Visual Cryptography Assignment

Deadline: 3 weeks from Posting date

Submission: Email a single zip file ac.soe.jnu@gmail.com or on canvas link

---

Step 1: One image of size 1000x1000 is given with this doc, named 'Targetimage'. Read this into an array of 1000x1000 as 2D (or 1D if you prefer) and store this in a text file as 'Targettext' file. If you read in color-code (like RGB or HSV), you have to use three separate arrays to store each component of the image in a separate file. [you can also use other libraries for this like OpenCV, Matlab, Mathematica; if you don't want to do it in Java.]

Step 2: Write a Test class in Java which will contain main(). Also write four different files which will run DES, 3DES, AES and RSA on a given Targettext 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 given length. Feel free to use random function generator for key generation. No need to write your own algorithms, all of them are already implemented in Java. For all algorithms, use ECB encryption with padding (if pads needed).

Step 3: Call all four algorithms from main() on **same** Targettext file(s) to encrypt. So the 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 keys and 4 ciphers (one from each algorithm), which would have stored in four (may be in 12 files with color-code) different arrays. Generate images from these arrays to visualize cipher.

File to submit in Zip:

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

Useful Resources:

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

Prof. A. Chaudhary
School of Engineering