Issa
Odeh

1.

a) $p = 467$, $\bar{a} = 2$, $a = 3$, $b = 5$

Alice sends key to Bob

$A = \bar{a}^{a} \bmod p$
$= 2^3 \bmod 467$
$= 8 \bmod 467$
$= 8$

Bobs send key to Alice

$B = \bar{a}^{b} \bmod p$
$= 2^5 \bmod 467$
$= 32 \bmod 467$
$= 32$

Shared key for both

$k = \bar{a}^{ab} \bmod p$
$= 2^{15} \bmod 467$
$= 32768 \bmod 467$
$= 78$

Shared key Recieved from bob

$k_a = B^a \bmod p$
$= 32^3 \bmod 467$
$= 32768 \bmod 467$
$= 78$

Shared key Recieved from Alice

$k_b = 8^5 \bmod p$
$= 32768 \bmod 467$
$= 78.$

$P = 467$, $\bar{a} = 2$, $a = 400$, $b = 134$

b).

Alice send key to Bob

$A = \bar{a}^{a} \bmod p$
$= 2^{400} \bmod 467$
$= 137$

Bobs sends key to Alice

$B = a^b \bmod p$
$= 2^{134} \bmod 467$
$= 64$

Shared key for both

$k = \bar{a}^{ab} \bmod p$
$= 2^{400 \times 134} \bmod 467$
$= 90$

Shared key Recieved by bob

$k_a = B^a \bmod p$
$= 64^{400} \bmod 467$
$= 90$

Shared key Recived by Alice

$k_b = 137^{134} \bmod 467$
$= 90$

c.) $p = 467$, $\bar{a} = 2$, $a = 228$, $b = 57$

Alice sends key to Bob

$= 2^{228} \mod 467$

$= 394$

Bobs send key to Alice

$= 2^{57} \mod 467$

$= 313$

Shared key for both

$K = \bar{a}^{ab} \mod p$

$= 2^{228 \times 57} \mod 467$

$= 206$

Shared key Recieved by Bob

$= 313^{228} \mod 467$

$= 206$

Shared key Recieved by Alice

$= 394^{57} \mod 467$

206

2. $q = 467$, $a = 2$, $x = 105$, $k = 213$, $m = 33$

Bobs side:

$B = 2^{105} \mod 467$

$= 444$

Alice public key:

$K_E = 2^{213} \mod 467$

$= 29$

Alice creates a mask

$k_m = 444^{213} \mod 467$

$= 292$

Then Alice encrypts date

$y = x \cdot k_m \mod p$

$= 33 \times 292 \mod 467$

$= 9636$

Public key now sent to bob

$k_m = k_E^{d} \mod p$

$= 29^{105} \mod 467$

$= 292$

Bobs decrypts cipher text

$x = y \cdot k_m^{-1} \mod p$

$= 9636 \cdot 292^{-1} \mod p$

$\boxed{\text{Decrypted} = 33}$

b) $q = 467$, $a = 2$, $x = 105$
k, 123, $M = 33$

Bobs side:

$2^{105} \bmod 467$

$B = 444$

Alice side:

$k_E = 2^{123} \bmod 467$

$= 125$

Alice creates mask for message:

$k_m = 444^{123} \bmod 467$

$= 278$

Alice encrypts data

$y = 33 \cdot 278 \bmod 467$

$= 9174$

public key sent to bob

$k_m = 125^{105} \bmod 467$

$= 278$

Then, bob decrypts ciph text

$x = 9636 \cdot 278^{-1} \bmod 467$

$\boxed{= 33}$

c). $q = 467$, $a = 2$, $x = 105$
$k = 45$, $M = 248$

Bobs side:

$2^{300} \bmod 467$

$= 317$

Alice side:

$K_E = 2^{45} \bmod 467$

$= 80$

Alice creates mask for message:

$K_m = 317^{45} \bmod 467$

$= 12$

Alice encrypts data:

$y = 248 \cdot 12 \bmod 467$

$= 2976$

Then, bob decrypts ciphertext

$x = 2976 \cdot 12^{-1} \bmod 467$

$\boxed{= 248}$

2). $q = 467$, $a = 2$, $X = 300$, $k = 47$, $M = 248$

Bobs Side:

$B = 2^{300} \bmod 467$
$= 317$

Alice Side
$= 2^{47} \bmod 467$
$= 320$

Alice Creats mask for message:
$K_m = 317^{47} \bmod 467$
$= 74$

Alice encrypts data
$Y = 248 \cdot 74 \bmod 467$
$= 18352$

Then, Bob decrypts the cipher text:
$X = 18352 \cdot 74^{-1} \bmod 467$
$\boxed{= 248}$

3). one secure way aganist a MTM attack is to encrypt the Diffie - Hellman value with the other side public key. All keys are store on a server and are safe. So No, it is not vulnerable.

7.

a)

y	y^2	$y^2 \bmod 11$
0	0	0
1	1	1
2	4	4
3	9	9
4	16	5
5	25	3
6	36	3
7	49	5
8	64	9
9	81	4
10	100	1

x	x^3+x+6	$(x^3+x+6) \bmod 11$	y_1	y_2
0	6	6	none	none
1	8	8	none	none
2	16	5	4	7
3	36	3	5	6
4	74	8	none	none
5	136	4	2	9
6	228	8	none	none
7	356	4	2	9
8	526	9	3	8
9	744	7	none	none
10	1016	4	2	9

points are : (2, 4), (2, 7), (3, 5), (3, 6), (5, 2), (5, 9)
(7, 2), (7, 9), (8, 3), (8, 8), (10, 2), (10, 9)

b. $y^2 = x^3 + x + 6 \pmod{11}$

13 $P = (x_3, y_3)$

$\lambda = \frac{3x^2 + a}{2y_1} = \frac{3(2)^2 + 1}{2 \times 4} = \frac{13}{8} \pmod{11} = 5$

$x_3 = \lambda^2 - x_1 - x_2$

$= 5^2 - 2 - 2$

$= 21$

$21 \bmod 11 = 10$

$y_3 = \lambda(x_1 - x_3) - y_1$

$= 5(2 - 10) - 4$

$= -40 - 4$

$= -44$

$= -44 \bmod 11 = 0$

So, $P(2, 4) = (10, 0)$

c). $P(\underset{x_1}{2}, \underset{y_1}{4})$ and $Q(\underset{x_2}{2}, \underset{y_2}{7})$

$m = \frac{7 - 4}{2 - 2} = \frac{3}{0} = \infty$