

Name:

Math 236
Fall 2006
Dr. Seelinger

HOMEWORK ON RSA ENCRYPTION

This homework/worksheet is based on the RSA Encryption Algorithm discussed in Chapter 12 of the text. For this assignment, we use the notation in Theorem 12.3 of the text with $n = 17110999$ and $e = 279841$. To do this assignment, you will need to use your TI-89 calculator or other such computational tool to compute some fairly large numbers. You will find out relatively quickly that the numbers we will use quickly exceed the capacity of the TI-89, so we will need to find ways (using laws of exponents) to break these computations down to more manageable steps for the TI-89.

1. In Part 1 of this assignment we will encrypt the message:

Exam 1 is on 9/28.

Our first step will be to translate this message into a string of digits. Use the table at the end of this assignment to replace each character with a two-digit number that should result in a number 36 digits long. What number did you get?

2. Since n is eight digits long, if we reduce the above number modulo n we lose part of the message. Therefore, we group the first six digits together to get a congruence class modulo n . Then we group the second six digits to get a second congruence class modulo n . We continue in this manner until the above message gives us six congruence classes modulo n , each six digits long. What is the first congruence class gotten in this way?
3. To encode the first part of the message, take the above six digit number, raise it to the e power, and reduce modulo n . What happens if you use the TI-89? What can you do to have the TI-89 give the correct answer? Any other ideas not using the TI-89?

4. What is the correct encoded number for the first six digits. Write your answer as eight digits, starting with a zero if necessary.

5. Do the same procedure for the other six digit numbers and put them together in one number 48 digits long. This is the encrypted message. What is this 42 digit number?

6. This second part you will be asked to “break” this code (using the n and e given above). The material in Chapter 12 should contain all the information you need to do this. As part of this problem, you will have to give a detailed write-up of your solution, including any programs you might use or write. This is a non-trivial problem and you should anticipate spending a significant amount of time on this.

Consider the following 80 digit number that represents an encrypted message.

13779295 08619324 01767826 02144786 03662431 04788166 07824046 10762192 10271052 12048684

Use the information given in the text and the computational tools available to you to decrypt this message. Be sure you give a full explanation on a separate page as to how you did this. Provide enough details so that someone else could reproduce your procedure.

What follows is a table assigns a two digit number to each character so you can convert an alphanumeric message into a message in the form of a number. Use this table for Questions 1 and 6 on this assignment.

Space	00	t	20	!	40
a	01	u	21	/	41
b	02	v	22	(42
c	03	w	23)	43
d	04	x	24	-	44
e	05	y	25	=	45
f	06	z	26	+	46
g	07	0	27	*	47
h	08	1	28	&	48
i	09	2	29		49
j	10	3	30	<	50
k	11	4	31	>	51
l	12	5	32]	52
m	13	6	33	[53
n	14	7	34	'	54
o	15	8	35	“	55
p	16	9	36	”	56
q	17	.	37	;	57
r	18	,	38	:	58
s	19	?	39		