COMP90043 Cryptography and Security

Semester 2, 2024, 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: CRT Exercises

Solve for x satisfying the following simultaneous congruences:

$$x \equiv 7 \pmod{11},$$
$$x \equiv 9 \pmod{13}.$$

Part C: 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

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

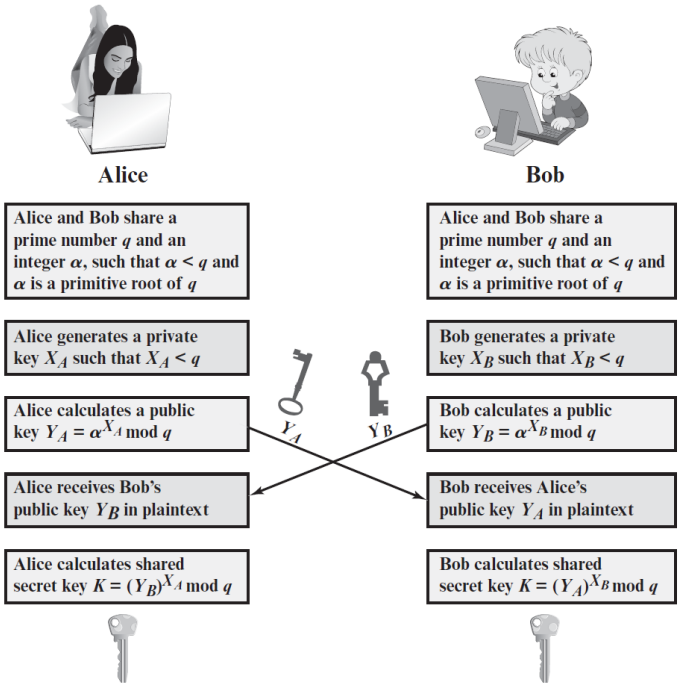
   e=5
   e=7

   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

$p = 3;\ q = 13;\ e = 5;\ M = 10;$ $n = \_\_\_\_;\ \varphi(n) = \_\_\_\_; d = \_\_\_\_;$ $C = M^e \ mod \ n = 10^5 \ mod \ \_\_\_\_ = \_\_\_\_;$ $M = C^d \ mod \ n = \_\_\_\_ \ mod \ \_\_\_\_ = \_\_\_\_;$	$p = 5;\ q = 7;\ e = 7;\ M = 12;$ $n = \_\_\_\_;\ \varphi(n) = \_\_\_\_; d = \_\_\_\_;$ $C = M^e \ mod \ n = 12^7 \ mod \ \_\_\_\_ = \_\_\_\_;$ $M = C^d \ mod \ n = \_\_\_\_ \ mod \ \_\_\_\_ = \_\_\_\_;$
$p = 11;\ q = 7;\ e = 11;\ M = 7;$ $n = \_\_\_\_;\ \varphi(n) = \_\_\_\_; d = \_\_\_\_;$ $C = M^e \ mod \ n = 7^{11} \ mod \ \_\_\_\_ = \_\_\_\_;$ $M = C^d \ mod \ n = \_\_\_\_ \ mod \ \_\_\_\_ = \_\_\_\_;$	

5. Choose the smallest possible e for the above RSA settings:

Smallest possible e: (e>=2, e is a valid key, e is not a multiple of either p or q)

a) p = 5, q = 11
b) p = 3, q = 17
c) p = 29, q = 37