Arnav Surve

03/08/23

CNIT 270

Hands

Math of RSA

1. p=29, q=67
2. n = pq = 29 \* 67 = 1943
3. φ(n) = (p-1)(-1) = 2866 = 1848
4. Select an appropriate e and d
   1. gcd(e, φ(n)) = 1
   2. gcd(23, 1848) = 1
   3. 1848 = 80 \* 23 + 8 23 = 2 \* 8 + 7 8 = 1 \* 7 + 1
   4. 1 = 8 - 7 = 8 - (23 - 2 \* 8) = 3 \* 8 - 23 = 3 \* (1848 - 80 \* 23) - 23 = 3 \* 1848 - 241 \* 23
   5. d = 241
   6. Public key = (e, n) = (23, 1943)  
      Private key = (d, n) = (241, 1943)
5. “ ‘Sup? ”

Ascii codes:  
‘ = 27

S = 83

u = 117

p = 112

? = 63

1. C ≡ M^e (mod n)
2. PU C = 1093 526 602 1012 = "'ĝǘŞ"
3. PR C =   
   27(mod 1943)   
   83(mod 1943)

117(mod 1943)

112(mod 1943)

63(mod 1943)

= “’Sup?”