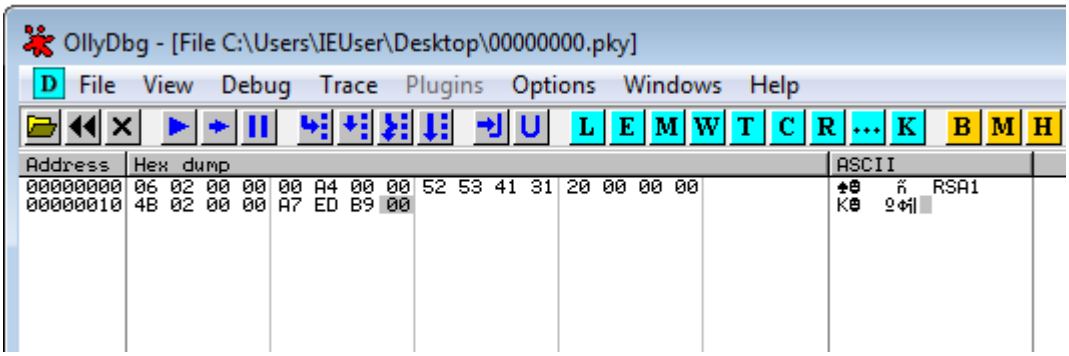
# COMP3334 Task 2

JAHJA Darwin, 16094501d

The screenshot below shows the content of the "00000000.pky" file generated by WannaCry.



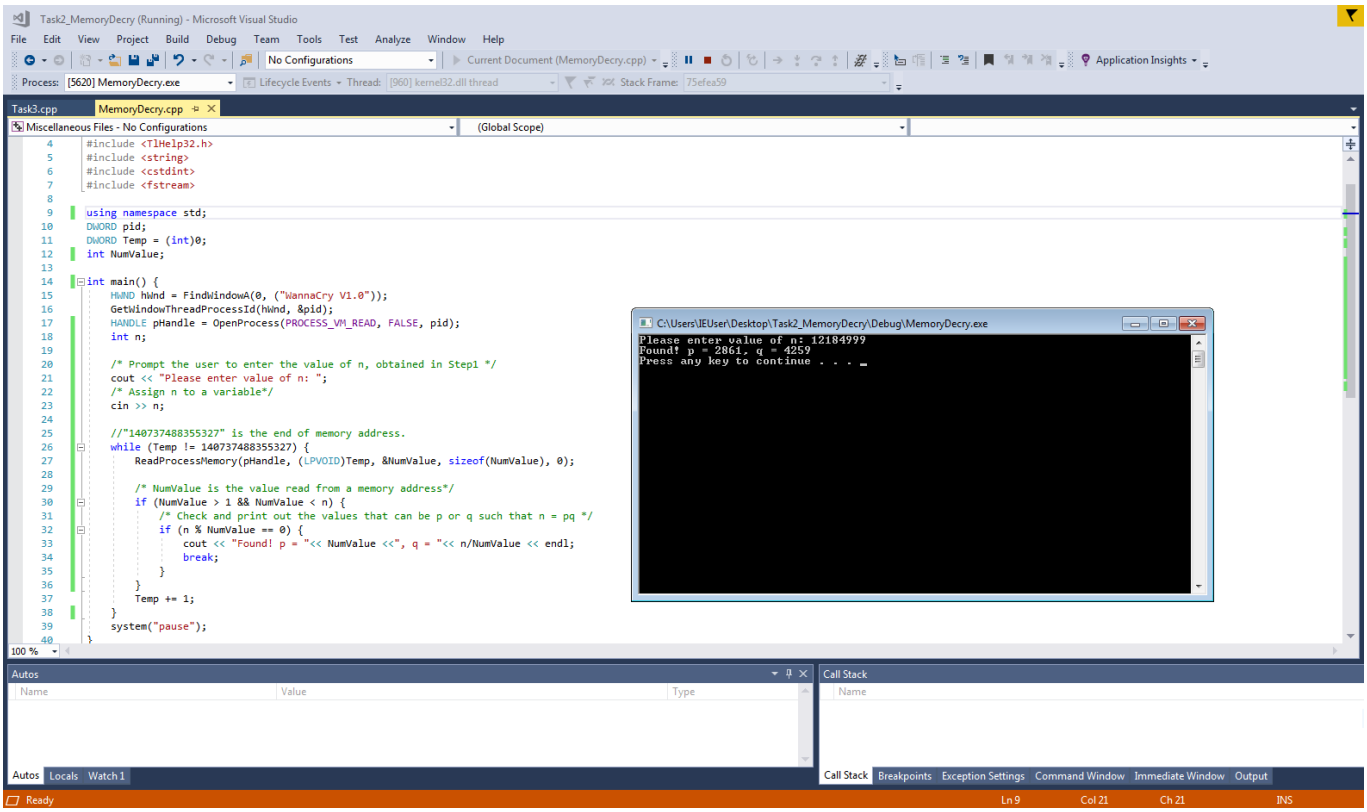

Here, we can know that the public exponent *e* and the Modulus *n* are "4B 02 00 00" and "A7 ED B9 00" respectively, which both are in little-endian format. Converting them into decimal, we get:

**e** = 0x24B = 587

**n** = 0xB9EDA7 = 12184999

---

Then, by running the C++ program to search the main memory, we can get *p* and *q*.




The above screenshot show the runtime of the C++ program. Here,

**p** = 2861, **q** = 4259

---

After that, we can calculate *d* which is the modular multiplicative inverse of *e*. I have written a python program for the calculation.

Task3.py saved

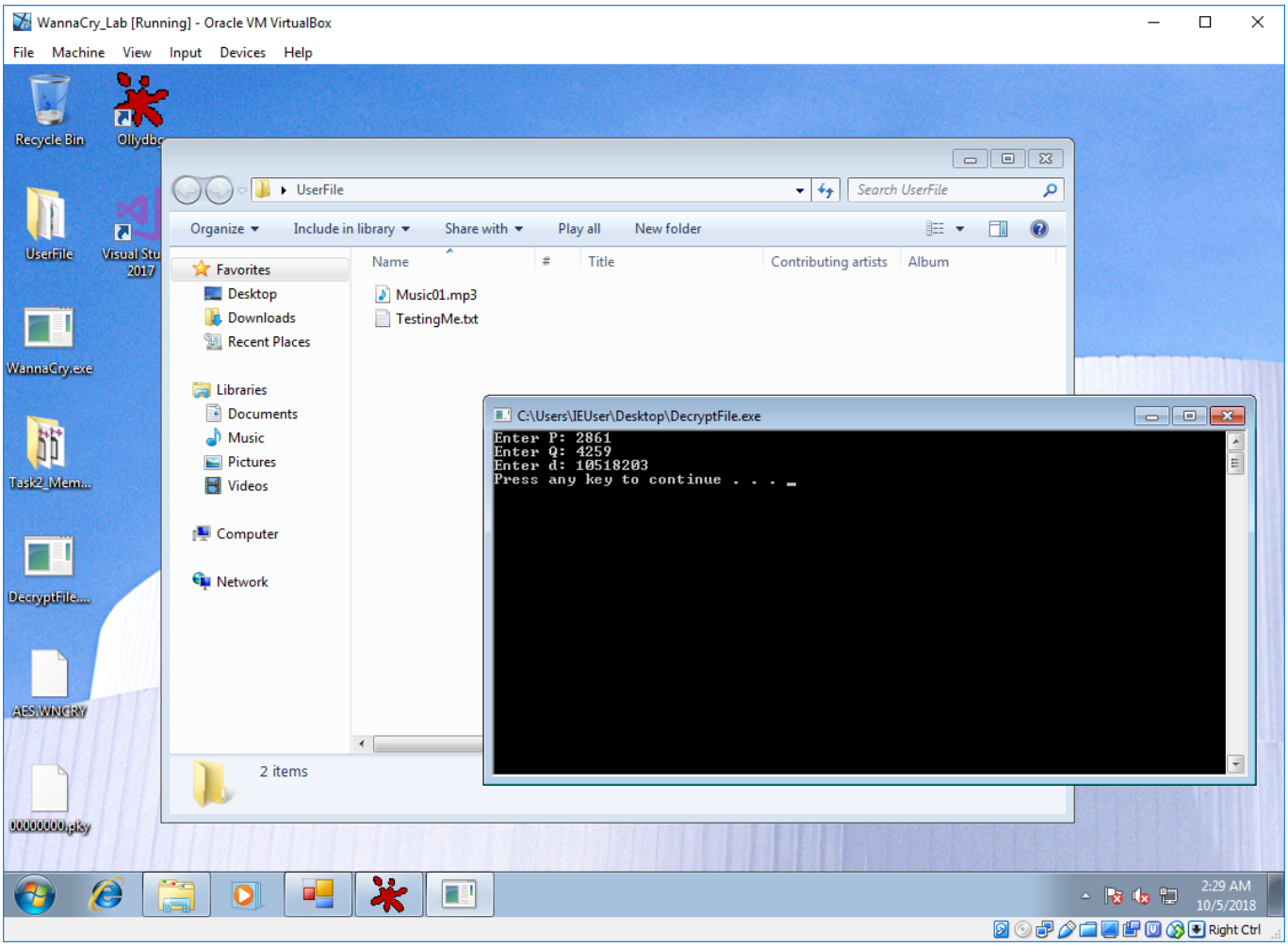
```python
# Task 3 to find d

def doElu(e, phi_n):
    A1, A2, A3 = 1, 0, phi_n
    B1, B2, B3 = 0, 1, e
    while True:
        if B3 == 0:
            return A3, None
        elif B3 == 1:
            return B3, B2
        Q = A3 // B3
        T1, T2, T3 = A1 - Q * B1, A2 - Q * B2, A3 - Q * B3
        A1, A2, A3 = B1, B2, B3
        B1, B2, B3 = T1, T2, T3

def main():
    e = 587
    p, q = 2861, 4259
    phi_n = (p - 1) * (q - 1)

    g, i = doElu(e, phi_n)

    if g == 1:
        res = phi_n + i
        print("The modular multiplicative inverse (d) is {}".format(res))
    else:
        print("There is no modular multiplicative inverse")

main()
```

```
Python 3.6.1 (default, Dec 2015, 13:05:11)
[GCC 4.8.2] on linux
>
The modular multiplicative inverse (d) is 10518203
>
```

Here, **d** = 10518203.

---

Finally, we can decrypt the file using the value of *p*, *q* and *d*


WannaCry_Lab [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Recycle Bin
UserFile
WannaCry.exe
Task2_Mem...
DecryptFile....
AES.WNCRY
00000000.pky
UserFile
Search UserFile
Organize
Include in library
Share with
Play all
New folder
Favorites
Desktop
Downloads
Recent Places
Libraries
Documents
Music
Pictures
Videos
Computer
Network
Name
Title
Contributing artists
Album
Music01.mp3
TestingMe.txt
2 items
C:\Users\IEUser\Desktop\DecryptFile.exe
Enter P: 2861
Enter Q: 4259
Enter d: 10518203
Press any key to continue . . .
2:29 AM
10/5/2018
Right Ctrl