Assignment #3 - RSA Cryptosystem, Diffie-Hellman Key Exchange (Total: 10 points)

name / student id : Kangsan Lee / 20172655

1. (2 points) Perform encryption and decryption using the RSA algorithm for the following. Show all steps.

(a) p = 3, q = 11, e = 7, M = 5 (0.5 points)

(a) $p=3,\ q=11,\ e=7,\ M=5$

$n = pq = 33,\ \varphi(n) = (p-1)(q-1) = 20$

$\gcd(\varphi(n), e) = \gcd(20, 7) = 1$

20	7	2	6	$1 = 7 - 6\times 1$
7	6	1	1	$1 = 7 - (20 - 7\times 2)\times 1 = 7\times 3 - 20\times 1$

Since $M=5,\ e=7,\ d=3,\ n=33$ $\quad 1 = 7\times 3 - 20\times 1 \bmod 20,\ \underline{d=3}$

Encryption : $C = M^e \bmod n = 5^7 \bmod 33 = \underline{14}$

Decryption : $C^d \bmod n = 14^3 \bmod 33 = \underline{5 = M}$

n=33, phi(n)=20, d=3, C=14, Decryption of C is same as M.

(b) p = 5, q = 11, e = 3, M = 9 (0.5 points)

(b) $p=5,\ q=11,\ e=3,\ M=9$

$n = 55,\ \varphi(n) = 40$

$\gcd(\varphi(n), e) = \gcd(40, 3) = 1$

40	3	13	1	$1 = 40 - 3\times 13$

since $M=9,\ e=3,\ d=27,\ n=55$ $\quad 1 = 40 - 3\times 13 \bmod 40 = 3\times 27 \bmod 40$

Encryption : $C = 9^3 \bmod 55 = \underline{14}$ $\quad \therefore \underline{d=27}$

Decryption : $14^{27} \bmod 55 = \underline{9 = M}$

n=55, phi(n)=40, d=27, C=14, Decryption of C is same as M.

(c) p = 17, q = 31, e = 7, M = 2 (1 point)

(c) $p=17,\ q=31,\ e=7,\ M=2$

$n = pq = 527,\ \varphi(n) = 16\times 30 = 480$

$\gcd(\varphi(n), e) = \gcd(480, 7) = 1$

480	7	68	4	$1 = 4 - 3\times 1$
7	4	1	3	$1 = 4 - (7 - 4\times 1)\times 1 = 4\times 2 - 7\times 1$
4	3	1	1	$1 = (480 - 7\times 68)\times 2 - 7\times 1 = 480\times 2 - 7\times 137$

since $M=2,\ e=7,\ d=343,\ n=527$ $\quad 1 = 480\times 2 - 7\times 137 \bmod 480$

Encryption : $C = 2^7 \bmod 527 = \underline{128}$ $\quad = 7\times(-137) \bmod 480 = 7\times 343 \bmod 480$

Decryption : $128^{343} \bmod 527 = \underline{2 = M}$ $\quad \therefore \underline{d = 343}$

n=527, phi(n)=480, d=343, C=128, Decryption of C is same as M.

2. (1 points) In a RSA system, the public key of a given user is e = 31, n = 3599. What is the private key of this user?

2.

$e = 31,\ n = 3599$

$n = pq = 3599$, divide 3599 with $2 \sim \sqrt{3599} \approx 60$, find $p = 59,\ q = 61$

$\varphi(n) = (p-1)(q-1) = 58 \times 60 = 3480$

$\gcd(\varphi(n), e) = \gcd(3480, 31) = 1$,

3480	31	112	8	$1 = 8 - 7 \times 1$
31	8	3	7	$1 = 8 - (31 - 8 \times 3) \times 1 = 8 \times 4 - 31 \times 1$
8	7	1	1	$1 = (3480 - 31 \times 112) \times 4 - 31 \times 1$
				$1 = 3480 \times 4 - 31 \times 449$

private key $d = 3031$

$1 = -31 \times 449 \bmod 3480 = 31 \times 3031 \bmod 3480$

$\therefore d = 3031$

n=pq=59*61,
gcd(phi(n), e)=1, d=3031
the private key(d) is 3031.

3. (2 points) Consider a Diffie-Hellman Key Exchange Scheme with a common prime q = 11 and a primitive root g = 2.

(a) Show that 2 is a primitive root of 11 (1 point)

(a)

$2^1 = 2 \bmod 11 = 2$	$2^5 = 32 \bmod 11 = 10$	$2^9 = 512 \bmod 11 = 6$
$2^2 = 4 \bmod 11 = 4$	$2^6 = 64 \bmod 11 = 9$	$2^{10} = 1024 \bmod 11 = 1$
$2^3 = 8 \bmod 11 = 8$	$2^7 = 128 \bmod 11 = 7$	
$2^4 = 16 \bmod 11 = 5$	$2^8 = 256 \bmod 11 = 3$	$\therefore$ 2 is a primitive root of 11

(b) If user A has public key YA = 9, what is A's private key XA? (0.5 points)

(b)

public key $Y_A = 9$, private key $X_A = ?$

$Y_A = 2^{X_A} \bmod 11 = 9$, $X_A = 6$ $(X_A < q = 11)$

XA=6

(c) If user B has public key YB = 3, what is the shared secret key K, shared with A? (0.5 points)

(c)

public key $Y_B = 3$, shared secret key $K = ?$

$Y_B = 2^{X_B} \bmod 11 = 3$, $X_B = 8$ $(X_B < q = 11)$

$K = 2^{X_A X_B} \bmod 11 = 2^{48} \bmod 11 = 3$

K = 2^(XA*XB) mod11 = 2^48 mod 11 = 3

4. (2 points) Using a spreadsheet (such as Excel), perform the below-mentioned operations. Document results of all intermediate modular multiplications. Determine the number of modular multiplications per major transformation (such as encryption, decryption, primality testing, etc.)

(a) Test all odd numbers in the range from 233 to 241 for primality using the Miller-Rabin test with base 2. (0.5 points)

for(j=0 to k-1), if a^((2^j)*q) mod n = n-1, n is probably prime.												
					2^j (j=0~max(k)-1)				a^((2^j)*q) mod n (j=0~max(k)-1)			
odd int n	**n-1**	**k**	**q**	**a**	**2^0**	**2^1**	**2^2**	**2^3**	**k=0**	**k=1**	**k=2**	**k=3**
233	232	3	29	2	1	2	4	8	1	1	1	
235	234	1	117	2	1	2	4	8	192			
237	236	2	59	2	1	2	4	8	167	160		
239	238	1	119	2	1	2	4	8	1			
241	240	4	15	2	1	2	4	8	233	64	240	1
243	242	1	121	2	1	2	4	8	11			
									if k=0, value==1 or value==n-1 -> n is probably prime.			
									elif k>0, value==n-1 -> n is probably prime.			
									else, n is not a prime number			

233, 239, 241 are probably prime.

(b) Encrypt the message block M = 2 using RSA with the following parameters: e = 23 and n = 233 x 241. (0.5 points)

Q4-(b)	Encrypt the message block M = 2 using RSA with the following parameters: e = 23 and n = 233 x 241.							
M	**e**	**p**	**q**	**n**				
2	23	233	241	56153				
C=M^e mod n								
21811								

C=21811

(c) Compute a private key (d, p, q) corresponding to the given above public key (e, n). (0.5 points)

Q4-(c)	Compute a private key (d, p, q) corresponding to the given above public key (e, n).								
M	**e**	**p**	**q**	**n**	**phi(n)**	**gcd(phi(n), e)**			
2	23	233	241	56153	55680	1			
Dividend	**Divisor**	**Quotient**	**Remainder**						
55680	23	2420	20		1 =	**3-2*1**			
23	20	1	3		1 =	3-(20-3*6)*1 = **3*7-20*1**			
20	3	6	2		1 =	(23-20*1)*7-20*1 = **23*7-20*8**			
3	2	1	1		1 =	23*7-(55680-23*2420)*8 = **23*19367-55680*8**			
					1 =	(23*19367-55680*8) mod 55680			**d=19367**
the private key (d, p, q) is (19367, 233, 241)									

the private key (d, p, q) is (19367, 233, 241).

(d) (0.5 points) Perform the decryption of the obtained ciphertext.

(i) without using the CRT

(i) without using the CRT						
Decryption : M = C^d mod n						
M	**C**	**d**	**n**	**p**	**q**	
2	21811	19367	56163	233	241	
M=21811^19367 mod 56163 = 2						

(ii) using the CRT.

(ii) using the CRT						
M	**C**	**d**	**n**	**p**	**q**	
2	21811	19367	56163	233	241	
dp = d mod (p-1) = 19367 mod 232 =				**111**		
dq = d mod (q-1) = 19367 mod 241 =				**167**		
c1 = c mod p = 21811 mod 233 =				**142**		
c2 = c mod q = 21811 mod 241 =				**121**		
c1^dp mod p = 142^111 mod 233 =				**2**		
c2^dq mod q = 121^167 mod 241 =				**2**		

5. (2 points) We learned about a man-in-the-middle attack on the Diffie-Hellman key exchange protocol in which the adversary generates two public-private key pairs for the attack. Could the same attack be accomplished with one pair? Explain.

I think it's possible to attack by using only one pair of public-private keys generated by attacker. First, the attacker prepares a fake private key(Xt) and computes the corresponding public key(Yt). Then, the attacker intercepts the public keys from both sides(Ya, Yb), transmit Yt to each other. Attacker can calculate two shared secret keys(Ka, Kb) with Xt, Ya, Yb. Each side can calculate the shared secret key with Yt and their own private key.

6. (1 point) RSA is widely used for the public key cryptosystem. There have been many research efforts to enhance the performance of the original RSA (e.g., computational cost, security strength, flexibility, etc.). Investigate one such paper and present its (a) motivation, (b) the encryption and decryption algorithm, and (c) performance.

There is a modified RSA called Dual RSA, which is designed to reduce the memory requirement for keys. The encryption algorithm is same as the standard RSA and decryption is done using the CRT method. Followings are the algorithms for Dual RSA.

Key Generation:

- Select the private exponent d with n_d bit (here $n_d > n/2$)
- Calculate e as inverse of the private exponent that comes out to be very large of the order of the modulus.
- The prime numbers p_1, q_1, p_2, q_2 are chosen such that the private and public exponents (d and e) are same for the two moduli, $N_1=p_1*q_1$ and $N_2=p_2*q_2$.

Thus the parameters generated are e, d, N_1 and N_2. For two instances the public and private exponents are calculated as common for both, resulting in less memory consumption.

Encryption Method

The encryption is done in two parts; part 1 is executed any time when server is offloaded and part 2 is executed when the message is received for encryption. Here the modulus N_1 is shown in the computations.

Part 1

The following statements can be calculated offline (before encrypting the message).

Select R as any random number $R \in Z_n^*$.

Calculate $C'=(R-1)^e \bmod N_1$ and

Calculate $R^{-1} \bmod N_1$

Part 2

To encrypt any plaintext M ,

Calculate $C=M*R^{-1} \bmod N_1$

(C', C) is the required cipher text.

Decryption Method

To decrypt the cipher text (C', C),

Calculate $R=C'^d \bmod N_1+1$

Calculate the message $M=C*R \bmod N_1$

In conclusuion part, the results show that besides less memory consumption, the proposed scheme is efficient in both encryption and decryption sides. the Dual RSA can be used for saving memory as well as computation cost.

https://www.longdom.org/open-access/an-improved-rsa-varian-0976-4860-5-161-169.pdf