Computer Security Assignment

Spring 2015

Deadline: 12 March 2015

Submission: Email a single zip file to achaudhary@truman.edu.

Step 1: One image of size 2250x2550 is given with this doc. Read this into an array of 2250x2550 as 2D or 1D and store this in a text file as 'Target file'. [you can also use other libraries for this like OpenCV, Matlab, Mathmetica; if you don't want to do it in Java.]

Step 2: Write a Test class in Java which will contain main (). Also write 4 different files which will run DES, 3DES, AES and RSA on a given Target Data. Use the block and key size for each algorithm as shown in table.

Algorithm	Block Size(Bits)	Key Size(Bits)	Time taken in Encryption (fill this column) in Nanoseconds
DES	64	56	
3DES	64	168	
AES	128	256	
RSA	128	256	

You are free to use any key of this length. Feel free to use random function generator for key generation. No need to write you own algorithms, all of them are already implemented in Java. For all algorithms, use block encryption with padding (if pads needed).

Step 3: Call all 4 algorithms from main() on **same** Target file to encrypt. So main() structure would be

```
Main(){
DES encryption          // Record execution time for this function
3DES encryption         // Record execution time for this function
AES encryption          // Record execution time for this function
RSA encryption          // Record execution time for this function
}
```

Step 4: Now you have time for 4 different encryption and 4 ciphers, which would be stored in 4 different arrays. Generate images from these arrary to visulize cipher.

File to submit in Zip:

1. Target file (target.txt)
2. Java code (5 files) (Test.java, algoname.java) //mention keys in code with comments
3. Table with encryption time for each algo in a pdf
4. Four Cipher arrarys (algoname.txt)
5. Four Cipher images (algoname.jpeg)

Useful Resourses:

For Image Operations

http://docs.oracle.com/javase/7/docs/api/javax/swing/ImageIcon.html
http://docs.oracle.com/javase/tutorial/2d/images/saveimage.html

For Encryption Algorithms

Java.security.*;
Javax.crypto.*;

To record time of each function using Java

http://docs.oracle.com/javase/7/docs/api/java/util/concurrent/TimeUnit.html

Feel free to contact me for any clarification - **Ankit Chaudhary**