CS 32: Data Structures

Machine Problem 2

Directions:

- Create a program that will solve the problem below.

- The program must written in the C programming language, using only the following libraries **stdio.h, stdlib.h, string.h**

- The program must compile using standard Linux GCC

- Input file must be named mp2.txt

- Input must follow the sample input

- Source Code: <studentnumber>.c (201512345.c)

- Output file must be named <studentnumber>.txt (i.e 201512345.txt)

- Output file must be of the **same format** as the one shown in the sample output

- The following are not allowed:

    o   Discussing of the MP outside of class.

    o   Downloading code from the internet

    o   Copying from your classmate

    o   Using your classmate/someone else's source code

- MP Deadline: April 16, 2017 11:59 PM

C Implementation of the RSA

1)   Implement the RSA using the C programming language

2)   You can only use the LONG LONG / LONG/ INT/CHAR data types.

3)   For each test case, you will be given the following

CASE i

p,q

e

action 1

action 2

action 3

Actions are of the following form:

Alice will send the message: xxxxxxxx to Bob

Bob received the message: yyyyyy from Alice

4)   The output will be based on the actions sent

Case i

Alice sent: yyyyy (encrypted message)

Bob received: zzzzzzzz (decrypted message)

5)   Messages that will be sent using the English Alphabet. Processing will not be case sensitive. To convert the text to numbers, we first convert the letters to Base 27 using the following mapping:

Letter	Base 27	Letter	Base 27
A	0	O	e
B	1	P	f
C	2	Q	g
D	3	R	h
E	4	S	i
F	5	T	j
G	6	U	k
H	7	V	l
I	8	W	m
J	9	X	n
K	a	Y	o
L	b	Z	p
M	c	<SPACE>	q
N	d		

HELLO WORLD = 74bbeqmehb3

6)   Workflow

Message -> convert to base 27 -> convert to base 10 -> perform action -> convert to base 27 -> convert to corresponding text

7) Output will be in upper case.

8) Follow the sample input and output

9) Limit is 192 bits.