Practical Assignment: Encryption

Jonathan Sumrall, Ryan Lengel

1DV200 Spring 2012

1. Steganography is a method of security through obscurity. It is sending data with- out any encryption, instead sending it disguised as something uninteresting. The difference between this and encryption is that an encrypted message is a message send as a message with techniques done to make it readable only to authorized parties, where as in steganography is not sent with encryption but rather it is thinly veiled behind innocuous data. Thus the steganographed data relies on undetection, and encrypted data relies on strong enough encryption methods. Digital watermarking is a method of steganography where data is embedded in a signal to make the new information added part of the original data. With visible digital watermarking the information can be easily visible in the data. It is often a logo or text identifying something. Hidden watermarking can be added to different data (audio, video, images) but cannot be viewed in the same manner. If used for steganography, it can be used for authentication of data or to send a secret message. It is possible to use this as a communication method for longer use. The purpose of watermarking is to put in information that has difficulty when removing it.

2. The hidden message is: Your package ready Friday 21st room three please destroy this immediately

3. We wrote a program that implements three different encryption methods. The first method is the most simple, the Caesar Cipher. The second is similar to an example in the book. A key can be used that is a string of letters that is used to make the first

part of the substitution ”master key”. Since a substitution works by switching letters for other letters, you build a master function that takes one letter and returns another. So the key for this second method will be the letters that match the first N letters of the alphabet, where N is the length of the given key. If the key is less than the size of the alphabet, then the remaining letters are, starting from the position of the last letter in the key, every K letters down the alphabet modulus the size of the alphabet to induce a wrap-around. In our implementation we set K to the value of 4. The third method we implemented is a transposition method as described by the first example in the textbook, the columnar transposition. For our implementation we did not see a reason to implement the 8 bit limit on the key based on the encryption methods we chose. Initially we were having some issues when dealing with string and char inputs, as *newline* characters were interfering when converting the string into character arrays. We were able to overcome this by reimplementing that particular section of the code using the Scanner class to read in the input.

4. We uploaded two files for students to attempt to decrypt. The first message is done using our substitution method with the key being ”computer”. The second file is a columnar transposition with the key size (number of columns) being 5.

5. We were able to decrypt one of the files that another student uploaded. The student is Saed Zahedi. After doing our encryption, I was able to recognize that he had used the substitution method with a reasonable level of certainty. In his example he encrypted the message with the template, and you could still see the template in the uploaded file. If you know someone has used the subsitution method, it is not too difficult to learn the letter-mapping function. A brute force method would be possible. Also letter frequency analysis would reduce the search space even more. Since we had the template intact, I was able to learn the mapping for 18 characters, which was more than sufficient to decode the message. By doing this we were able to learn his message was (omitting the template and his name): ”Here is my secret message everything is really possible please destroy after reading”.