Домашнее задание (модуль 12)

12.5 Практическая работа

1. Представьте, что вам нужно безопасно передать кому-то несколько текстовых файлов. Запакуйте эти файлы в tar.gz архив и зашифруйте его с помощью симметричного шифрования.

Проверьте, что вы сможете затем расшифровать и распаковать архив.

Цель задания

Научиться работать с OpenSSL и симметричными шифрами.

Что оценивается

Правильность использования инструментов.

Как отправить задание на проверку

Пришлите через форму для сдачи домашнего задания:

- скриншоты команд, которые вы вводили для архивирования, шифрования и расшифровывания;
- скриншоты с успешно распакованными и расшифрованными текстовыми файлами.

Ответ:

Скриншоты команд для архивирования:

```
vgusev2007@skillbox-vgusev2007:~/skillbox/12/12_5/task_1$ echo "Hello Bob! I'm Alice. Hru?" > message.txt
```

```
vgusev2007@skillbox-vgusev2007:~/skillbox/12/12_5/task_1$ tar caf message.txt.tar.gz message.txt
vgusev2007@skillbox-vgusev2007:~/skillbox/12/12_5/task_1$ file message.txt.tar.gz
message.txt.tar.gz: gzip compressed data, from Unix, original size modulo 2^32 20480
```

```
vgusev2007@skillbox-vgusev2007:~/skillbox/12/12_5/task_1$ l
message.txt  message.txt.tar.gz
```

```
vgusev2007@skillbox-vgusev2007:~/skillbox/12/12_5/task_1$ rm message.txt ; l
message.txt.tar.gz
```

Скриншоты команд для шифрования:

```
vgusev2007@skillbox-vgusev2007:~/skillbox/12/12_5/task_1$ openssl enc -aes-256-cbc -in message.txt.tar.gz -out me
ssage.txt.tar.gz.enc -iter 10
enter AES-256-CBC encryption password:
Verifying - enter AES-256-CBC encryption password:
vgusev2007@skillbox-vgusev2007:~/skillbox/12/12_5/task_1$ l ; rm -f message.txt.tar.gz ; l
message.txt.tar.gz  message.txt.tar.gz.enc
message.txt.tar.gz.enc
```

Скриншоты команд для расшифровывания:

```
vgusev2007@skillbox-vgusev2007:~/skillbox/12/12_5/task_1$ openssl enc -aes-256-cbc -d -in message.txt.tar.gz.enc
 -out message.txt.tar.gz -iter 10
enter AES-256-CBC decryption password:
vgusev2007@skillbox-vgusev2007:~/skillbox/12/12_5/task_1$ file message.txt.tar.gz
message.txt.tar.gz: gzip compressed data, from Unix, original size modulo 2^32 10240
```

```
 Left      File      Command      Options      Right
<- message.txt.tar.gz/utar://  .[^]>  <- ~/skillbox/12/12_5/task_1  .[^]>
.n             Name          Size   Modify time   .n             Name          Size   Modify time
/..                        UP--DIR  Aug 29 08:31  /..                        UP--DIR  Aug 29 08:03
 message.txt                    27  Aug 29 08:27   message.txt.tar.gz             157  Aug 29 08:32
                                                   message.txt.tar.gz.enc         176  Aug 29 08:29
```

```
message.txt
Hello Bob! I'm Alice. Hru?
```

2. Письменно ответьте на вопрос: изменится ли хеш текстового файла, если добавить в него пустую строку? Напомню, что для вычисления хеш-суммы можно использовать команду md5sum.

Цель задания

Потренироваться в использовании утилиты для вычисления хеш-суммы.

Что оценивается

Правильность ответа.

Как отправить задание на проверку

Пришлите ответ на вопрос и скриншоты с хеш-суммой файла до и после изменений через форму для сдачи домашнего задания.

Ответ:

Да, хеш-сумма изменится, так-как добавление пустой строки, в файл, это изменение файла (как минимум, мы говорим о том, что мы добавили символ переноса строки (каретки))

Скриншоты:

```
vgusev2007@skillbox-vgusev2007:~/skillbox/12/12_5/task_2$ echo "Hello skillbox!" > foo.txt
vgusev2007@skillbox-vgusev2007:~/skillbox/12/12_5/task_2$ md5sum foo.txt
db21ce036eb158effa2595c6baccdd7f  foo.txt
vgusev2007@skillbox-vgusev2007:~/skillbox/12/12_5/task_2$ echo >> foo.txt
vgusev2007@skillbox-vgusev2007:~/skillbox/12/12_5/task_2$ md5sum foo.txt
5cc106b001aa19337e4489551102cb64  foo.txt
```

3. Сгенерируйте самоподписанный сертификат и настройте Nginx на работу по HTTPS для тестовой веб-странички, как было показано на уроке.

Цель задания

Отработать на практике создание самоподписанных сертификатов и настройку работы Nginx с SSL.

Что оценивается

Работоспособность решения.

Как отправить задание на проверку

Пришлите через форму для сдачи домашнего задания:

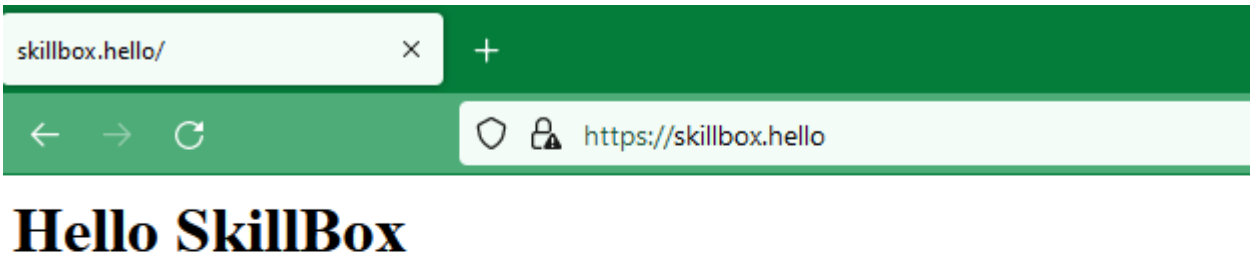
- скриншот конфигурационного файла nginx,
- скриншот браузера с открытой по HTTPS веб-страницей.

Ответ:

Скриншот конфигурационного файла nginx:

```
listen 443 ssl default_server;
ssl_certificate /etc/nginx/ssl/server.crt;
ssl_certificate_key /etc/nginx/ssl/server.key;

# listen [::]:443 ssl default_server;
#
# Note: You should disable gzip for SSL traffic.
# See: https://bugs.debian.org/773332
#
# Read up on ssl_ciphers to ensure a secure configuration.
# See: https://bugs.debian.org/765782
#
# Self signed certs generated by the ssl-cert package
# Don't use them in a production server!
#
# include snippets/snakeoil.conf;

root /var/www/html;

# Add index.php to the list if you are using PHP
index index.html index.htm index.nginx-debian.html;

server_name skillbox.hello;
```

Скриншот браузера с открытой по HTTPS веб-страницей:



4. Воспользовавшись инструкцией, сгенерируйте ключевую пару «открытый и закрытый ключ». При помощи открытого ключа зашифруйте файл. Затем расшифруйте его при помощи приватного ключа. Убедитесь, что зашифрованный файл нельзя прочитать как текстовый, а расшифрованный файл совпадает с исходным.

Инструкция:

1. **Генерируем приватный ключ**
   openssl genpkey -algorithm RSA -out private.key -pkeyopt rsa_keygen_bits:8192
2. **Извлекаем из приватного ключа публичный ключ**
   openssl rsa -in private.key -pubout -out public.key
3. **Шифруем файл**
   openssl rsautl -encrypt -pubin -inkey публичный_ключ.key -in файл_с_открытым_текстом.txt -out зашифрованный_файл.txt.enc
4. **Расшифровываем файл**
   openssl rsautl -decrypt -inkey приватный_ключ.key -in зашифрованный_файл.txt.enc -out файл_с_открытым_текстом.txt.new

Цель задания

Самостоятельно познакомиться с генерацией ключевой пары при помощи утилиты openssl и шифрованием файла — при помощи асимметричной криптографии.

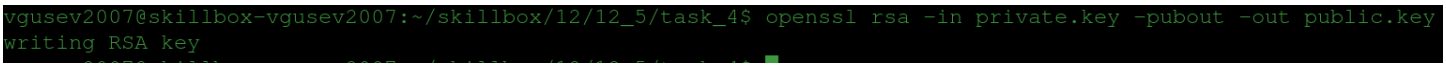
Как отправить задание на проверку

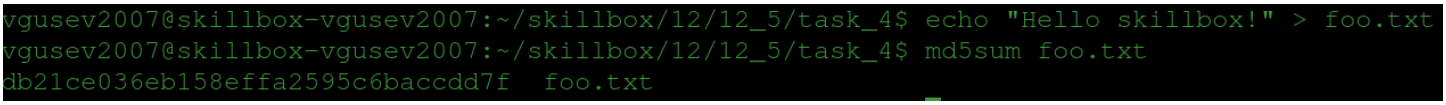
Пришлите через форму для сдачи домашнего задания:

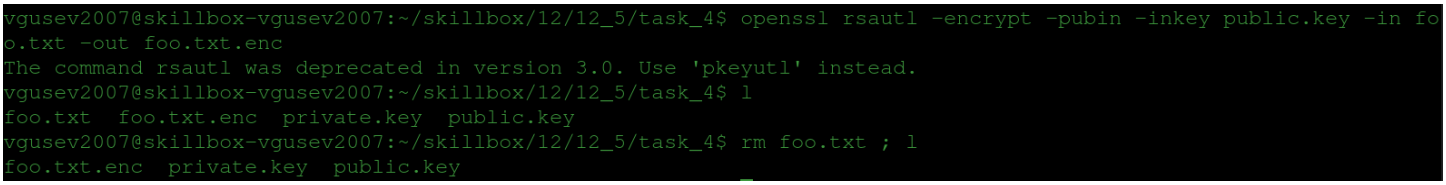
- скриншот с использованными командами для шифрования и расшифровки,
- скриншоты с успешно расшифрованным текстовым файлом.

Ответ

Скриншот с использованными командами для шифрования:







Скриншот с успешно расшифрованным текстовым файлом: