

# **Отчёт прохождения внешнего курса**

**Безопасность в сети**

Криптография на практике

# Содержание

<b>1</b>	<b>Цель работы</b>	<b>5</b>
<b>2</b>	<b>Выполнение контрольных заданий</b>	<b>6</b>
<b>3</b>	<b>Выводы</b>	<b>13</b>
	<b>Список литературы</b>	<b>14</b>

## Список иллюстраций

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

## Список таблиц

# **1 Цель работы**

Провести контроль усвоения теоритического материала раздела “Криптография на практике”

## 2 Выполнение контрольных заданий

В асимметричной криптографии, также известной как криптография с открытым ключом, каждая сторона обладает парой ключей: открытым и закрытым (или секретным). Открытый ключ доступен для общего использования, в то время как закрытый ключ хранится конфиденциально у владельца. К протоколам асимметричной криптографии относятся электронно-цифровая подпись и протокол генерации общего ключа. Последний позволяет установить общий секретный ключ без необходимости физического взаимодействия между сторонами.(рис. 2.1).

В асимметричных криптографических примитивах

Выберите один вариант из списка

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

☒ Абсолютно точно.

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

Следующий шаг    Решить снова

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

Рис. 2.1: Задание 1

Криптографическая хэш-функция, эффективно вычисляется, дает на выходе фиксированное число бит независимо от объема входных данных, но главное она стойкая к коллизиям. Это значит что двое разных входных данных не могут дать один выходной(рис. 2.2).

Криптографическая хэш-функция

Выберите все подходящие ответы из списка

✓ Прекрасный ответ.

Верно решили 798 учащихся  
Из всех попыток 11% 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](#).

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

Следующий шаг    Решить снова

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

Рис. 2.2: Задание 2

К ним относятся именно RSA, ECDSA, ГОСТ Р 34.10-2012, остальные отношения не имеют(рис. 2.3).

К алгоритмам цифровой подписи относятся

Выберите все подходящие ответы из списка

✓ Абсолютно точно.

Верно решили 820 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 из 1

Рис. 2.3: Задание 3

Этот процесс также является симметричным и использует ключ (который должен быть отличным от ключа, использованного для шифрования) и само сообщение для создания кода аутентификации. Этот примитив можно представить как симметричный аналог подписи. Обычно код аутентификации сообщения создается с использованием хэш-функции или симметричного шифрования.(рис. 2.4).

Код аутентификации сообщения относится к

Выберите один вариант из списка

✓ Хорошая работа.

Верно решили 934 учащихся  
Из всех попыток 69% верных

☐ асимметричным примитивам  
☒ симметричным примитивам

Следующий шаг
 Решить снова

Ваши решения Вы получили: 1 балл из 1

Рис. 2.4: Задание 4

Обмен ключам Диффи-Хэллмана - это асимметричный примитив генерации общего секретного ключа(рис. 2.5).

Обмен ключам Диффи-Хэллмана - это

Выберите один вариант из списка

✓ Всё правильно.

Верно решили 927 учащихся  
Из всех попыток 46% 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 из 1

Рис. 2.5: Задание 5

Конечно же к протоколам с публичным(открытым ключом)(рис. 2.6).

Протокол электронной цифровой подписи относится к

Выберите один вариант из списка

✓ Абсолютно точно.

Верно решили 894 учащихся  
Из всех попыток 70% верных

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

Следующий шаг
 Решить снова

Ваши решения Вы получили: 1 балл из 1

Рис. 2.6: Задание 6

Нам в первую очередь нужна сама подпись, потом открытый ключ(никак не секретный) и потом также сообщение. ТОлько так пройдет верификация (рис. 2.7).



Алгоритм верификации электронной цифровой подписи требует на вход

Выберите один вариант из списка

✓ Всё правильно.

Верно решили 888 учащихся  
Из всех попыток 45% верных

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

Следующий шаг    Решить снова

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

Рис. 2.7: Задание 7

Конечно конфиденциальность. Это же подпись. Она указывает на человека, которому принадлежит(рис. 2.8).

Электронная цифровая подпись не обеспечивает

Выберите один вариант из списка

✓ Правильно, молодец!

Верно решили 889 учащихся  
Из всех попыток 51% верных

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

Следующий шаг    Решить снова

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

Рис. 2.8: Задание 8

Только усиленная квалифицированная. Это касается серьёзных документов. Никакая другая не подойдёт (рис. 2.9).

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

Выберите один вариант из списка

✓ Правильно, молодец!

Верно решили 889 учащихся  
Из всех попыток 67% верных

- ☐ простая
- ☒ усиленная квалифицированная
- ☐ усиленная неквалифицированная

Следующий шаг    Решить снова

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

Рис. 2.9: Задание 9

Только в удостоверяющем, сертификационном центре. Иные организации таких полномочий не имеют.(рис. 2.10).

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

Выберите один вариант из списка

✓ Верно. Так держать!

Верно решили 887 учащихся  
Из всех попыток 60% 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 из 1

Рис. 2.10: Задание 10

Мастеркарт и мир. Биткоин это валюта, банкомат - устройство, выдающее и принимающее деньги.(рис. 2.11).

Выберите все подходящие ответы из списка

✓ Отличное решение!

Верно решили 818 учащихся  
Из всех попыток 23% 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 из 1

Рис. 2.11: Задание 11

Нам нужны доказательства из разных категорий. Минимум две. В эти категории входят наша биометрия, то что мы знаем(пароль) и то что имеем (например телефон). Пароль и капча таковыми не являются, капча это вообще защита от автоматических атак, ну и пин код с паролем тоже из одной категории(рис. 2.12).

Примером многофакторной аутентификации является

Выберите все подходящие ответы из списка

☒ Так точно!

Верно решили **804** учащихся  
Из всех попыток **23%** 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** из 1

Рис. 2.12: Задание 12

При онлайн платежах сегодня используется многофакторная аутентификация покупателя перед банком-эмитентом(рис. 2.13).

При онлайн платежах сегодня используется

Выберите один вариант из списка

☒ Всё получилось!

Верно решили **863** учащихся  
Из всех попыток **59%** верных

- ☒ 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

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

Рис. 2.13: Задание 13

Сложность нахождения прообраза конечно же. Это очень важное свойство(рис. 2.14).

Какое свойство криптографической хэш-функции используется в доказательстве работы?

Выберите один вариант из списка

☒ Прекрасный ответ.

Верно решили **878** учащихся  
Из всех попыток **48%** верных

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

Следующий шаг

Решить снова

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

Рис. 2.14: Задание 14

Снова задание с подвохом. Здесь подходят все варианты. Об этом говорилось в лекции(рис. 2.15).

Консенсус в некоторых системах блокчейн обладает свойствами

Выберите все подходящие ответы из списка

☒ Верно.

Верно решили 789 учащихся  
Из всех попыток 22% 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](#).

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

[Следующий шаг](#) [Решить снова](#)

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

Рис. 2.15: Задание 15

(рис. 2.16).

Секретные ключи какого криптографического примитива хранят участники блокчейна?

Выберите один вариант из списка

☒ Здорово, всё верно.

Верно решили 877 учащихся  
Из всех попыток 47% верных

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

[Следующий шаг](#) [Решить снова](#)

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

Рис. 2.16: Задание 16

## **3 Выводы**

Мы успешно прошли контроль усвоения теоритического материала раздела  
“Криптография на практике”

## **Список литературы**