RSA Decrypt Actions

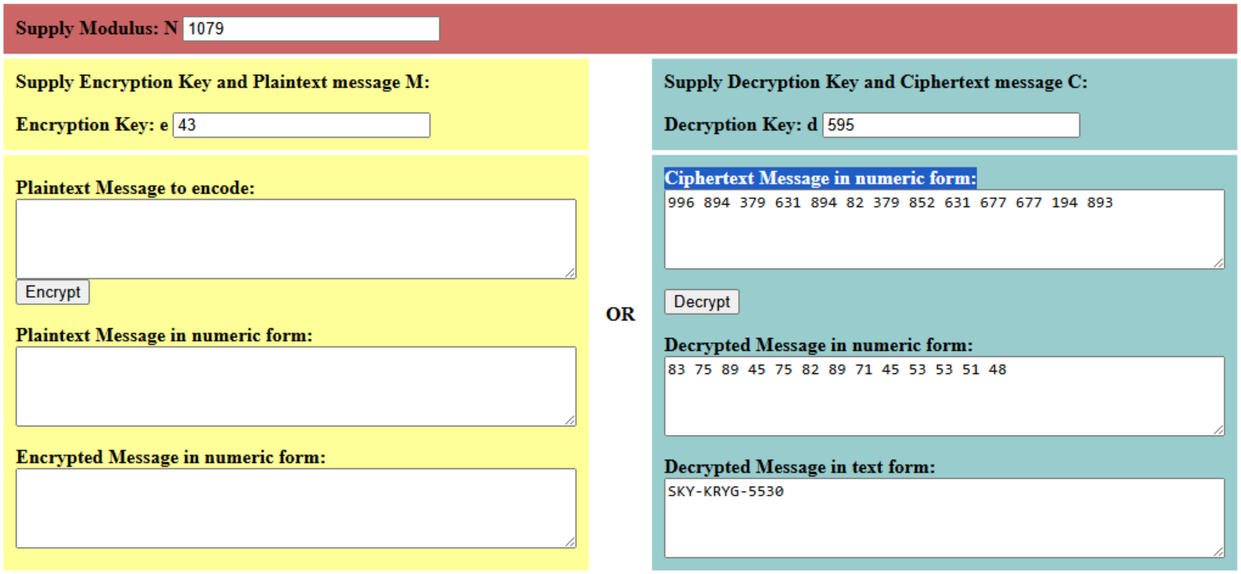
GIVEN

n = 1079

e = 43

c = 996 894 379 631 894 82 379 852 631 677 677 194 893 (this is our encrypted message)

1. Using N=1079, ask Google what are the primes of 1079: 13 and 83
2. p is the smaller prime = 13 q is the larger prime = 83
3. Open https://www.cs.drexel.edu/~popyack/IntroCS/HW/RSAWorksheet.html
4. Set p and q. N=1079 automatically r=984
5. Several candidates for **1 mod r** appear. Enter each candidate in the K Box and then calculate. When you calculate K, we're looking for a candidate that has e=43 in it. You just have to calculate each candidate until you get 43 in the factors box. In this case, **K= 25585** (factors are 5*7*17*43)
6. We now know that since e is 43, d=5*7*17 or **d=595**
7. Now skip to another calculator: https://www.cs.drexel.edu/~popyack/Courses/CSP/Fa17/notes/10.1_Cryptography/RSA_Express_EncryptDecrypt_v2.html
8. Enter N, e, and d in their appropriate boxes. Enter the message c in **the Ciphertext Message Box**



Supply Modulus: N 1079

Supply Encryption Key and Plaintext message M:

Encryption Key: e 43

Plaintext Message to encode:

Plaintext Message in numeric form:

Encrypted Message in numeric form:

Supply Decryption Key and Ciphertext message C:

Decryption Key: d 595

Ciphertext Message in numeric form:

```
996 894 379 631 894 82 379 852 631 677 677 194 893
```

Decrypted Message in numeric form:

```
83 75 89 45 75 82 89 71 45 53 53 51 48
```

Decrypted Message in text form:

```
SKY-KRYG-5530
```