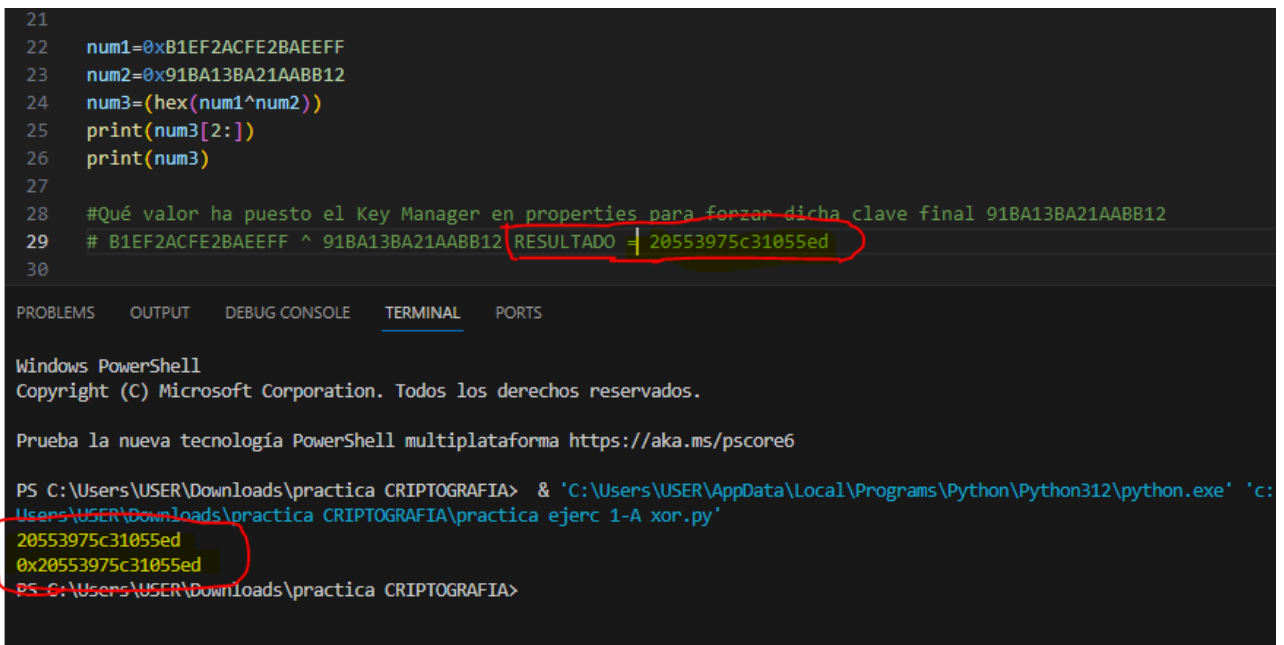


SOLUCIONES PRÁCTICA CRIPTOGRAFÍA

1. Tenemos un sistema que usa claves de 16 bytes. Por razones de seguridad vamos a proteger la clave de tal forma que ninguna persona tenga acceso directamente a la clave. Por ello, vamos a realizar un proceso de disociación de la misma, en el cuál tendremos, una clave fija en código, la cual, sólo el desarrollador tendrá acceso, y otra parte en un fichero de propiedades que rellenará el Key Manager. La clave final se generará por código, realizando un XOR entre la que se encuentra en el properties y en el código.

RESPUESTA:

20553975c31055ed



The image shows a code editor window with a Python script and a PowerShell terminal window below it. The Python script defines two hexadecimal keys, performs an XOR operation, and prints the result. The PowerShell terminal shows the execution of the script, with the output highlighted by a red circle.

```
21
22 num1=0xB1EF2ACFE2BAEEFF
23 num2=0x91BA13BA21AABB12
24 num3=(hex(num1^num2))
25 print(num3[2:])
26 print(num3)
27
28 #Qué valor ha puesto el Key Manager en properties para forzar dicha clave final 91BA13BA21AABB12
29 # B1EF2ACFE2BAEEFF ^ 91BA13BA21AABB12 RESULTADO = 20553975c31055ed
30
```

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL PORTS

Windows PowerShell
Copyright (C) Microsoft Corporation. Todos los derechos reservados.

Prueba la nueva tecnología PowerShell multiplataforma <https://aka.ms/pscore6>

PS C:\Users\USER\Downloads\practica CRIPTOGRAFIA> & 'C:\Users\USER\AppData\Local\Programs\Python\Python312\python.exe' 'c:\Users\USER\Downloads\practica CRIPTOGRAFIA\practica ejerc 1-A xor.py'

20553975c31055ed
0x20553975c31055ed
PS C:\Users\USER\Downloads\practica CRIPTOGRAFIA>

La clave fija en código es B1EF2ACFE2BAEEFF, mientras que en desarrollo sabemos que la clave final (en memoria) es 91BA13BA21AABB12. ¿Qué valor ha puesto el Key Manager en properties para forzar dicha clave final?

RESPUESTA:

8653f75d31455c0

```
22 num1=0xB1EF2ACFE2BAEEFF
23 num2=0xB98A15BA31AEBB3F
24 num3=(hex(num1^num2))
25 print(num3[2:])
26 print(num3)
27
28 # B1EF2ACFE2BAEEFF ^ B98A15BA31AEBB3F RESULTADO = 8653f75d31455c0
29
```

PROBLEMS OUTPUT DEBUG CONSOLE **TERMINAL** PORTS

Windows PowerShell
Copyright (C) Microsoft Corporation. Todos los derechos reservados.

Prueba la nueva tecnología PowerShell multiplataforma <https://aka.ms/pscore6>

PS C:\Users\USER\Downloads\practica CRIPTOGRAFIA> & 'C:\Users\USER\AppData\Local\Programs\Python\Python3\Users\USER\Downloads\practica CRIPTOGRAFIA\practica ejerc 1-A xor.py'

8653f75d31455c0
0x8653f75d31455c0
PS C:\Users\USER\Downloads\practica CRIPTOGRAFIA>

2 Para este caso, se ha usado un AES/CBC/PKCS7. Si lo desciframos, ¿qué obtenemos?

Recipe

AES Decrypt

Key: A2CFF885901A5449E... HEX IV: 0000000000000000... HEX

Mode: CBC Input: Hex Output: Raw

Input

4d0f5238c29ce9a152f5297185f2bdc13d7c517a4f09de74e577f927fe672c8ece7ffa3440a2165e0de7bb5451cf84161257b376b2c00f92cee144a
ddda07f8b9d27bef25b0621be95ed5986947ce282

Output

Esto es un cifrado en bloque típico. Recuerda, vas por el buen camino. Ánimo.

¿Qué ocurre si decidimos cambiar el padding a x923 en el descifrado?

RESPUESTA: es igual al PKCS7 porque tiene padding de 1 byte, NO OCURRE NADA. Fallaría en una situación normal porque no tiene el PKCS7

¿Cuánto padding se ha añadido en el cifrado?

se ha añadido el último dígito porque, al poner NO PADDING en Cyberchef, no quitará el padding.

Recipe

AES Decrypt

⌛

⏸

Key

A2CFF885901A5449E...

HEX ▾

IV

0000000000000000...

HEX ▾

Mode

CBC/NoPadding

Input

Hex

Output

Hex

Input

4d0f5238c29ce9a152f5297185f2bdc13d7c517a4f09de74e577f927fe672c8ece7ffa3440a2165e0de7bb5451cf84161257b376b2c00f92cee144a
ddda07f8b9d27bef25b0621be95ed5986947ce282

160

1

Raw Bytes

LF

Output

4573746f20657320756e206369667261646f20656e20626c6f7175652074c3ad7069636f2e2052656375657264612c2076617320706f7220656c206
275656e2063616d696e6f2e20c3816e696d6f2e01