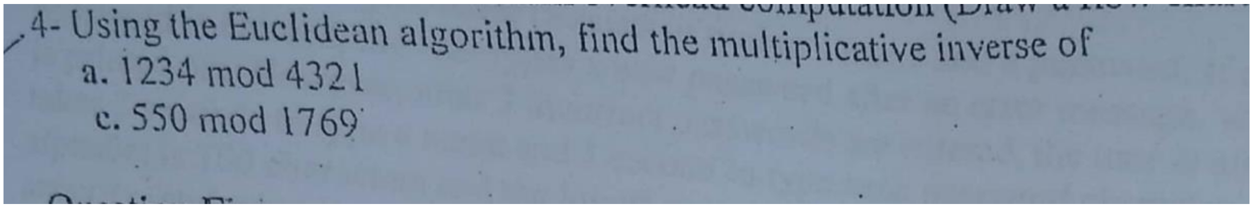
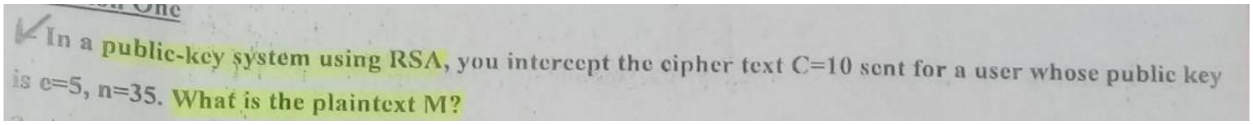
RSA Example



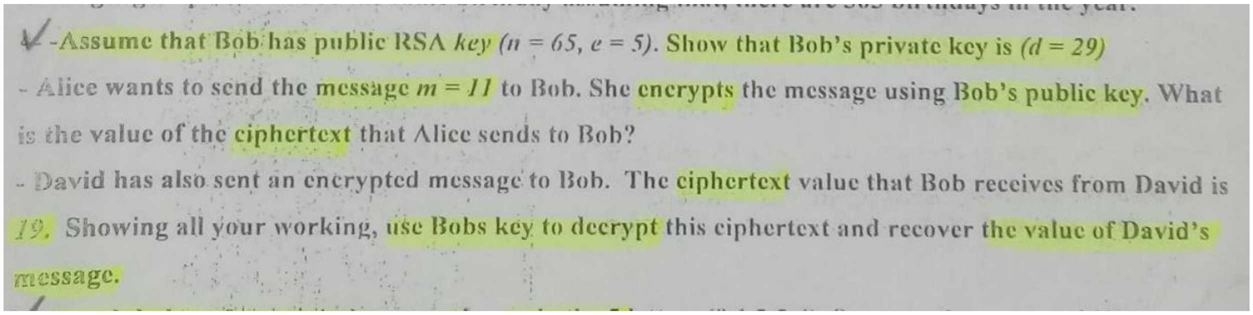
4- Using the Euclidean algorithm, find the multiplicative inverse of

a. 1234 mod 4321

c. 550 mod 1769



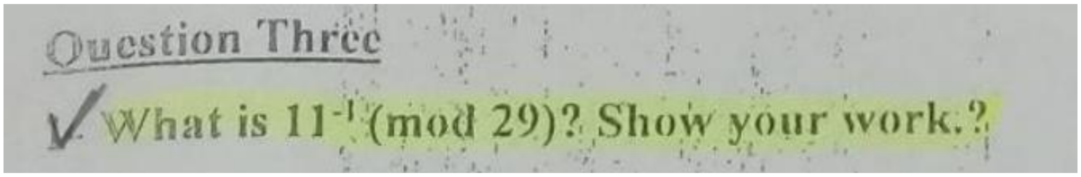
✓In a public-key system using RSA, you intercept the cipher text C=10 sent for a user whose public key is e=5, n=35. What is the plaintext M?



✓-Assume that Bob has public RSA *key* $(n = 65, e = 5)$. Show that Bob's private key is $(d = 29)$

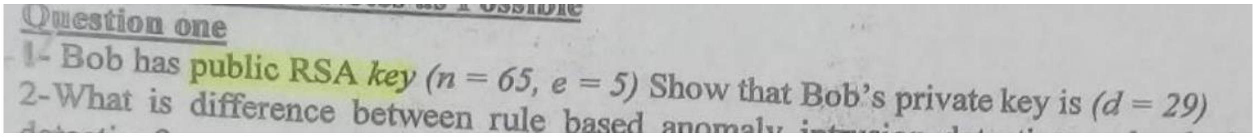
- Alice wants to send the message $m = 11$ to Bob. She encrypts the message using Bob's public key. What is the value of the ciphertext that Alice sends to Bob?

- David has also sent an encrypted message to Bob. The ciphertext value that Bob receives from David is *19*. Showing all your working, use Bobs key to decrypt this ciphertext and recover the value of David's message.



Question Three

✓What is 11^{-1} (mod 29)? Show your work.?

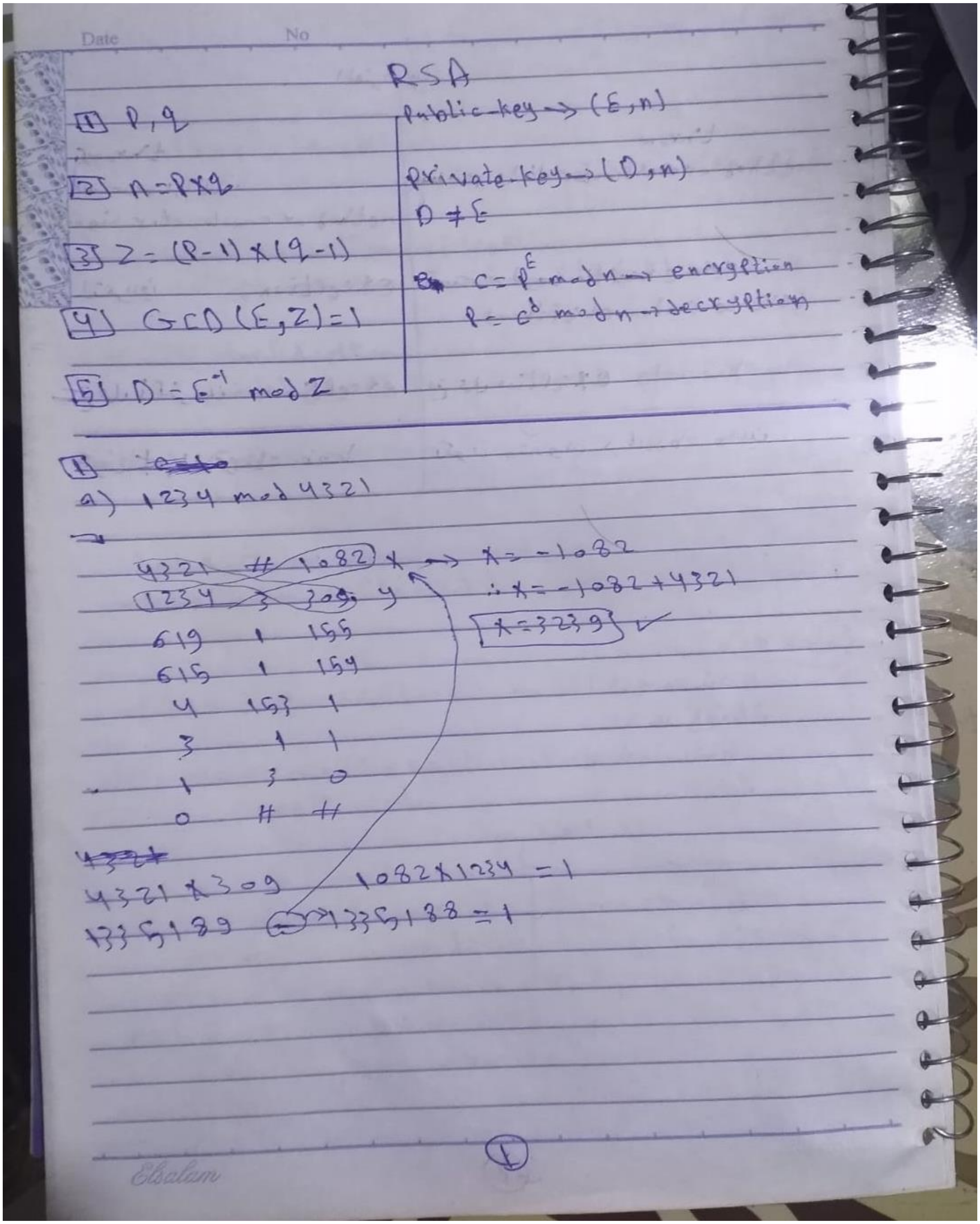


Question one

1- Bob has public RSA *key* $(n = 65, e = 5)$ Show that Bob's private key is $(d = 29)$

2-What is difference between rule based anomaly

Answer:



Date No

RSA

1 P, q

2 $n = P \times q$

3 $Z = (P-1) \times (q-1)$

4 $GCD(E, Z) = 1$

5 $D = E^{-1} \bmod Z$

public-key → (E, n)

private-key → (D, n)

$D \neq E$

$C = P^{E} \bmod n$ → encryption

$P = C^{D} \bmod n$ → decryption

1

a) 1234 mod 4321

→

4321	#	1082	x
1234	3	309	y
619	1	155	
615	1	154	
4	153	1	
3	1	1	
1	3	0	
0	#	#	

→ $x = -1082$

$\therefore x = -1082 + 4321$

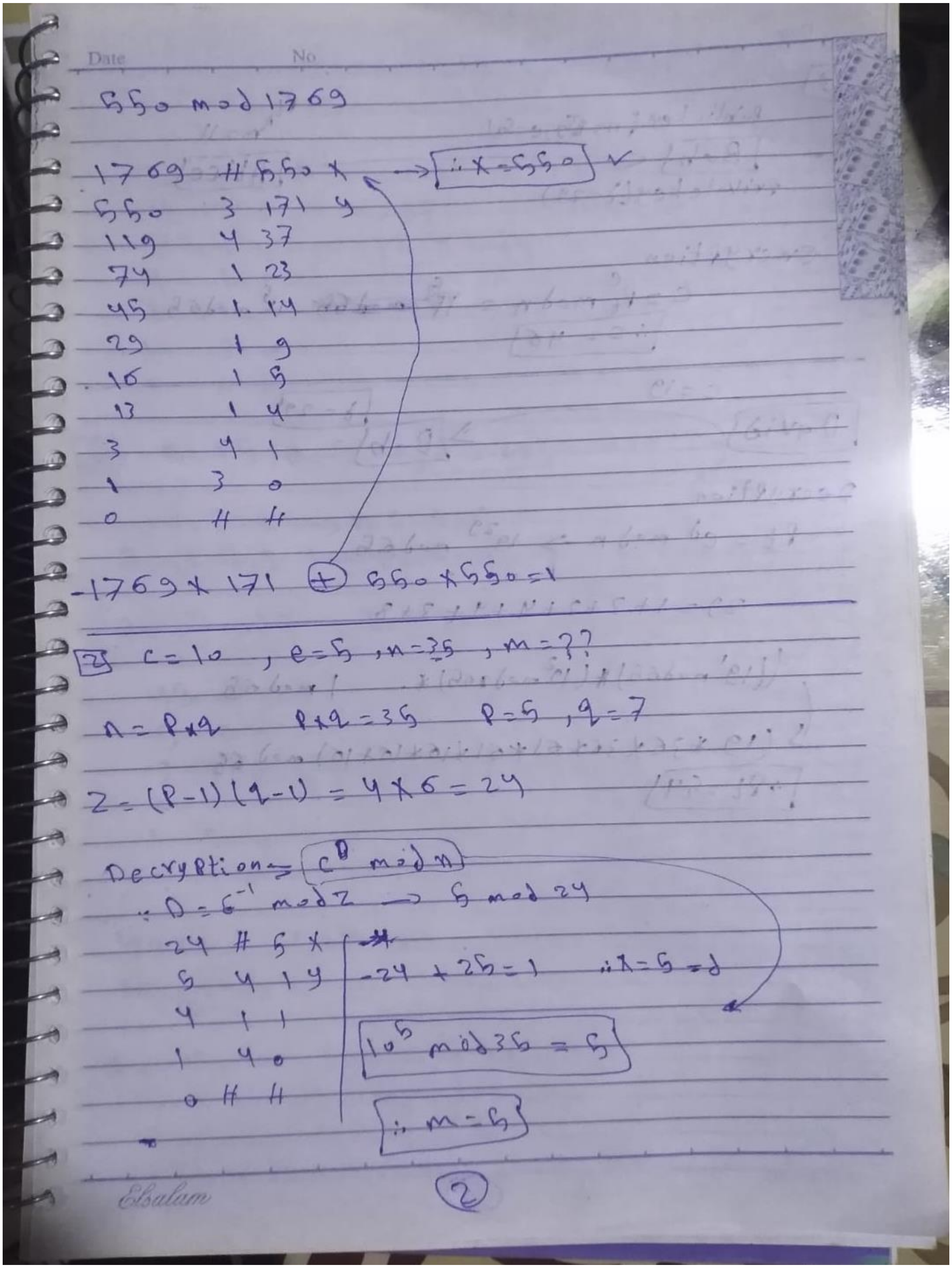
$\boxed{x = 3239}$ ✓

~~4321~~

4321×309 $1082 \times 1234 = 1$

1335189 $-$ → $1335188 = 1$

1



Date No

$550 \bmod 1769$

1769	#	550	x
550	3	171	y
119	4	37	
74	1	23	
45	1	14	
29	1	9	
16	1	5	
13	1	4	
3	4	1	
1	3	0	
0	#	#	

$\rightarrow \boxed{\therefore x = 550}$ ✓

$-1769 \times 171 \;\textcircled{+}\; 550 \times 550 = 1$

$\boxed{2}$ $c = 10$, $e = 5$, $n = 35$, $m = ??$

$n = p \times q \qquad p \times q = 35 \qquad p = 5 , q = 7$

$z = (p-1)(q-1) = 4 \times 6 = 24$

Decryption $\Rightarrow \boxed{c^{D} \bmod n}$

$\therefore D = 6^{-1} \bmod z \rightarrow 5 \bmod 24$

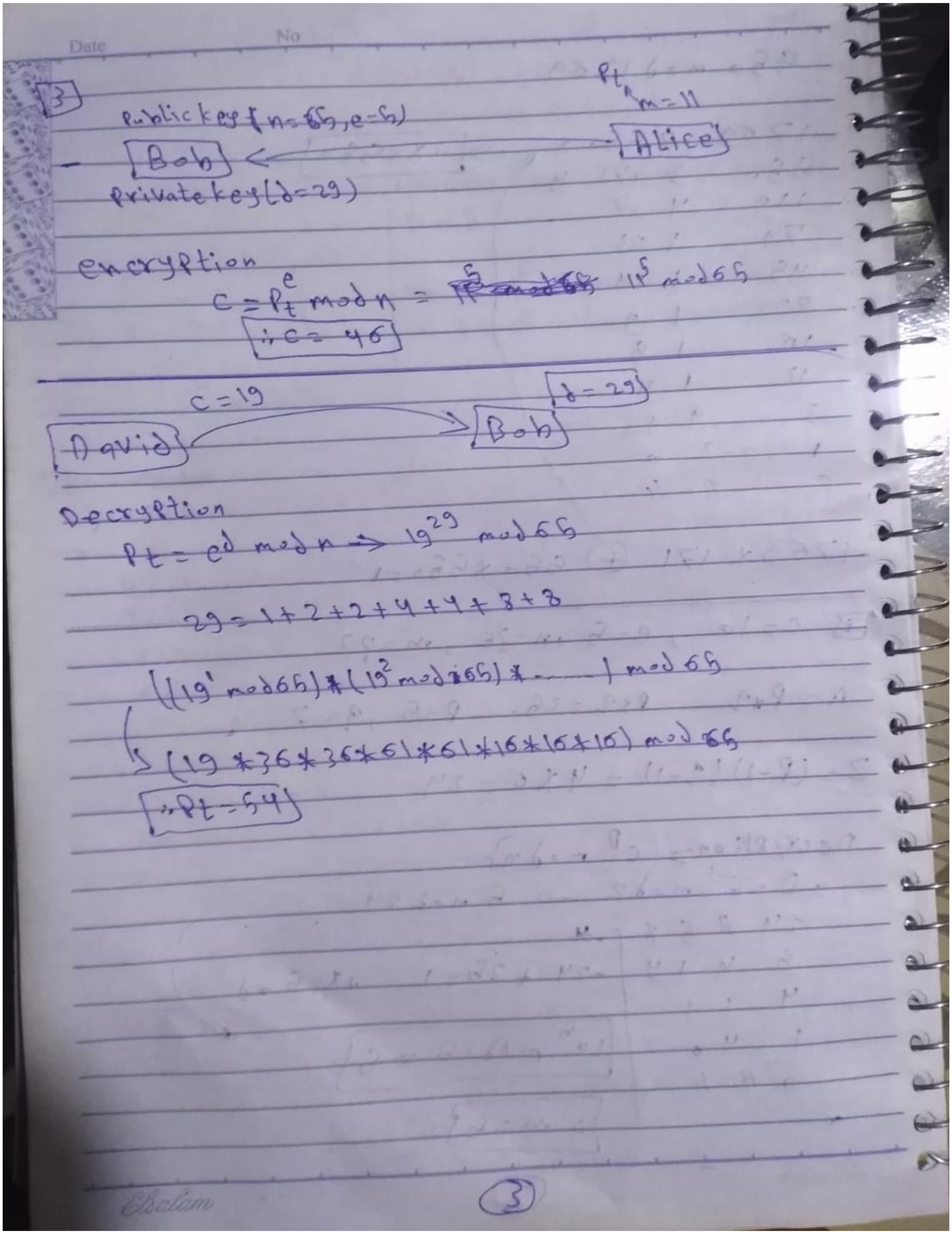
24	#	5	x
5	4	1	y
4	1	1	
1	4	0	
0	#	#	

$-24 + 25 = 1 \qquad \therefore x = 5 = d$

$\boxed{10^{5} \bmod 35 = 5}$

$\boxed{\therefore m = 5}$

Elsalam



Date No

3

P_t $m=11$

publickey {n=65, e=5)

Bob ← Alice

privatekey (d=29)

encryption

$C = P_t^e \bmod n = \cancel{11^5 \bmod 65}\ 11^5 \bmod 65$

$\boxed{\therefore C = 46}$

$\boxed{d = 29}$

$C = 19$

David → Bob

Decryption

$P_t = C^d \bmod n \Rightarrow 19^{29} \bmod 65$

$29 = 1 + 2 + 2 + 4 + 4 + 8 + 8$

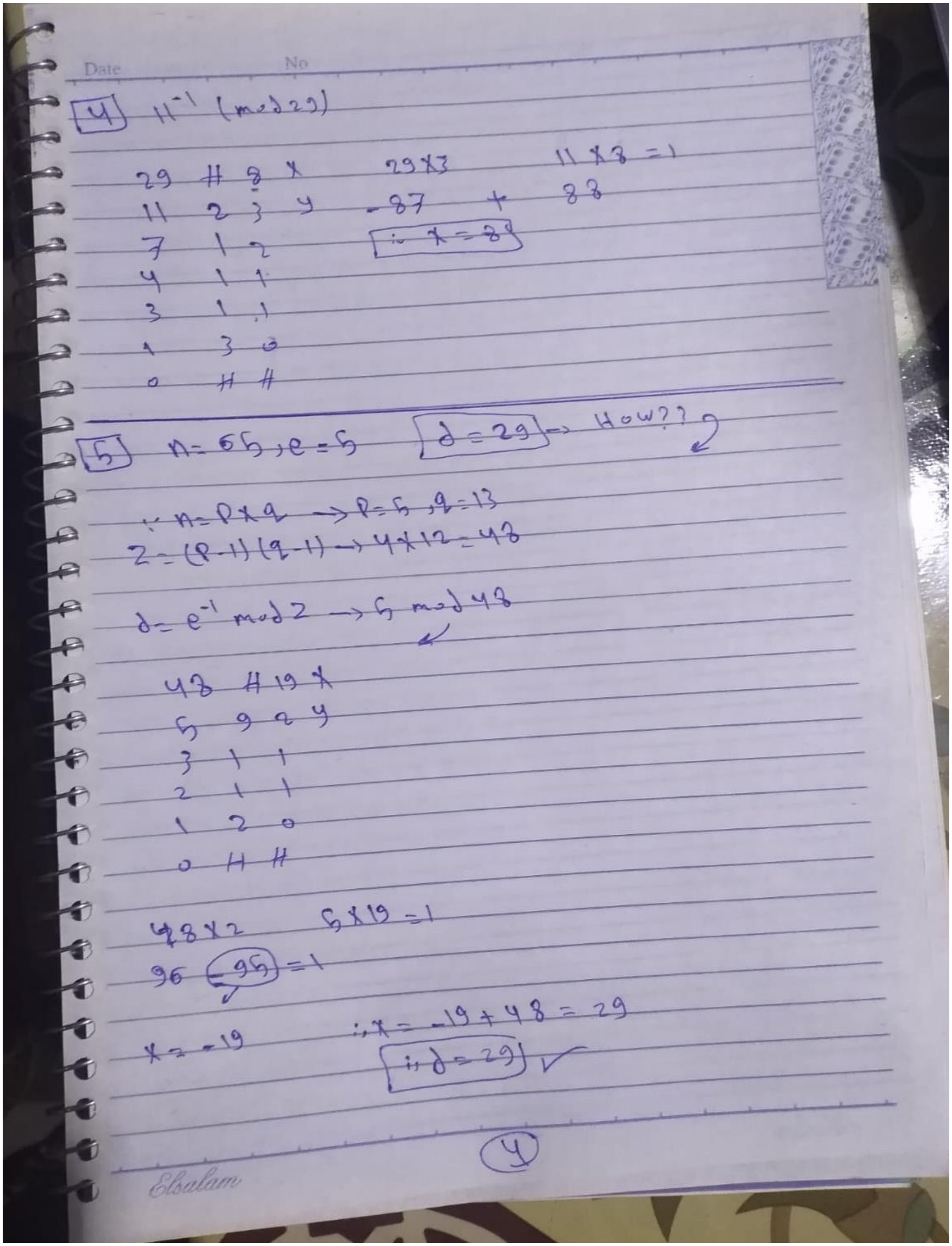
$((19^1 \bmod 65) * (19^2 \bmod 65) * \dots\dots) \bmod 65$

$\hookrightarrow (19 * 36 * 36 * 61 * 61 * 16 * 16 * 16) \bmod 65$

$\boxed{\therefore P_t = 54}$

Elsalam

3



Date No

$\boxed{4}$ $11^{-1} \pmod{29}$

29	#	8	x
11	2	3	y
7	1	2	
4	1	1	
3	1	1	
1	3	0	
0	#	#	

29×3 $\qquad$ $11 \times 8 = 1$

$-87 + 88$

$\boxed{\therefore x = 8}$

$\boxed{5}$ $n = 55, e = 5$ $\quad \boxed{d = 29} \rightarrow$ How??

$\because n = p \times q \rightarrow p = 5, q = 13$

$Z = (p-1)(q-1) \rightarrow 4 \times 12 = 48$

$d = e^{-1} \bmod Z \rightarrow 5 \bmod 48$

48	#	19	x
5	9	2	y
3	1	1	
2	1	1	
1	2	0	
0	#	#	

48×2 $\qquad$ $5 \times 19 = 1$

$96 - 95 = 1$

$x = -19$ $\qquad$ $\therefore x = -19 + 48 = 29$

$\boxed{\therefore d = 29}$ ✓