив, представляющий собой общий для сторон секретный ключ.

Обмен ключам Диффи-Хэллмана - это

Select one option from the list

✓ Totally right.

☐ симметричный примитив генерации общего секретного ключа

☐ асимметричный примитив генерации общего открытого ключа

☒ асимметричный примитив генерации общего секретного ключа

☐ асимметричный алгоритм шифрования

Next step Solve again

Рис. 2.5: Задание 5

Алгоритм обмена ключами ДН - асимметричный алгоритм генерации общего секретного ключа, где стороны получают общий ключ из собственного секрета и открытого ключа на основе общего секрета, переданного другой стороной.

2.2 Цифровая подпись

Протокол электронной цифровой подписи относится к

Select one option from the list

✓ Well done!

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

Next step

Solve again

Рис. 2.6: Задание 6

Протоколы ЭЦП относятся к протоколам с открытым ключом, где секретный ключ используется для непосредственно подписания документа, открытый - для проверки подлинности подписи.

Алгоритм верификации электронной цифровой подписи требует на вход

Select one option from the list

✓ You are right, well done!

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

Next step

Solve again

Рис. 2.7: Задание 7

Алгоритм верификации требует на вход подпись, сообщение, которое было ею подписано, и открытый ключ.

Электронная цифровая подпись не обеспечивает

Select one option from the list

✓ Good job.

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

Next step

Solve again

Рис. 2.8: Задание 8

ЭЦП не обеспечивает конфиденциальности, скорее, наоборот - она обеспечи-

вает подтверждение личности отправителя документа.

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

Select one option from the list

Great work!

Correct answer
Total 68

☒ усиленная квалифицированная
☐ простая
☐ усиленная неквалифицированная

Next step Solve again

Рис. 2.9: Задание 9

Для отправки налоговой отчетности ЭЦП должна быть подтверждена, поэтому подойдет только усиленная квалифицированная подпись.

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

Select one option from the list

You're right!

Correct answer for
Total 61% of tries

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

Next step Solve again

Рис. 2.10: Задание 10

Квалифицированный сертификат проверки можно получить только в специализированных сертификационных центрах. Минкомсвязи непосредственно этим не занимаются.

2.3 Электронные платежи

Выберите из списка все платежные системы.

Select all correct options from the list

✓ Yes!

You've solved a complex problem, congratulations! Now you can ask questions, or compare your solution with others on [solution forum](#)

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

Next step

Solve again

Рис. 2.11: Задание 11

Платежными системы из перечисленных являются только МИР и мастеркард. Биткоин - криптовалюта, ПОС-терминал и банкомат - технические средства проведения банковских операций.

Примером многофакторной аутентификации является

Select all correct options from the list

✓ Correct.

You've solved a complex problem, congratulations! Now you can help other learners in questions, or compare your solution with others on [solution forum](#).

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

Next step

Solve again

Рис. 2.12: Задание 12

Многофакторная аутентификация сочетает “то, что я знаю” и “то, что у меня есть”. Комбинации ПИН + пароль и пароль + капча не удовлетворяют этому критерию.

При онлайн платежах сегодня используется

Select one option from the list

✓ Correct.

- ☒ 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

Next step

Solve again

Рис. 2.13: Задание 13

При онлайн-платежах используется многофакторная аутентификация перед

банком-эмитентом, так как только он обладает данными о конкретном плателъщике и обязан удостовериться, что платеж проводится легитимным клиентом.

2.4 Блокчейн

Какое свойство криптографической хэш-функции используется в доказательстве работы?

Select one option from the list

✓ Good news for you, correct!

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

Next step Solve again

Рис. 2.14: Задание 14

В доказательстве работы используется свойство сложности нахождения прообраза (нарочно не придумаешь), остальные не обеспечивают доказательства как такового.

Консенсус в некоторых системах блокчейн обладает свойствами

Select all correct options from the list

✓ Right.

You've solved a complex problem, congratulations! Now you can help other learners in c questions, or compare your solution with others on [solution forum](#).

☒ постоянства

☒ живучесть

☒ открытость

☒ консенсус

Next step

Solve again

Рис. 2.15: Задание 15

Секретные ключи какого криптографического примитива хранят участники блокчейна?

Select one option from the list

✓ Correct.

☐ обмен ключами

☐ шифрование

☒ цифровая подпись

☐ хэш-функция

Next step

Solve again

Рис. 2.16: Задание 16

Участники блокчейна хранят секретные ключи цифровой подписи. Обмен ключами и шифрование осуществляются независимо от них.

3 Выводы

Получены и закреплены на практике знания о криптографических примитивах и областях их применения.