# server.py

```
#!/usr/bin/env python3
import pyDes
import hmac
import hashlib
import socket
import os
HOST = '127.0.0.1'
PORT = 65432
Secret_key = b'key'

def encryption(data):
k = pyDes.des("DESCRYPT", pyDes.CBC, "\0\0\0\0\0\0\0\0", pad=None,
padmode=pyDes.PAD_PKCS5)
d = k.encrypt(data)
return d

def decryption(data):
k = pyDes.des("DESCRYPT", pyDes.CBC, "\0\0\0\0\0\0\0\0", pad=None,
padmode=pyDes.PAD_PKCS5)
return k.decrypt(data)

def check_integrity(d,b):
digest_maker = hmac.new(Secret_key,d,hashlib.sha512)
return hmac.compare_digest(digest_maker.hexdigest(),b)

with socket.socket(socket.AF_INET, socket.SOCK_STREAM) as s:
s.bind((HOST, PORT))
s.listen()
conn, addr = s.accept()
with conn:
print('Connected by', addr)
while True:
received_msg = conn.recv(1024)
integrity = conn.recv(1024)
integrity = integrity.decode()
if check_integrity(received_msg,integrity):
received_msg=decryption(received_msg)
print ('integrity is fine. the message is from B: '+received_msg.decode('utf-8'))
else:
print ('integrity of the message is incorrect')
p = input('A :')
p = encryption(p)
hash_integrity = hmac.new(Secret_key, p, hashlib.sha512)
conn.sendall(p)
d = hash_integrity.hexdigest()
d = d.encode()
conn.sendall(d)
```