You intercept the following ciphertext generated using the following RSA public-key: pk={e,n}={23,20413}

Determine the prime numbers p and q:

I utilized the following script to determine p and q:

```
import math

def findprimes(a):
  primes = []
  for i in range(2,a-1):
    diff = a/i
    if diff.is_integer():
      primes.append(i)
  if len(primes) == 0:
    print("{} is prime".format(a))
  else:
    print(primes)


def main():
  findprimes(20413)


if __name__ == "__main__":
  main()
```

findprimes.py

Thus: $p = 137$, and $q = 149$.

Determine Euler's totient function $\phi(n)$:

I calculated $\phi(n)$ as follows:

$$\begin{aligned}\phi(n) &= (p-1)\cdot(q-1)\\ \phi(n) &= (137-1)\cdot(149-1)\\ \phi(n) &= 20,128\end{aligned}$$

Determine the private-key={d,n}:

To compute d, the following relationship must hold:

$$d \cdot e \equiv 1 \mod \phi(n) \tag{1}$$

Knowing that $e = 23$, and $\phi(n) = 20,128$, I calculated $d = 13127$:[1]

$$\begin{aligned}e \cdot d &= 23 \cdot 13127\\ e \cdot d &= 301921\\ &= 301921 \mod 20128 = 1\end{aligned}$$

[1]Website used for calculation: https://www.cs.drexel.edu/ jpopyack/IntroCS/HW/RSAWorksheet.html

Compute the plaintext for EACH of the following ciphertext :

{236, 2743, 7983, 5919, 20213, 5520, 19563, 17083, 17083, 19326, 5919, 17258, 5919, 17215, 19563, 20213, 4940, 496}

The plaintext is shown below, in Hex: {41, 6E, 64, 20, 73, 74, 69, 6c, 6c, 2c, 20, 49, 20, 72, 69, 73, 65, 2e}[2]

Determine the ENGLISH plaintext:

I converted the Hex values above into ASCII characters, resulting in the following English:
And still, I rise.

[2]Calculated using the following website: http://extranet.cryptomathic.com/rsacalc/index