DateSeptember 5, 2016 | **Name ***

[TWCTF-2016: Crypto] Twin Primes Writeup

Standard

> **Challenge description:**
> *Decrypt it.*
> twin-primes.7z

We have 4 files in the archive:

- **encrypt.py** – A Python script uses RSA algorithm to encrypt the flag
- **encryped** – The encrypted message
- **key 1** – n, and e of one of the keys used in the encryption process
- **key 2** – n, and e of the other key used in the encryption process

Are you ready for your math lesson? Here we go.
After reading encrypt.py we know that:

- n1 = p*q
- n2 = (p+2)(q+2)
- p and q are twin primes. *i.e* p is prime and p+2 is also prime; similar for q.

Now let's turn the equation into an equation with one unknown and then solve it for the unknown.We can Isolate q to be $q = \frac{n^2}{p+2} - 2$ and substitute q in the other equation. Now we have an equation in one unknown: $n1 = p\left(\frac{n2}{p+2} - 2\right)$

Solve the equation and you'll get: $2p^2 + (n1 - n2 + 4)p + 2n1 = 0$

We need to solve this quadratic equation in order to find p and q. After that it will not be a problem to find the d's and build the keys.
The rest is in the script:

```python
from sympy import *
from Crypto.Util.number import *
import Crypto.PublicKey.RSA as RSA
import os

# n from key1
n1 = 19402643768027967294480695361037227649637514561280461352708420192197328993512710

# n from key2
n2 = 19402643768027967294480695361037227649637514561280461352708420192197328993512710

# e from key1 && key2
e=long(65537)

# a,b and c of the quadratic equation
a = 2
b = n1-n2+4
c = 2*n1

x = Symbol('x')

# solve the equation and put the solutions in x1_2, one of the solutions will be p,
x1_2 = solve(a*x**2+b*x+c)

p = x1_2[0]
q = x1_2[1]

# create d1 and d2 form p and q
d1 = inverse(e, (p-1)*(q-1))
d2 = inverse(e, (p+1)*(q+1))

# constructs the paramter to key1 and key2
key1=RSA.construct((n1,e,d1))
key2=RSA.construct((n2,e,d2))

# decrypt the flag
encrypted_flag = open('/Megabeets/encrypted',"r").read()
long_to_bytes(key1.decrypt(key2.decrypt(encrypted_flag)))

# result: "TWCTF{3102628d7059fa267365f8c37a0e56cf7e0797ef}"
```

view raw twin-primes.py hosted with ♥ by GitHub

Viewed using Just Read