

## Problem Set # 8

**Exercise 1:** (★) 4 points

Let  $\phi$  be Euler's function. Show that  $\phi(n^m) = n^{m-1}\phi(n)$  for all natural number  $n, m$ .

**Exercise 2:** (★) 4 points

Let  $N$  be a product of two distinct primes. Show that if we know  $\varphi(N)$ , then we can easily factorize  $N$ .

**Exercise 3:** (★) 4 points

Find the last two digits of the decimal expansion of  $3^{1123}$  (For example the last two digits of 1729 are 29).

**Exercise 4:** (★) 4 points

Show that there is no solution to the equation  $\phi(n) = 14$ .

**Exercise 5:** (★) 4 points

You receive a message that was encrypted using the RSA system with public key  $(65, 29)$ , where 65 is the base and 29 is the exponent. The encrypted message in two blocks, is  $3/2$ . Find the private key and decrypt the message.

---

<sup>1</sup>(★) = easy , (★★)= medium, (★★★)= challenge