

PRATICA S3 L4

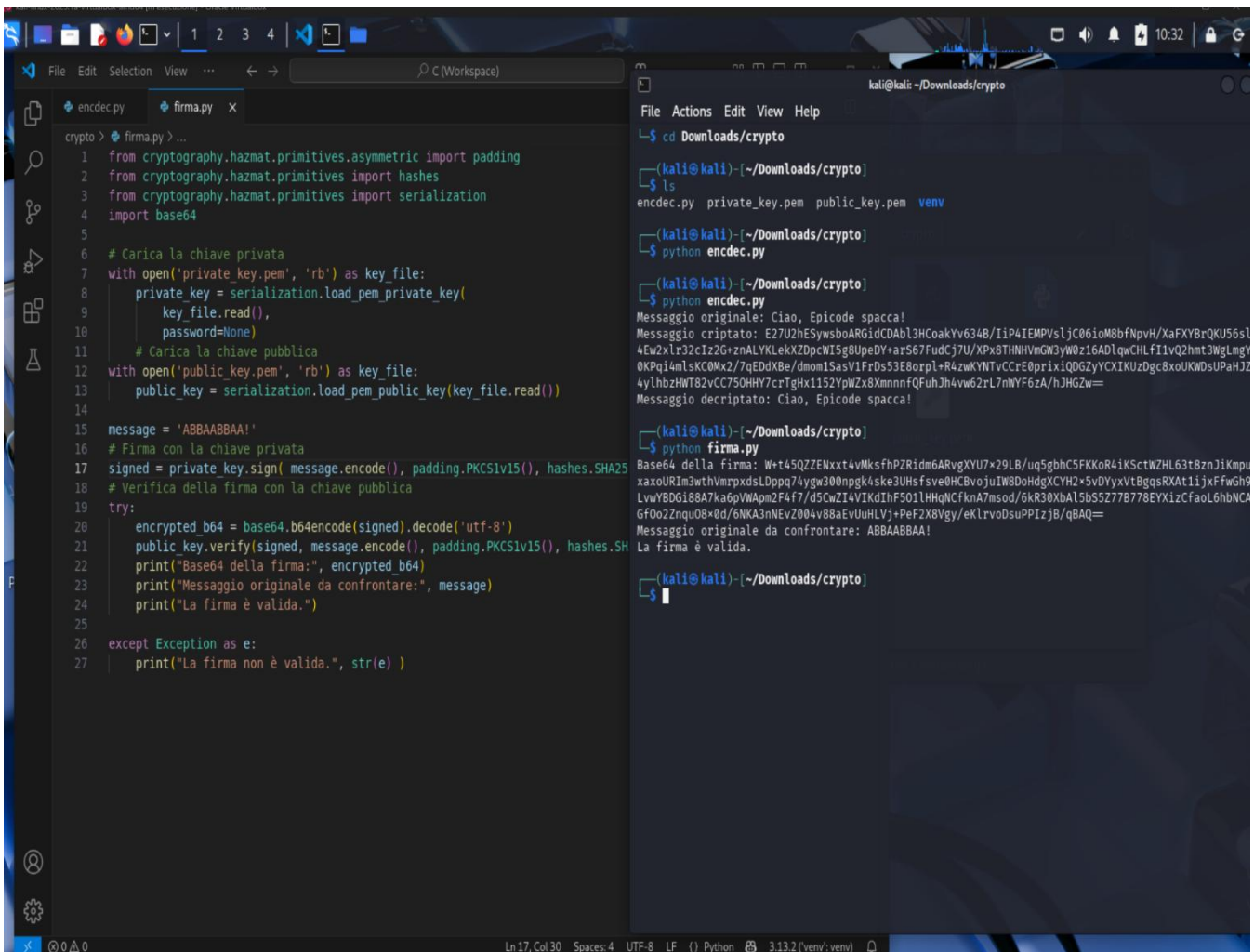
Messaggio cifrato: "HSNFRGH"

= EPICODE

QWJhIHZ6b2VidHl2bmdyIHB1ciB6ciBhciBucHBiZXRI

= Abbiamo bisogno di un piano per la missione.

Esercizio su kali



The screenshot shows a Kali Linux environment with a code editor on the left and a terminal on the right. The code editor displays a Python script named `encdec.py` that implements RSA encryption and decryption using the `cryptography` library. The script uses a private key (`private_key.pem`) and a public key (`public_key.pem`) located in the `~/Downloads/crypto` directory. The message to be encrypted is `'ABBAABBA!'`. The terminal shows the execution of the script, which outputs the original message, the encrypted message, and the decrypted message.

```
File Edit Selection View ... C (Workspace)
crypto > firma.py ...
1 from cryptography.hazmat.primitives.asymmetric import padding
2 from cryptography.hazmat.primitives import hashes
3 from cryptography.hazmat.primitives import serialization
4 import base64
5
6 # Carica la chiave privata
7 with open('private_key.pem', 'rb') as key_file:
8     private_key = serialization.load_pem_private_key(
9         key_file.read(),
10         password=None)
11 # Carica la chiave pubblica
12 with open('public_key.pem', 'rb') as key_file:
13     public_key = serialization.load_pem_public_key(key_file.read())
14
15 message = 'ABBAABBA!'
16 # Firma con la chiave privata
17 signed = private_key.sign(message.encode(), padding.PKCS1v15(), hashes.SHA256)
18 # Verifica della firma con la chiave pubblica
19 try:
20     encrypted_b64 = base64.b64encode(signed).decode('utf-8')
21     public_key.verify(signed, message.encode(), padding.PKCS1v15(), hashes.SHA256)
22     print("Base64 della firma:", encrypted_b64)
23     print("Messaggio originale da confrontare:", message)
24     print("La firma è valida.")
25 except Exception as e:
26     print("La firma non è valida.", str(e))
```

```
kali@kali:~/Downloads/crypto
$ cd Downloads/crypto
$ ls
encdec.py private_key.pem public_key.pem venv
$ python encdec.py
Messaggio originale: Ciao, Epicode spacca!
Messaggio criptato: E27U2hESywsboARGidCDAb13HCoakYv634B/iP4IEMPVslJC06ioM8bfNpVH/XaFXyBrQKU56s1
4Ew2xlr32ci22G+znALYkLekXZDpcWISg8UpeDY+ar567FudCj7U/XPx8THNHVmgW3yW0z16ADlqwCHLfi1vQ2hmt3WgLmg1
0KPq14mLsKCOmx2/7qEDdXBe/dmom1SasV1Fr0s53E8orpl+R4zWKYNTvCCrE0prixIQD6ZyYCXIKUzDgc8xoUKWdsUPahJ2
4yLhbzHWT82vCC750HHY7crTgHx1152YpWZx8XmnnfQFuhJh4vw62rL7nWYF6zA/hJHGZw=
Messaggio decrittato: Ciao, Epicode spacca!
$ python firma.py
Base64 della firma: W+t45QZ2ZENxt4vMksfhpZRI6m6ARvgXYU7x29LB/uq5gbhC5FKK0R4iKStWZHL63t8znJiKmpu
xaxouRIm3wthVmrpxdsLDppq74ygw300ngk4sks3Uhsfsve0HCbvojuIwBDoHdgXCyH2x5vDYxxVtBggsRXAt1ijxFwGh9
LvwYBDG188A7ka6pVMApm2F4f7/d5CwZI4VIKdIhF501lHHqNCfknA7msod/6kr30xbAl5bS5Z778778EYXizCfaol6hbNCA
GF0o2Znqu0Bx0d/6NKA3nNEVZ004v88aEvUuHLVj+PeF2X8Vgy/eKlrvoDuPPiZjB/qBAQ=
Messaggio originale da confrontare: ABBAABBA!
La firma è valida.
```