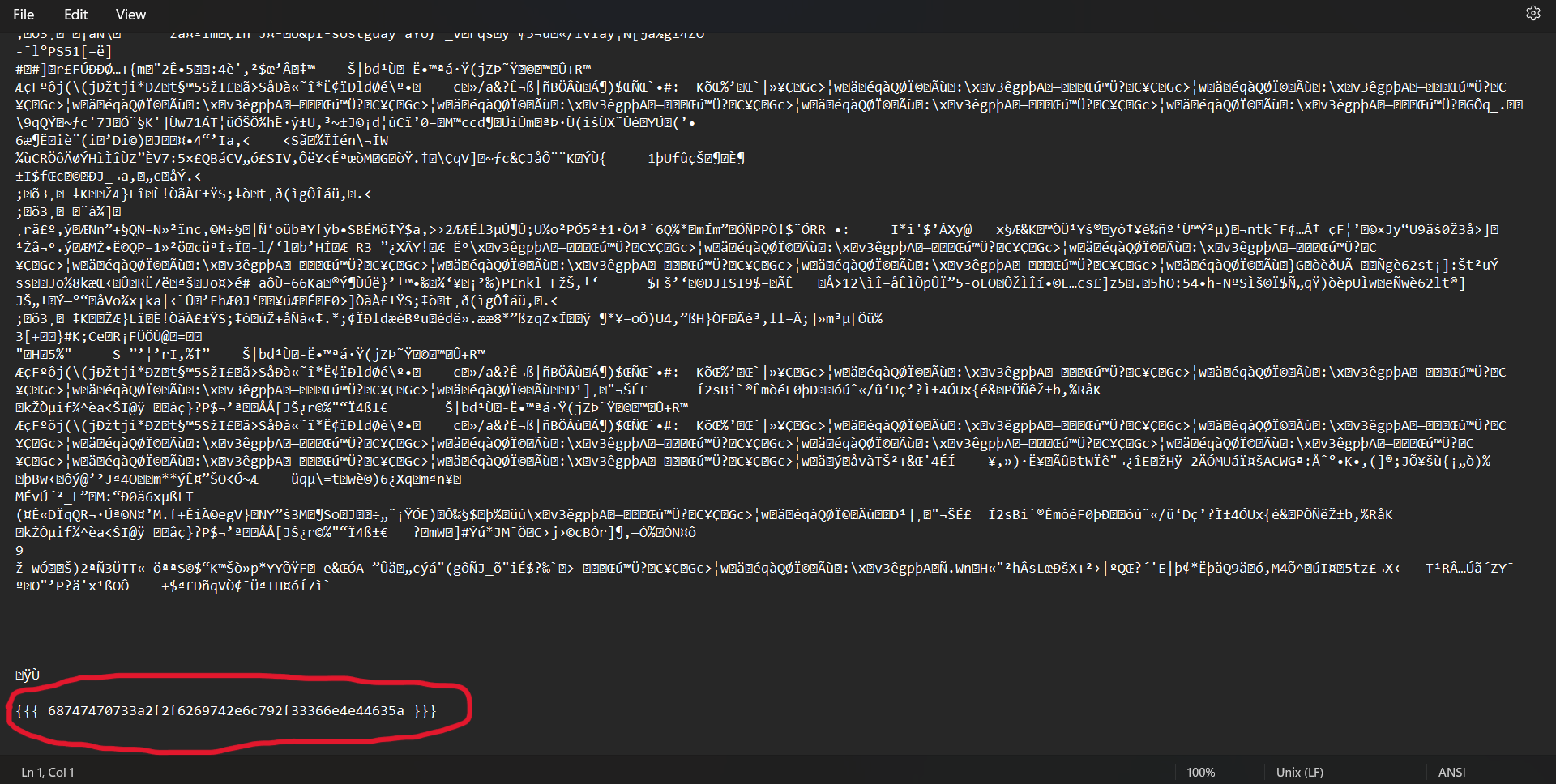
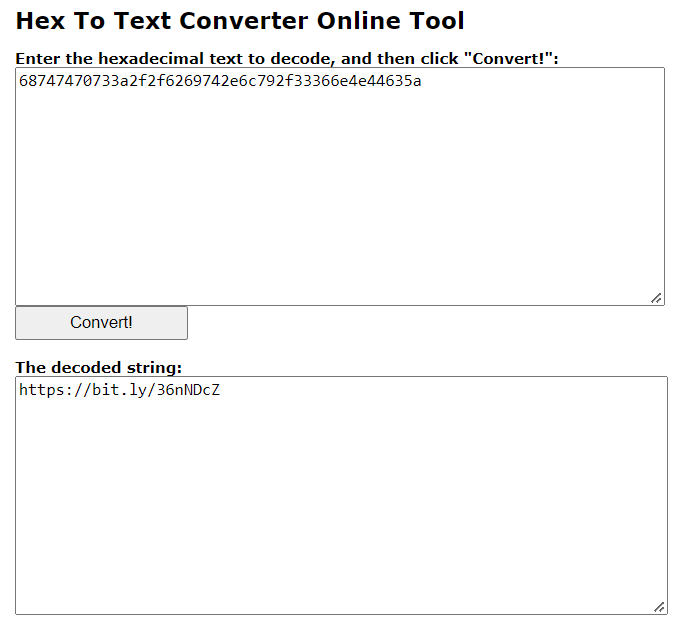
**Writeup for Archived Note:**

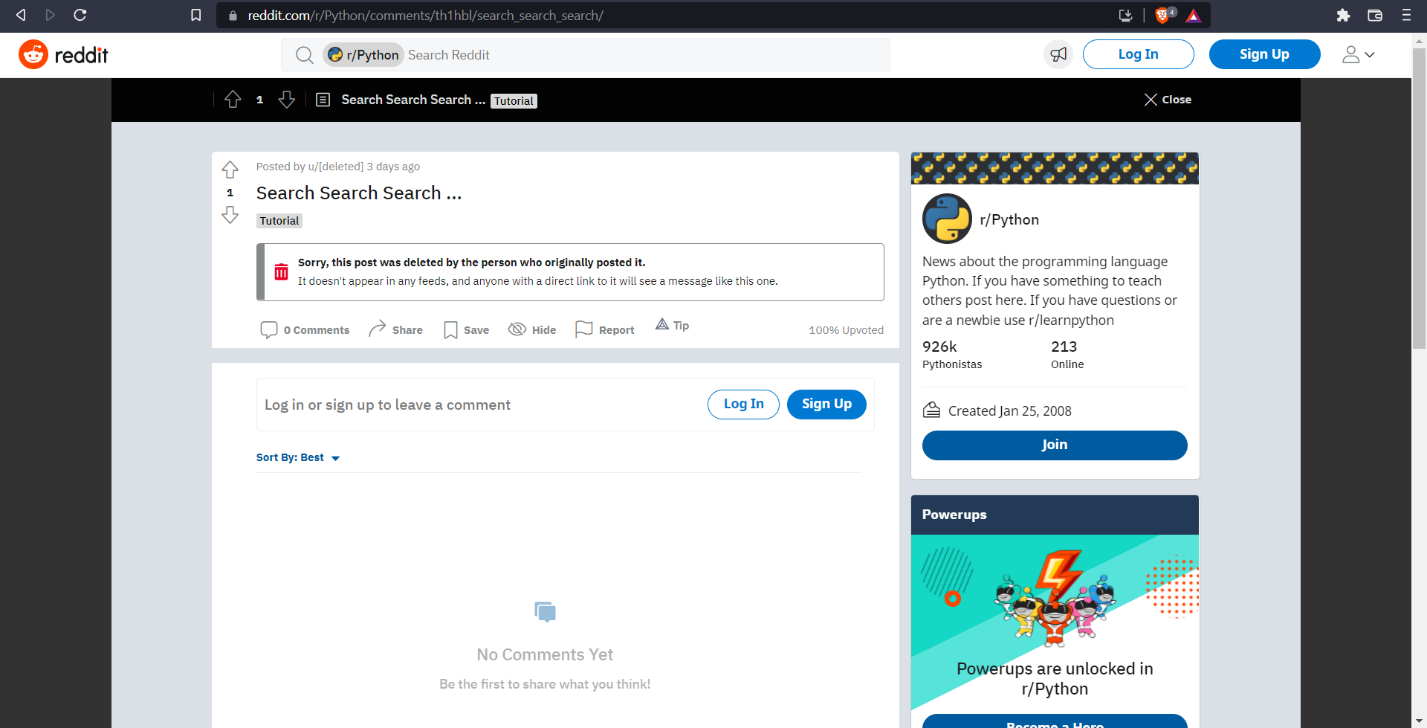
There is image given in Question, which is QR code, scanning QR code you will get a dictionary of keys which is

{‘public’: (2, 2683, 2576), ‘private’: 1025, ‘k\_value’: 847}

QR code also contain a string embedded using Steganography, decoding steganographic image will give string, i.e., 68747470733a2f2f6269742e6c792f33366e4e44635a, which is hex encoded, on decoding that hex string we get a shortened link, <https://bit.ly/36nNDcZ> .



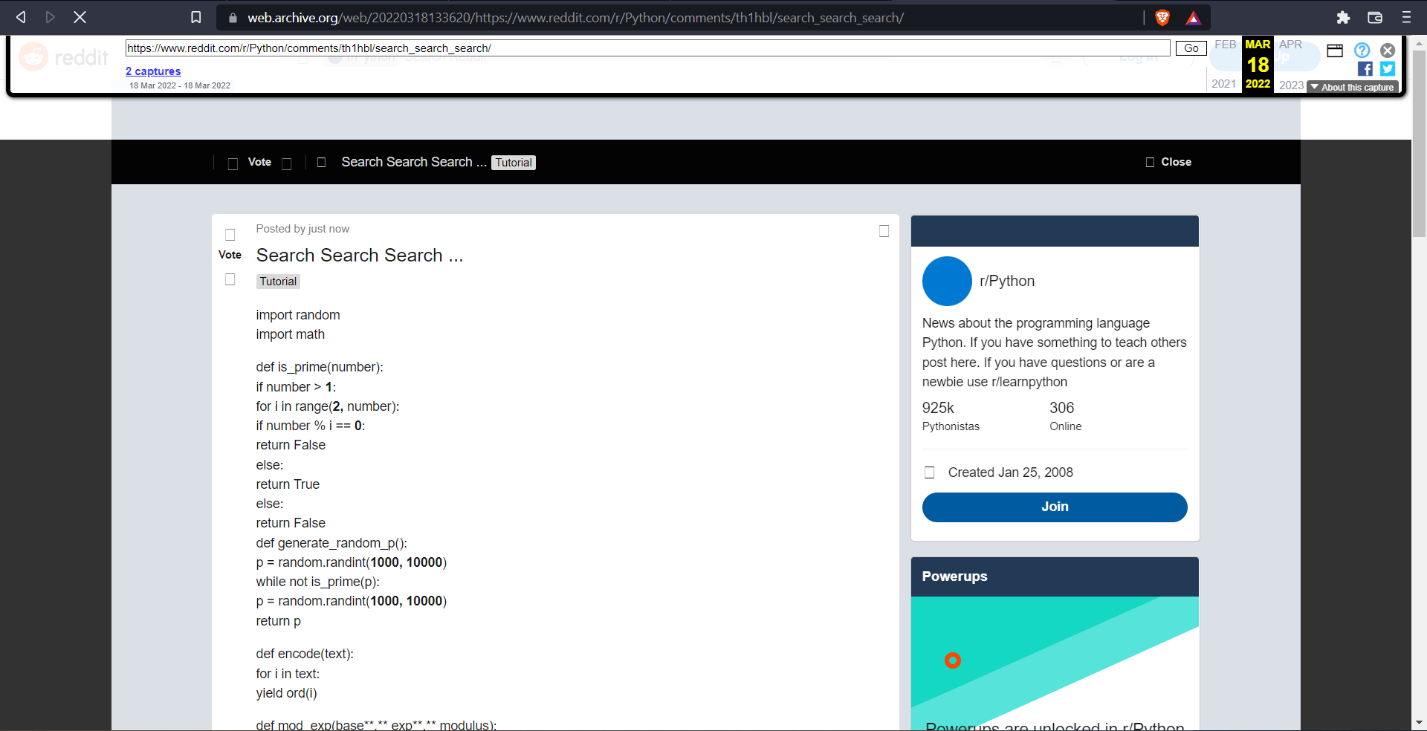




On visiting the link, it redirects us to Reddit Post, which is deleted.

Now reading Question again, question name states that there’s something archived on internet.

Heading to Way Back Machine, and searching for same link, we get an archived web page with the original post.



There is Python Encryption Script for Elgamal Cipher Encryption, we must write decryption script for the same.

Ciphertext is given in Question and key we got through QR code, passing them through decryption function we get final Flag

decrypt.py

def decrypt(key**,** message):  
 x = key['private']  
 p = key['public'][**1**]  
 decoded\_msg = ''  
 for item in message:  
 first = item[**0**]  
 second = item[**1**]  
 m = (second \* (first \*\* (p - **1** - x))) % p  
 decoded\_msg += str(chr(m))  
 return decoded\_msg

this can be used as decrypt function for Elgamal Cipher.

Decrypting Ciphertext given in Question Description will give us Flag.

Flag: vishwaCTF{elg4m4l\_1s\_0v3r\_p0w3r3d}