Tony Wong; Brent Yurek
CS 342 - Project 3
RSA Encryption
PDF README

---

To compile:

UNIX Environment:
$ make rsa

Dr. Java:
Open RSA.java in its directory and click on compile

---

To run:

UNIX Environment:
$ make run

Dr. Java:
Click on run

---

MISC. notes:

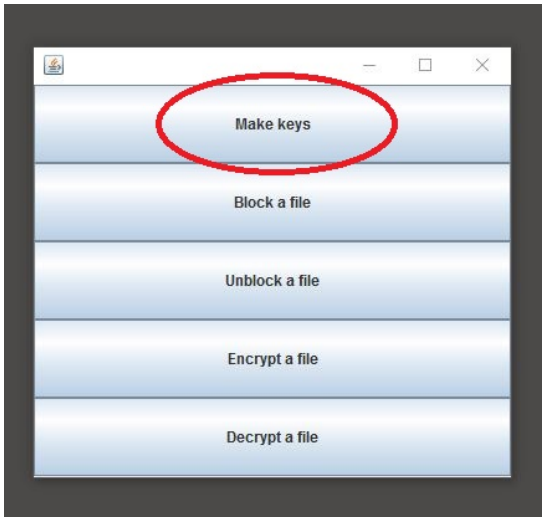
- Prime numbers are pulled from a file named "primeNumbers9.rsc". This means that the primes within are 9-digit in length. This is the longest set of primes that can encrypt/decrypt a blocking length of 8 in reasonable time.
- Blocking size is limited to a size of 8. This is to ensure reasonable running time in conjunction with the 9-digit prime length. This means that the encryption and decryption process might take a few seconds for a relatively short message file (roughly 100 characters).

---

The following procedure assumes there already exists a message file.
In this example, the file is named "message".

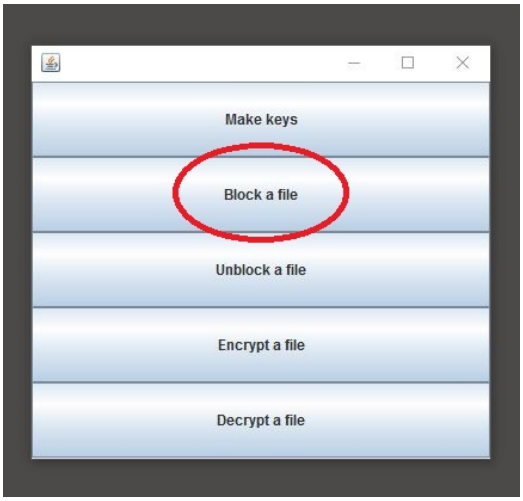
Step 1: Make keys

1) Click on "Make keys" - this creates the public and private key pairs
NOTE: This creates private/public key files named prikey/pubkey respectively.
A pop-up message displays when this process is completed.

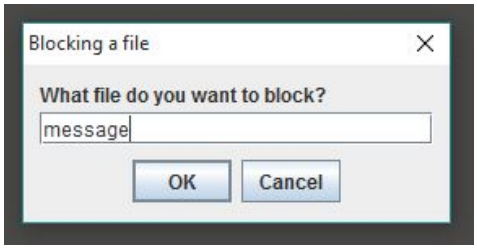



Step 2: Blocking a file

1) Click on "Block a file"

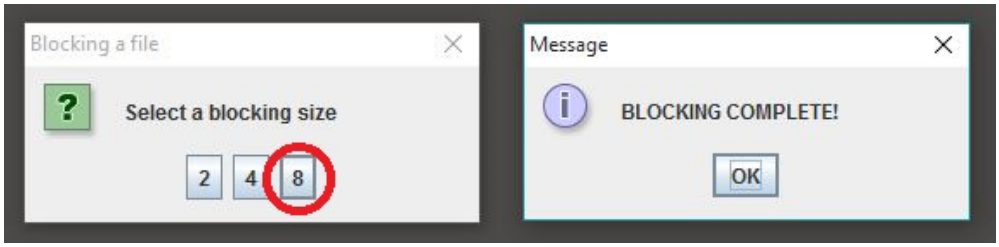



2) Type in the name of the file to be blocked (e.g., message) and click OK



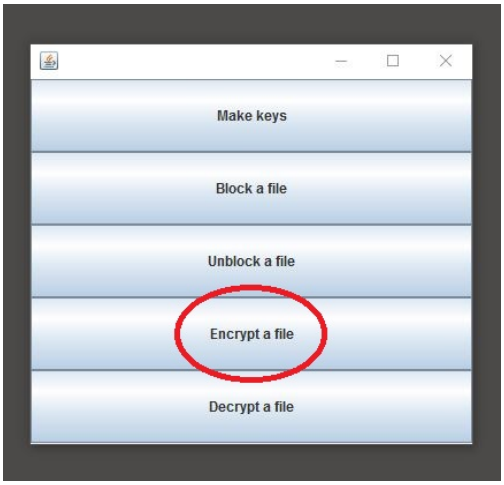

3) Type in the name of the output (e.g., BLK) and click OK


4) Select a blocking size by clicking on it
A pop-up message displays when this process is completed.



Step 3: Encrypting a file

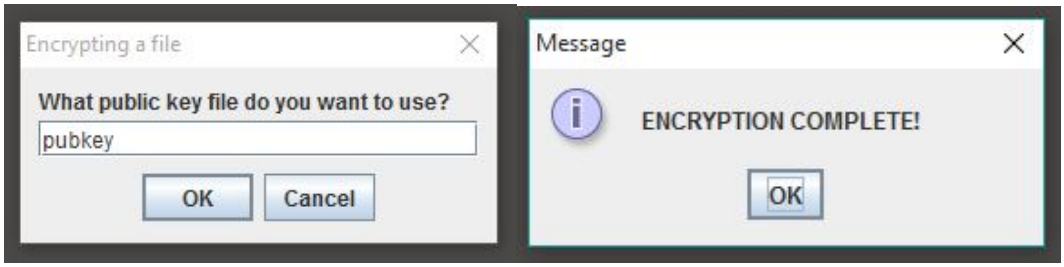
1) Click on "Encrypt a file"




2) Type in the name of the file to be encrypted (e.g., BLK) and click OK

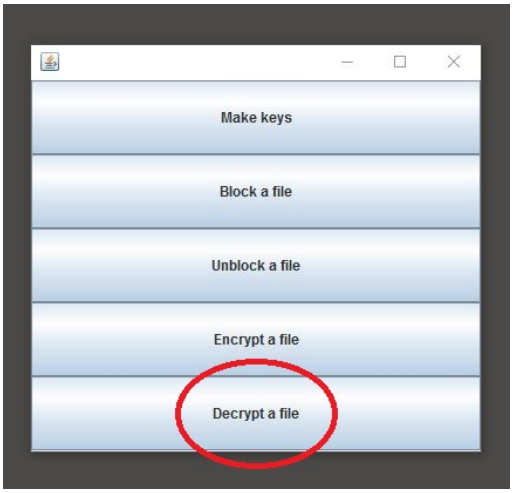

3) Type in the name of the output (e.g., ENC) and click OK


4) Type in the name of the public key file (e.g., pubkey) and click OK
A pop-up message displays when this process is completed.



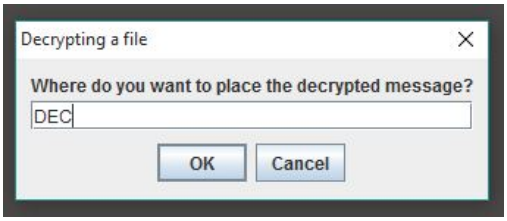
Step 4: Decrypting a file

1) Click on "Decrypt a file"

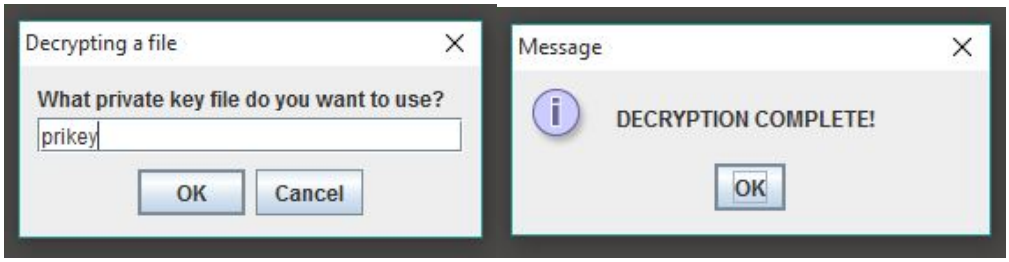



2) Type in the name of the file to be decrypted (e.g., ENC) and click OK


3) Type in the name of the output (e.g., DEC) and click OK

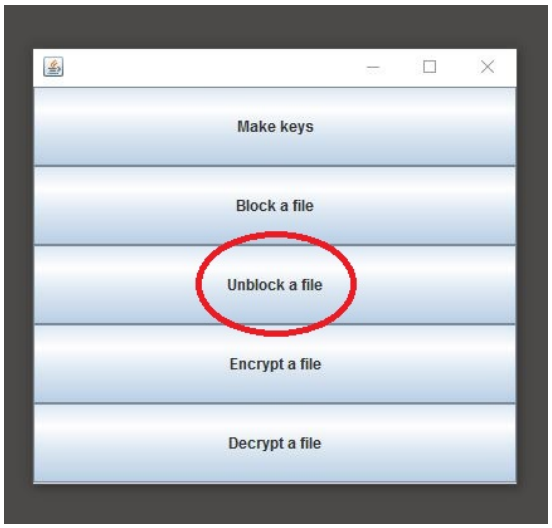



4) Type in the name of the private key file (e.g., prikey) and click OK.
NOTE: This might take some time! Takes about 3 seconds for this particular message.
A pop-up message displays when this process is completed.



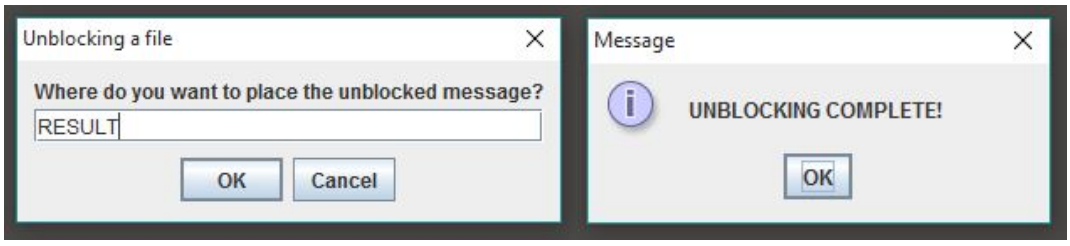
Step 5: Unblocking a file

1) Click on "Unblock a file"



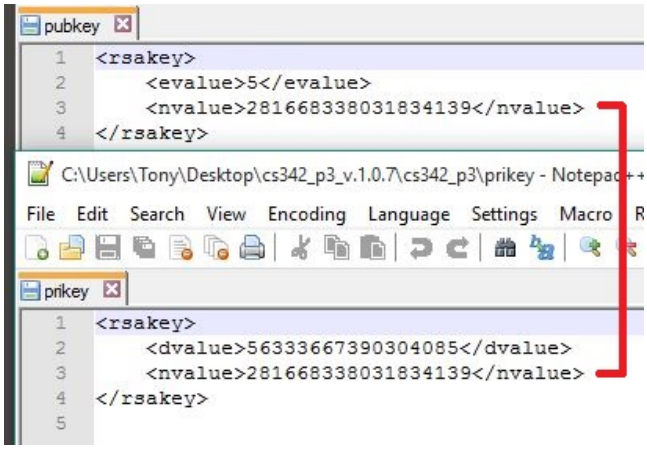

2) Type in the name of the file to be unblocked (e.g., DEC) and click OK


3) Type in the name of the output (e.g., RESULT) and click OK
A pop-up message displays when this process is completed.

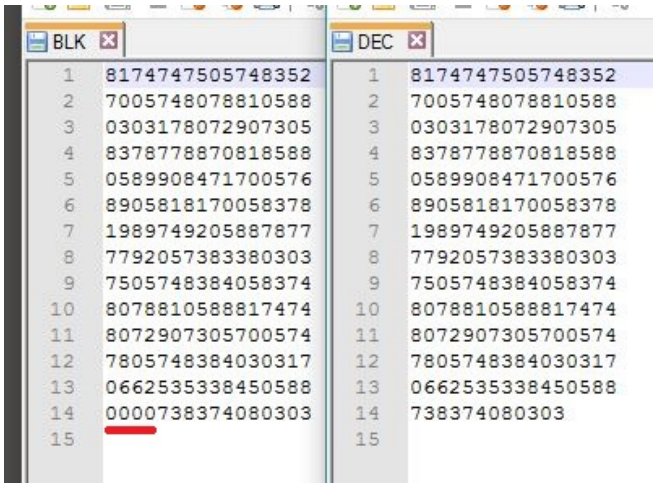


How to verify that steps are working correctly:

1) Check to see if keys are made.
   a) Open up prikey and pubkey and see if they are in XML format.
   b) Verify that they share the same n value




2) Check to see if the blocked file and decrypted file are the same except for padding on last line




3) Check if the original message and output message from entire process is the same.