Journal of Innovative Technology Convergence
Vol. 3, No. 1 June 2021, pp. 35-42

Cross-Crypto Algorithm: Leveraging the Features of the ROT13 and Vigenère Ciphers

Ryan Ercel O. Paderes*

Abstract: Nowadays, the Internet has become the primary option for conducting business transactions, accessing various services, and communicating. Being online also brings cybersecurity threats that have been rapidly increasing. Various security techniques and cryptography schemes have been employed to safeguard our systems and online transactions; however, some of these techniques might be unreliable or insufficient. This paper deals with the integration of features of the ROT13 algorithm and Vigenère ciphers to form a cross-crypto algorithm for encrypting and decrypting the files or information that we intend to transmit online. The proposed technique employs a two-stage encryption process, leveraging the features of both the ROT13 and Vigenère cipher algorithms.

Keywords: Cross-Crypto Algorithm, ROT13, Vigenère Cipher, Cryptography

1. Introduction

We are living in a digital era, and definitely, people are using high-end technology devices where they are able to store their important files. The use of the Internet is rapidly increasing, so privacy and confidentiality become more and more important. Even if people tend to have a permanent online presence, they are still concerned with their own privacy and prefer to have their online transactions confidential. There are times that people feel that a number of private photos, audit logs, or some important documents on the computer, more so on the Internet, are not secured. In this regard, there is an increasing demand for file encryption that will be helpful to secure these files.

Security is as important as privacy. Most of the data that exists today is confidential and should be protected. Such information includes bank account numbers, credit card details, email addresses, personal information, passwords, *etc*. Without cryptography, this data can be maliciously exploited by cybercriminals. Cryptography, which comes from the Greek words kryptos and graphein, which mean hidden and writing, respectively, refers to the use of codes and ciphers to protect secret messages [1][2]. It provides security and protection to information and communications through methods such as

* College of Computer Studies, University of Antique, Sibalom, Antique, Philippines
Email: jingryan19@gmail.com

Received [February 6, 2021]; Revised [April 23, 2021]; Accepted [May 8, 2021]

Published by InnoCon Publishing
ISSN 2704-4440

encryption, sender/receiver identity authentication, digital signatures, and other related techniques. Cryptography functions often include confidentiality, integrity, availability, authenticity, and non-repudiation.

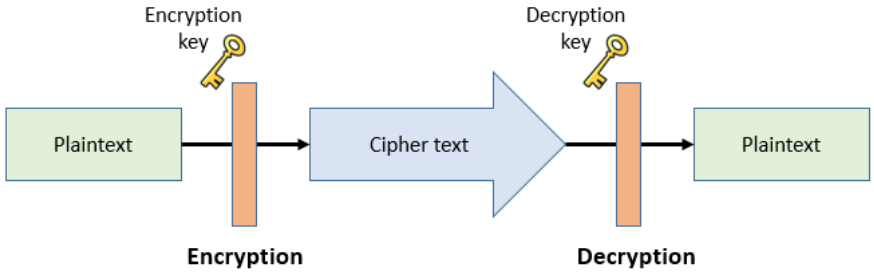

Figure 1. Cryptography

Encryption is one of the techniques used in cryptography, as depicted in Figure 1, to provide security and protection to information and communication. Encryption is generally a technique used to conceal messages by converting them into unreadable forms. This technique employs algorithms to encode the message to help safeguard private information, documents, files, and sensitive data and provide robust security in communications. Encryption is used to guarantee the integrity, confidentiality, and authenticity of information. The messages that undergo the encryption process result in cipher texts that can only be decrypted or accessed by individuals who hold the correct encryption key [3]. Encryption algorithms include Advanced Encryption Standard (AES) [4], Data Encryption Standard (DES) [5], Rivest-Shamir-Adleman (RSA) [6], Blowfish [7], Elliptic Curve Cryptography (ECC) algorithm [8], Vigenère cipher [9], and many more.

Nowadays, there are many existing encryption algorithms that can be used to protect information over the Internet. However, its reliability cannot be guaranteed. Thus, in this study, a reliable cross-crypto algorithm has been devised that leverages the features of both the ROT13 and Vigenère Cipher algorithms. This cross-crypto algorithm is aimed at encrypting a file or files with the use of a substitution cipher and a polyalphabetic cipher using a more reliable encryption algorithm. In addition, a backup of the original files to be encrypted is created in case of damage during the encryption or decryption, and a backup of the encrypted files for transmission is also created in case of damage during the transmission.

The rest of this paper is organized as follows: Section 2 discusses the related cryptography algorithms that were utilized in the realization of the cross-crypto algorithm; Section 3 outlines the processes involved in the encryption and decryption of files using the cross-crypto algorithm; and Section 4 concludes the study.

2. Related Algorithms

This section discusses the related algorithms that help in realizing a reliable and functional cross-crypto algorithm to secure and maintain the confidentiality of information or files. The algorithms used in the encrypting and decrypting processes include ROT13 and Vigenère Cipher.

2.1 Tabula Recta

A Tabula Recta, invented by Johannes Trithemius in 1508, refers to a square with 26 alphabets in it [10][11]. Each alphabet was shifted one letter to the left from the one above it and started again with A after reaching Z, as shown in Figure 2. The tabula recta is used to define a polyalphabetic cipher and is often referred to in discussing pre-computer ciphers, such as the Vigenère cipher.

	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 2. Tabula Recta

2.2 Vigenère cipher

The Vigenère cipher refers to a form of polyalphabetic substitution utilized for encrypting alphabetic text by using a series of different Caesar ciphers [9]. It makes use of the tabula recta, a matrix of 26 alphabets invented by Johannes Trithemius in 1508, to perform the encryption process. The tabula recta, also known as the Vigenère square or Vigenère table, consists of a matrix of alphabets written in 26 rows, each shifted cyclically to the left in each row, as shown in Figure 2.

The Vigenère cipher consists of Caesar ciphers in sequence with different shift values from the alphabets in the tabula recta. Choosing the alphabet to substitute each character of the plaintext depends on the pairing of its key. A key, whose length must be the same as the plaintext, can be any text chosen randomly by the sender of the plaintext. If the key is shorter than the plaintext, its alphabets are repeated to match the length of the plaintext.

For example, the plaintext to be encrypted is “COMPUTER SCIENCE”. The sender of the message chooses a keyword and repeats it until it matches the length of the plaintext. In this case, the chosen key is “COMSCI”, and to match the plain text, the key becomes “COMSCICOMSCICOM”. In the tabula recta, the keys are indicated as rows and the plaintext as columns. The resulting cipher text will be the intersection of the pairs of the key and plaintext alphabets.

- Plaintext: COMPUTERSCIENCE
- KEY: COMSCICOMSCICOM
- Cipher text: ECYHWBGFEUKMPQQ

In this example, the first letter of the key is “C”, which means we go to row C, and the first letter of the plaintext is also “C”, which means we go to column C. Their intersection corresponds to “E”, which will be the first alphabet of the Vigenère cipher text. For the second pair, the plaintext alphabet “O” is paired with the key “O”, resulting in “C”, which will be the second alphabet for the Vigenère cipher text. After repeating the process for the entire plaintext, the derived cipher text, which will be transmitted to the receiver, results in “ECYHWBGFEUKMPQQ”. Figure 3 shows the Vigenère cipher encryption process.

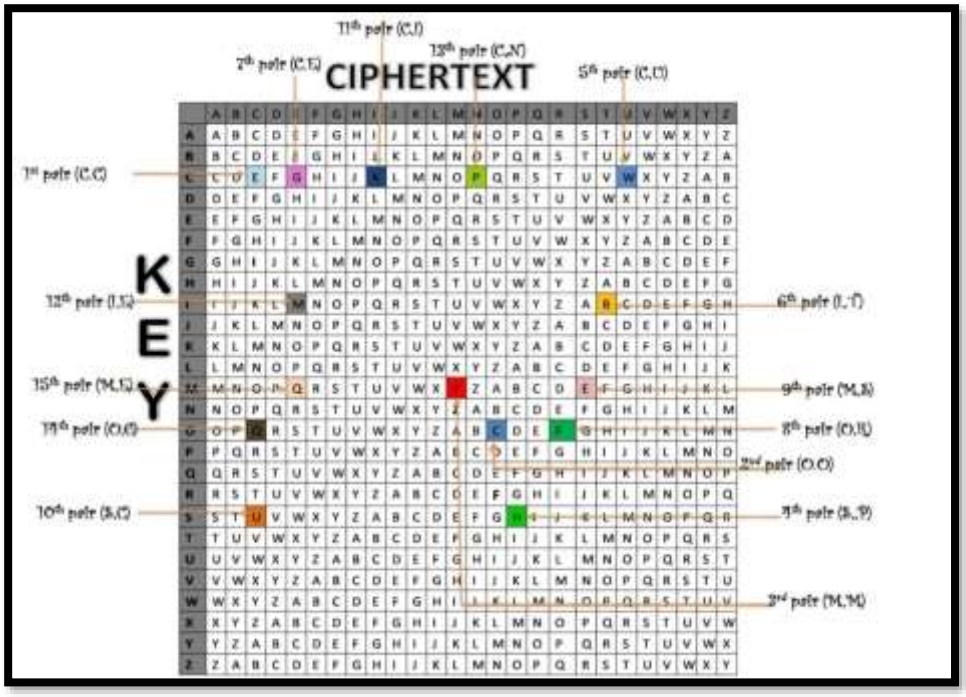

Figure 3. The Vigenère Algorithm Encryption Process

2.3 ROT13

ROT13, or ROT-13, literally means to rotate by 13 places. In order to encrypt or decrypt a message, every letter is shifted 13 places. ROT 13 divides the alphabet of 26 letters into 2 groups (*i.e.*, 2 ×13), where the first group consists of letters from A to M and the second group consists of letters from N to Z, as shown in Figure 4. The substitution of plaintext letters is so simple that every letter is replaced by the 13th letter in the alphabet [12]. For example, the letter “A” becomes “N”, “B” becomes “O”, …, and “M” becomes “Z”. Then, “N” becomes “A”, “O” becomes “B”, …, and “Z” becomes “M”. The substitution is limited to alphabetic characters only, and other characters, such as numbers, symbols, punctuation, and spaces, remain unchanged after the ROT13 encryption or decryption process.

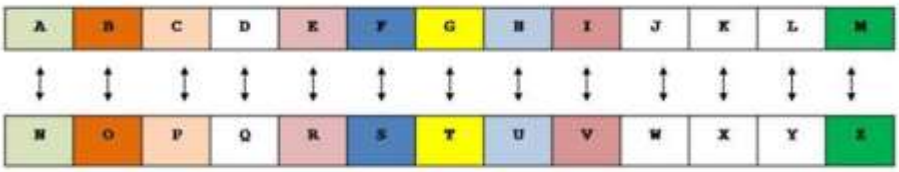

Figure 4. The ROT13 Substitution Process

The ROT13 algorithm is also known as a reciprocal cipher. The same process for encrypting a message is applied to the decrypting process; thus, the ROT13 algorithm is considered to provide virtually no cryptographic security and is often cited as an acknowledged example of weak encryption [13]. However, ROT13 can be used to hide spoilers, punch lines, puzzle solutions, and offensive materials from casual glances.

3. The Proposed Cross-Crypto Algorithm

The proposed cross-crypto algorithm is developed by combining the ROT13 and Vigenère Cipher algorithms to enhance the security of information or files being transmitted over the Internet. It utilizes the features of the two algorithms to come up with a more secure and reliable encryption technique, as depicted in the framework shown in Figure 5.

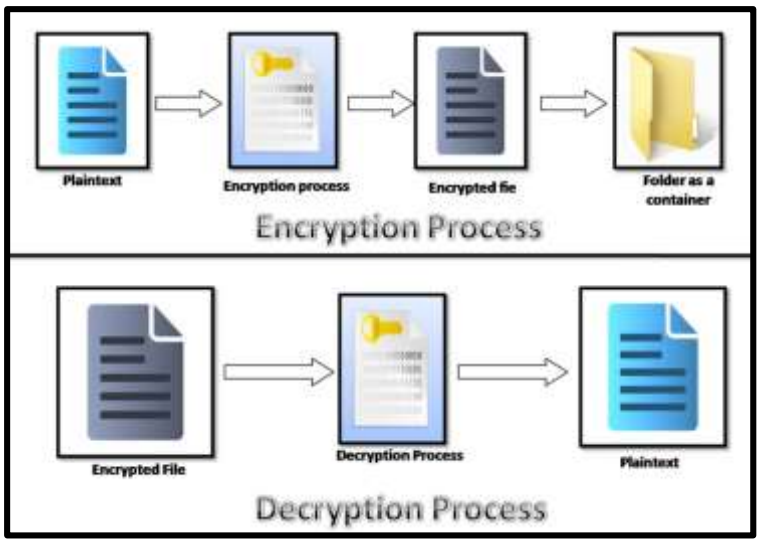

Figure 5. The Cross-Crypto Algorithm Operations

The concept of this study is to provide a key for the encryption and decryption process, which must consist of a minimum of six (6) and a maximum of fifteen (15) characters. Only the letters of the alphabet can be repeated, and numbers or special characters will not be allowed.

3.1 The Encryption Process

From the word "ROT13" itself, it means that the word itself rotates by 13 places. The alphabet has 26 letters and has exactly two sets of thirteen letters that match the length of the rotation. It is separated into two sets so that each letter has its own counterpart, and then the sequence continues at the beginning of the alphabet. The first set of letters is from A to M, and the second set is from N to Z. The first set of letters is the counterpart to the second set of letters, and then the sequence continues at the beginning of the alphabet.

For example, the counterpart of "A" is "N", and vice versa, the counterpart of "B" is "O", and so on. Only those letters that occur in the English alphabet are affected; numbers, symbols, spaces, and all other characters are left unchanged. Since there are 26 letters in the English alphabet and $26 = 2 \times 13$, the ROT13 function has its own counterpart. In Figure 6, for example, the plaintext to be encrypted is "COMPUTERSCIENCE".

The first step in the encryption process is to "shift each letter of the plaintext (*i.e.*, keyword) by forwarding thirteen letters in the alphabet" in order to come up with the first cipher text, as shown in Figure 6. The plaintext "COMPUTERSCIENCE" will be used for this example.

- Plaintext: COMPUTERSCIENCE
- First cipher text: PBZCHGREFPVRAPR

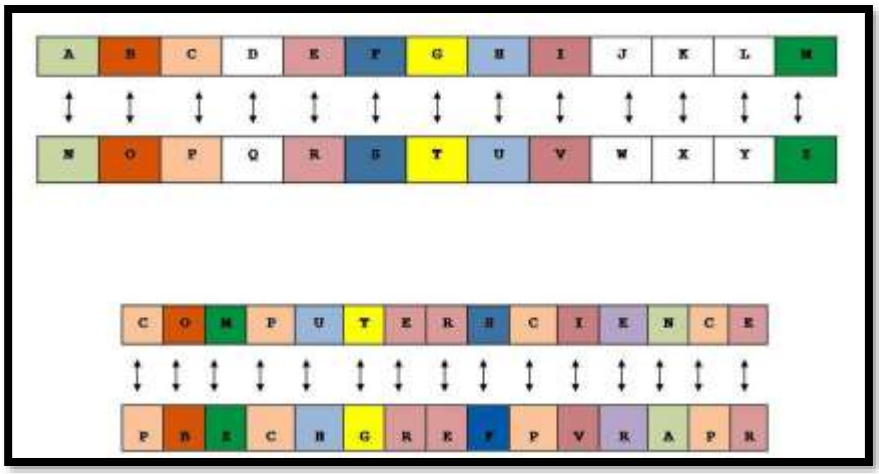

Figure 6. The First Stage of the Encryption Process Using ROT13

The second step in the encryption process is to encrypt the first cipher text, "PBZCHGREFPVRAPR". A keyword will be chosen, in this case, the keys will be comprised of 6 characters, "COMSCI", but the keyword is repeated to match the length of the first cipher text (*i.e.*, COMSCICOMSCICOM). Then, use the Tabula Recta to encode the keyword. From the first cipher text, we will be using the Tabula Recta to come up with the final cipher text. Figure 7 illustrates the second step in the encryption process.

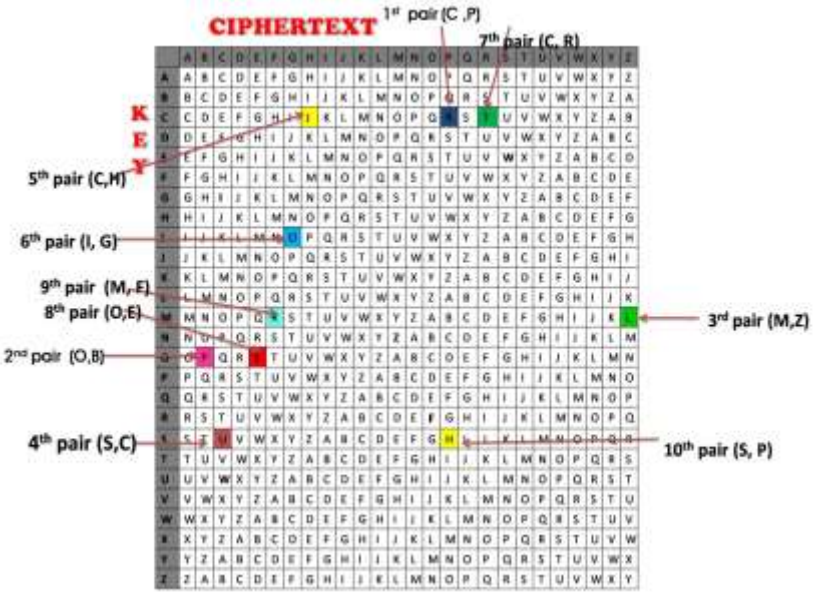

Figure 7. The Second Stage of Encryption Process Using the Vigenere Cipher

The process is performed by going down to the rows and columns of the Tabula Recta. The top row represents the first cipher text, and the letters in the leftmost column represent the keyword COMSCI. Encode the first letter of the cipher text, which is “P”, and the first letter of the keyword, which is “C”. That is, “P” is paired with “C”, which means that in column P and row C of the Tabula Recta, it corresponds to the letter “R”, which will be the first character in the final cipher text. Repeat the process in the next pair, which is comprised of “B” from the first cipher text and “O” from the keyword, which results in “P”. Thus, the second character of the final cipher text will be “P”. Repeat the process until the last character of the first cipher text comes up with the final cipher text.

- Plaintext: COMPUTERSCIENCE
- First cipher text: PBZCHGREFPVRAPR
- Keyword: COMSCICOMSCICOM
- Final cipher text: RPLUJOTSRHXZCDD

3.2 The Decryption Process

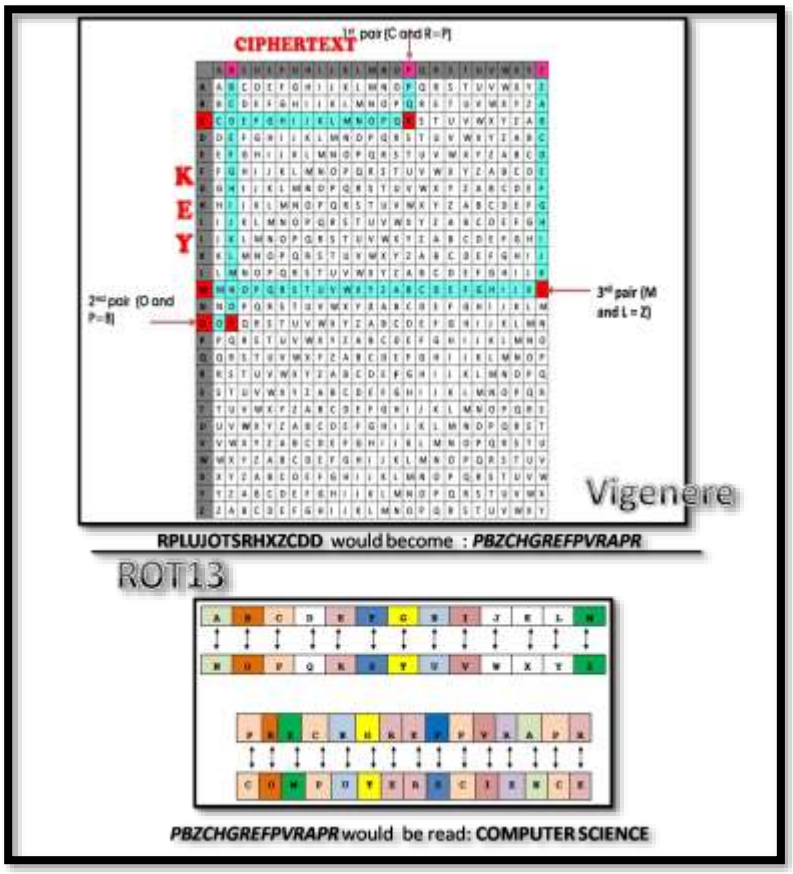

Figure 8. The Decryption Process for the Proposed Cross-Crypto Algorithm

The first step in the decryption process is to refer to the first column of the graph and find the first letter of the keyword, in this case, “C” in the keyword “COMSCICOMSCICOM”. Then, in this row, locate the column of the table that corresponds to the first letter of the final cipher, in this case, “R”, from the cipher “RPLUJOTSRHXZCDD”. In Figure 8, it is indicated by the first pair of “C” and “R”, which results in “P”. “P” will be the first character in the next cipher to be decrypted. Repeat the process until the last letter of the first cipher text, “PBZCHGREFPVRAPR” has been reached.

The next step in the decryption process is to decipher the first cipher text, "PBZCHGREFPVRAPR" based on the table of ROT13, as shown in Figure 6. Find the counterpart of every letter of the cipher text to obtain the plaintext "COMPUTERSCIENCE".

4. Conclusions and Recommendations

This study leveraged the features of both the ROT13 and Vigenère Cipher algorithms to develop a functional and reliable Cross-Crypto algorithm in securing the information and files that are being transmitted over the Internet. Using the combination of ROT13 and Vigenère Cipher in file encryption and decryption processes can be helpful because it can create a more reliable and unbreakable cipher. Ordinary people without the knowledge of the said algorithm cannot easily decrypt the files.

In the future, further studies and experiments on this study will be conducted to fully strengthen the security of the combined encryption method. That is, it is aimed at integrating hash functions and signatures into the Cross-Crypto algorithm.

References

[1] ISO, "*What is Cryptography?*", www.iso.org/information-security/what-is-cryptography (Accessed August 12, 2020).

[2] New World Encyclopedia, "*Cryptography*", www.newworldencyclopedia.org/entry/Cryptography (August 12, 2020).

[3] Simplilearn, "*What Is Data Encryption: Types, Algorithms, Techniques and Methods*", www.simplilearn.com/data-encryption-methods-article (August 12, 2020).

[4] M. J. Dworkin, E. B. Barker, J. R. Nechvatal, J. Foti, L. E. Bassham, E. Roback, J. F. Dray, "*Advanced Encryption Standard (AES)*", Federal Information Processing Standards, (NIST FIPS), National Institute of Standards and Technology, Gaithersburg, MD, doi: 10.6028/NIST.FIPS.197 (Accessed September 10, 2020).

[5] Ziaullah, "*Data Encryption Standard (DES)*", Medium, www.medium.com/@ziaullahrajpoot/data-encryption-standard-des-dc8610aafdb3 (Accessed September 10, 2020).

[6] N. Malviya, "*Introduction to the Rivest-Shamir-Adleman (RSA) Encryption Algorithm*", Infosec, www.infosecinstitute.com/resources/cryptography/introduction-to-the-rivest-shamir-adleman-rsa-encryption-algorithm/ (Accessed February 5, 2021).

[7] Schneier on Security, "*The Blowfish Encryption Algorithm*", www.schneier.com/academic/blowfish/ (December 6, 2020).

[8] N. Sullivan, "*A (Relatively Easy to Understand) Primer on Elliptic Curve Cryptography*", The Cloudflare Blog, www.blog.cloudflare.com/a-relatively-easy-to-understand-primer-on-elliptic-curve-cryptography (December 6, 2020).

[9] J. Rubin, "*Vigenere Cipher*", www.juliantrubin.com/encyclopedia/mathematics/vigenere_cipher.html (August 12, 2020).

[10] A. Ahmed, "*Understanding Cryptography - Part 3*", Medium, www.medium.com/@neothedefender/understanding-cryptography-part-3-23db63c96d62 (December 6, 2020).

[11] D. Salomon, "*Data Privacy and Security*", Springer Science & Business Media, Berlin, Germany, 2012, ISBN: 038721707X.

[12] B. Schneier, "*Applied Cryptography, Second Edition: Protocols, Algorithms, and Source Code in C (cloth)*", John Wiley & Sons, Inc., New Jersey, United States, January 1996, ISBN: 0471128457.

[13] C. Swenson, "*Modern Cryptanalysis: Techniques for Advanced Code Breaking*", John Wiley & Sons, Inc., New Jersey, United States, March 2008, ISBN-13: 978-0470135938.