

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.

```
connection
m from you: 1
m from server: 1024
m from you:
```

```
1024
connection
('127.0.0.1', 44326)
m from server: 1
m from you: 1024

```

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

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

```
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
```

```
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:
```

```
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
```