

## Question 2

a) (i) The RSA scheme has since that time reigned supreme as the most widely accepted and implemented approach to public-key encryption. Diffie-Hellman key exchange is to enable two users to exchange a secret key securely. Perform encryption and decryption using the RSA algorithm as in Figure 1, for the following:

$p = 3; q = 17, e = 5; M = 5;$

[Note: MUST show the workings of calculation to prove the answer is correct. ]  
(8 marks)

$$(a)(ii) \quad p=3, q=17, e=5, M=5$$

$$\text{Encryption} \Rightarrow C = M^e \pmod{n}$$

$$\begin{aligned} n &= p \times q \\ &= 3 \times 17 \\ &= 51 \end{aligned}$$

$$\begin{aligned} C &= 5^5 \pmod{51} \\ &= 3125 \pmod{51} \\ &= 14 \end{aligned}$$

$$\text{Decryption} \Rightarrow M = C^d \pmod{n}$$

$$\begin{aligned} \phi(n) &= (p-1)(q-1) \\ &= (17-1)(3-1) \\ &= 16 \times 2 \\ &= 32 \end{aligned}$$

$$\begin{aligned} d(5) \pmod{32} &= 1 \\ (13 \times 5) \pmod{32} &= 1 \end{aligned}$$

$$\therefore d = 13$$

$$\begin{aligned} M &= 14^{13} \pmod{51} \\ &= 5 \end{aligned}$$

a) (ii) The RSA scheme has since that time reigned supreme as the most widely accepted and implemented approach to public-key encryption. Diffie-Hellman key exchange is to enable two users to exchange a secret key securely. Perform encryption and decryption using the RSA algorithm as in Figure 1, for the following:

$p = 11$ ;  $q = 13$ ,  $e = 11$ ;  $M = 7$ ;

[Note: MUST show the workings of calculation to prove the answer is correct.]  
(8 marks)

$$(a)(ii) \quad p=11, q=13, e=11, M=7$$

$$\begin{aligned} n &= pq \\ &= 11 \times 13 \\ &= 143 \end{aligned}$$

$$\begin{aligned} C &= M^e \pmod{n} \\ &= 7^{11} \pmod{143} \\ &= 106 \end{aligned}$$

$$\begin{aligned} \phi(n) &= 10 \times 12 \\ &= 120 \end{aligned}$$

$$\begin{aligned} d(11) \pmod{120} &= 1 \\ (11 \times 11) \pmod{120} &= 1 \\ (21 \pmod{120}) &= 1 \\ \therefore d &= 11 \end{aligned}$$

$$\begin{aligned} M &= C^d \pmod{n} \\ &= 106^{11} \pmod{143} \\ &= 7 \end{aligned}$$

b) (i) Consider a Diffie-Hellman scheme with a common prime  $q = 23$  and a primitive root  $\alpha = 5$ . Use the Diffie-Hellman Key Exchange Algorithm, as shown in Figure 2 for the following: Alice has public key  $Y_A = 10$ , what is Alice's private key  $X_A$ ?

[Note: MUST show the workings of calculation to prove the answer is correct.]

(3



b) (ii) Use the Diffie-Hellman Key Exchange Algorithm, as shown in Figure 2 for the following: Bob has public key  $Y_B = 8$ , what is the shared secret key  $K$ ?

[Note: MUST show the workings of calculation to prove the answer is correct.]

(6



(b) (i)  $q = 23, \alpha = 5, Y_A = 10, X_A = ?$

$$10 = 5^{X_A} \mod 23$$

$$10 = 5^3 \mod 23$$

$$X_A = 3$$
  

(ii)  $Y_B = 8$

$$\left[ \begin{array}{l} K = (Y_B)^{X_A} \mod q \\ = 8^3 \mod 23 \\ = 6 \end{array} \right] \quad \left[ \begin{array}{l} K = (Y_A)^{X_B} \mod q \\ = 10^6 \mod 23 \\ = 6 \end{array} \right]$$
  

$$Y_B = \alpha^{X_B} \mod q$$

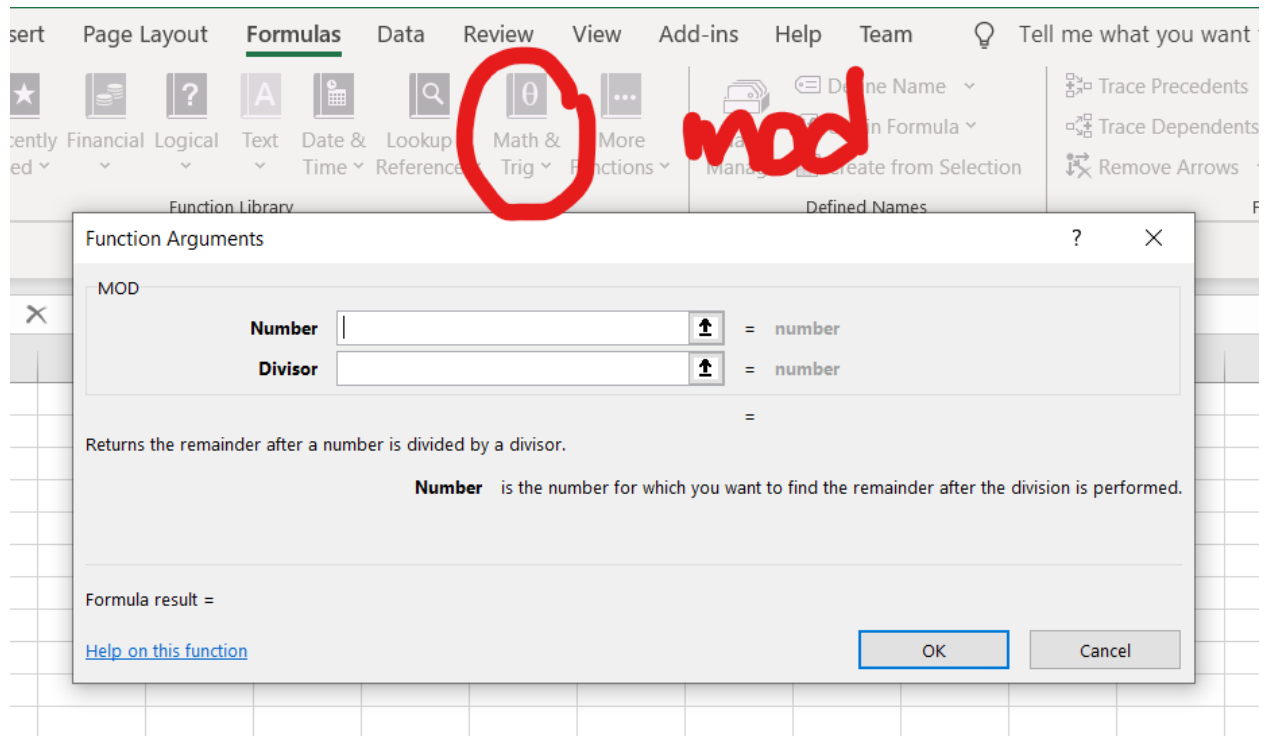
$$8 = 5^{X_B} \mod 23$$

$$X_B = 6$$
  

use excel

1. At the ribbon, choose Formulas
2. Choose Math & Trig
3. Scroll down to find mod
4. Click & it will come out a dialog to input Number & Divisor

## Excel (mod function)



#### Question 4

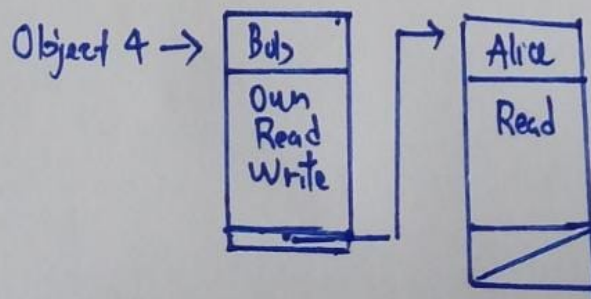
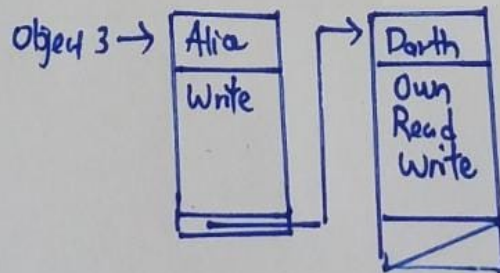
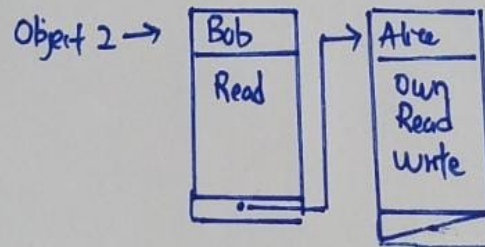
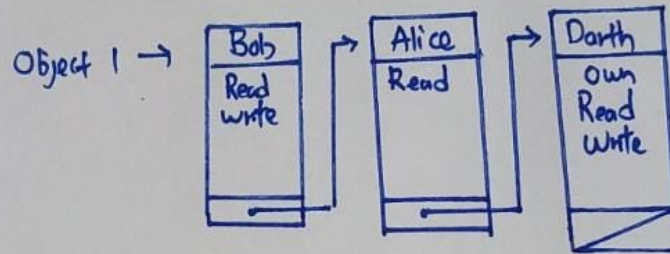
(ii)

Control Access Matrix

	Object 1	Object 2	Object 3	Object 4
Bob	Read Write	Read		Own Read Write
Alice	Read	Own Read Write	Write	Read
Darth	Own Read Write		Own Read Write	

(iii)

### Access Control List





OCT May 2021

1. Sub bytes  
(Using S-box)

09	36	40	82
6A	A5	7C	9B
D5	38	E3	2F
30	BF	39	FF

Sub Bytes



01	05	09	13
02	06	10	14
03	07	11	15
04	08	12	16

2. Shift Rows  
(Left rotate each row  
by 0,1,2,3 bytes  
respectively)

01	05	09	13
02	06	10	14
03	07	11	15
04	08	12	16

Shift Rows



01	05	09	13
06	10	14	02
11	15	03	07
16	04	08	12