# client1.py

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

s = sc.socket()
host = sc.gethostname()
port = 12345
s.connect((host,port))
key = b'key'
pass_phrase = "hogefuga"
secret_key = generate_secret_key(pass_phrase)
cipher = AESCipher(secret_key)
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:
k = input("enter a string")
s.send((cipher.encrypt(k)).encode())
s.send((hmac.new(key,k.encode(),hashlib.sha512).hexdigest()).encode())
k = s.recv(1024)
hash_msg = s.recv(1024).decode()
if check(cipher.decrypt(k),hash_msg):
print("recieved the message :" , cipher.decrypt(k))
else:
print('incorrect integrity')
```