Problem 3

By Noel Santillana Herrera

RSA encryption scheme

Given:

Public key(n, e) = (15151, 17)

Ciphertext = y = 832

- **Find the prime factorization of n**

  n = 15151 = p * q = 109 * 139

  The prime factorizations are p = 109 and q = 139

- **Compute ϕ(n)**

  ϕ(n) = (p-1)(q-1) = 108 * 138 = 14904

- **Finding the private key *d***

  Know that e = 17

  To find *d*, we use the formula:

  e^{-1} mod (ϕ(n))

  d = 17^{-1} mod 14904 = 6137

- **Decrypting ciphertext *y***

  You get a plaintext by decrypting the ciphertext

  plaintext = y^d mod n

  832^{6137} mod 15151 = 1781