COMP90043: Cryptography and Security

Week 5: RSA and Diffie-Hellman

Recap:

1. What is public key cryptography?
2. What is the integer factorization problem?
3. RSA Algorithm

   $C = M^e \bmod n$

   $M = C^d \bmod n = (M^e)^d \bmod n = M^{ed} \bmod n$
4. Man in the Middle Attack

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 which can be summarized as follows for any a and b such that (a > b).

GCD(a,b) $a = q_1 b + r_1$ $b = q_2 r_1 + r_2$ $r_1 = q_3 r_2 + r_3$ $r_2 = q_4 r_3 + r_4$ … (1) $r_{n-2} = q_n r_{n-1} + r_n$ (2) $r_{n-1} = q_{n+1} r_n + r_{n+1}$, **where $r_{n+1} = 1$ (GCD exists)** (3) $r_n = q_{n+2} r_{n+1} + r_{n+2}$, **where $r_{n+2} = 0$**	Now we can perform a back substitution to get d as follows: From (2) we get $r_{n+1} = 1 = r_{n-1} - q_{n+1} r_n$ We know r_n from (1), so we can substitute $= r_{n-2} - q_{n+1}(r_{n-2} - q_n r_{n-1})$ We continue this for each r while simplifying each step until we can represent the r_{n+1} in terms of b.

a) For the following, for each of the given values of e, calculate the value of d such that

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

e = 5	e = 7
GCD(ϕ(n), e) = GCD(72, 5) $\phi(n) = 72 = q_1e + r_1 = 14 * 5 + 2$ $e = 5 = q_2r_1 + r_2 = 2 * 2 + 1$ $r_1 = 2 = q_3r_2 + r_3 = 2 * 1 + 0$ Back Substitution we get $1 = [e - q_2r_1]\ \phi(n) = [5 – (2*2)] \bmod \phi(n)$ $1 = [e – q_2\ (\phi(n) - q_1e)]\ \phi(n)$ $= [5 – (2*(72-(14*5)))]\ \phi(n)$ $= [5 + (-2*(72-(14*5)))]\ \phi(n)$ $= [5 +(-2*72 + 2*(14*5))]\ \phi(n)$ $= [5 + (-2*72 + 28*5)]\ \phi(n)$ $= [5 + 28*5 – 2*72]\ \phi(n)$ $= [29*5 – 2*72]\ \phi(n)$ From the above if we want to determine $d.e = 1 \bmod \phi(n)$ where e = 5, then **d = 29**	GCD(ϕ(n), e) = GCD(**72**, 7) $\phi(n) = 72 = q_1e + r_1 =$ ______________________ $e = 7 = q_2r_1 + r_2 =$ __________________________ $r_1 = \quad = q_3r_2 + r_3 =$ _________________________ Back Substitution we get $1 = [e - q_2r_1]\ \phi(n) = [\qquad\qquad] \bmod \phi(n)$ $1 = [e – q_2\ (\phi(n) - q_1e)]\ \phi(n)$ = _______________________________________ = _______________________________________ = _______________________________________ = _______________________________________ = _______________________________________ = _______________________________________ From the above if we want to determine $d.e = 1 \bmod \phi(n)$ where e = 7, then **d =** ____________

b) For the following, for each of the given values of e, calculate the value of d such that

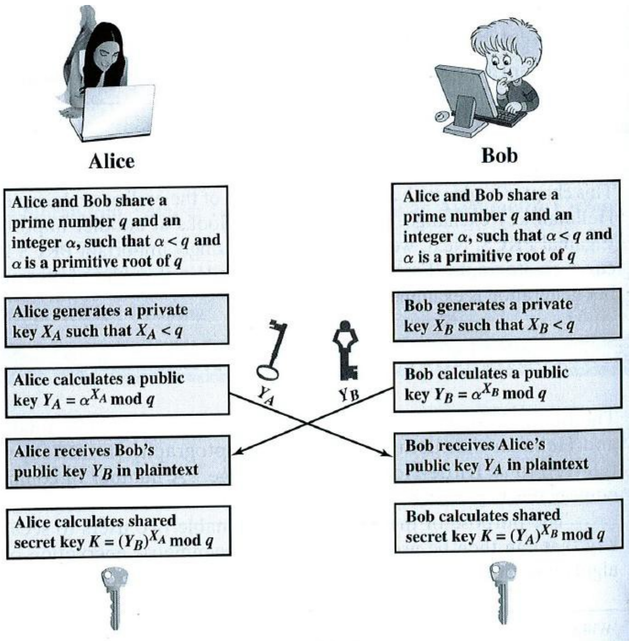
$$d.e = 1 \bmod \phi(n)$$

p =23 q = 37 n = p.q =__________ ϕ(n) = _

e = 5	e = 61
GCD(ϕ(n), e) = GCD(____, 5) $\phi(n) = \qquad = q_1e + r_1 =$ _____________________ $e = 5 = q_2r_1 + r_2 =$ _________________________	GCD(ϕ(n), e) = GCD(, 61) $\phi(n) = \qquad = q_1e + r_1 =$ _____________________ $e = 61 = q_2r_1 + r_2 =$ ________________________

r_1 =_____= $q_3r_2 + r_3$ = ________________________	r_1 =____= $q_3r_2 + r_3$ = ________________________
Back Substitution we get	Back Substitution we get
1 = [e - q_2r_1] $\phi(n)$ = [ ] mod $\phi(n)$	1 = [e - q_2r_1] $\phi(n)$ = [ ] mod $\phi(n)$
1 = [e – q_2 ($\phi(n)$- q_1e)] $\phi(n)$	1 = [e – q_2 ($\phi(n)$- q_1e)] $\phi(n)$
= ________________________________	= ________________________________
= ________________________________	= ________________________________
= ________________________________	= ________________________________
= ________________________________	= ________________________________
= ________________________________	= ________________________________
= ________________________________	= ________________________________
From the above if we want to determine	From the above if we want to determine
d.e = 1 mod $\phi(n)$	d.e = 1 mod $\phi(n)$
where e = 5, then **d =** _____________	where e = 7, then **d =** __________

3. The Diffie-Hellman key exchange algorithm can be defined as follows:



(Image borrowed from Cryptography and Network Security, Stallings, 6^{th} Edition)

Using the above algorithm, can you show that Diffie-Hellman can be subject to a man-in-the-middle attack?

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

   $C = M^e \bmod n$

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

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

   a) p =3; q = 13; e = 5; M = 10

      n = _ ϕ(n) = _ d = _ _

      $C = M^e \bmod n = 10^5 \bmod$ _ =_ M =

      $C^d \bmod n$ =_mod _ =______

   b) p =5; q = 7; e = 7; M = 12

      n = _ ϕ(n) = _ d = _ _

      $C = M^e \bmod n = 12^7 \bmod$ _ =_ M =

      $C^d \bmod n$ =_mod _ =______

   c) p =11; q = 7; e = 11; M = 7

      n = _ ϕ(n) = _ d = _ _

      $C = M^e \bmod n = 7^{11} \bmod$ _ =_ M =

      $C^d \bmod n$ =_mod _ =_______

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 ?

   M =

Homework:

Show that the RSA encryption and decryption functions are inverse operations by trying with some example messages. You can use the package magma online (http://magma.maths.usyd.edu.au/calc/).