	I SSa
	Odeh
(C .	Shared key for both
a)	2 1/4
. ~	P=467, a=2, a=3, 0=3 k=aab mo & P Alice sends key to Bob = 215 moz 467
	Alice sends key to Bob = 215 mod 467
	$A = a^{2} \mod p$ = $32769 \mod 467$ = $2^{3} \mod 467$ = 78
	= 8 mod 461
	= 8 Shalle Cey Recipie from bob
	Ka-Ba moèp
	Bobs send key to Alice = 323 mod 467
	8 = a 6 m 0 2 p
	= 25 moz 467 = 78
	= 32 mo & 467
	232 Share key Recivit from 4/16
-600	Fb= 85 mod P
	= 3267 mo 1 467
	278.
6).	12=467, a= 2, a= 400, b=134
0)	Alice sent key to Bob Shared key for both
	A = a = a mo > P
	= 2400 mo 2 467 = 2400 x 134 moz 467
	= 137
	Bobs sink lery to Alice Shalle key Recieved by bob B = ab mod P - 2134 mod 467 = 44400 mod 467 = 40
	B= ab mod P 167 = 84 mod P = 44400 mod 467 = 90
	- 2134 mod 467 = 44400 mod 467
	= 64
MIL	
100	Sharp ley Recitably Alice 16/05/137/34 moly 467
	= 90
	2 10
1	
The State of the last	

	1 ch as kay 5 c hoth
) p=467, a=2, a=228, b	57 Shared Key For both K= aab mod P
Als a No Ken La	
Alice sends key to B	= 206
= 394	-00
= 3.1	Shared try Recipied by 806
Bobs sind key to Al	14 = 3 1328 mod 467
= 257 MOZ 467	= 206
3 313	Ve
The second secon	Share key Recieved by Alice
	39457 mod 467
	206
9= 467 a= 2, x=105	1) Alice Crates a mask
K= 213, m= 83	Km = 444213 moz 467
	292
Bobs side:	
B = 2105 mod 467	Then Alice energy's late
= 444	V= x 1/m mod P
	= 33 x 7 92 mor 467
Alice public key:	= 9 636
KE = 2213 mod 467	
= 29	I Public key now sent to bob
	Kn= 1 K= 1 mod P
	= 2 9 las mod 467
	= 292
	Boto declypts cipher text
	1- y. Km mod P = 9636.292-1 mod P
	= 9636.292-1 mod P
	Decryptic = 33

0	Alice encipts data
6)	9=467, 9=2, X= 105 Y=33.278 mod 467
V	$k_{123} M_{233} = 9174$
	Bobs side: public key sent to bob
	2 105 moè 467 Km= 125 105 moè 467
	B = 444 = 278
	Alice side: Then, bob deciyers ciph fort
	K = 2123 mod 467 X = 9636. 278 mod 467
	= 125
	Alice Creates Mask for
	message: Km= 444123 mod 467
	Km= 444123 mod 467
	= 278
1)	
().	9=467, a=2, x=105
1	1'= 415, M= 248
	and and and set a day
	Bobs site: Alice enclypts data;
	= 317 Y= 248.12 MOd 467 = 2976
	- 317
	Alice side: Then, bob decrypts ciphertext
	K = 245 mg 4/67 X = 2976. 12-1 mo & 4/67
	$K_{2} = 2^{45} \text{ mps 4/67}$ $X = 2976. 2^{-1} \text{ mo } 64/67$ $= 248$
	Alice (18475 MADE FOI
100	m185a91;
100	Kun 317 15 mar 467
	m185age: Km= 31745 mor 467

12). 9=467, a= 4 1=300, K=47, M=248 Bobs Side: Alice encrypts data B= 2300 mod 467 12 248. 74 mod 467 = 317 218382 Alice Side Then, Bob Eccrypts the = 247 mo & 467 cipher tex: X= 18352, 74-1 mod 467 = 320 1-248 Alice Clasts mask for M155 age: Km = 31747 Mod 467 - 74 one secure way aganista MTM attack is to encrypt the Diffie - Hellman value with the other six Public Key. All keys are store on a sourt and are safe. So No, it is not vulnerable.

					1
1,					
27 Y	12 12 M	02 1/			
6	0 0				
1-1-	4 4	1 - 1 - 1			
3	9 9				
1	16 5				
15	25 3				
6	36 3				
17	The same of the sa				
8	64 9				
9	814		- v- v- v	V = 1 (10 - x	
10	100 1				
<u> </u>	2				
X	13 t X + 6	(x3+x+6)mod 11	4,	1/2	
	,		38 18 60	A 173 13 13	
10	6	6	none		
1	16	5	none	none	
3		3	5	/	
17	36	8		6	
5	74	4	101e	none 9	
5	229	8	none	non	
17	356	4	7	9	
16	526	9	3	8	
19	526 7-14	7		more l	
10	10/6	4		-9	
-					
points	all: (2,4),(2,7),(3,5),(3,6)	1, (5, 2), (5	19)
	(7,2)	1(7,9)(3,5	1(818)	(10,2), /10,1	9)
		1		3 1 00	1

A A A A A

b 12 = 13 + x +6 (mod 11) 13 p= (x3, y3) $\lambda = \frac{3}{2}\frac{1^{2}+a}{2} = \frac{3(2)^{2}+1}{8} = \frac{13}{8} (mod 11) = 5$ $x_3 = x^2 - x_1 - x_2$ 552-2-2 = 2121 mod 11 = 10 $\frac{1}{3} = \frac{\lambda(x_1 - x_3) - y_1}{5 \cdot 2 - 100 - 4}$ 2 -40-4 = -44 - - 44 mod 11 =0 So, \$(2,4) = (10,0) (), P(2,4) and Q(2,7) m = 7 - 4 = 3 = 8