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

Encryption $\Rightarrow C = M^e \pmod n$

$n = p * q$
$= 3 \times 17$
$= 51$

$C = 5^5 \bmod 51$
$= 3125 \bmod 51$
$= 14$

Decryption $\Rightarrow M = C^d \pmod n$

$\phi(n) = (p-1)(q-1)$
$= (17-1)(3-1)$
$= 16 * 2$
$= 32$

$d(5) \bmod 32 = 1$
$(13 * 5) \bmod 32 = 1$

$\therefore d = 13$

$M = 14^{13} \bmod 51$
$= 5$

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

$n = pq$
$= 11 \times 13$
$= 143$

$C = M^e \pmod n$
$= 7^{11} \bmod 143$
$= 106$

$\phi(n) = 10 \times 12$
$= 120$

$d(11) \bmod 120 = 1$
$(11 * 11) \bmod 120 = 1$
$121 \bmod 120 = 1$
$\therefore d = 11$

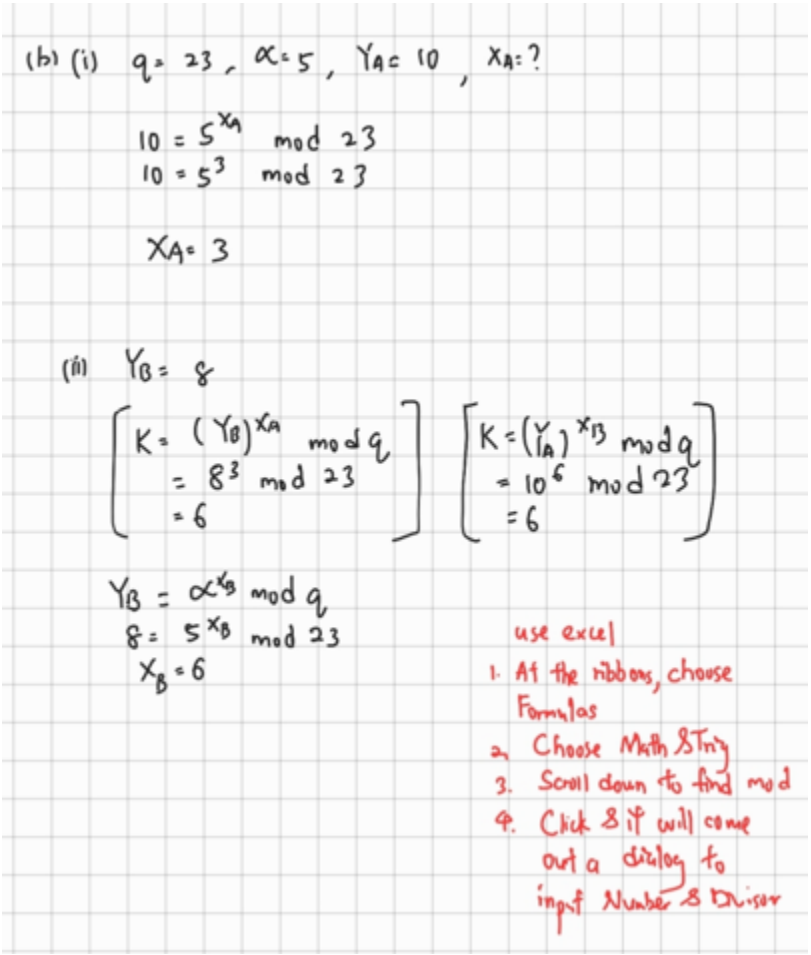
$M = C^d \pmod n$
$= 106^{11} \bmod 143$
$= 7$

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

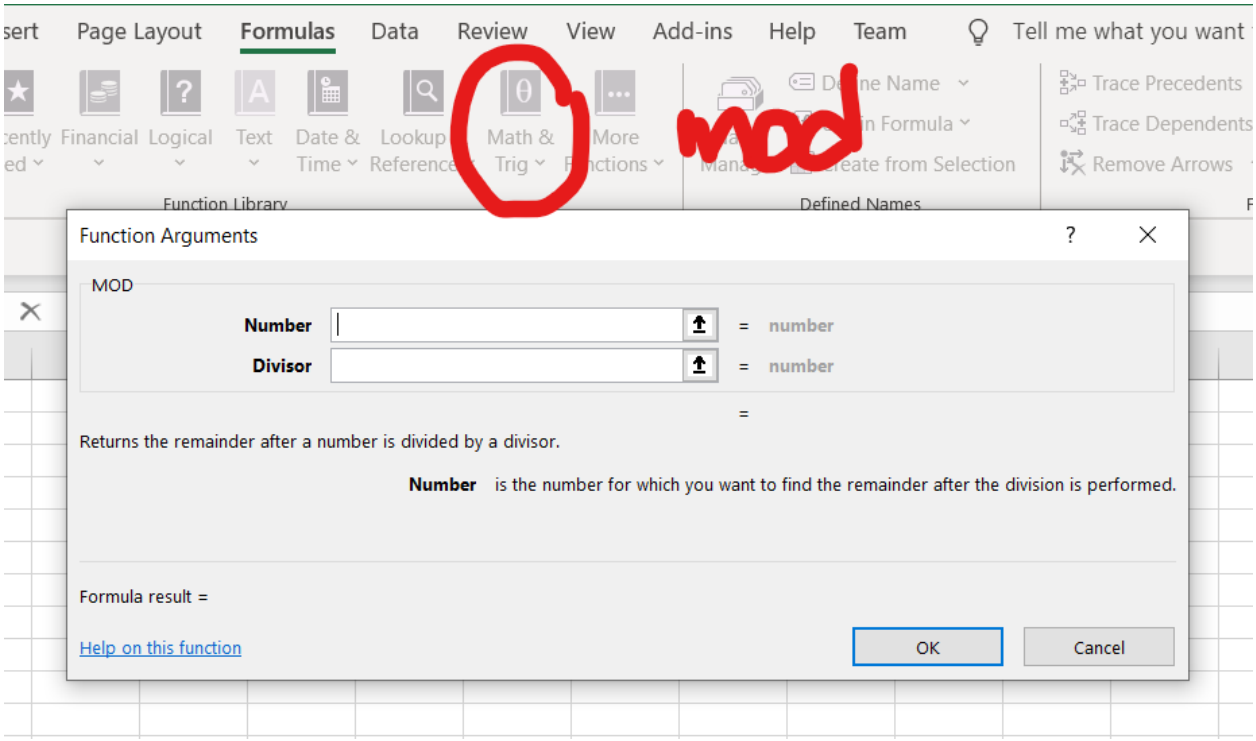
[Note: MUST show the workings of calculation to prove the answer is correct.] (3 marks)

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

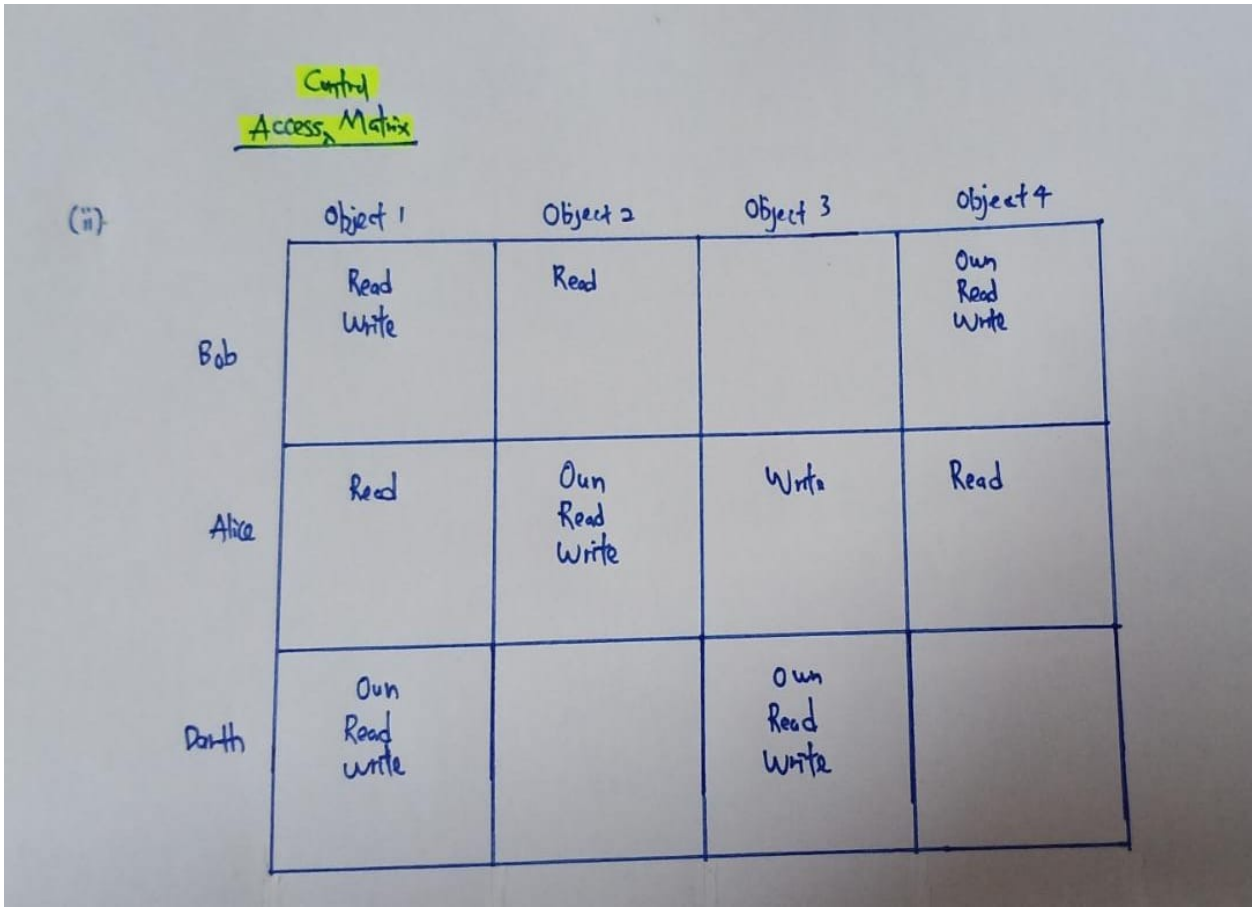
[Note: MUST show the workings of calculation to prove the answer is correct.] (6 marks)



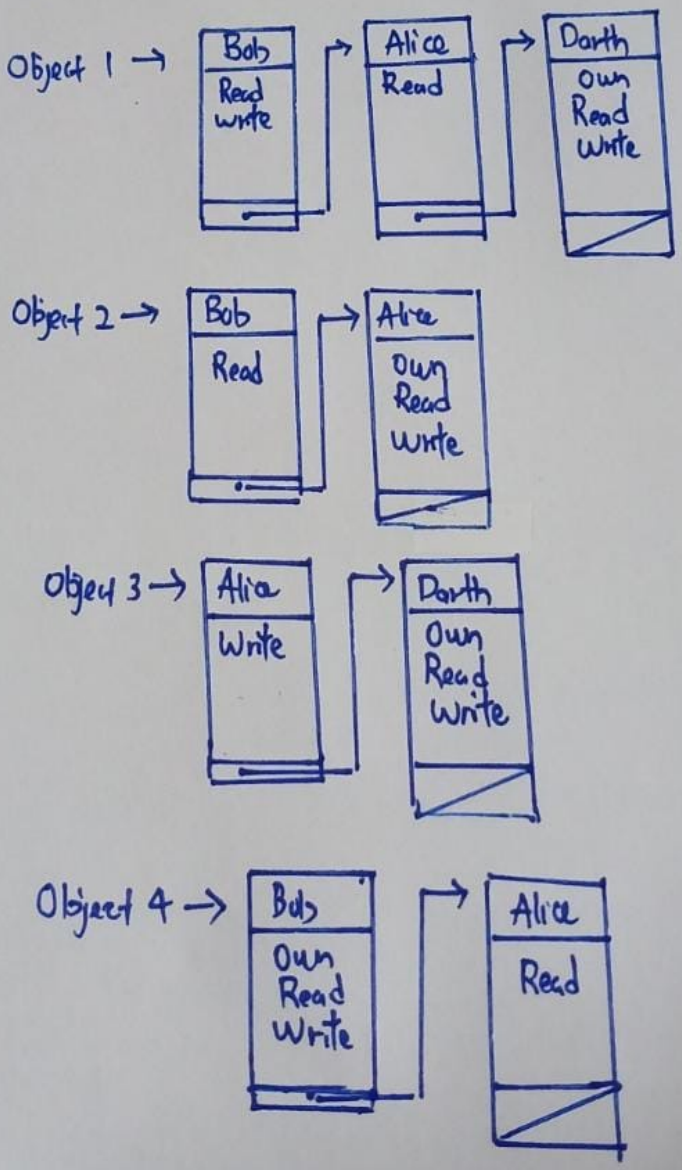
Excel (mod function)

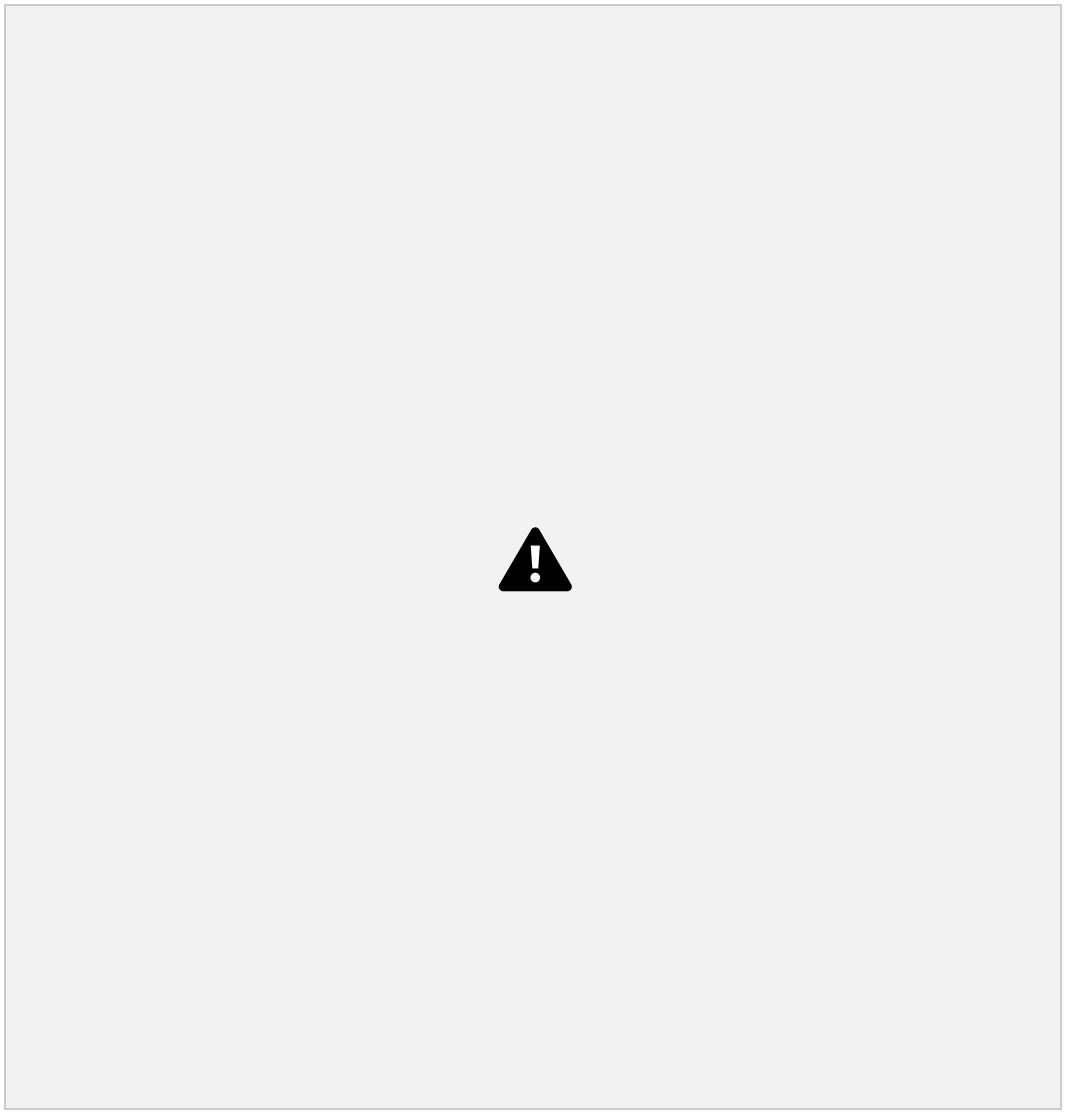


Question 4


Control Access Matrix
(ii)
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