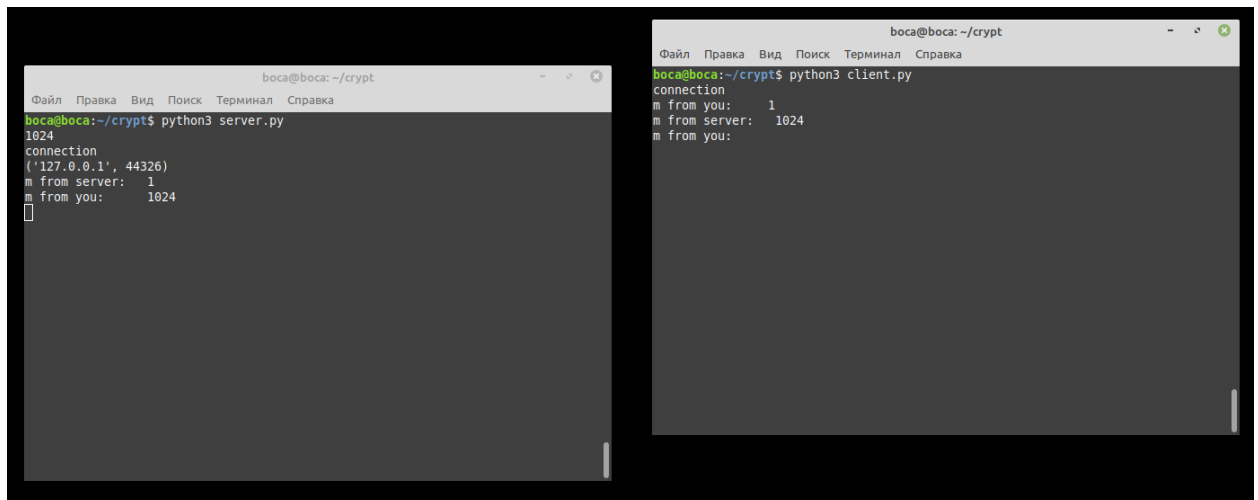


python_year2_study

Репозиторий для учебных проектов и программ на второй курс

Ассиметричное шифрование.

Программа представляет из себя клиент-серверный чат с ассиметричным шифрованием. Клиент и сервер при отправке и получении сообщения шифруют его каждый на своей стороне. Приватный ключ программы берут из разных источников.

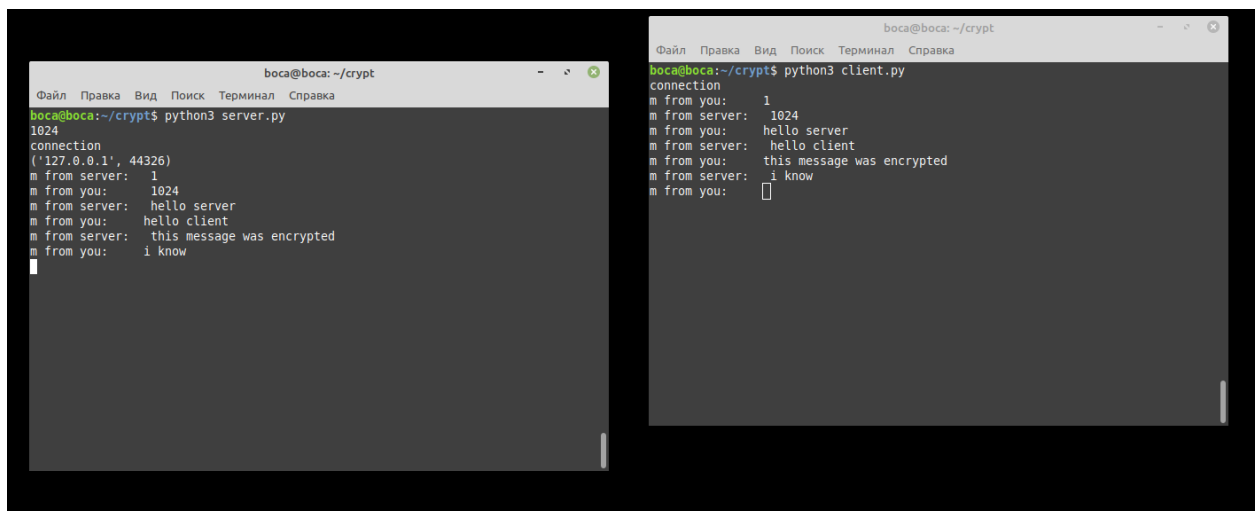


```
boca@boca: ~/crypt
python3 server.py
1024
connection
('127.0.0.1', 44326)
m from server: 1
m from you: 1024

```

```
boca@boca: ~/crypt
python3 client.py
connection
m from you: 1
m from server: 1024
m from you:
```

При первой отправке сообщения сервер ждёт клиента, после чего отправляет ему отладочное сообщение с цифрой 1024. После клиент и сервер поочередно отправляют друг другу сообщения.



```
boca@boca: ~/crypt
python3 server.py
1024
connection
('127.0.0.1', 44326)
m from server: 1
m from you: 1024
m from server: hello server
m from you: hello client
m from server: this message was encrypted
m from you: i know

```

```
boca@boca: ~/crypt
python3 client.py
connection
m from you: 1
m from server: 1024
m from you: hello server
m from server: hello client
m from you: this message was encrypted
m from server: i know
m from you:
```

При несоответствии ключа дешифровка сообщения будет некорректной у обеих сторон. Ключ не передаётся вместе с сообщением, так что стороннее приложение не сможет прочитать сообщение.

```
boca@boca: ~/crypt
Файл  Правка  Вид  Поиск  Терминал  Справка

boca@boca:~/crypt$ nano server.py
boca@boca:~/crypt$ python3 server.py
1024
connection
('127.0.0.1', 44322)
m from server:  cd
m from you:      1024
m from server:  \a
m from you:      k
m from server:  f
m from you:      ^X
m from server:
m from you:      ^CTraceback (most recent call last):
  File "server.py", line 127, in <module>
    mess(conn, key_full_m)
  File "server.py", line 63, in mess
    msg1 = input('m from you:\t')
KeyboardInterrupt

boca@boca:~/crypt$ nano client.py
boca@boca:~/crypt$ python3 client.py
connection
m from you:      hi
m from server:    6579
m from you:      af
k
m from server:    p
m from you:      m from server:
m from you:      ^X
^CTraceback (most recent call last):
  File "client.py", line 93, in <module>
    mess(sock, key_full_s)
  File "client.py", line 64, in mess
    msg = sock.recv(1024).decode()
KeyboardInterrupt

boca@boca:~/crypt$
boca@boca:~/crypt$ python3 client.py
connection
m from you:      1
m from server:    1024
m from you:      hello server
```