RSA Practice

Euler's Totient Function $\phi(n)$

Compute $\phi(n)$ where $n = 24$

Compute $\phi(n)$ where $n = 23$

Compute $\phi(n)$ where $n = 29$

RSA Calculations

Example (As Demonstrated in Hands' Video)

1. Select two prime numbers p & q

   $p = 7$, $q = 11$

2. Calculate n

   $n = pq = 77$

3. Calculate $\phi(n)$

   $\phi(n) = (p-1)(q-1) = 60$

4. Select e such that e is relatively prime (i.e. they don't share any factors) to $\phi(n)$ and is less than $\phi(n)$

   $e = 17$

5. Determine d such that $(d \cdot e) mod \phi(n) = 1$ and $d < \phi(n)$
   In other words, find some number so that when you multiply it times e and divide by $\phi(n)$ and get a remainder of 1. The most efficient way to find this pair is to find multiples of $\phi(n)$ and add 1 (such as $(\phi(n) * 15) + 1$]. The factors of that sum can be your d & e. d must be a whole number.
   $d = 60 \cdot 15 = 900 + 1 = 901 \div 17 = 53$

6. You now know your public key, $PU = e, n$, and private key, $PR = d$
   $PU = 17, 77$
   $PR = 53$

7. To encrypt the text M =“Hello World” where each plaintext character is represented by a number between
   01 = A and 26=Z;
   27 = “ ” (blank space)
   27 = . (period)
   28 = ’ (apostrophe)
   29 = ? (question mark)

8. encoded plaintext is :
   h e l l o w o r l d 08 05 12 12 15 27 23 15 18 12 04

9. using the public key to encrypt (letter by letter), the ciphertext ($C = M^e \mod (n)$) is:

$$0817 mod 77 = 57$$
$$05^{17} mod 77 = 3$$
$$12^{17} mod 77 = 45$$
$$\ddots$$
$$04^{17} mod 77 = 16$$

   or 57 3 45 45 71 69 38 67 72 45 16

10. To show how decryption reverses this process, $M = C^d \mod (n)$ can be computed for the first letter.

$$28^{53} mod 77 = 7$$

Your Turn

1. You are given two prime numbers $p = 29$ & $q = 67$.

2. Calculate n and $\phi(n)$.

3. Select an appropriate e and d that meet our criteria.

4. Use e and d to find PU and PR.

5. Then, encrypt the text M =’Sup? to give the ciphertext C. (include the apostrophe and question mark)

6. Use the private key to decrypt the message demonstrating that the reverse process works as expected.