CMSC 414	S06	Exam	1
-----------------	------------	-------------	---

Page 1 of 4

Name:		
1 101110.		

Total points: 30. Total time: 115 minutes. 4 problems over 4 pages. No book, notes, or calculator

1. [10 points]

Suppose Bob uses RSA with n=77 and e=5. Are these valid numbers for RSA. Explain. If you answer yes, obtain the corresponding d.

CMSC	414	206	Evam	1
CIVIOL	414	SVV	Lixaiii	1

Page	2	of	4
ı azı	_	VI.	_

2. [5 points]

Assume that Bob uses RSA and the following hold:

Bob's signature of message m=2 is 5
Bob's signature of message m=3 is 4
Obtain Bob's signature for the message m=12. Show your derivation here.

3. [5 points]

How many numbers between 1 and 250000 are relatively prime to 250000? Explain

CMSC	414	S06	Exam	1
	TIT	\mathbf{v}	LAAIII	_

Page 3 of 4

Name:		
1 441110 .		

4. [10 points]Using the efficient algorithm, compute 131²⁵ mod-15

CMSC	414	S06	Evam	1
	717	171717	IJAAIII	

Page 4 of 4

Name:		
1 tallic.		

5. [10 points] Obtain a formula that yields a number x in Z_{45} such that x mod-5 = x_1 and x mod-9 = x_2 . Or if you think such a formula does not exist, explain.