RSA Cryptosystem Key Generation

In RSA cryptosystem, we first pick p=7, q=13.

1. Please continue to generate a set of public and private keys (hint: you can pick a small e).

N = p\*q = 7 \* 13 = 91

Φ(N) = (p-1)(q-1) = 6 \* 12 = 72

Choose random e, 1 < e < Φ(N) 🡪 1 < e < 72, where e is relatively prime to Φ(N).

* Choose e = 7

d = e-1 mod Φ(N)

de = 1 mod Φ(N)

Try d = 31 🡪 31 \* 7 = 217 = 3\*72 + 1

So, the keys become:

**Public key: <7, 91>**

**Private key: <31, 91>**

1. Please use your keys to encrypt message: "jayhawk". To convert characters to integer values, you can use ASCII, or encode a->1, b->2, c->3, etc.

jayhawk = {9, 0, 24, 7, 0, 22, 10}

c = memod(n) = m7mod(91)

c = {9, 0, 80, 84, 0, 22, 10}

1. Please use your keys to decrypt the ciphertext.

m = cemod(n) = m31mod(91)

m = {9, 0, 24, 7, 0, 22, 10}

It’s evident that the public and private keys match after seeing the unencrypted text is equivalent to the decrypted text.