Внешний курс. Этап 3

Криптография на практике

Татьяна Александровна Буллер

Содержание

1	Цель работы														
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

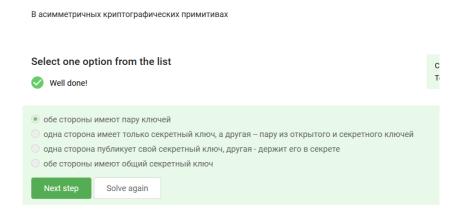


Рис. 2.1: Задание 1

В ассиметричных 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.

Рис. 2.2: Задание 2

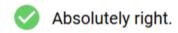
Хорошая хэш-функция должна выдавать стойкие к коллизиям результаты, что, однако, не всегда соответствует правде на практике. На выходе, вне зависимости от объема входных данных, она дает фиксированное число бит, но не обеспечивает конфиденциальность данных.

Select all correct options from the list ✓ Yes! You've solved a complex problem, congratulations! Now you can help othe questions, or compare your solution with others on solution forum. AES SHA2 ✓ RSA ✓ ECDSA ✓ FOCT P 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.

Select one option from the list



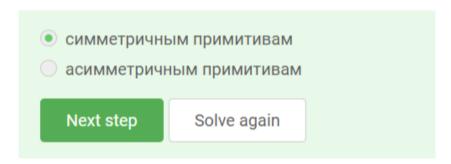


Рис. 2.4: Задание 4

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.

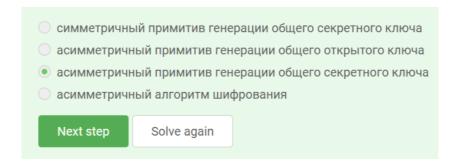


Рис. 2.5: Задание 5

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

2.2 Цифровая подпись

Select one option from the list

Well done!

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

Next step

Solve again

Протокол электронной цифровой подписи относится к

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.

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

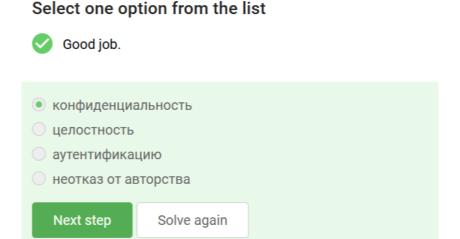


Рис. 2.8: Задание 8

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

вает подтверждение личности отправителя документа.

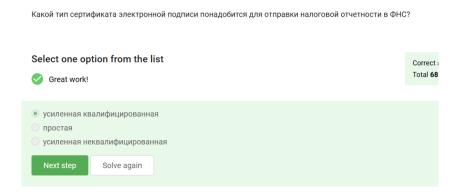


Рис. 2.9: Задание 9

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

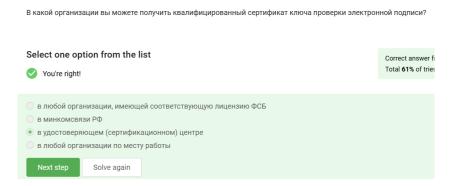


Рис. 2.10: Задание 10

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.

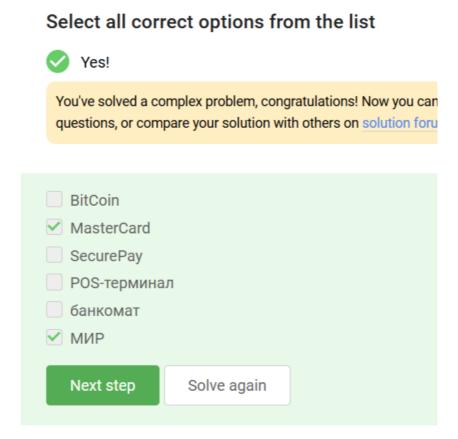


Рис. 2.11: Задание 11

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.

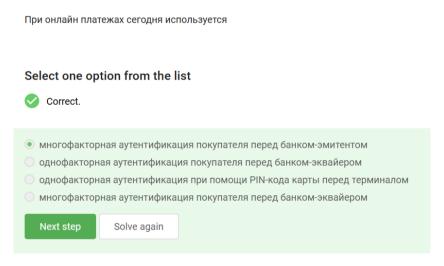


Рис. 2.13: Задание 13

При онлайн-платежах используется многофакторная аутентификация перед

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

2.4 Блокчейн

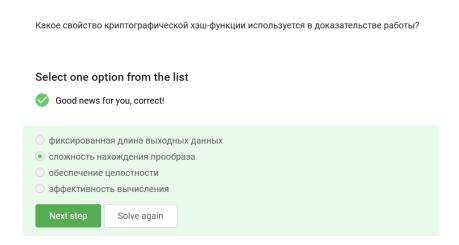


Рис. 2.14: Задание 14

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

Select all correct options from the list Right. You've solved a complex problem, congratulations! Now you can help other learners in conquestions, or compare your solution with others on solution forum.

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.