COMP90043 Cryptography and Security

Semester 2, 2020, Workshop Week 5

Part A: Recap

1. What is public key cryptography?

2. What is the integer factorization problem?

3. RSA Algorithm
   $C = M^e \bmod n$
   $M = C^d \bmod n = (M^e)^d \bmod n = M^{ed} \bmod n$

Part B: RSA Exercises

1. Given the parameters below, fill in the blanks accordingly for the relevant RSA

   parameter: p =13 q = 7 n = p.q = ________

   a) Using Euler's Totient Function, calculate

      $\phi(n) = \phi($ $\quad) =$ ____

2. For the RSA algorithm to work, it requires two coefficients – e and d. Where e represents the encryption component (generally the public key) and d represents the decryption component (generally the private key)

   In order to calculate d, we can use Extended Euclidean Algorithm.

   a) Suppose $\phi(n) = 72$. For each of the following given values of e, calculate the value of d such that

      $$d.e = 1 \bmod \phi(n)$$

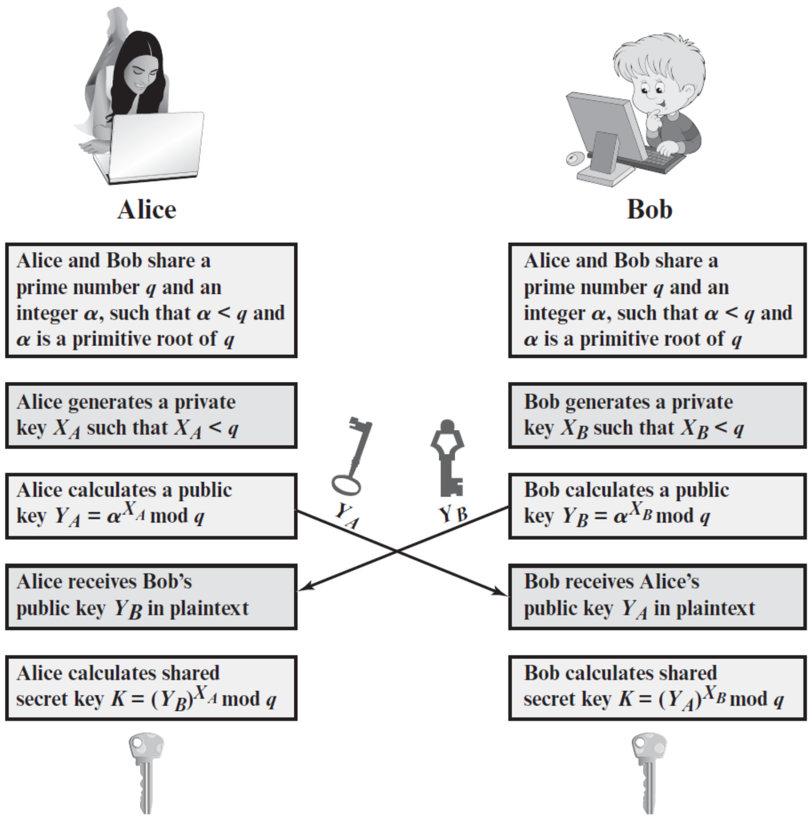
      e=5
      e=7

   b) Suppose we have two primes p=23 and q=37. For the following e, calculate the value of d such that

      $$d.e = 1 \bmod \phi(n)$$

      e=5
      e=61

3. The Diffie-Hellman key exchange algorithm can be defined as follows, show that Diffie-Hellman is subject to a man-in-the-middle attack.



4. Given the encryption and decryption formulas for RSA as follow:

$$C = M^e \ mod \ n$$

$$M = C^d \ mod \ n = (M^e)^d \ mod \ n = M^{ed} \ mod \ n$$

Perform encryption and decryption for the given values of p, q, e and M

<table>
<tr>
<td>$p = 3;\ q = 13;\ e = 5;\ M = 10;$
$n =$ _____; $\varphi(n) =$ _____; $d =$ _____;
$C = M^e \ mod \ n = 10^5 \ mod$ _____ $=$ _____;
$M = C^d \ mod \ n =$ _____ mod _____ $=$ ____;</td>
<td>$p = 5;\ q = 7;\ e = 7;\ M = 12;$
$n =$ _____; $\varphi(n) =$ _____; $d =$ _____;
$C = M^e \ mod \ n = 12^7 \ mod$ _____ $=$ _____;
$M = C^d \ mod \ n =$ _____ mod _____ $=$ ____;</td>
</tr>
<tr>
<td>$p = 11;\ q = 7;\ e = 11;\ M = 7;$
$n =$ _____; $\varphi(n) =$ _____; $d =$ _____;
$C = M^e \ mod \ n = 7^{11} \ mod$ _____ $=$ _____;
$M = C^d \ mod \ n =$ _____ mod _____ $=$ ____;</td>
<td></td>
</tr>
</table>

5. In a public-key system using RSA, you intercepted the cipher text C = 8 sent to a user whose public key is e = 13; n = 33. What is the plaintext M ?