Network Security Via Cryptographic Validity

Aparicio Carranza
CUNY – NYCC of Technology
186 Jay Street, V626
Brooklyn, NY, USA
718 – 260 - 5897
acarranza@citytech.cuny.edu

Harrison Carranza
Marist College
3993 North Road, Poughkeepsie, NY, USA
845 – 625 - 8336
harrison.carranza2@marist.edu

Sunghoon Jang
CUNY - NYCC of Technology
186 Jay Street
Brooklyn, NY, USA
718 – 260 - 5886
sjang@citytech.cuny.edu

ABSTRACT
Computer and network security is one of most important areas of study nowadays. With the inception of the Internet in the 1990s, the industry has grown at an exponential rate and will continue to rise in the near future. People all around the globe are using this method of communication either for email, chatting, games, transfer of information, and other uses. Although this technology sounds wonderful, there is a downside to it as well. The Internet involves people with malicious intentions and the use of malware, which is software that contains malicious code used for targeting network infrastructures. It is for this reason that the studies of computer networking and security have been emphasized within the last few years. One solution for combating malwares and other threats traveling within the Internet is the use of cryptography. This method consists of encryption and decryption of information, which renders a very robust solution in counter attacking dangerous code that is likely to enter a private network. In this research we will explore some of the cryptographic techniques using hardware/software solution modules to verify the robustness of block ciphers mode, data encryption standard, advanced encryption standard, classical transposition ciphers, public and private key ciphers, and RSA as it applies to network security.

General Terms
Experimentation, Security.

Keywords
Security, Cryptography, Encryption/Decryption, Block Ciphers Mode, DES, Public/Private Keys.

1. INTRODUCTION
In the field of technology, security has become a very crucial topic for several reasons. This topic involves cryptography being a fundamental concept that provides protection from threats and malicious software that are flying around the networks or other sources. The various techniques that are presented in cryptology can help to send or receive messages without much preoccupation of interception from malevolent sources that will use it for criminal intentions [1], [2].

Cryptology is the general science and art of building and analyzing different encryption and decryption methods. It is based on two related concepts: cryptography and cryptanalysis. Cryptography refers to the science of building new more powerful and efficient encryption-decryption methods [1], [8]. Cryptanalysis is the use of techniques and the discovery of weaknesses in existing methods so that plaintext messages can be recovered without the knowledge of a certain key [2], [5]. The basic idea is that this vast concept covers from hiding a message to finding out ways to be able to hide that message in certain ways that cannot be deciphered by other parties [4], [8]. Using several methods that can be applied to network security, we can figure out which technique is more efficient for implementing the various cryptographic procedures.

There are several techniques used in cryptology. Some of the most common methods in this field are the Simple Cipher Analysis, Block Cipher Analysis, Data Encryption Standard Analysis, Keyword Cipher Analysis, Permutation Cipher Analysis, and Vigenere Cipher Analysis [7]. Simple Cipher Analysis involves the shifting of the letters in the message. For this method, the letters are encrypted by a certain number that make all the letters in the message change to a different letter based on the shift [3]. By running all the possibilities, which are from 1-26, one can find out what the hidden message is. Another method, the Block Cipher Analysis, is used to separate the encrypted message, which was derived from the previous method, and split them into several blocks, which is left up to the discretion of the cryptologist [1], [2]. This can also be performed without encrypting he message, but hidden, it makes it more difficult to decipher [8].

One of the fundamental methods of cryptology is the Data Encryption Standard Analysis. This technique allows us to encrypt messages and convert them into their ASCII code values. These values consist of 7 bits, either ones (1's) or zeros (0's) that represent an alphanumeric value on a keyboard [6]. The Keyword Cipher Analysis is the method that has a similarity to the Simple Cipher Analysis. The reason is that in the Simple Cipher, the letters were shifted by a certain amount but were all the same amount. In the Keyword Cipher, the cryptologist gets to choose the value of an actual letter to encrypt the message. This shows that the mix up of the letters being assigned to other letters helps us to make the deciphering of the hidden message more difficult and prevent the hackers from finding a pattern that will easily allow them to figure out the secret message [4]. This method is much more efficient that the Simple Cipher.

The method that requires the use of probability is the Permutation Cipher Analysis, which involves the likeliness of a word, phrase, or letters to appear in a message [7]. It is related to Block Ciphers method because it uses the splitting up of the message into blocks, but without encrypting it. It is up to the cryptologist to play around with the possibilities of encrypting the message. The task would be to find ways to mix up the words in patterns known to the cryptologist so then the steps could be retraced to figure out what the message was to begin with. Another method used in cryptology is the Vigenere Cipher Analysis. This technique makes use of a chart that contains the letters of the alphabet along the side and along the upper part of the table [1], [2]. This method is similar to a coordinate system in which a keyword that is left up to the discretion of the cryptologist is typed and then the letters from the message itself and the keyword are located on the chart. By using the first two letters, for example, we can find what letter

they have in common. The method works using the side or the upper portion of the chart. Once the number of letters in the keyword runs out, then it starts from the beginning and the same concept is applied. For this to be efficient, one has to be familiar with the Vigenere table [3], [5].

In this report, we present the different aspects of firewalls as they are key components in safeguarding the flow of traffic in a networked environment. In Section 2, we discuss "Typical Cryptographic Communication Model," Section 3, shows "Steps to Implement Different Methods of Cryptography". Our Conclusion is presented in Section 4.

2. TYPICAL CRYPTOGRAPHIC COMMUNICATION MODEL

The basic communication model in cryptography is shown in Figure 1 and Figure 2. In Figure 1, Alice and Bob, who are the ones communicating with each other, are having a conversation that has somebody listening in on their message, known as Eve. She is eavesdropping on the conversation and can intercept that information. In Figure 2, however, the model is similar but Alice and Bob use ciphertext to hide their message so only they could understand the conversation and whoever is listening will not be able to comprehend a word of it. This model shows the encryption and decryption of a message for use of transmitting data to another location without worrying about another source taking that message and using it for other purposes.

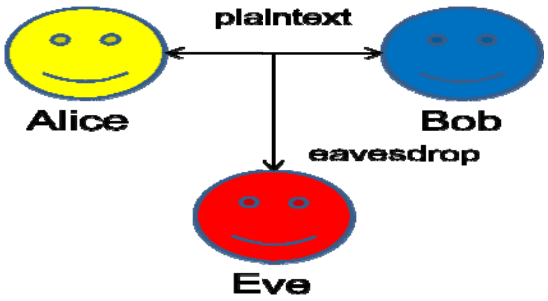

Figure 1: Basic Communication Model

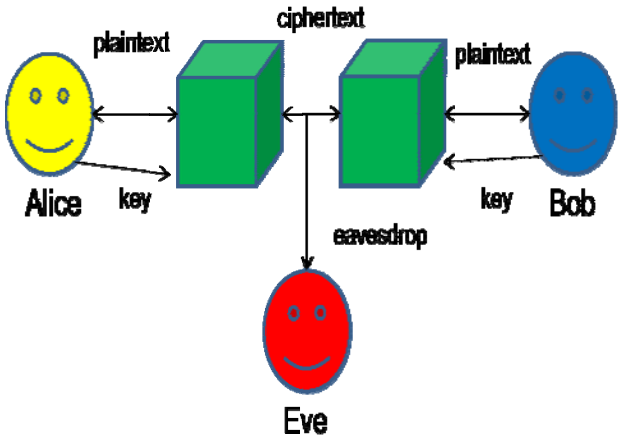

Figure 2: Typical Communication Model with Ciphers

3. STEPS TO IMPLEMENT DIFFERENT METHODS OF CRYPTOGRAPHY

The Systems used for these steps were an HP Notebook with 4GB RAM, 500GB hard disk space and Intel CPU (i5-450M: 2.4GHz) and a Lenovo Notebook 4GB RAM, 320GB hard disk space and Intel CPU (i3-380M: 2.53GHz). For implementing the different methods of cryptology, Windows 7 was used with Cryptographic Analysis Program, or CAP4, to be able to experiment with the various techniques as well as Linux with MATLAB running to run experiments related to cryptology.

One of the methods used was the application of CAP4, which is used to convert plaintext to cipher-text and vice versa for the discovery of different methods of Cryptology, this is shown in Figure 3.

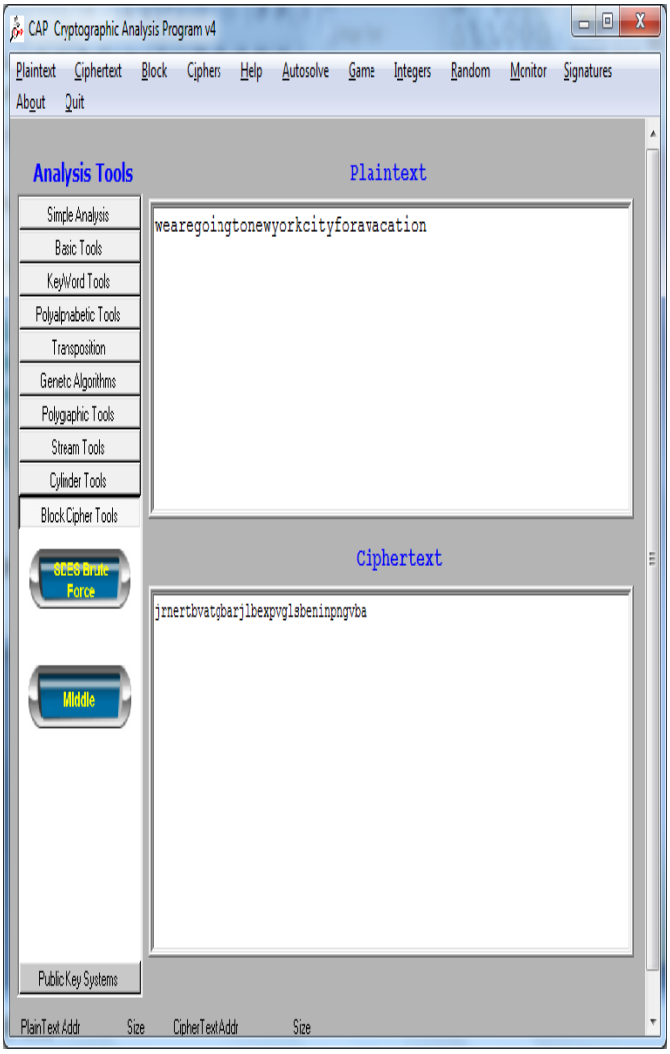

Figure 3: Simple Cipher Analysis Window

Since the message is currently in a plaintext form, to convert it to a cipher-text, type in the value that will be used for shifting the message to encrypt it, as shown in Figure 4.

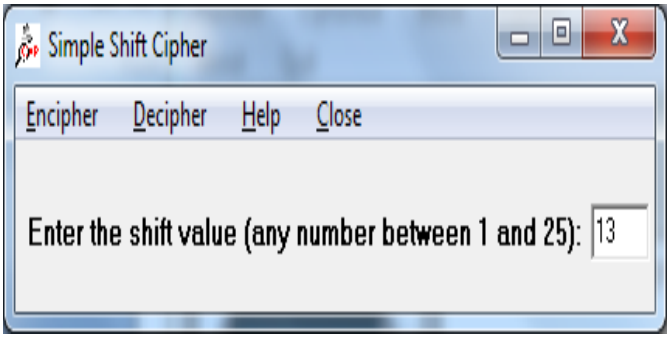

Figure 4: Simple Cipher Analysis Shift Value

According to Figure 5, the sample text shows a long list of encrypted messages with a key next to it. The only key that actually displays a meaningful message is 13, because that is the shift value used in the previous step.

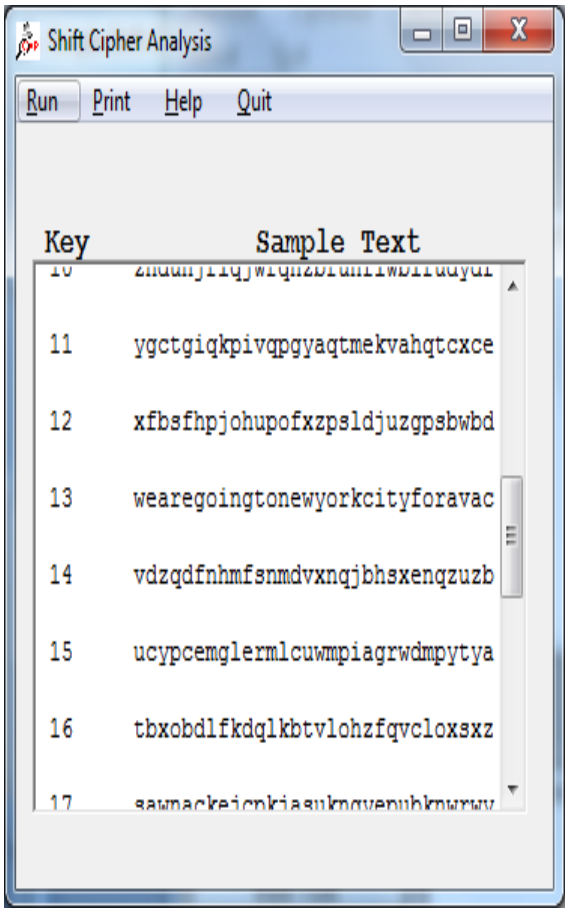

Figure 5: Simple Cipher Analysis Sample Text List

Another method used is the Block Cipher Analysis, as shown in Figure 6. This method separates the encrypted message into blocks of a certain amount, depending on what the user may decide. Here, it is split into blocks of five.

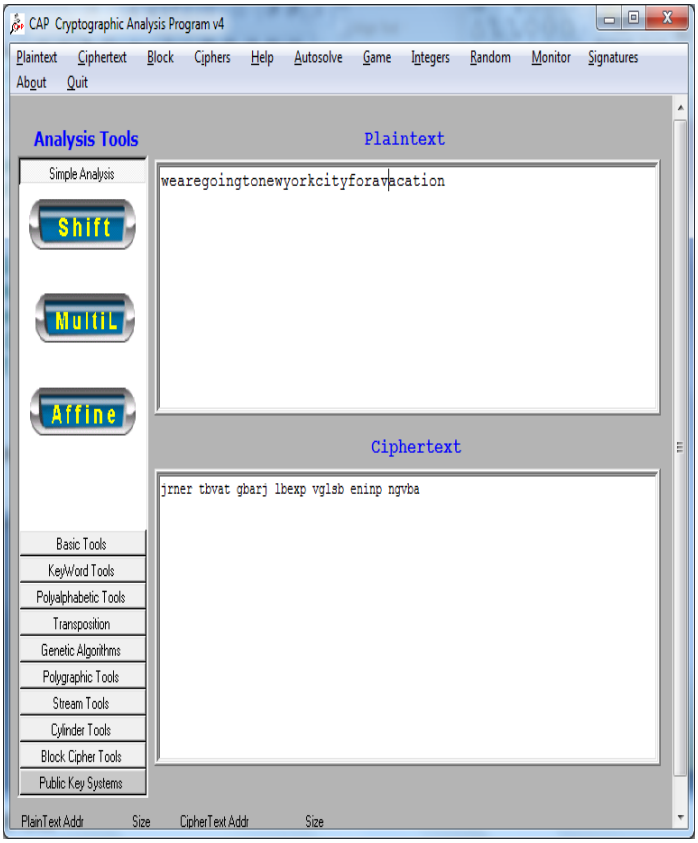

Figure 6: Block Cipher Analysis Window

In Figure 7, we are prompted to choose a value for this method. In this case, we use 5 as the block size because the message is 35 characters long and therefore 5 is an even number that fits into that length.

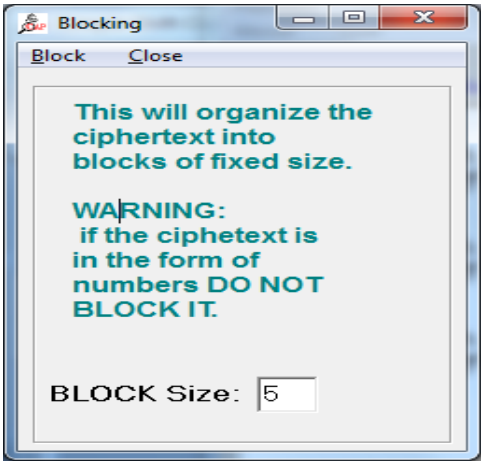

Figure 7: Block Cipher Analysis Size Blocking

One of the methods studied involves Data Encryption Standard, which converts a plain message into its respective character ASCII code. Each character is represented by a series of bits that are 1s or 0s, which is shown in Figure 8.

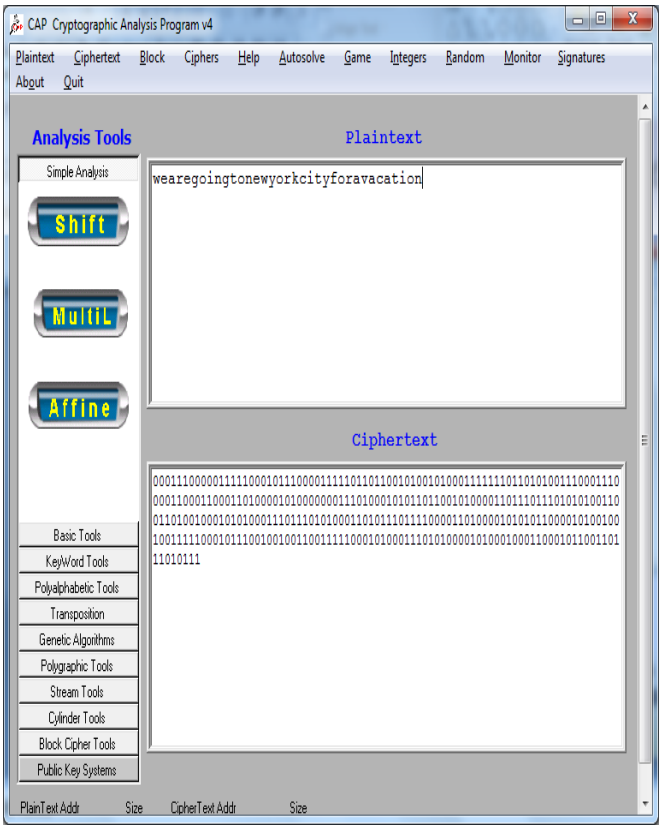

Figure 8: Data Encryption Standard Analysis Window

One of the methods experimented with was the use of Keyword Cipher Analysis, which is similar to the Simple Shift Cipher because the letters or characters are shifted a certain amount. The difference here is that the cryptologist assigns a certain letter or character to another letter or character by entering a keyword that will mix up all the alphabet letters to make a message that no one can be able to decipher, as shown below in Figure 9.

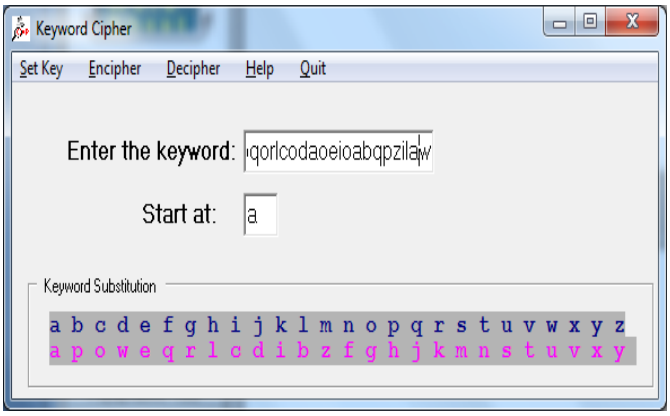

Figure 9: Keyword Cipher Analysis Options

One possibility in trying to decrypt a message or to test to see if our encrypted message cannot be deciphered that simply is by running the Word Patterns program in which we type in a letter or character that would give us a certain amount of matches of certain words or ciphers that are likely of being inside the hidden message. Options include possible letter substitutions that could lead to the discovery that a Keyword Cipher was used to encrypt this message. This is demonstrated below in Figure 10.

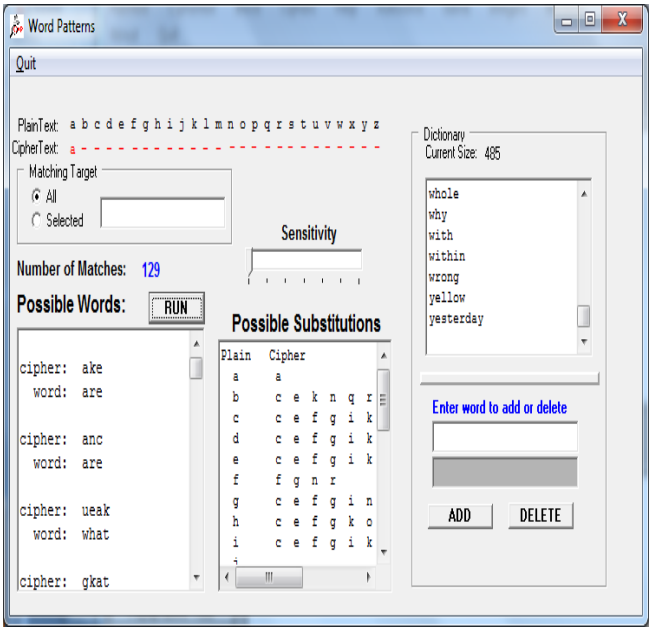

Figure 10: Word Patterns Window

Once the keyword has been typed, the message then is converted into a cipher-text based on the typed keyword, as shown in Figure 11. The letter assigned to another letter will appear in the hidden message. For example, a ‘w’ would be replaced by a ‘u’ and the first letter of the cipher-text is ‘u’ because that was what was assigned by the cryptologist.

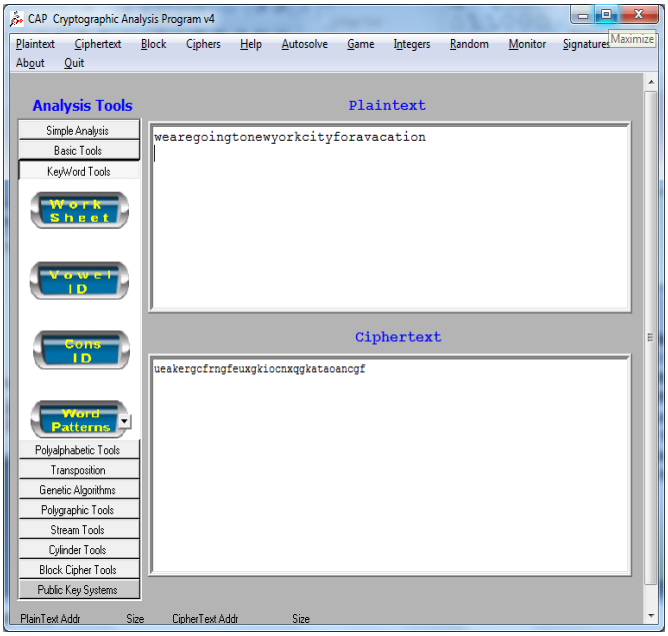

Figure 11: Keyword Plaintext and Cipher-text

One of the methods that uses probability is called Permutation, as displayed in Figure 12, in which one can separate the message into blocks, similar to the Block Cipher, and then rearrange them in many ways to disorient whomever is trying to access that message.

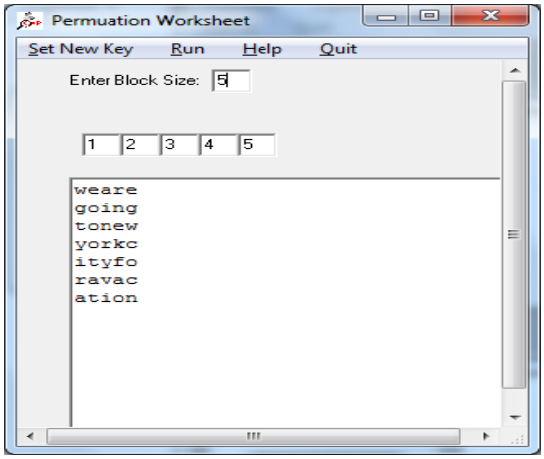

Figure 12: Permutation Worksheet displaying message in blocks

One of the words in the message is 'vacation'. Since it is assumed that it is a known word, it is typed and there are possible key permutations that appear to give us possibilities that the word exists in the message. In total there are about 32 matches, as shown in Figure 13. Since 'tio' is part of the word 'vacation', there are positive indications that this word is hidden in the complete message.

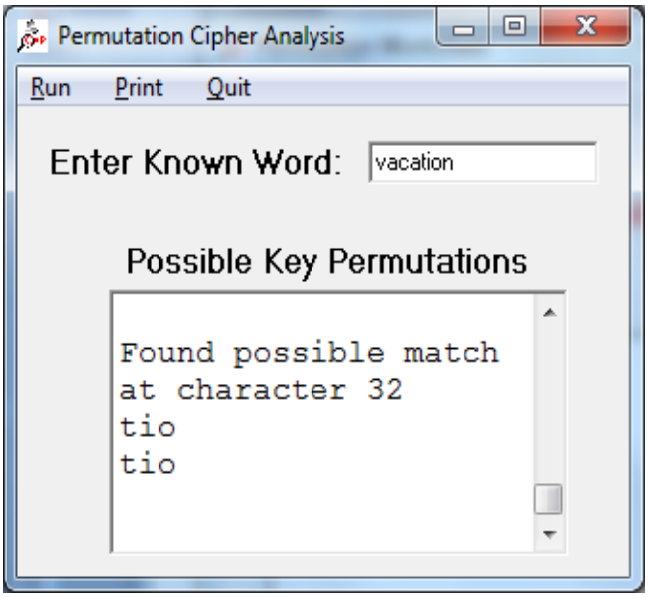

Figure 13: Permutation Key Possibilities

Based on the permutation key and cipher block cipher methods, we can rearrange the message that has been separated into blocks. The first letter of each block is taken to form a word, followed by the second letter of each block for another separate word, and so on. By performing this method, the results below are obtained (Figure 14).

Figure 14: Combination of blocks rearranged to form different words

A fundamental method in cryptography is the use of the Vigenere Table, shown in Figure 15. This table is a chart that lists all the letters of the alphabet on the top and along the side. Using our example, 'wearegoingtonewyorkcityforavacation', we can use this table by typing in a keyword separately in order to match the letter we are looking for (Figure 16). This would represent a coordinate system for cryptology. The 'h' is typed as the first letter of the keyword and the 'w' from the actual message can be matched up. When the two letters are match on the table, our result is a 'd', which would represent the first letter of the cipher-text. In this method, choosing either side will produce the same result.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Figure 15: Vigenere Table

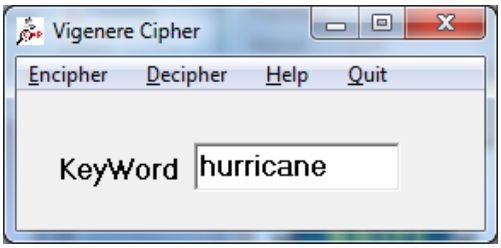

Figure 16: Vigenere Cipher Keyword

Based upon the previous figures, we can see the plaintext message along with the encrypted cipher-text that was produced by using the Vigenere method. The figure below, Figure 17, displays the actual message that would be produced from using this technique.

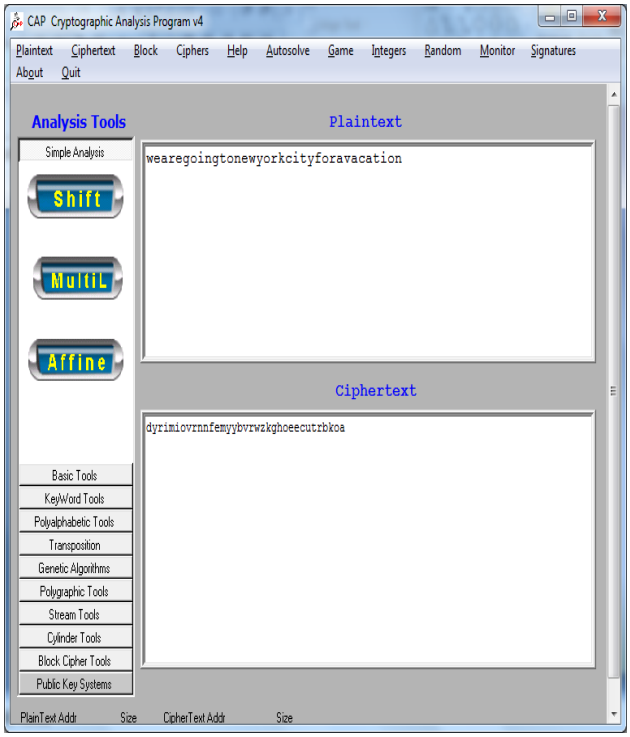

Figure 17: Vigenere Method Plaintext and Cipher-text

4. CONCLUSION

Cryptology is a fundamental concept in the technology industry. In security, it helps to protect the data that we have stored on our machine hard drives as well as only allow access to certain users by means of setting up encrypted passwords or messages. Cryptography is very useful for sending messages via the Internet without worrying too much if it gets intercepted or falling into the wrong hands because then it would be of no use to them. By analyzing various and different techniques of cryptanalysis, there are options available to secure our valuable information from malicious hackers, or crackers. This concept will only continue to grow because the demand of network security using cryptographic techniques will be of good use when it comes to dealing with confidential information being sent across a long distance. Based on my experimentations, I found that the Vigenere Analysis, Keyword Analysis, and Data Encryption Standard are some of the best methods to use in the field of cryptology. Overall, learning cryptography is not only useful but fun because it allows us to use critical thinking to find a way to encrypt a given message and deductive reasoning to decrypt it.

5. REFERENCES

[1] R.J. Spillman. Classical and Contemporary Cryptology. Pearson Prentice Hall: Upper Saddle River, New Jersey, 2005

[2] W. Trappe and L.C. Washington. Introduction to Cryptography with Coding Theory. Pearson Prentice Hall, Upper Saddle River, New Jersey, 2006

[3] R. Nichols. Classical Cryptography Course, v1 and v2 Aegean Park Press, 1996.

[4] Rob Churchhouse. Codes and Ciphers. Cambridge, 2002.

[5] Paul Garrett. Making, Breaking Codes. Prentice Hall, 2001.

[6] E. Biham and A. Shamir. Differential Cryptanalysis of the Data Encryption Standard Springer-Verlag, 1993.

[7] N. Fergus and B. Schneier. Practical Cryptography. Wiley, 2003.

[8] Bruce Schneier. Secrets and Lies. Wiley, 2000.