**DFSC 3316 Lab 2 Spring 2023 Burris**

Due: Wednesday March 29 prior to the start of class. Do not procrastinate! Expect to receive additional labs prior to this due date. You may use Java, “C,” Ada, Python or another language with permission so long as you explicitly complete all lab requirements. **You may not use libraries for the RSA encryption and decryption! You must write the RSA code!** You need not physically demonstrate the “D,” “C” and “B” options. **To receive a grade of “A” you may need an appointment with me outside of class to demonstrate and discuss your software**!

**“D” Option (best grade is 60):**

Write a program to accomplish RSA encryption and decryption. For encryption, the program should accept the name of the file containing the raw text and the name of the file to place the encrypted results. For decryption, the program should accept the name of the file containing the cipher text and name of the file to place the decrypted results. The program should accept the public and private keys either from a separate file, the terminal or a keystore. It should also accept the block size as an input parameter.

**Test your program using:**

P = 137

Q = 131

E = 3

Public keys (n,e) = (17947, 3) and private keys (n, d) = (17947, 11787).

For blocking, you may use 2, 4, 6, or 8 bit blocks but management would prefer blocks of 2 bytes equal 16 bits (there may be a hidden catch hint: Encryption is accomplished by breaking text up into numerical blocks smaller than n. For binary data, the largest power of 2 less than n should be used. Explain how you modify the problem to utilize 2 byte blocks). **Clearly state your block size as part of your solution!**

File contents to encrypt:

**Hello World.**

**Nice Day!**

**An “A” for the class would be nice. :)-**

**“C” Option (best grade is 70):**

First complete the “D” option. Now write a separate program to accept “p,” “q,” and “e” from the terminal. Prove e and (p-1)\*(q-1) are relatively prime. If they are not relatively prime, you program must show explicitly why.

Test your program using:

Data set 1:

P = 11

Q = 3

E =3

Data set 2:

P = 11

Q = 3

E = 7

Data set 3:

P = 11

Q = 3

E = 8

**“B” Option (best grade is 80):**

First complete the “D” and “C” options. Our CEO needs to send specific instruction to all retail stores in our organization using the Internet with sockets as the communications medium. Our employees must be able to verify the message is from the CEO and has not been modified. The CEO’s technical advisors have decided the instructions should be encrypted using RSA and contain a digital signature. You are free to exchange keys in any manner you find convenient. ***Use must use your “D” option code to encrypt the message*** and hash used in the digital signature. **You must use “your RSA code” for all encryption and decryption! You may not use libraries or programming language facilities.** You may however use any available code to compute the hash, e.g., SHA, MD4, or MD5. Both the client and server may be single threaded. Use the data for the “D” option. Management would be impressed if you used the following key information in addition to the “D” option data:

P = 47

Q = 71

E = 79

D = 1019

Public keys (n,e) = (3337, 3) and private keys (n, d) = (3337, 7). If you use these keys, highlight the section of code on the program listing with a marker!

Clearly state the blocking factor. To receive credit, you must convenience me your digital signatures accept correct transmissions and reject invalid transmissions.

**“A” Option (best grade is 90):**

Implement the “B” option but the server must be **multithreaded**. You may use sockets, servlets, or RMI. As part of your demonstration, you must convenience me multiple threads are executing. During the demonstration, you must convenience me you are servicing multiple clients simultaneously! One way to do this is to place a dummy input operation in your server code. That will make the code stop until the user responds so the code can finish. All keys must be stored and retrieved by your software from “key stores” or their equivalent. You may use the facilities in Java to create and retrieve keys when implementing the “A/A+” Options only.

**“A+” Option (best grade is 100):**

Implement the “A” Option with additional features of sufficient technical value to be worth the additional 10 points. You must clearly state your goal and strategy to achieve the goal on a cover sheet prior to the A+ option results and code.

**Submission:**

For all options, you must submit a printed copy of the source code. Submit a printed copy of all data and results (inputs and outputs). **To receive a grade of “B” or better, you must make an appointment with me outside of class to demonstrate and discuss your software**! Expect new keys as well as plain text during the demonstration.

The hard copy should be submitted in the following order:

1. “Lab cover sheet stating the highest grading option completed.
2. “D” option results followed by the “D” option code.
3. “C” option cover sheet followed by the “C” option results then the “C” option code.
4. “B” option cover sheet followed by the “B” option results then the “B” option code.
5. “A” option cover sheet followed by the “A” option results then the “A” option code.
6. “A+” option cover sheet followed by the “A+” option results then the “A+” option code.