**Cryptography: Decoding 6 (Hard)**

**Our officers have obtained several artifacts from a flag that was encrypted with RSA.**

**We need you to decrypt the flag.**

Given:

Modulo - n = 1829

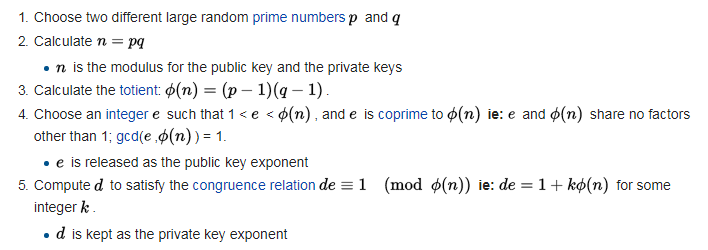
Encryption Key - e = 11

Cipher Text - c = 539 685 1763 536 1725 1006 685 953 536 1319 103 1319 843

Needed:

Decryption Key - d

RSA Algorithm Explained:



(Source: <https://simple.wikipedia.org/wiki/RSA_(algorithm)#Operation> )

**What is the value of p (the smaller prime)?**

**What is the value of q (the larger prime)?**

<https://www.calculatorsoup.com/calculators/math/prime-factors.php>

n = 1829 = pq = 31 x 59

p = 31

q = 59

**What is the plaintext of the encrypted message?**

ϕ(n) = (p – 1)(n – 1) = (30)(58) = 1740

de = 1 (mod ϕ(n)) 🡪 11d = 1 (mod 1740)

<https://planetcalc.com/3311/>

d = 791

<https://www.cs.drexel.edu/~introcs/Fa11/notes/10.1_Cryptography/RSA_Express_EncryptDecrypt.html>

Decrypted Message: SKY-EGKU-5259