COMP90043 Cryptography and Security
Semester 2, 2020, Workshop Week 5 Solutions

Part B: RSA Exercises

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

   parameter: $p = 13$ $q = 7$ $n = p.q = 91$

   a) Using Euler's Totient Function, calculate

      $\phi(n) = \underline{\phi(91) = \phi(7\ .\ 13) = \phi\ (7)\ .\ \phi\ (13) = (7\text{-}1).(13\text{-}1) = 6.12 = 72}$

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

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

Copyright © University of Melbourne 2020

e = 5	e = 7
GCD(ϕ(n), e) = GCD(72, 5) ϕ(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] ϕ(n) = [5 – (2*2)] mod ϕ(n) 1 = [e – q_2 (ϕ(n)- q_1e)] ϕ(n) = [5 – (2*(72-(14*5)))] ϕ(n) = [5 + (-2*(72-(14*5)))] ϕ(n) = [5 +(-2*72 + 2*(14*5))] ϕ(n) = [5 + (-2*72 + 28*5)] ϕ(n) = [5 + 28*5 – 2*72] ϕ(n) = [29*5 – 2*72] ϕ(n) From the above if we want to determine d.e = 1 mod ϕ(n) where e = 5, then **d = 29**	GCD(ϕ(n), e) = GCD(72, 7) ϕ(n) = 72 = $q_1e + r_1$ = 10 * 7 + 2 e = 7 = $q_2r_1 + r_2$ = 3 * 2 + 1 r_1 = 2 = $q_3r_2 + r_3$ = 2 * 1 + 0 Back Substitution we get 1 = [e - q_2r_1] ϕ(n) = [7 – (3*2)] mod ϕ(n) 1 = [e – q_2 (ϕ(n)- q_1e)] ϕ(n) = [7 – (3*(72-(10*7)))] ϕ(n) = [7 + (-3*(72-(10*7)))] ϕ(n) = [7 +(-3*72 + 3*(10*7))] ϕ(n) = [7 + (-3*72 + 30*7)] ϕ(n) = [7 + 30*7 – 3*72] ϕ(n) = [31*7 – 3*72] ϕ(n) From the above if we want to determine d.e = 1 mod ϕ(n) where e = 7, then **d = 31**

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 mod ϕ(n)

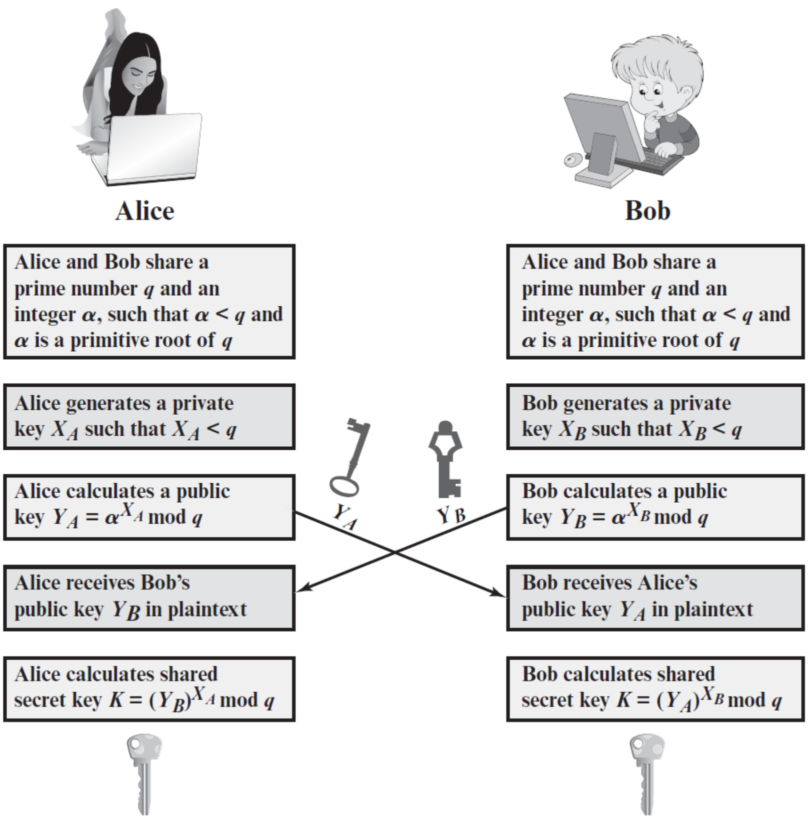
n = p.q = 851 ϕ(n) = 792

e = 5	e = 61
GCD(ϕ(n), e) = GCD(792, 5) ϕ(n) = 792 = $q_1e + r_1$ = 158 * 5 + 2 e = 5 = $q_2r_1 + r_2$ = 2 * 2 + 1	GCD(ϕ(n), e) = GCD(792, 61) ϕ(n) = 792 = $q_1e + r_1$ = 12 * 61 + 60 e = 61 = $q_2r_1 + r_2$ = 1 * 60 + 1

Copyright © University of Melbourne 2020

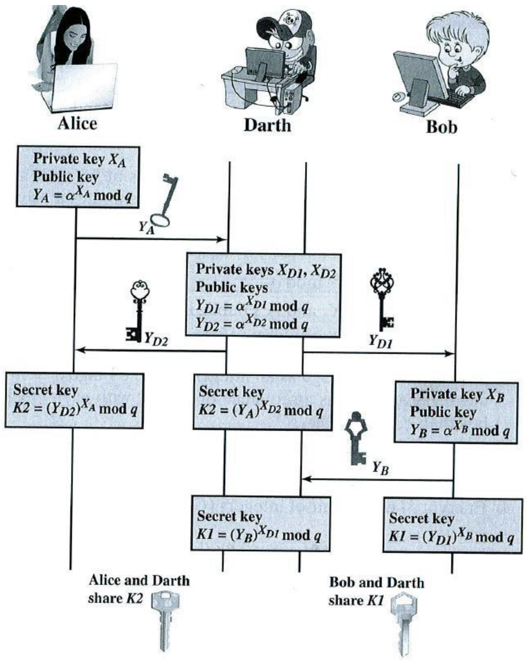
r_1 = 2 = $q_3r_2 + r_3$ = 2 * 1 + 0	r_1 = 60 = $q_3r_2 + r_3$ = 60 * 1 + 0
Back Substitution we get	Back Substitution we get
1 = [e - q_2r_1] ϕ(n) = [5 – (2*2)] mod ϕ(n)	1 = [e - q_2r_1] ϕ(n) = [61 – (1*60)] mod ϕ(n)
1 = [e – q_2 (ϕ(n)- q_1e)] ϕ(n)	1 = [e – q_2 (ϕ(n)- q_1e)] ϕ(n)
= [5 – (2*(792-(158*5)))] ϕ(n)	= [61 – (1*(792-(12*61)))] ϕ(n)
= [5 + (-2*(792-(158*5)))] ϕ(n)	= [61 + (-1*(792-(12*61)))] ϕ(n)
= [5 +(-2*792 + 2*(158*5))] ϕ(n)	= [61 +(-1*792 + 1*(12*61))] ϕ(n)
= [5 + (-2*792 + 316*5)] ϕ(n)	= [61 + (-1*792 + 12*61)] ϕ(n)
= [5 + 316*5 – 2*792] ϕ(n)	= [61 + 12*61 – 1*792] ϕ(n)
= [317*5 – 2*792] ϕ(n)	= [13*61 – 1*72] ϕ(n)
From the above if we want to determine	From the above if we want to determine
d.e = 1 mod ϕ(n)	d.e = 1 mod ϕ(n)
where e = 5, then **d = 317**	where e = 7, then **d = 13**

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.



Copyright © University of Melbourne 2020

A man in the middle attack is possible as shown in the below figure, where an attacker generated two separate keys and then intercepts the communication between Alice and Bob. The communication is compromised as the attacker uses the generated key to convince Alice or Bob that it belong to the other person. When this key is used to establish the connection, what Alice or Bob are actually doing is establishing a connection with the attacker who then is establishing another simultaneous connection to the other person after reading everything sent on the first connection.



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

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

$p = 3;\ q = 13;\ e = 5;\ M = 10;$ $n = 39;\ \varphi(n) = 24; d = 5;$ $C = M^e \, mod \, n = 10^5 \, mod \, 39 = 4;$ $M = C^d \, mod \, n = 4^5 \, mod \, 39 = 10;$	$p = 5;\ q = 7;\ e = 7;\ M = 12;$ $n = 35;\ \varphi(n) = 24; d = 7;$ $C = M^e \, mod \, n = 12^7 \, mod \, 35 = 33;$ $M = C^d \, mod \, n = 33^7 \, mod \, 35 = 12;$
$p = 11;\ q = 7;\ e = 11;\ M = 7;$ $n = 77;\ \varphi(n) = 60; d = 11;$ $C = M^e \, mod \, n = 7^{11} \, mod \, 77 = 7;$ $M = C^d \, mod \, n = 7^{11} mod \, 77 = 7;$	

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?

   To show this, note that we know that $n = 33$, which has only two prime dividers. Therefore, $p = 3$ and $q = 11$. $\varphi(n) = 2 \times 10 = 20$. Using the Extended Euclidean Algorithm, d, the multiplicative inverse of $e \, mod \, \varphi(n) = 11 \, mod \, 20$, is found to be 17. Therefore, we can determine M to be $M = C^d \, mod \, n = 8^{17} \, mod \, 33 = 2$.

Copyright © University of Melbourne 2020