RSA
Working with strings

Letter	A	B	C	D	E	F	G	H	I	J	K	L	M
Numeric Value	0	1	2	3	4	5	6	7	8	9	10	11	12

Letter	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Numeric Value	13	14	15	16	17	18	19	20	21	22	23	24	25

We will consider string of character as a number written in base 26 system.

- String that consists of one letter: x_0 – any value between 0 and 25
- String that consists of two letters: x_1 x_0 will be converted to decimal number using the following rule: $x_1 * 26 + x_0$
- String that consists of three letters: x_2 x_1 x_0 will be converted to decimal number using the following rule: $x_2 * 26^2 + x_1 * 26 + x_0$
- String that consists of four letters: x_3 x_2 x_1 x_0 will be converted to decimal number using the following rule: $x_3 * 26^3 + x_2 * 26^2 + x_1 * 26 + x_0$
- In general string of k characters: $x_{k-1} + x_{k-2} + .. + x_1 + x_0$will be converted to decimal number using the following rule:
  $x_{k-1} * 26^{k-1} + x_{k-2} * 26^{k-2} + \ldots + x_1 * 26 + x_0$

1 character string range between 0 and 25
2 characters string range between 0 and 675 (the maximal value is ZZ: 25*26 + 25 = 675)
3 characters string range between 0 and 17575 (ZZZ: 25*26^2 + 25*26 + 25 = 17575)

In general, k character string range is between 0 and $(26^k - 1)$

To convert decimal value to string of characters perform modulo 26 and then divide 26 process similar to converting decimal to binary.

Example 1: find the string that corresponds to the numeric value num = 126037
Solution:

```
i=0
while(num > 0):
        x[i]=num%26
        num = num/26
        i++
```

x[0] = 126037 % 26 = 15
126037/26 = 4847
x[1] = 4847 % 26 = 11
4847/26 = 186

x[2]= 186 % 26 = 4
186 / 26 = 7
x[3] = 7 % 26 = 7
7/26 = 0 – stops the process

The string in numeric values: 7 4 11 15, in letters: HELP

Example 2:
YANA - numeric values: 24 0 13 0
decimal value is: $24 * 26^3 + 0 * 26^2 + 13 * 26 + 0 = 422162$

Example 3:
Suppose Alice chooses p = 17 q = 43.
Alice calculates m = 731, n = 16*42= 672, and chooses e = 29.
Alice calculates d = 533
Alice publishes her public key: m = 731, e = 29

Bob would like to send a message HI (7 8).
Decimal value of HI is 7 * 26 + 8 = 190 (valid value to encrypt in this case)
The valid range of plaintexts is: from 0 to 730
Ciphertext is: $ciphertext = 190^{29}\, mod\, 731 = 46$

Do decrypt, Alice performs the following:
$plaintext = 46^{533}\, mod\, 731 = 190$

How to find the actual text? We need to convert 190 to the string of characters.
Step 1: 190%26 = 8 = x0
Step 2: 190/26 = 7
Step 3: 7 % 26 = 7 = x1
String is 7 8 = HI

Practice: Working in teams of 2 students. Each student creates public and private keys and publishes public key for the second student to use. Encrypt the message and send to the other student for decryption. Assume that there are no spaces in the message, letters only and limit the length of the word to 6 – 8 characters.

Example 4 (from Invitation to Cryptology by Thomas H. Barr):
Brute force attack to factor m.

Suppose Alice published her public key: m = 459659 and e = 5. Assume that the text is 4 letters long and Eve has intercepted the ciphretext 223376 and Eve would like to find original message.

Brute force solution is to factor m = 459659 and find p and q. Eve would need to test prime numbers in range 2 to integer part of sqrt(459659) = 678 (rounded up).

In table of primes there are 123 primes between 2 and 678. Exhaustive search will find p = 673. Dividing m by p will find q = 683.
Eve now can calculate n= 672 * 682 = 458 304 and find d = 91661 and decrypt the message: 223376 ^ 91661 mod 459659 = 126037. See example 1 to find that the plaintext is HELP

Practice 1: (from Invitation to Cryptology by Thomas H. Barr): Eve knows m = 11885807, e = 6395437, and ciphertext is 8468422. Perform a cryptanalysis to break the code and decrypt the message.

Practice 2: Working in teams of 2 students. Each student will send m, e and ciphertext and the other student would try to factor m, find p, q, and d and decipher the message.

Example 5: (from Introduction to Cryptography with Coding Theory, Trappe, Washington). Suppose Eve knows m = p*q and n = (p-1)*(q-1). In this case there is a quick way to find p and q. (In the book m is called n, and n is called ϕ(n))

Solution:

1. Note: p + q = m – n + 1
   Explanation: n = (p-1)*(q-1) yields n = p*q - (p+q) + 1 = m –(p+q)+1)

2. We know p + q, and p * q, then p and q are roots of the following quadratic equation: z^2 - (p+q)*z + p*q = 0 using the values we know:
   z^2 - (m-n+1)*z + m = 0

3. To solve the equation, find discriminant = (m-n+1)^2 – 4*m and the final formula for solutions is:

$$p = \frac{(m-n+1)+\sqrt{discriminant}}{2}$$

$$q = \frac{m-n+1-\sqrt{discriminant}}{2}$$

Example:
Assume Eve knows m = 221 and n = 192. Find p and q.
Solution:
m - n + 1 = 221 - 192 +1 = 30
sqrt(discriminant) = sqrt(30^2 – 4*221) = 4
p = (30 + 4)/2 = 17
q = (30 – 4)/2 = 13
221 = 17 * 13

Practice: Working in teams of 2 students. Each student will supply m and n to the student. Apply the technique explained above to find p and q.