International Journal of
Advances in Scientific Research and Engineering (ijasre)

E-ISSN : 2454-8006

DOI: 10.31695/IJASRE.2021.34010

Volume 7, Issue 5
May - 2021

Encryption of Data based on Triple encryption and Affine Algorithm

Zahraa Salah Dhaief

Department of Computer Science

College of Education, Mustansiriyah University

Baghdad

Iraq

ABSTRACT

In recent years in view of the recent scientific and technological development, Encryption has emerged as a solution and is critical in the information security system. To protect the shared data, a variety of techniques are needed. To begin, data must be encrypted before being sent from sender to receiver using a cryptographic algorithm for encryption. Second, the receiver can display the original data using decryption techniques.

Encryption is a well-known method of safeguarding classified information. It is a procedure for converting text or data into an unreadable format for the purpose of hiding this data or is converting plaintext to cipher text is an operation. In conjunction with an algorithm or a key. The current research focuses on using cryptography to protect data as it is being transmitted, we implemented three encrypt techniques (Caesar-Reversing-zigzag) by combining the three codes called triple encryption for encrypting the message, re-encoding the encrypted text using the affine cipher. The present work is implemented by using Visual Basic 6.

Key Words: *Cryptography, Encryption, Caesar Cipher, Reversing Cipher, Affine Cipher***.**

1. INTRODUCTION

With the emergence of internet-based digital forms of communication, multimedia data protection is becoming increasingly important. The usage of a diverse set of data, videos, and photographs in a variety of applications nowadays draws a lot of attention to security and privacy concerns. In transit or storage, multimedia data encryption helps to avoid unnecessary and unauthorized disclosure of sensitive information. Cryptography has three main goals in terms of multimedia information security: confidentiality, data integrity, and authentication [1].

2. CRYPTOGRAPHY

Secret writing necessitates the use of cryptography. It's the science of data security. Cryptography is used to ensure that a message's contents are sent in a safe and unaltered manner. Cryptography offers a variety of security targets to ensure personal privacy. The concept of encryption is that we should encrypt our precious data in a hidden code that cannot be read by unauthorized people, even if it is hacked [2].

There are a few key terms in cryptography.

1. **Plain Text: -** A readable secret message or information that will get encrypted.

2. **Encrypted Text or Cipher Text:** - Cipher text is material that has been encrypted with the aid of a key.

3. **Key: -** key can be defined as an attribute or word which used in plaintext encryption - Decryption [2].

A simple message or piece of information is converted into ciphertext, which is then decrypted back into plaintext, as seen in the block diagram below.

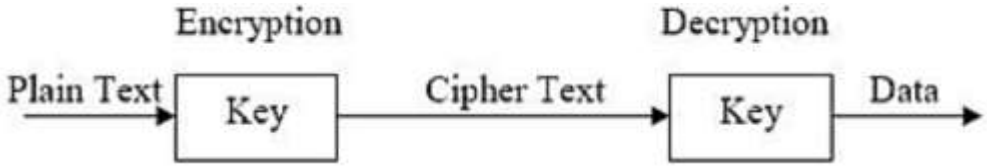

Figure 1.1: An easy-to-understand block diagram of cryptography.

Cryptography is a crucial method for safeguarding multimedia information. Before being transmitted over the internet, all multimedia files are encrypted. Because of the file's encryption, it is worthless to someone who does not have access to the keys. As a result, someone other than the service provider does not have access to the key for decrypting the content. Encryption is a method of protecting data from unauthorized access by transforming it into a format that no one can read. Data encryption is the process of making data, during transmission, such as text, image, or audio, it becomes unreadable, invisible, or impenetrable. The receiver simply reverses data encryption, which is known as data decryption, to recover the original data. C = E (P, K) can be used to define the encryption method where P denotes the original results. E stands for Encryption Algorithm. Encryption Key (K) C= Cipher code, which is sent out and can be intercepted. P= D(C, K) can be used to explain the decryption process where C stands for Cipher Message and D stands for Decryption Algorithm. P= Recovered data; K= Decryption Key [1].

3. ENCRYPTION ALGORITHMS

In the field of information security, every encryption algorithm is commonly accessible and used. Symmetric (private) and asymmetric (public) keys encryption are the two types. Only one key is employed to encrypt and decrypt data in symmetric keys encryption, also known as secret key encryption. Asymmetric keys use two types of keys: private and public keys. A public key is employed to encrypt data, and a private key is used to decrypt it (e.g. RSA). Public key encryption is focused on computationally intensive mathematical functions. Cryptography algorithms such as DES and AES have many examples of strong and weak keys. DES uses a single 64-bit key, while AES employs a variety of 128,192,256-bit keys. To solve the problem of key distribution, asymmetric key encryption or public key encryption is used. Asymmetric keys use two types of keys: private and public keys. A public key is employed to encrypt data, and a private key is employed to decrypt it (E.g. Digital Signatures and RSA). Since customers often use two keys: a public key that can be employed by anyone and a private key that is single employed by the customer. They do not need to be distributed prior to transmission. Public key encryption, on the other hand, is based on mathematical functions and is computationally intensive. [3].

4. PROPOSED ALGORITHMS

4.1 Caesar Cipher

Is an old method created by Tsar Julius to work encrypted messages between sectors of the Army has proven effective in his time. To interact with his troops, Julius Caesar used a cipher that was additive. As a result, the Caesar Cipher is often used to refer to additive ciphers. Caesar communicated using a key in the number three. One of the wide spread famous encryption-decryption algorithms in cryptography is the Caesar cipher. The Caesar cipher is a substitution type cipher that replaces every letter in the plaintext with a letter located a certain the number of letters in the alphabet. The encryption is represented using modular arithmetic. With a change of three, for example, A will be replaced by D, B by E, C by F, and so on10. As seen in Table 1, this is the scheme. The genuine alphabets are appeared in the first row, while the second row shows the replacement alphabets. The algorithm can then be written as follows: [4].

Substitute the cipher text letter for each plaintext letter p:

$C = E(3, p) = (p + 3) \bmod 26$ ..... (1)

A change can be of any size, so the Caesar algorithm in general is:

$C = E(k, p) = (p + k) \bmod 26$ ..... (2)

Where k is a number between one and twenty-six. The decryption algorithm is straightforward.

$p = D(k, C) = (C - k) \bmod 26$ .....(3)

DOI: 10.31695/IJASRE.2021.34010

Table 1.1. Demonstrates layout for encoding text that involves substituting an alphabet three spaces down the line for each alphabet

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
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

Example: Encode the following message **"hello"** by using the code Caesar**.**

P: h→07 encryption (07+3) mod26 **c: 10→k**

P: e→04 encryption (04+3) mod26 **c: 07→h**

P: l→11 encryption (11+3) mod26 **c: 14→O**

P: l→11 encryption (11+3) mod26 **c: 14→O**

P: O→14 encryption (14+3) mod26 **c: 17→R**

To decrypt the message **"khoor"** we subtracting the character of the decryption key which is 3

c: 10→k decryption(10-3)mod26 **p:07→h**

c: 07→h decryption(07-3)mod26 **p:04→e**

c: 14→l decryption(14-3)mod26 **p:11→l**

c: 14→l decryption(14-3)mod26 **p:11→l**

c: 17→r decryption(17-3)mod26 **p:14→O**

4.2 Reverse Cipher

The reverse cipher scrambles a letter by printing it backwards, the way a very simple and all in the matter is replaced by the character the first place last character, second letter letter pre last.

So **"Hello"** becomes **"olleH."** Decryption is as simple as reversing the reversed message to obtain the original message. Encryption and decryption follow similar steps.

The reverse cipher is an extremely vulnerable cipher. You can tell it's in reverse order just by looking at the cipher text [5].

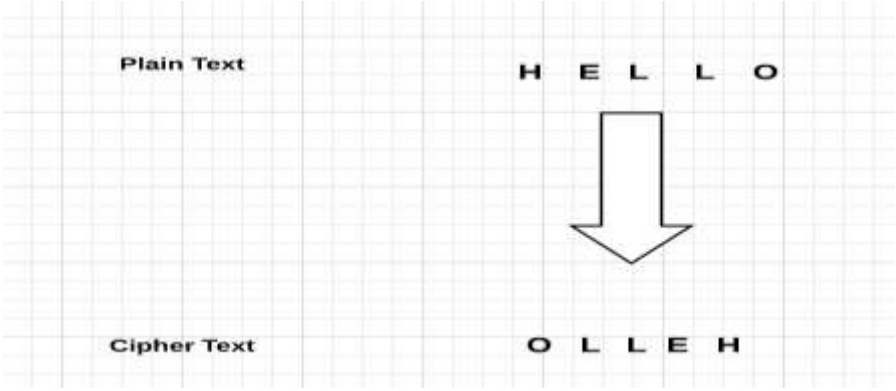

Figure 1.2: Example how to work reverse cipher

4.3 Zig-zag Cipher

Zig-zag Cipher is a form of traditional cryptography which employs character permutation methods to render the original message unreadable unless the recipient has the key to decrypt it. An insecure classical cryptography algorithm is used in the Zig-zag Cipher algorithm. This is supported by research that shows that the Zig-zag Cipher algorithm is more difficult [6].

Zig-zag transpositions may be achieved in order by creating rows or columns in a matrix format. If the key digit is i the location of the transposition message matrix column is the following:

DOI: 10.31695/IJASRE.2021.34010

(1, i) (2, i + 1) (3, i) (4, i + 1) (5, i)... (m, n) .... (4)

The same key is used for decryption after a transposition is processed with a lock on a symmetric encryption cipher. The location of the transposition message matrix row if the main digit is i is the following:

(i, 1) (i + 1, 2) (i, 3) (i + 1, 4) (i, 5) ... (m, n) ..... (5)

The number of rows specifies the number of digits in the key used in the zig-zag cipher algorithm by using row transpositions, and when using transposition columns, it is determined by the number of columns [6].

Example: if we used the word **(computer)**

The order in columns **c m u e**

o p t r

Are choosing rows it is produced text encrypted next cmueoptr.

When decoded be this way in the opposite of any we choose the pillars first and then rows and we get the text of the original.

4.4 Affine cipher

Is one of ways encryption unilateral alphabet (no replacement character with a letter the last) this way like Caesar cipher largely but this way needs two keys instead of one key , Caesar cipher is case of special of the affine cipher which it have two keys. The Affine cipher is a variation on the Caesar cipher in that the plaintext is multiplied by a value and a modification is applied to it. Congruent functions can be used to express the mathematical encryption of plaintext P to generate cipher text C:

[E (P) = (ax + b) mod m] where n denotes the size of the alphabet, and (a) denotes an integer that should be close to (m) in terms of primness. (If the decryption is not skewed, it isn't relatively prime) The number of changes is denoted by the letter b. (The affine cipher with m = 1 is known as the Caesar cipher.) x = plaintext is translated to an integer in the order of the alphabet from 0 to m-1. E (P) = cipher text is translated to an integer ranging from (0 to m-1) in alphabetical order. The decryption function, on the other hand, can be written as follows:

[D(x) = a-1(x – b) mod m] where (a-1) is the multiplicative inverse of a modulus m in order to satisfy the equation: Only if (a and m) are comprised does (1 = aa-1 mod m) have a multiplicative inverse. If this is not the case, the algorithm will be terminated. The opposite of the encryption function is the decryption function, which is easy to write as following way [7]:

D (E (P)) = a-1 (E (P) – b) mod m

= a-1 (((ax + b) mod m) – b) mod m

= a-1 (ax + b – b) mod m

= a-1ax mod m

D (E(x)) = x mod m

Example: - using the Affine Cipher encrypt the following message "**hello**" by using the keys following (7, 2)

P: h→07	encryption (07x7+2) mod26	c: 25→Z
P: e→04	encryption (04x7+2) mod26	c: 04→E
P: l→11	encryption (11x7+2) mod26	c: 01→B
P: l→11	encryption (11x7+2) mod26	c: 01→B
P: O→14	encryption (14x7+2) mod26	c: 22→Z

DOI: 10.31695/IJASRE.2021.34010

To decrypt the message we should find the inverse of the first key (7) with reverse and we subtracting the character from the second key (2).

c: 25→Z	decryption ((25-2) x7) mod26	p: 07→H
c: 04→E	decryption ((04-2) x7) mod26	P:e→04
c: 01→B	decryption ((01-2) x7)mod26	P: l→11
c: 01→B	decryption ((01-2) x7) mod26	P: l→11
c: 22→Z	decryption (14x7+2)mod26	P: O→14

DOI: 10.31695/IJASRE.2021.34010

5. GENERAL STRUCTURE OF THE PROPOSED SYSTEM

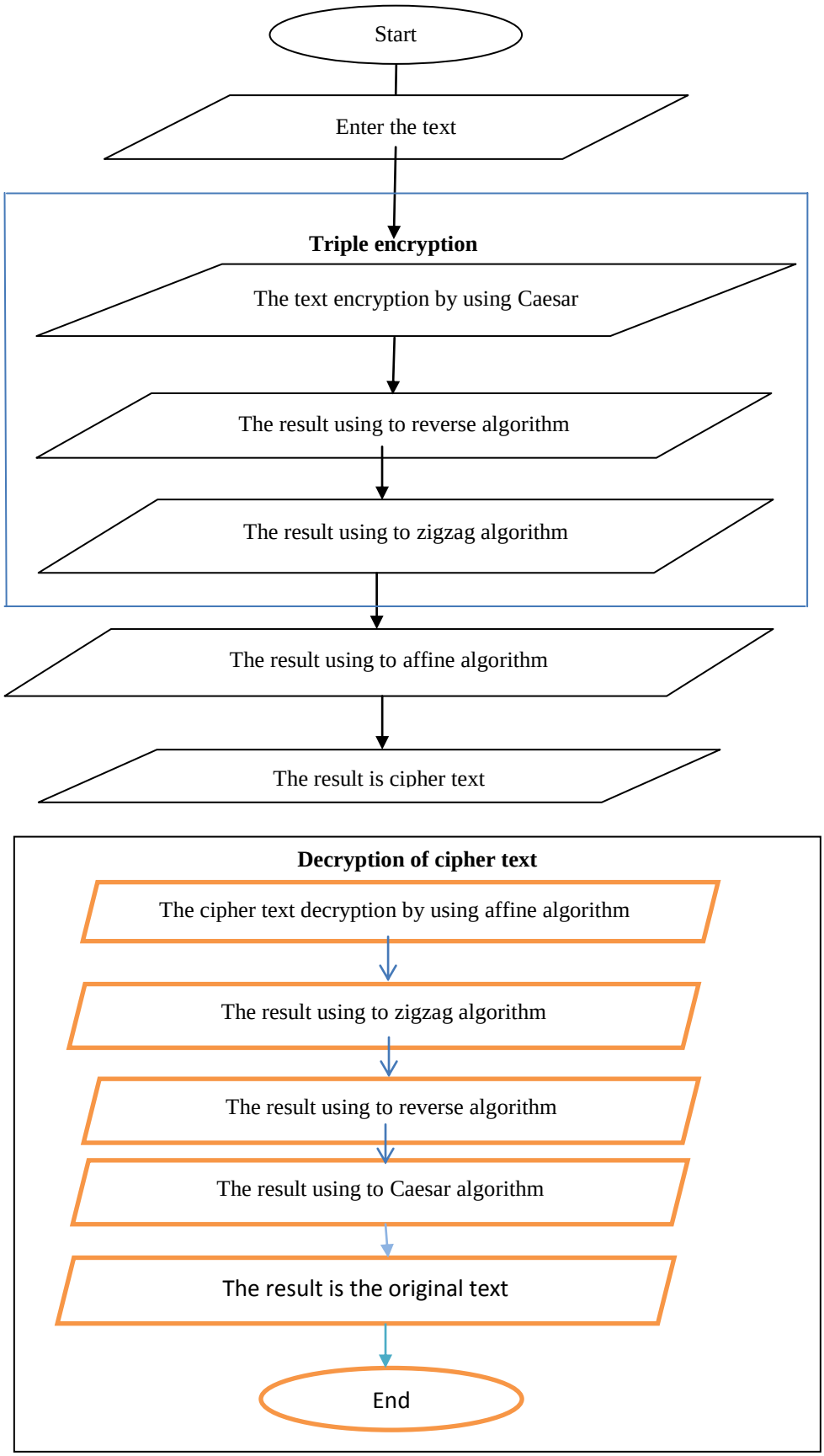

Figure 1.3: Flowchart of text encryption, text decryption of the Proposed System

DOI: 10.31695/IJASRE.2021.34010

6. THE PROPOSED ENCRYPTION & DECRYPTION METHOD

This segment will illustrate a proposed method to encryption and decryption text. Figures (4) and (5) of the General Algorithm demonstrate this.

Input: (Enter plain text) **Output: (** Encrypted text)
Process: **Step1:** Enter plain text. **Step2:** Perform triple cipher of plain text. **Step3:** Resultant text is encrypted text. **Step4:** Enter encrypted text in place plaintext of affine algorithm. **Step5:** Perform affine algorithm. **Step6:** Resultant text is encrypted text. **Step7:** End.

Figure 1.4: General algorithm of Proposed Method *(*Encryption text process)

Input: (Enter encrypted text) **Output: (plain text)**
Process: **Step1:** Enter encrypted text. **Step2:** Perform affine algorithm. **Step3:** Resultant text is encrypted text. **Step4:** Enter encrypted text in place plaintext of triple cipher of encrypted text. **Step5:** Perform triple cipher. **Step6:** Resultant text is plain text. **Step7:** End.

Figure 1.5: General algorithm of Proposed Method (Decryption text Process)

7. Proposed Algorithm Implementation

To illustrate how the proposed algorithm will operate, the process is divided into two processes (Encryption by using codes (Caesar-Reversing-zigzag) by combining the three codes, then resultant text is encrypted text and encrypting the text using the affine code. But if we want to decode the chiphertext, we reverse the sequence of the encryption process, starting with the Affine algorithm, and then we start with the triple encryption from algorithm (zigzag- Reversing- Caesar).

DOI: 10.31695/IJASRE.2021.34010

Step 1: Enter the plain text for encryption by using three algorithms.

Figure 1.6: Enter the plain text for encryption by using three algorithms.

Step2: Enter encrypted text in place plaintext of affine algorithm

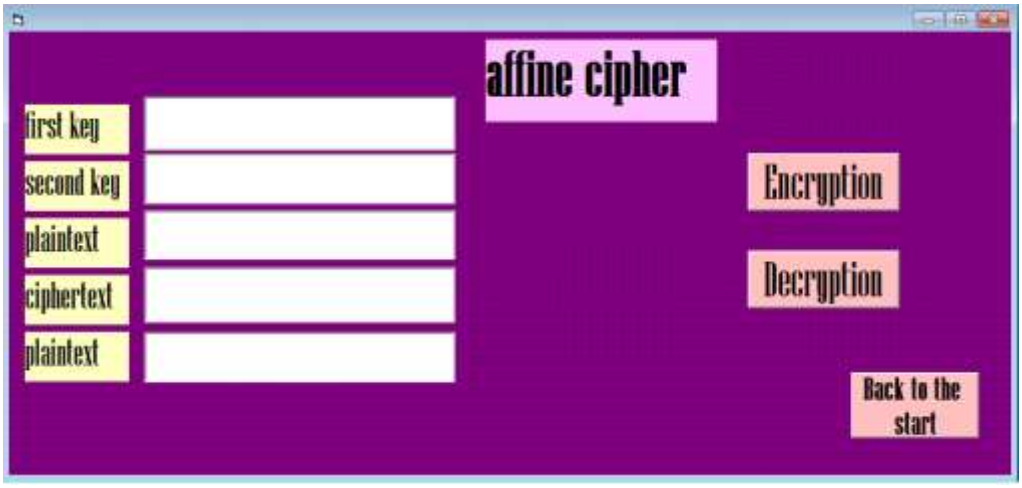

Figure 1.7: Enter encrypted text in place plaintext of affine algorithm

Step3: Enter cipher text in place affine algorithm and then click decryption

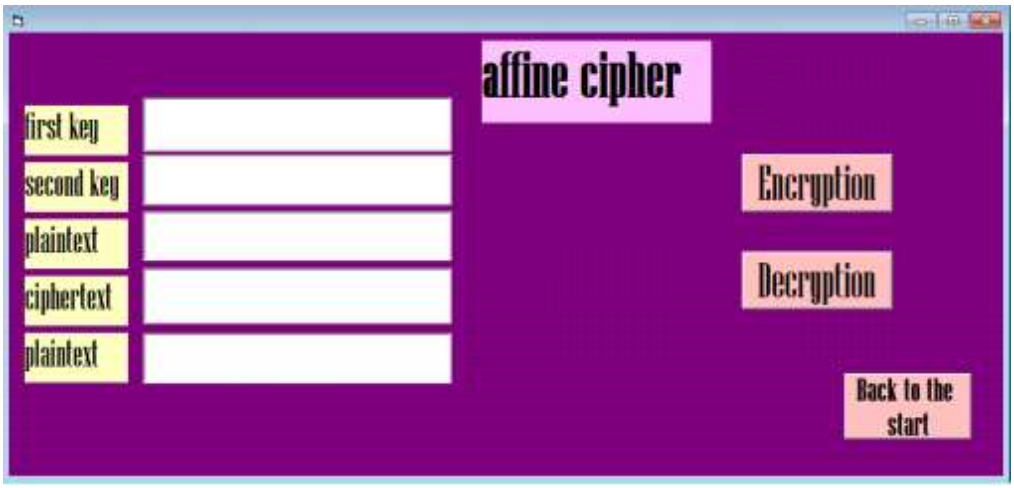

Figure 1.8: Enter cipher text in place affine algorithm and then click decryption

DOI: 10.31695/IJASRE.2021.34010

Step4: Enter cipher text to decryption by using triple encryption

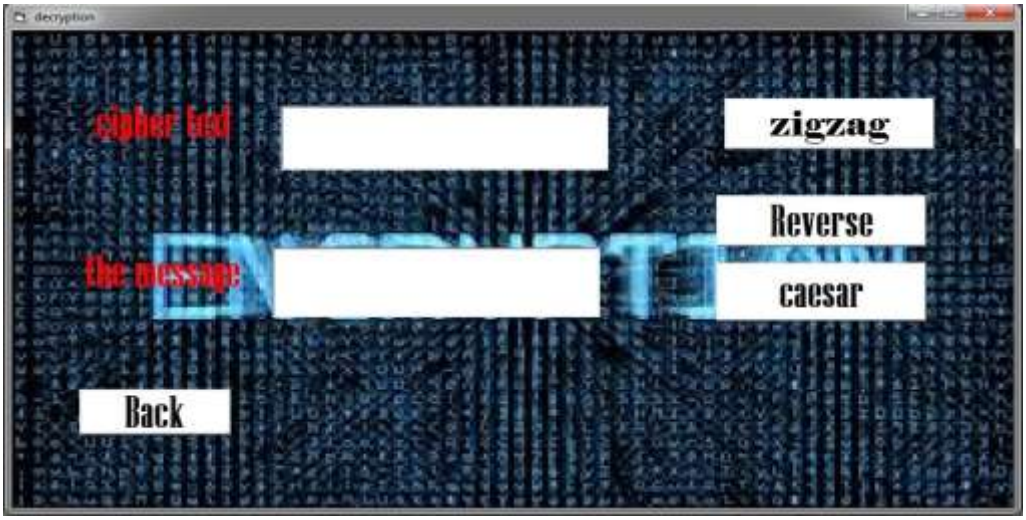

Figure 1.9: Enter cipher text to decryption by using triple encryption.

Table 1.2. Results Test Text

Plain text	Encryption				Decryption	Plain text
	Triple Encryption			Affine	Cipher text	
	Caesar	Reverse	Zigzag			
hello	khoor	roohk	rokoh	gxlxc	gxlxc	hello
world	zruog	gourz	guzor	zpexg	zpexg	world
computer	frpsxwhu	uhwxsprf	uwsrhxpf	pvjgcyaw	pvjgcyaw	computer
science	vflhqfh	hfqhlfv	hqlvfhf	cdoswcw	cdoswcw	science

8. CONCLUSIONS

When encrypting more than once using triple encryption (Caesar, reverse and zigzag) together, and then encode the text resulting from this process using affine an algorithm, resulting in a strong encrypted text that cannot be easily broken due to the use of more than algorithm with use keys in affine algorithm. The outcome of the decryption procedure for propped system was used affine algorithm and combination (Caesar, reverse and zigzag) it identical plaintext when you encrypt several times, the encryption you get is different each time.

ACKNOWLEDGMENT

The author wishes to express his gratitude to Mustansiriyah University (www.uomustansiriyah.edu.iq) in Baghdad, Iraq, for its assistance with this project.

REFERENCES

[1] Kshitij Bhetwal." MULTIMEDIA SECURITY USING ENCRYPTION AND DECRYPTION".

[2] Anurag Rawal*, Gaurav Chhikara, Gaganjot Kaur, Hitesh Khanna."Cryptography Algorithm". Student, Department of CSE Manav Rachna University Faridabad, Haryana, India.

[3] Dr. Prerna Mahajan & Abhishek Sachdeva . "A Study of Encryption Algorithms AES, DES and RSA for Security".

DOI: 10.31695/IJASRE.2021.34010

[4] Benni Purnamaa, Hetty Rohayani.AHb
. "A New Modified Caesar Cipher Cryptography Method with Legible Ciphertext from a Message to Be Encrypted". *Informatic System, b Computer System, STIKOM Dinamika Bangsa, Jambi 36138, Indonesia*.

[5] https://www.tutorialspoint.com/cryptography_with_python/cryptography_with_python_reverse_cipher.htm.

[6] M A Budiman, Amalia and N I Chayanie Departemen Ilmu Komputer, Fakultas Ilmu Komputer dan . "An Implementation of RC4+ Algorithm and Zig-zag Algorithm in a Super Encryption Scheme for Text Security". Teknologi Informasi, Universitas Sumatera Utara, Jl. Universitas No. 9-A, Kampus USU, Medan 20155, Indonesia.

[7] Sriramoju Ajay Babu . "MODIFICATION AFFINE CIPHERS ALGORITHM FOR CRYPTOGRAPHY PASSWORD".1Programmer Analyst , Randstad Technologies, EQT Plaza 625 Liberty Avenue, Suite 1020 Pittsburgh, Pennsylvania -15222, USA.

* Correpondance author email: zehraa_84@uomustansiriyah.edu.iq

DOI: 10.31695/IJASRE.2021.34010