

## **Lab 14: XOR Encryption in Python (10 pts.)**

**Course Name:** Ethical Hacking and Offensive Security(HOD401)

**Student Name:** Nguyễn Trần Vinh – SE160258

**Instructor Name:** Mai Hoàng Đình

**Lab Due Date:** 28/10/2023

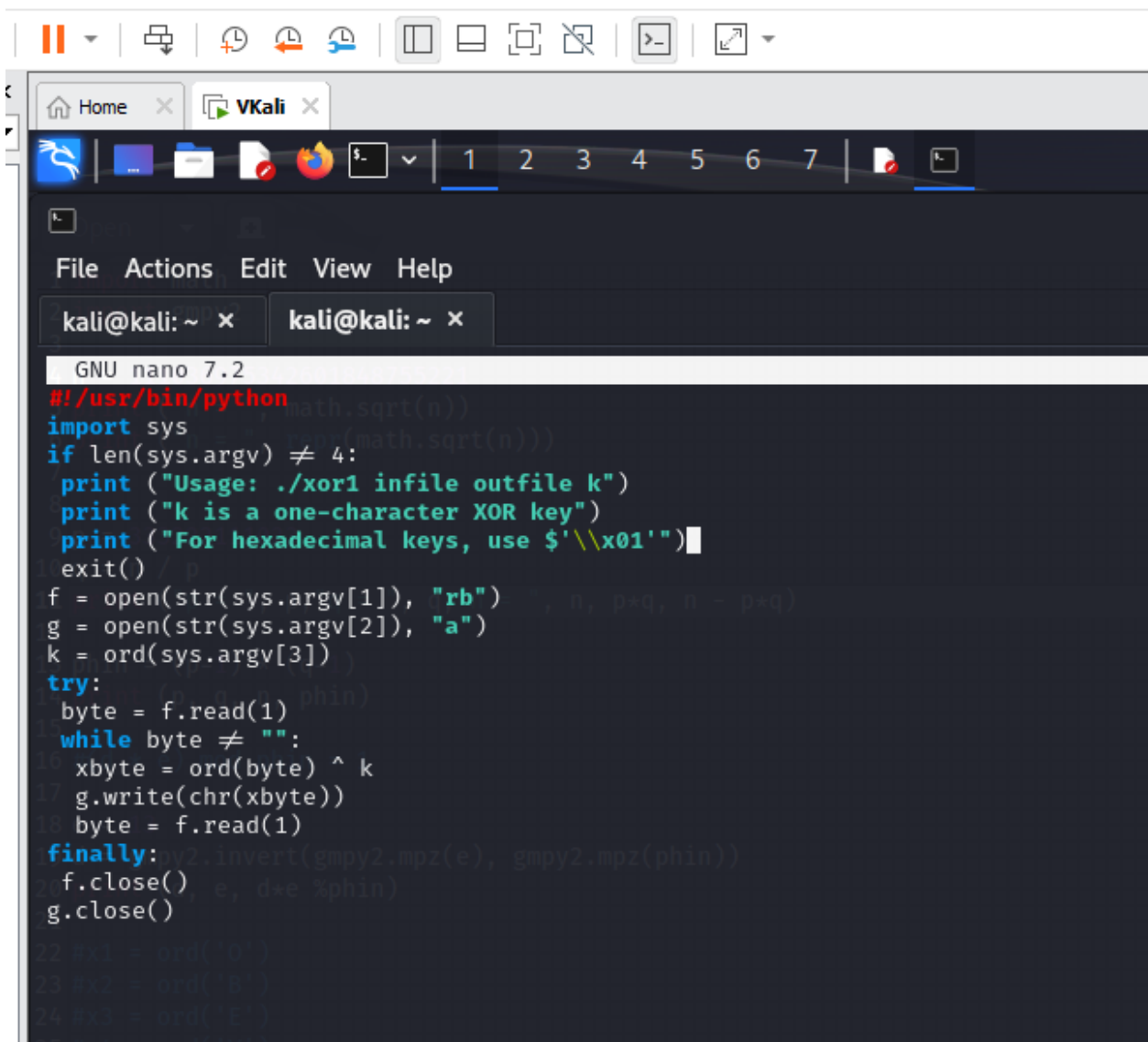
### **What you need:**

- A Kali Linux machine, real or virtual. You could also use OS X, or Windows with Python installed.

### **Purpose**

- Encrypt and decrypt files using XOR in Python.

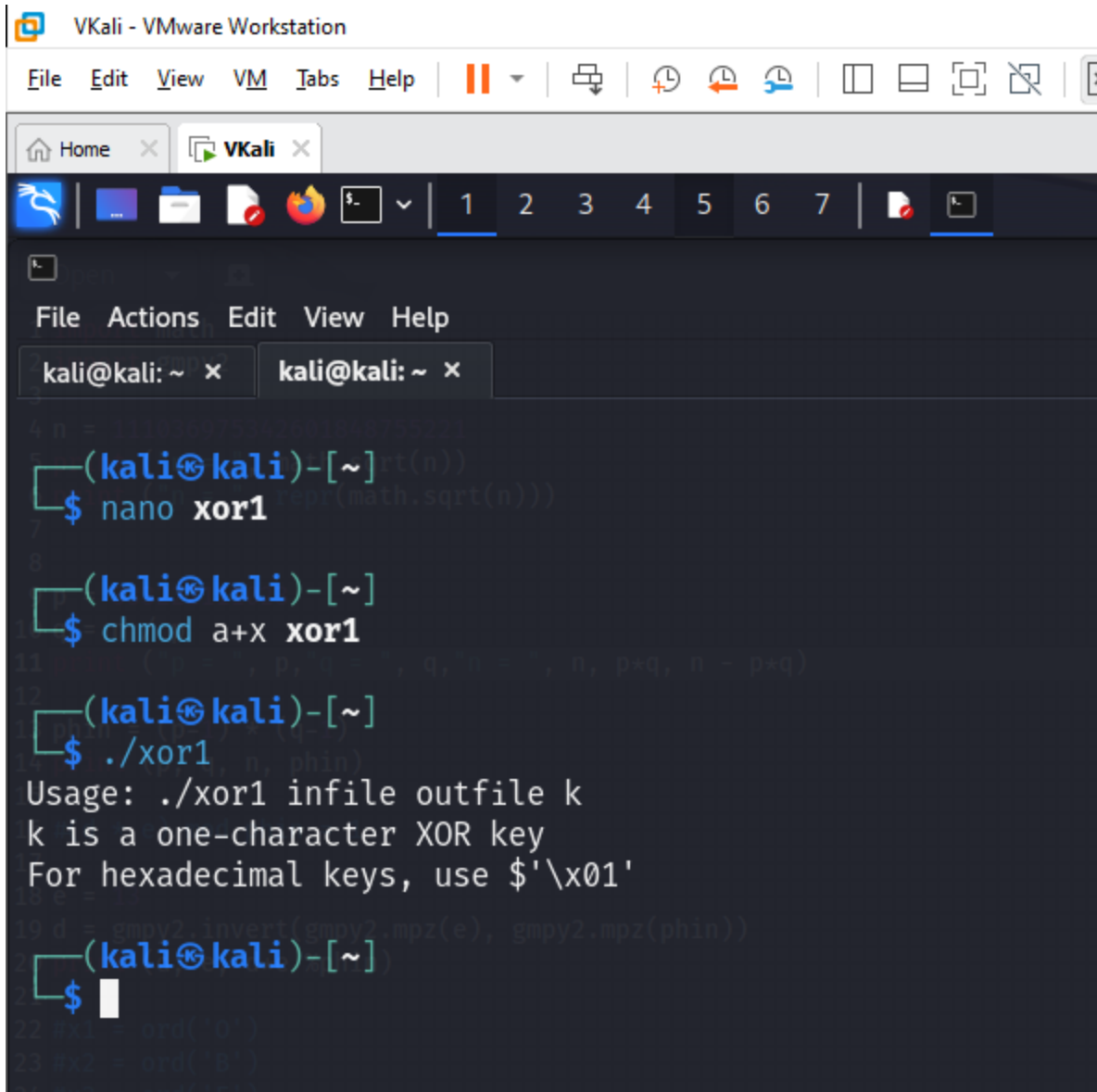
### **XOR in Python**

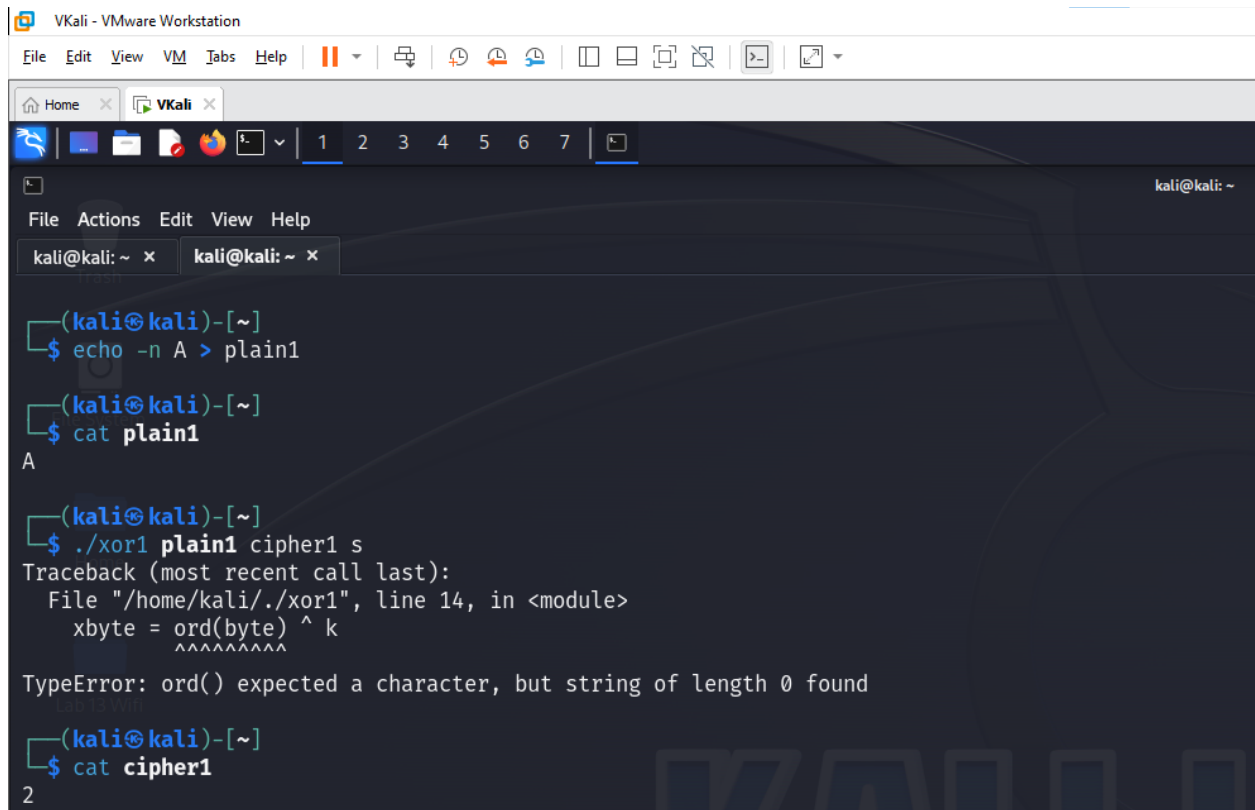


The image shows a Kali Linux desktop environment with a terminal window open. The terminal window has a title bar with 'Home' and 'VKali' tabs. Below the title bar is a taskbar with icons for a file manager, a terminal, and a web browser. The terminal window itself has a menu bar with 'File', 'Actions', 'Edit', 'View', and 'Help'. Below the menu bar are two tabs, both labeled 'kali@kali: ~'. The terminal content shows the GNU nano 7.2 editor with a Python script for XOR encryption. The script takes four arguments: the script name, an input file, an output file, and a key. It reads the input file byte by byte, XORs each byte with the key, and writes the result to the output file. The script also includes a usage message and a warning about hexadecimal keys.

```
GNU nano 7.2
#!/usr/bin/python
import sys
if len(sys.argv) != 4:
    print ("Usage: ./xor1 infile outfile k")
    print ("k is a one-character XOR key")
    print ("For hexadecimal keys, use '$'\x01'")
    exit()
f = open(str(sys.argv[1]), "rb")
g = open(str(sys.argv[2]), "a")
k = ord(sys.argv[3])
try:
    byte = f.read(1)
    while byte != "":
        xbyte = ord(byte) ^ k
        g.write(chr(xbyte))
        byte = f.read(1)
    finally:
        f.close()
        g.close()
```

## Encrypting a Single Character

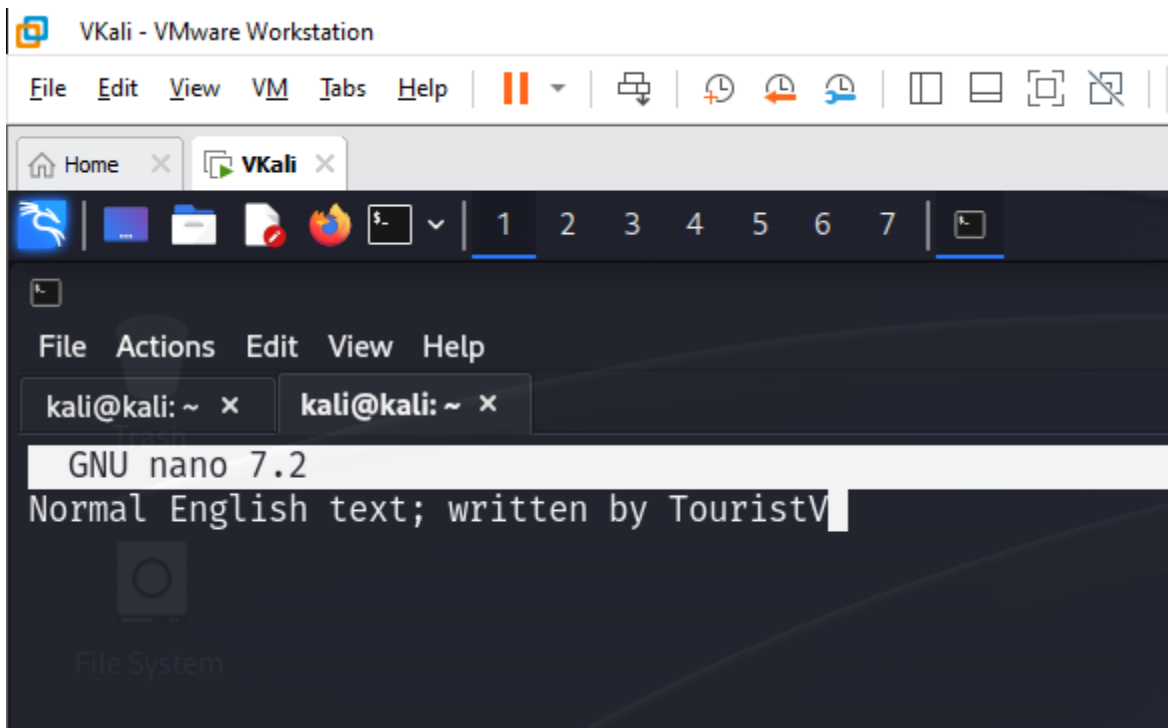


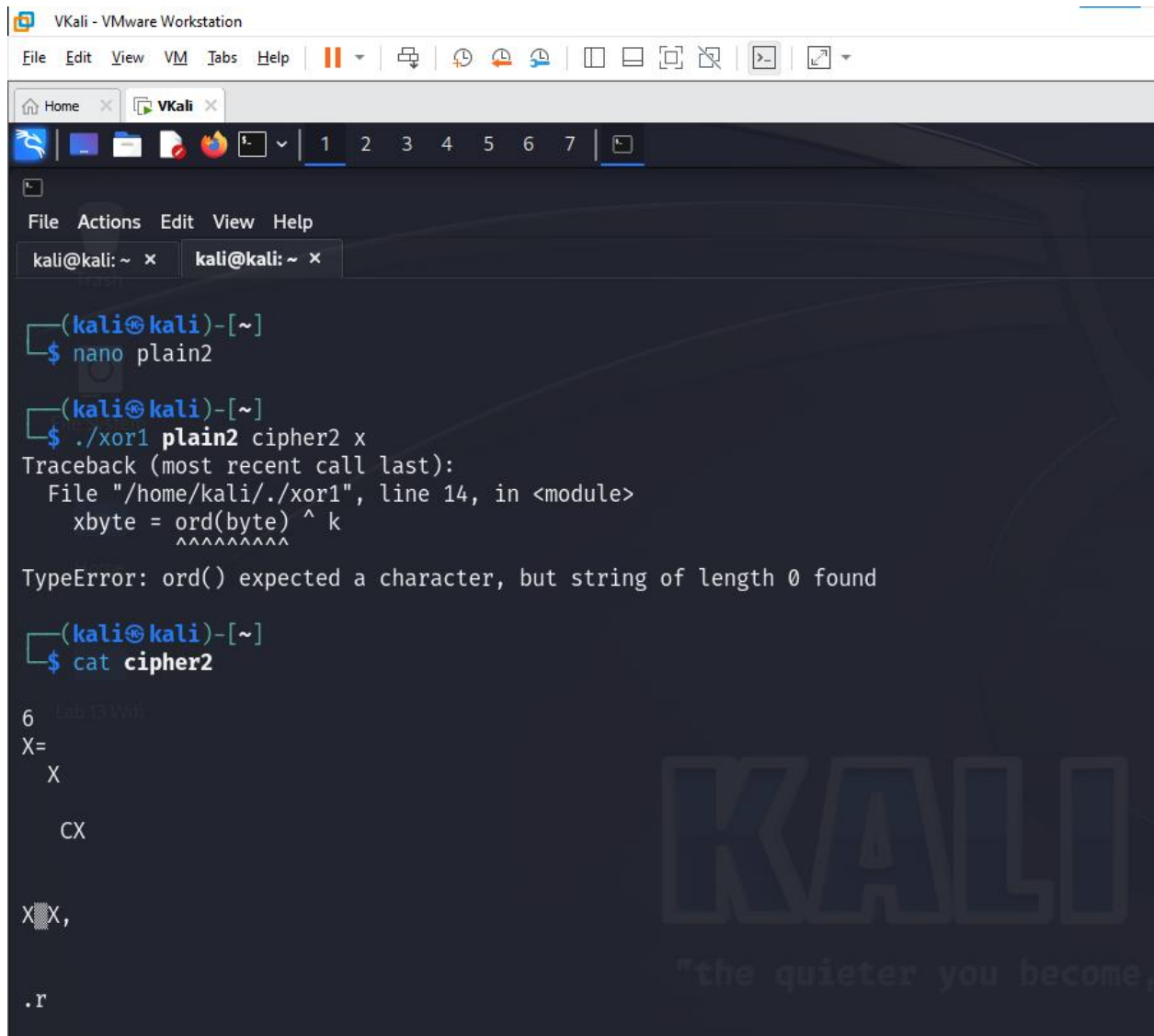


The screenshot shows a Kali Linux terminal window within a VMware Workstation. The terminal has a dark background with blue and green text. The user is at the root prompt. They create a file named 'plain1' containing the character 'A'. Then, they run a script './xor1 plain1 cipher1 s'. The script fails with a 'TypeError: ord() expected a character, but string of length 0 found' at line 14. The error message is displayed in green. The terminal window has a menu bar (File, Actions, Edit, View, Help) and a tab bar with two open tabs, both labeled 'kali@kali: ~'. The VMware Workstation window title is 'VKali - VMware Workstation'.

```
(kali@kali)-[~]
$ echo -n A > plain1
(kali@kali)-[~]
$ cat plain1
A
(kali@kali)-[~]
$ ./xor1 plain1 cipher1 s
Traceback (most recent call last):
  File "/home/kali/./xor1", line 14, in <module>
    xbyte = ord(byte) ^ k
            ^^^^^^^^^
TypeError: ord() expected a character, but string of length 0 found
(kali@kali)-[~]
$ cat cipher1
2
```

## Encrypting a Text File





```

VKali - VMware Workstation
File Edit View VM Tabs Help
Home VKali
File Actions Edit View Help
kali@kali: ~ x kali@kali: ~ x
(kali@kali)-[~]
$ nano plain2
(kali@kali)-[~]
$ ./xor1 plain2 cipher2 x
Traceback (most recent call last):
  File "/home/kali/./xor1", line 14, in <module>
    xbyte = ord(byte) ^ k
             ^^^^^^^^^
TypeError: ord() expected a character, but string of length 0 found
(kali@kali)-[~]
$ cat cipher2
6
X=
X
CX
X
X,X,
.r

```

## Decrypting a Text File

VMware Workstation

File Edit View VM Tabs Help

Home VKali

File Actions Edit View Help

kali@kali: ~ x kali@kali: ~ x

```
(kali@kali)-[~]  
$ ./xor1 cipher2 plain2r x  
  
Traceback (most recent call last):  
  File "/home/kali/./xor1", line 14, in <module>  
    xbyte = ord(byte) ^ k  
             ^^^^^^^^^  
TypeError: ord() expected a character, but string of length 0 found  
  
(kali@kali)-[~]  
$ cat plain2r  
Normal English text; written by TouristV
```