server1.py

```
import socket as sc
import hmac
import hashlib
from simple_aes_cipher import AESCipher, generate_secret_key

pass_phrase = "hogefuga"
secret_key = generate_secret_key(pass_phrase)
cipher = AESCipher(secret_key)
s = sc.socket()
port = 12345
key = b'key'
host = sc.gethostname()
s.bind((host,port))
s.listen(5)
client,addr = s.accept()
def check(string,hash_msg):
m = hmac.new(key,string.encode(),hashlib.sha512)
print (m)
return hmac.compare_digest(m.hexdigest(),hash_msg)
while True:
print("connection is from " , addr)
string = client.recv(1024)
hash_msg = client.recv(1024).decode()
if check(cipher.decrypt(string),hash_msg):
print("recieved the message properly :" , cipher.decrypt(string))
else:
print('incorrect integrity')
k =""
print("processing the request")
m =input('enter the message:')
client.send((cipher.encrypt(m)).encode())
client.send((hmac.new(key,m.encode(),hashlib.sha512).hexdigest()).encode())
print("send it back to the client")
```