Programming Assignment

RSA Public-Key Cryptosystem

- **This assignment 8 points worth, over 20 pts of assignment grade.**

Overview:

Write a program to implement the RSA public-key cryptosystem.

It executes block ciphering in ECB mode. Cipher text stealing is applied, when necessary.

Your software should have a GUI, but frontend of your implementation is not important and will not be evaluated.

Part 1 . Key generation

The RSA public key cryptosystem involves three integer parameters *d*, *e*, and *n* that satisfy certain mathematical properties. The *private key* (*d*, *n*) is known only by Bob, while the *public key* (*e*, *n*) is published on the Internet.

The RSA cryptosystem is easily broken if the private key *d* or the modulus *n* are too small (e.g., 32 bit integers). So, the size of the numbers should be at least 1024 bit (around 309 digits).

Design a scheme to pick two large prime numbers, with given sizes above.

Test the numbers for primality, using Fermat's primality test. Test each of them with 20 random integers.

You can use BigInteger data type for java.

The program should let us to compute/create private and public key pairs. You may bind it with a button ("create key pair" button).

Part 2 . Input handling

The algorithm will take the given text and encrypt it block by block.

If Alice wants to send Bob a message (e.g., her credit card number) she encodes her message as an integer *M* that is between 0 and *n-1*. Block sizes will be 16 bit long.

The algorithm will take the text, convert it character by character into mathematical integer representation, using ascii code table, and then split it into blocks.

Cipher text stealing is applied for padding, when necessary.

The program should let us to enter a text to encrypt, and it should let us select the key pair to use, from already existing ones. You may name/number the created key pair and show the list of them. User can select from the list.

Part 3 . Algorithm implementation

The sender (Alice) computes:

$C = M^e \bmod n$

and sends the integer *C* to Bob. As an example, if M = 2003, e = 7, d = 2563, n = 3713, then Alice computes
$C = 2003^7 \bmod 3713 = 129{,}350{,}063{,}142{,}700{,}422{,}208{,}187 \bmod 3713 = 746.$

When Bob receives the encrypted communication *C*, he decrypts it by computing:
$M = C^d \bmod n$.

Continuing with the example above, Bob recovers the original message by computing:
$M = 746^{2563} \bmod 3713 = 2003.$

Develop the code to implement the RSA algorithm.

The algorithm will use Electronic Code Book Mode block operation.

It will then encrypt the given text value, and return back a text value. You may bind it with a button (“Encrypt” button).

The algorithm will also let users to select and decrypt the given text file. You may bind it with a button (“Decrypt” button).