

ECE646

Lab #4

Kryptos – Properties of secret-key ciphers

The final report is due at the beginning of class on
Tuesday, November 14th, 7:20PM.

BACKGROUND

Expected Background: understanding of Lectures 7 and 8

Required Reading:

- W. Stallings, *Cryptography and Network Security*, 4th/3rd Edition: Chapters 3 and 6.1, or 2nd Edition: Chapter 3 and 4.1.
- A. Menezes, P. van Oorschot, and S. Vanstone, *Handbook of Applied Cryptography*, Chapter 7.4.
- Kryptos Version 3.01 User Manual (PDF), available at <http://kryptosproject.sourceforge.net/>

1. INSTALLATION

In order to complete this lab you might want to install Kryptos on your personal computer/notebook. You can download Kryptos v. 3.0.1 from <http://kryptosproject.sourceforge.net/>

The Hex Utility Viewer, and Bit Modifier Tool are linked via the class webpage.

Alternatively, you may use computers located in the GMU ECE labs, S&T II rooms 203 and 265, which have Kryptos already installed but not the Hex Utility Viewer, and Bit Modifier Tool. You can download them using the link on the class webpage and put them on your desktop.

2. YOUR COMPUTER SYSTEM

Please describe computer system used in your experiments. Make sure that all experiments are performed using the same or equivalent computer system. In particular please note that not all machines available in the lab 203 have the same system parameters. Please provide at least the following information about your system:

Processor type:

Clock frequency:

Cache size:

RAM size:

Hard disk type and capacity:

Operating system:

Please include any other parameters that might affect the results of your measurements.

For Sections 3 through 7 set the Crypto Library in Kryptos to Crypto++

3. LENGTH OF CIPHERTEXT

Length of a ciphertext/message after encryption and decryption

T1. Using an arbitrary text editor prepare a top-secret message (ASCII text file) you will be using in your experiments. Encrypt and decrypt your message using DES in the following modes of operation

- a. ECB
- b. CBC
- c. CBC_CTS
- d. CTR with the message block size equal to the cipher block size
- e. CFB with the feedback size equal to 8 bits

Fill the given below table:

Mode of operation	Size of original message [bytes]	Size of ciphertext [bytes]	Size of decrypted message [bytes]
ECB			
CBC			
CBC CTS			
CTR with j=64			
CFB with j=8			

Repeat the same operations using the original message expanded with one extra space character added at the end of the message. Record your results.

Mode of operation	Size of original message [bytes]	Size of ciphertext [bytes]	Size of decrypted message [bytes]
ECB			
CBC			
CBC CTS			
CTR with j=64			
CFB with j=8			

Q1. Explain any differences in the sizes of output files for various modes of operation of a block cipher.

A1.

4. SECURITY OF VARIOUS MODES OF OPERATION

T2. Create a message that consists of several tens of repetition of the same letter (without any new-line characters in between them). Encipher this message in the following modes of operation

- a. ECB*
- b. CBC*
- c. CTR with the message block size equal to the cipher block size*
- d. CFB with the feedback size equal to 8 bits*

Compare the obtained ciphertexts.

Q2. Does any of the ciphertexts have any special features that differentiate it from the ciphertexts obtained in different operational modes. Can you explain the obtained results?

A2.

5. RESISTANCE TO TRANSMISSION ERRORS

Resistance to transmission errors I

T3. Copy ciphertext files obtained in Task 2 to a different directory. In every ciphertext file, change one (preferably positioned in the middle of the file) character. Decipher modified ciphertexts and analyze the obtained decrypted files.

Hint: You can use Bit Modifier Tool, 010.exe, to change a single bit within a given block of the ciphertext, and Hex Utility Viewer, Utility.exe, to determine positions that changed in the decrypted file.

Q3. Determine how many bytes and at which positions have changed in the decrypted file compared to the original plaintext file. Which mode of operation is the most resistant to transmission errors?

Mode of operation	Number of bytes changed compared to the original plaintext file	Positions of bytes changed compared to the original plaintext file
ECB		
CBC		
CTR with j=64		
CFB with j=8		

A3.

Resistance to transmission errors II

T4. Copy ciphertext files obtained in Task 2 to a different directory. In every ciphertext file, delete one (preferably positioned in the middle of the file) character. Decipher modified ciphertexts and analyze the obtained decrypted files.

Hint: You can use Hex Utility Viewer, Utility.exe, to determine positions that changed in the decrypted file.

Q4. Determine how many bytes and at which positions have changed in the decrypted file compared to the original plaintext file. Which mode of operation is the most resistant to skipping bytes during transmission?

Mode of operation	Number of bytes changed compared to the original plaintext file	Positions of bytes changed compared to the original plaintext file
ECB		
CBC		
CTR with j=64		
CFB with j=8		

A4.

6. WEAK KEYS

- T5. Encrypt the plaintext file generated in Task 1 twice using DES with the same*
- a. weak key*
 - b. semi-weak key*
 - c. random key*

Repeat the same experiment using

- A. ECB mode*
- B. CTR mode with the same IV used in both encryptions*
- C. CBC mode with the same IV used in both encryptions.*

Compare the obtained ciphertext files.

Q5. Is there anything special about any of the ciphertexts obtained using the described above double encipherments? Explain the obtained results.

A5.

7. PROPERTIES OF DES

Effect of changing a single bit of the DES key

T6. Encrypt the plaintext file generated in Task 2 using DES in the ECB mode with a randomly generated DES key. Decrypt the obtained ciphertext using the same key, and a key that differs at exactly one bit. Compare the obtained decrypted messages.

Q6. How many bits and how many bytes have changed in the decrypted file as a result of a change of a single bit of the key? What property of the DES algorithm is responsible for the obtained number of changes?

A6.

8. PERFORMANCE

Speed of encryption for various secret key ciphers I

T7. Select a large file with a size chosen in such a way that the time of its encryption using DES in the ECB mode is equal to about 20 seconds.

Measure the time of encryption and decryption of the same file (without the time necessary for file i/o) in the ECB mode using the following ciphers:

- a. Triple DES*
- b. IDEA*
- c. RC5 32/12/8*
- d. RC5 32/12/16*
- e. RC5 32/24/16*
- f. Rijndael 128 (Rijndael with a 128-bit key)*

Q7-1. Set the Crypto Library in Kryptos to Crypto++. Fill the given below tables. Comment on whether the obtained results are consistent with your expectations.

A7-1.

File size [bytes]:

Cipher	Time of encryption in seconds	Time of encryption in clock cycles	Time of decryption in seconds	Time of decryption in clock cycles
DES				
Triple DES				
IDEA				
RC5 32/12/8				
RC5 32/12/16				
RC5 32/24/16				
Rijndael 128				

Cipher	Encryption throughput in Mbits/s	Encryption time in clock cycles/block of data	Decryption throughput in Mbits/s	Decryption time in clock cycles/block of data
DES				
Triple DES				
IDEA				
RC5 32/12/8				
RC5 32/12/16				
RC5 32/24/16				
Rijndael 128				

Q7-2. Set the Crypto Library in Kryptos to OpenSSL. Fill the given below tables. Comment on whether the obtained results are consistent with your expectations.

A7-2.

File size [bytes]:

Cipher	Time of encryption in seconds	Time of encryption in clock cycles	Time of decryption in seconds	Time of decryption in clock cycles
DES				
Triple DES				
IDEA				
Blowfish (128 key)				
Rijndael 128				

Cipher	Encryption throughput in Mbits/s	Encryption time in clock cycles/block of data	Decryption throughput in Mbits/s	Decryption time in clock cycles/block of data
DES				
Triple DES				
IDEA				
Blowfish (128 key)				
Rijndael 128				

Q7-3: Does the performance of the two libraries differ? If so, please comment on it.

A7-3.

Speed of encryption for various secret key ciphers II

T8. Repeat the encryption of the same file using one of the Crypto Libraries and one of the given above ciphers ten times. Determine the mean, median, minimum, maximum, and the standard deviation for the obtained set of execution times in seconds and in the number of clock cycles.

Q8. Fill the given below table. Explain the obtained results.

A8.

Library:				
Cipher:				
Measurement number	Encryption time without i/o in seconds	Encryption time without i/o in clock cycles	Encryption time with i/o in seconds	Encryption time with i/o in clock cycles
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
Mean				
Median				
Minimum				
Maximum				
Standard deviation				

Speed of secret-key ciphers vs. public key ciphers

T9. Select the Crypto++ library. Compare the speed of encryption and decryption between Triple DES and RSA with the key size 1024-bits, and $e=3$. Choose the size of a message used for encryption and decryption in such a way that all operations take at least 0.5 s without file I/O.

Q9. Explain the obtained results.

A9.

Bonus Assignment Debugging Kryptos

Please let us know about any features of the GMU educational software toolset, including Kryptos, Hex Utility Viewer, and Bit Modifier Tool that

- a. did not work as expected
- b. could be improved
- c. could be added

in order to enrich your educational experience and make using software easier and more intuitional.

Please give this feedback online at <http://sourceforge.net/projects/kryptosproject/>
Request new features via the Feature Request link, report bugs via the Bug link and give general comments in the Public Forums.

Please also let us know if you have any ideas for additional exercises that could be performed using this software.

Ideas of additional exercises regarding secret-key ciphers: