

# COMP 106

## PROGRAMMING PROJECT (Voluntary)

**Due to: 8 December 2011, Thursday**

### RSA Cryptosystem

In this programming project, you are going to write a program in Java to hack a secret message encrypted by using the RSA cryptosystem. All you know is the modulo number  $n$  ( $n = pq$ , but you don't know  $p$  and  $q$ ), and that the encryption key  $e$  is the largest appropriate number which is less than both  $p$  and  $q$ .

Assume that, before encryption, the message (written in English alphabet with capital letters) is decomposed into blocks of 2 letters (with no space between words) and then each letter is represented by a two-digit number between 0 and 25; as a result the original message that will be encrypted is a sequence of at most four digit numbers. For example, the message "COME ON" is (before encryption) transformed into 214 1204 1413.

Your program should recover and print the original messages **as text** when  $n$  and the encrypted code are given as follows:

**Case 1:**  $n = 154433$ , the encrypted code: 12073 35548 147170

**Case 2:**  $n = 355207$ , the encrypted code: 16664 193571 170801 37555

Do not use any result of some paper work in the program code. Do every computation on computer!

#### Hints:

1. In both parts, the number  $n$  is not that large for a computer so you can find the prime factorization ( $n=pq$ ) by trying all possibilities (however you may use some means to reduce the computation).
2. For modular inverse computation, you can use the *extended* Euclidean algorithm as explained in Exercise 48 in Section 3.7 of your textbook.
3. For modular exponentiation, you can use the algorithm given on page 226 in Section 3.6 of your textbook.
4. To represent a given letter (type *char*) with a number (type *int*), you can use casting. For example the statement `x = (int) 'D' - (int) 'A'` returns the integer code 3 of the letter D or vica versa.

Your program interface has to look like the following (note that the program continues asking message blocks until the user enters the sentinel value -1):

```
> Enter n: 39203
> Enter the first encrypted message block: 5992
> Enter the next encrypted message block: 5851
> Enter the next encrypted message block: 5674
> Enter the next encrypted message block: -1
> Starting decryption.....
> p: 199
> q: 197
> e: 193
> d: 18097
> Original message is " COMEON "
```

Send your source file with the name `p1surname.java` to your TA's e-mail address ([ysahillioglu@ku.edu.tr](mailto:ysahillioglu@ku.edu.tr)). Your TA will confirm your submission with an e-mail (if not, ask for confirmation).

**Requirements for Programming Style:** In grading your programming project, your programming style will also be taken into account. So please try to follow the instructions below:

1. Inside the code where appropriate, use comments to explain your code.
2. Use functions where appropriate.
3. At the beginning of your functions, explain the inputs, the outputs of your function and what your function does.
4. When naming variables and functions, use the following style:

Variable Names: First letter lower case, First letter of every other word capitalized

Example: `char catName[20];`

Methods: First letter of each word capitalized

Example: `void GetCatName();`

Constants: All capitals

Example: `#define CATNAMELENGTH 20`

5. Your program should contain at the very beginning of the code, the following information:

Name:

Student ID:

Course:

***While doing all your homeworks, remember that:***

- ***You should not give or take any files***
- ***You should not give or take help other than simple verbal hints.***