

Внешний курс. Блок 3: Криптография на практике

Основы информационной безопасности

Чувакина Мария Владимировна

Содержание

1	Цель работы	5
2	Выполнение блока 3: Криптография на практике	6
2.1	Введение в криптографию	6
2.2	Цифровая подпись	7
2.3	Электронные платежи	8
2.4	Блокчейн	9
3	Выводы	10

Список иллюстраций

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

Список таблиц

1 Цель работы

Пройти третий блок курса “Основы кибербезопасности”

2 Выполнение блока 3: Криптография на практике

2.1 Введение в криптографию

Для ответа на вопрос используется определение асимметричного шифрования с двумя ключами (рис. 2.1).

```
mvchuvakina@dk6n64 ~ $ getenforce
bash: getenforce: команда не найдена
mvchuvakina@dk6n64 ~ $ sestatus
bash: sestatus: команда не найдена
mvchuvakina@dk6n64 ~ $
```

Рис. 2.1: Вопрос 4.1.1

Отмечены основные условия для криптографической хэш-функции (рис. 2.2).

```
mvchuvakina@dk6n64 ~ $ sudo systemctl start httpd
Пароль:
Извините, пользователю mvchuvakina не разрешено выполнять «/usr/sbin/systemctl start httpd» как root на dk6n64
.dk.sc1.pfu.edu.ru.
mvchuvakina@dk6n64 ~ $ sudo systemctl enable httpd
Пароль:
Извините, пользователю mvchuvakina не разрешено выполнять «/usr/sbin/systemctl enable httpd» как root на dk6n64
.dk.sc1.pfu.edu.ru.
mvchuvakina@dk6n64 ~ $ service httpd status
bash: service: команда не найдена
mvchuvakina@dk6n64 ~ $
```

Рис. 2.2: Вопрос 4.1.2

Отмечены алгоритмы цифровой подписи (рис. 2.3).

```
mvchuvakina@dk6n64 ~ $ ps auxZ | grep httpd
mvchuvakina@dk6n64 ~ $ ps -eZ | grep httpd
mvchuvakina@dk6n64 ~ $
```

Рис. 2.3: Вопрос 4.1.3

В информационной безопасности аутентификация сообщения или аутентификация источника данных-это свойство, которое гарантирует, что сообщение не было изменено во время передачи (целостность данных) и что принимающая сторона может проверить источник сообщения (рис. 2.4)

```
mvchuvakina@dk6n64 ~ $ sestatus -bigrep httpd
bash: sestatus: команда не найдена
mvchuvakina@dk6n64 ~ $
```

Рис. 2.4: Вопрос 4.1.4

Определение обмена ключами Диффи-Хэллмана. (рис. 2.5).

Вопрос 4.1.5

Рис. 2.5: Вопрос 4.1.5

2.2 Цифровая подпись

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

Вопрос 4.2.1

Рис. 2.6: Вопрос 4.2.1

Алгоритм верификации электронной подписи состоит в следующем. На первом этапе получатель сообщения строит собственный вариант хэш-функции подписанного документа. На втором этапе происходит расшифровка хэш-функции, содержащейся в сообщении с помощью открытого ключа отправителя. На третьем

этапе производится сравнение двух хэш- функций. Их совпадение гарантирует одновременно подлинность содержимого документа и его авторства (рис. 2.7).

Вопрос 4.2.2

Рис. 2.7: Вопрос 4.2.2

Электронная подпись обеспечивает все указанное, кроме конфиденциальности (рис. 2.8).

Вопрос 4.2.3

Рис. 2.8: Вопрос 4.2.3

Для отправки налоговой отчетности в ФНС используется усиленная квалифицированная электронная подпись

Верный ответ указан на изображении (рис. 2.9).

Вопрос 4.2.5

Рис. 2.9: Вопрос 4.2.5

2.3 Электронные платежи

Известные платежные системы - Visa, MasterCard, МИР (рис. 2.10).

Вопрос 4.3.1

Рис. 2.10: Вопрос 4.3.1

Верный ответ на изображении (рис. 2.11).

Вопрос 4.3.2

Рис. 2.11: Вопрос 4.3.2

При онлайн платежах используется многофакторная аутентификация (рис. 2.12).

Вопрос 4.3.3

Рис. 2.12: Вопрос 4.3.3

2.4 Блокчейн

Proof-of-Work, или PoW, (доказательство выполнения работы) — это алгоритм достижения консенсуса в блокчейне; он используется для подтверждения транзакций и создания новых блоков. С помощью PoW майнеры конкурируют друг с другом за завершение транзакций в сети и за вознаграждение. Пользователи сети отправляют друг другу цифровые токены, после чего все транзакции собираются в блоки и записываются в распределенный реестр, то есть в блокчейн. (рис. 2.13).

Вопрос 4.4.1

Рис. 2.13: Вопрос 4.4.1

Консенсус блокчейна — это процедура, в ходе которой участники сети достигают согласия о текущем состоянии данных в сети. Благодаря этому алгоритмы консенсуса устанавливают надежность и доверие к самой сети. (рис. 2.14).

Вопрос 4.4.2

Рис. 2.14: Вопрос 4.4.2

Ответ - цифровая подпись (рис. 2.15).

Вопрос 4.4.3

Рис. 2.15: Вопрос 4.4.3

3 Выводы

Я прошла третий блок