USN | | | | | | | | | | |

Internal Assessment Test IV – Feb. 2022

Sub:	**Cryptography**					Sub Code:	**18EC744**	Branch:	**EC**
Date:	**03/02/2022**	Duration:	90 min's	Max Marks:	**50**	Sem / Sec:	**7 A, B, C, D**		OBE

Answer any FIVE FULL Questions

		MARKS	CO	RBT
1	Given $p = 19, q = 23, M = 5\ and\ e = 7$. Use RSA algorithm to find $n, \emptyset(n), d\ and$ Cipher text. Also find the message M from decryption.	**[10]**	CO4	L3
2	Construct the finite field $GF(2^3)$ multiplication table using the polynomial arithmetic modulo $(x^3 + x + 1)$, show the calculation steps	**[10]**	CO4	L3
3	Explain all possible attacking approach on RSA algorithm.	**[10]**	CO4	L1
4	Consider a Diffie Hellman scheme with a common prime $q = 11$ and primitive root $\alpha = 2$ a) Show that 2 is a primitive root of 11. b) If user A has public key $Y_A = 9$, what is $A's$ private key X_A? c) If user B has public key $Y_B = 7$, what is $B's$ private key X_B? d) Find the secret key $K_A\ and\ K_B$.	**[10]**	CO4	L2
5	Consider the elliptic curve defined over $E_{23}(1,1)$. Let $P = (3,10)$ and $Q = (9,7)$. Find $(P + Q)$ and $2P$.	**[10]**	CO4	L2
6	Explain the Man-in-middle attack on Diffie-Hellman algorithm.	**[10]**	CO4	L1

----------All The Best---------

CMR INSTITUTE OF TECHNOLOGY

USN | | | | | | | | | | |

Scheme and Solution of Internal Assesment Test – IV

Sub:	**Cryptography**		Sec	7 A, B, C, D			Code:	**18EC744**
Date:	**03/02/2022**	Duration:	90 mins	Max Marks:	50	Sem: VII	Branch:	ECE

Solution

1 *Given $p = 19, q = 23, M = 5$ and $e = 7$. Use RSA algorithm to find $n, \emptyset(n), d$ and Cipher text. Also find the message M from decryption.* **[10 marks]**

$n = pq = 19 \times 23 = 437$

$\emptyset(n) = (p-1) \times (q-1) = 18 \times 22 = 396$

$e = 3$

$ed \ mod \ \emptyset(n) \equiv 1 \Rightarrow d = e^{-1} \ mod \ \emptyset(n) \Rightarrow d = 7^{-1} \ mod \ 396 \Rightarrow d = -113 \ mod \ 396 =$ **283**

q	r_1	r_2	r	t_1	t_2	$t = t_1 - qt_2$
56	396	7	4	0	1	−56
1	7	4	3	1	− 56	57
1	4	3	1	−56	57	−113
3	3	1	0	57	− 113	396
	1	0		**−113**	396	

$PU = \{7,437\}$ *and* $PR = \{283,437\}$

$C = M^e \ mod \ n \Rightarrow C = 5^7 mod \ 437 = 339$

$M = C^d \ mod \ n = 339^{283} \ mod \ 437 = 5$

$339^{283} \ mod \ 437$

$(283)_{10} = (100011011)_2$

$1: 339 \ mod \ 437 = 339$

$0: (339)^2 \ mod \ 437 = 427$

$0: (427)^2 \ mod \ 437 = 100$

$0: (100)^2 \ mod \ 437 = 386$

$1: (386)^2 \times 339 \ mod \ 437 = 310$

$1: (310)^2 \times 339 \ mod \ 437 = 424$

$0: (424)^2 \ mod \ 437 = 169$

$1: (169)^2 \times 339 \ mod \ 437 = 7$

$1: (7)^2 \times 339 \ mod \ 437 = 5$

2 *Construct the finite field $GF(2^3)$ multiplication table using the polynomial arithmetic modulo $(x^3 + x + 1)$, show the calculation steps* **[10 marks]**

×		**000**	**001**	**010**	**011**	**100**	**101**	**110**	**111**
		000	**1**	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
000	**0**	000 0	000 0	000 0	000 0	000 0	000 0	000 0	000 0
001	**1**	000 0	001 1	010 x	011 $x+1$	100 x^2	101 x^2+1	110 x^2+x	111 x^2+x+1
010	x	000 0	010 x	100 x^2	110 x^2+x	011 $x+1$	001 1	111 x^2+x+1	101 x^2+1
011	$x+1$	000 0	011 $x+1$	110 x^2+x	101 x^2+1	111 x^2+x+1	100 x^2	001 1	010 x
100	x^2	000 0	100 x^2	011 $x+1$	111 x^2+x+1	110 x^2+x	010 x	101 x^2+1	001 1
101	x^2+1	000 0	101 x^2+1	001 1	100 x^2	010 x	111 x^2+x+1	011 $x+1$	110 x^2+x
110	x^2+x	000 0	110 x^2+x	111 x^2+x+1	001 1	101 x^2+1	011 $x+1$	010 x	100 x^2
111	x^2+x+1	000 0	111 x^2+x+1	101 x^2+1	010 x	001 1	110 x^2+x	100 x^2	011 $x+1$

[10 marks]

.

	×	000	001	010	011	100	101	110	111
		0	1	2	3	4	5	6	7
000	0	0	0	0	0	0	0	0	0
001	1	0	1	2	3	4	5	6	7
010	2	0	2	4	6	3	1	7	5
011	3	0	3	6	5	7	4	1	2
100	4	0	4	3	7	6	2	5	1
101	5	0	5	1	4	2	7	3	6
110	6	0	6	7	1	5	3	2	4
111	7	0	7	5	2	1	6	4	3

(b) Multiplication

3 *Explain all possible attacking approach on RSA algorithm.* **[10 marks]**

There are 5 possible approaches to attack the RSA algorithms. Those are:

a) Brute-Force attack
b) Mathematical Attack
c) Timing Attack
d) Hardware Fault based Attack
e) Chosen Cipher text attack

a) **Brute-Force attack:** This means trying with all possible private keys. The defence against the brute force approach is similar like other algorithm i.e. to use a larger key size. But larger key size slower the system as the encryption/ decryption are complex.

b) **Mathematical Attack:** There are 3 approaches to attack RSA mathematically

(i) Factor $'n'$ into its 2 prime factors. This enables calculating $\emptyset(n) = (p-1) \times (q-1)$, which in turn enables determination of $d = e^{-1} \, mod \, \emptyset(n)$

(ii) Determine $\emptyset(n)$ directly, without first determining $p \; and \; q$, which enables determination of $d = e^{-1} \, mod \, \emptyset(n)$

(iii) Determine d directly, without first determining $\emptyset(n)$

For a large $'n'$ with large prime factors, factoring is a hard problem, but it is not as hard as it used to be.

History:

a) In 1977 the 3 inventors of RSA gave one challenge to decode a cipher, they printed in Mertine Gardner's 'Mathematical Game" Column. They offered $100 rewards for the return of a plaintext sentence. In April 1994, a group claimed the prize after only 8 months of work.
b) Now a day's these factorization can be done using
   (i) General Number Field Sieve (GNFS)
   (ii) Special Number Field Sieve (SNFS)
c) Thus we need to be careful in choosing a key size for RSA
d) The team that produced the 768-bit factorization made the following observation:
   (i) Factoring a 1024 bit RSA modulus would be thousand times harder than factorizing a 768 bit modulus. Hence 1024 bit RSA can be used for another three to four years.
   (ii) They suggested few points to avoid the value of $'n'$ being factorized more easily.
   A) $p \; and \; q$ should differ in length but only few digits.
   B) Both $(p-1) \; and \; (q-1)$ contains a large prime factor.
   C) $GCD(p-1, q-1)$ should be small.

[10 marks]

c) **Timing Attack:**

(i) Paul Kocher, a cryptographic consultant, demonstrated that a cryptanalyst can determine a private key by keeping track of how long a computer takes to decipher the message.
(ii) It has been observed that processing '1' takes longer time than '0'. Hence like fashion the entire key can be predicted.
(iii) Though timing attack is a serious threat, this can be counter measured in the following ways.
1) Constant Exponentiation Time: Ensure it takes same amount of time. This is a simple fix but degrades the performance

2) Random Delay: a random delay is added to confuse the timing attack.
3) Blinding: Multiply the cipher text by a random number before performing the exponentiation.

d) Hardware Fault based Attack: In this method, the attacker includes faults in the signature computation by reducing the power of the processor. This fault causes the software to produce invalid signatures, which can then be analysed by the attacker to recover the private key. This type of attack is not considered as a serious threat to RSA, because it requires that the attacker should have physical access to the target machine.

e) Chosen Cipher text attack

(i) RSA Algorithm is more vulnerable to chosen cipher text attack (CCA).

(ii) As we know in chosen cipher text attack, the cryptanalyst can choose the number of cipher text and get it decrypted with the target's private key. Means, the cryptanalyst can select a plaintext and find the cipher text using target's public key and then able to get the same plaintext back.

(iii) It is clearly observed, the cryptanalyst doesn't get any new information but it exploits the properties of RSA. It can be better explained with an example:
$E(PU, M_1) \times E(PU, M_2) = E(PU, [M_1 \times M_2])$
$Compute\ X = (C \times 2^e) mod\ n$
$X\ is\ a\ chosen\ cipher\ text\ and\ receive\ back\ Y = X^d\ mod\ n$
$X = (C\ mod\ n) \times (2^e\ mod\ n) = (M^e\ mod\ n) \times (2^e\ mod\ n) = (2M)^e\ mod\ n$
Hence from $2M$ it is easy to deduce M

To overcome this optimal asymmetric encryption padding (OAEP) is used. In this method, the message to be encrypted is padded.

4 *Consider a Diffie Hellman scheme with a common prime $q = 11$ and primitive root $\alpha = 2$*

a) Show that 2 is a primitive root of 11.

b) If user A has public key $Y_A = 9$, what is A's private key X_A? **[10 marks]**

c) If user B has public key $Y_B = 7$, what is B's private key X_B?

d) *Find the secret key K_A and K_B.*

Ans $q = 11$ *and* $\alpha = 2$
$\alpha = 2$ is the primitive root of 11

$2^1\ mod\ 11 = 2$	$2^6\ mod\ 11 = 9$
$2^2\ mod\ 11 = 4$	$2^7\ mod\ 11 = 7$
$2^3\ mod\ 11 = 8$	$2^8\ mod\ 11 = 3$
$2^4\ mod\ 11 = 5$	$2^9\ mod\ 11 = 6$
$2^5\ mod\ 11 = 10$	$2^{10}\ mod\ 11 = 1$

[2 marks]

+

$Y_A = \alpha^{X_A}\ mod\ q \Rightarrow\ 9 = 2^{X_A}\ mod\ 11 \Rightarrow\ X_A = 6$
$Y_B = \alpha^{X_B}\ mod\ q \Rightarrow\ 7 = 2^{X_B}\ mod\ 11 \Rightarrow\ X_B = 7$

[8 marks]

$K_A = {Y_B}^{X_A}\ mod\ q \Rightarrow\ K_A = 7^6\ mod\ 11 = 117649\ mod\ 11 = 4$
$K_B = {Y_A}^{X_B}\ mod\ q \Rightarrow\ K_B = 9^7\ mod\ 11 = 4$

$K_A = K_B = 4$

5 *Consider the elliptic curve defined over $E_{23}(1,1)$. Let $P = (3,10)$ and $Q = (9,7)$. Find $(P + Q)$ and $2P$.* **[10 marks]**

$\Delta = \left(\frac{y_Q - y_p}{x_Q - x_P}\right) mod\ p \Rightarrow \Delta = \left(\frac{7-10}{9-3}\right) mod\ 23 = \left(\frac{-3}{6}\right) mod\ 23 = \left(\frac{-1}{2}\right) mod\ 23 = 11$
$x_R = \left(\Delta^2 - x_P - x_Q\right) mod\ p = (11^2 - 3 - 9) mod\ 23 = 109\ mod\ 23 = 17$
$y_R = (\Delta(x_P - x_R) - y_P)\ mod\ p = (11(3-17) - 10) mod\ 23 = -164\ mod\ 23 = 20$
$P + Q = (17,20)$

[10 marks]

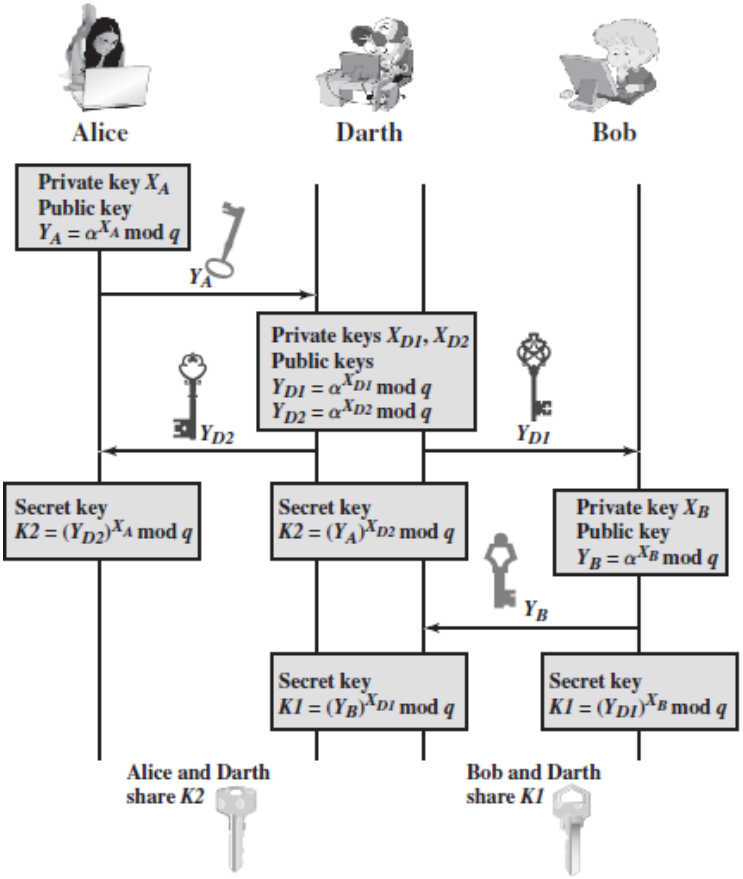
$\Delta = \left(\frac{3{x_P}^2 + a}{2y_P}\right)\ mod\ p = \left(\frac{3(3^2)+1}{2 \times 10}\right) mod\ 23 = \left(\frac{5}{20}\right) mod\ 23 = \left(\frac{1}{4}\right) mod\ 23 = 4^{-1} mod 23 = 6$

q	r_1	r_2	r	t_1	t_2	$t = t_1 - qt_2$
5	23	4	3	0	1	-5
1	4	3	1	1	-5	6
3	3	1	0	-5	6	-23
	1	0		6	-23	

$x_R = (\Delta^2 - 2x_P) \ mod\ p = (6^2 - 2 \times 3) \ mod\ 23 = 30 \ mod\ 23 = 7$
$y_R = (\Delta(x_P - x_R) - y_P) \ mod\ p = (6(3-7) - 10) \ mod\ 23 = (-34) \ mod\ 23 = 12$
$2P = (7,12)$

6 *Explain the Man-in-middle attack on Diffie-Hellman algorithm.* **[10 marks]**

Ans **MAN-IN-MIDDLE ATTACK:** **[10 marks]**



Man-in-the-Middle Attack

a) Diffie Hellman Algorithm is insecure against man in middle attack.
b) <u>The attack proceeds as follows:</u>
   (1) Darth prepare for the attack by generating 2 random key X_{D_1} *and* X_{D_2} and computes its corresponding private key Y_{D_1} *and* Y_{D_2}.
   (2) Alice sends Y_A to Bob.
   (3) Darth intercepts Y_A and transmits Y_{D_1}. Darth also calculate the $K_2 = (Y_A)^{X_{D_2}} \ mod\ q$
   (4) Bob receives Y_{D_1} and calculate $K_1 = \left(Y_{D_1}\right)^{X_B} \ mod\ q$
   (5) Bob transmits the Y_B to Alice.
   (6) Darth intercepts Y_B and transmits Y_{D_2} to Alice and Darth calculate $K_1 = (Y_B)^{X_{D_1}} \ mod\ q$
   (7) Alice receives Y_{D_2} and calculate $K_2 = \left(Y_{D_2}\right)^{X_A} \ mod\ q$
   (8) At this point, Bob and Alice think that they share a secret key, but instead Bob and Darth shared secret key K_1 and Alice and Darth shared the secret key K_2. All the future communication between Bob and Alice is compromised.