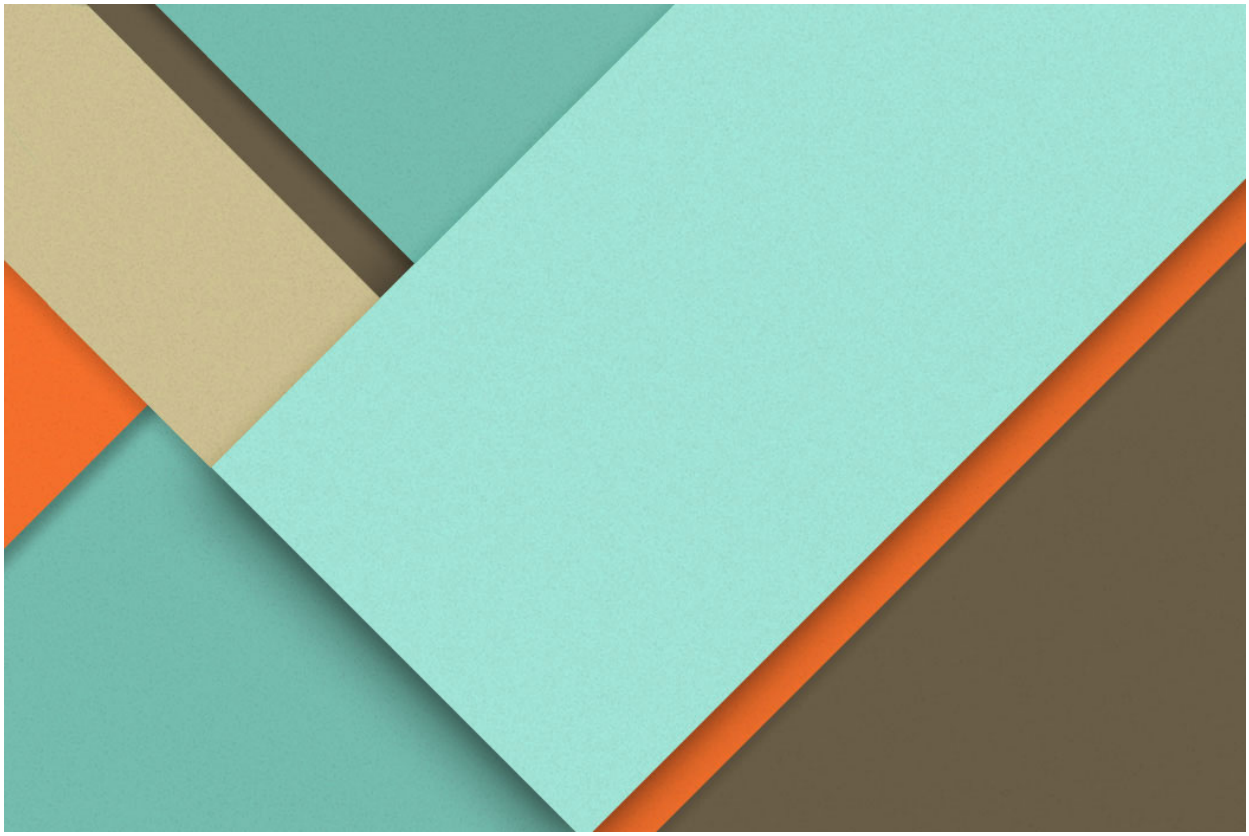


CYPHER TEXT

27.12.2022

Anagha Nagesh

Vimal Jyothi Engineering college
Chemperi,Kannur

Kerala

ABSTRACT

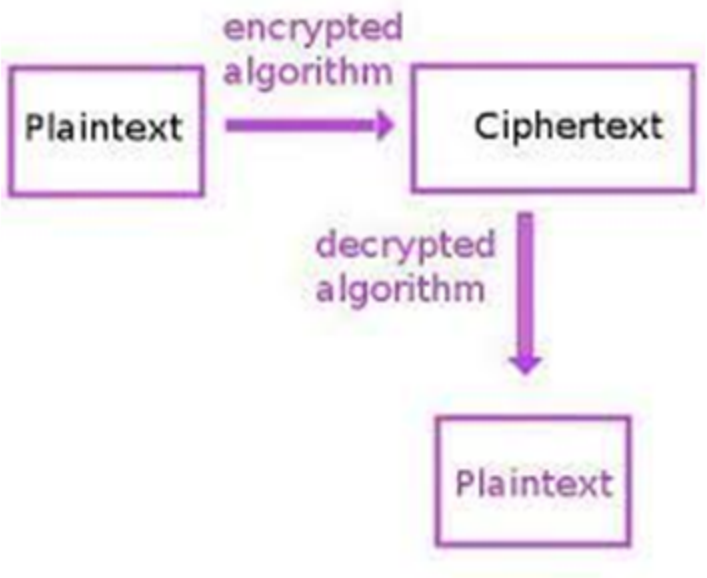
The project we are doing comes under Cryptography. The main idea of our project is to create a cipher for the data given by the user and also the reverse process i:e converting the generated cipher to plain text or original data. Protecting the users data from being modified or misuse is the main aim of Network Security. So as to protect the data we are generating the cipher from the user's data so that it will not be in readable format and this cipher will be seen through the network to the receiver so that any intruder who accessed the data could not understand it.

We will be generating a Java applet that will take the user input and displays the cipher and also form the cipher to plain text. The algorithm we are developing will accept the data and then take each character from the string and based on the equivalent ASCII number of that character the necessary function will be taken and the cipher text is generated.

INDEX

INTRODUCTION

Plain text is the term used to refer to the information in plain language that the sender desires to send to one or more receiving computers or individuals. Also referred to as clear text, plain text is commonly referred to as the input to a cipher or encryption algorithm. In cryptographic circles, plain text is commonly used as the input to a cipher or encryption algorithm. The output of these ciphers is normally referred to as cipher text. The outputted text can be a result of one or more rounds of encryption employed.



Conversion of a plain text to cipher text

CRYPTOGRAPHY

A cryptographic key is a string of characters used within an encryption algorithm for altering data so that it appears random. Like a physical key , it locks(encrypts) data so that only someone with the right key can unlock(decrypt) it.

ENCRYPTION AND DECRYPTION

*Encryption

The process of encoding a message so that its meaning is not obvious.

->Types of encryption

-Symmetric encryption

There is only one key, and all communicating parties use the same (secret) key for both encryption and decryption.

-Asymmetric encryption

There are two keys: one key is used for encryption, and a different key is used for decryption.

*Decryption

It decodes the encrypted information so that an authorized user can only decrypt the data because decryption requires a secret key or password.

Encoding: The process of translating entire words or phrases to other words or phrases.

Enciphering: Translating letters or symbols individually.

Encryption: The group term that covers both encoding and enciphering.

PLAIN TEXT AND CIPHER TEXT

*Plain text

The original form of a message.

*Cipher text

The encrypted form.

MODERN CIPHERS

Current day ciphers are significantly more secure than the classic cipher techniques. They are created to be able to withstand a variety of attacks on the ciphertext. Attackers are not able to determine what the key used in modern ciphers are even with access to a significant amount of plain text and corresponding ciphertext.

Modern cryptography relies on cryptographic keys, usually a short string of text, for encoding and decoding messages in combination with cryptographic algorithms.

Based on the type of keys used, cryptography is classified as either symmetric or asymmetric key cryptography. Both symmetric and asymmetric key cryptography provide data confidentiality. Asymmet-ric key encryption is sometimes called public key encryption. Digital signatures, one of the by-products of public key cryptography, enable the verification of authenticity, integrity, and non-repudiation.

CRYPTANALYSIS ATTACK MODELS

There are a number of cryptanalysis attack models in use today for attempting to crack or break cipher texts. Some of the most common include: ciphertext-only, batch chosen, chosen ciphertext, and the related key attack.

Ciphertext-only attack

In the ciphertext-only attack, the cryptanalyst can only gain access to code or cipher texts.

Known-plaintext attacks

In the known plaintext attacks, the individual or group conducting the attack only has access to a group of cipher texts where he or she knows the corresponding plain text.

Chosen-plaintext attack

In this, the individual or group conducting the attack only has access to a group of cipher texts where he or she knows the corresponding plain texts.

CRYPTANALYSIS

Cryptanalysis which is the study of the cryptographic algorithm and the breaking of those secret codes. The person practicing Cryptanalysis is called a **Cryptanalyst**. It helps us to better understand the cryptosystems and also helps us improve the system by finding any weak point and thus work on the algorithm to create a more secure secret code.

To determine the weak points of a cryptographic system, it is important to attack the system. These attacks are called **Cryptanalytic attacks**. The attacks rely on the nature of the algorithm and also knowledge of the general characteristics of the plain texts.

In cryptanalysis, attack models or attack types[1] are a classification of cryptographic attacks specifying the kind of access a cryptanalyst has to a system under attack when attempting to "break" an encrypted message (also known as *cipher text*) generated by the system. The greater the access the cryptanalyst has to the system, the more useful information they can get to utilize for breaking the cipher.

TYPES OF CIPHERS

There are various types of ciphers, including:

- Substitution ciphers

Replace bits, characters, or character blocks in plaintext with alternate bits, characters or character blocks to produce ciphertext. A substitution cipher may be monoalphabetic or polyalphabetic*:*

  - A single alphabet is used to encrypt the entire plaintext message. For example, if the letter A is enciphered as the letter K, this will be the same for the entire message.
  - A more complex substitution using a mixed alphabet to encrypt each bit, character or character block of a plaintext message. For instance, the letter A may be encoded as the letter K for part of the message, but later it might be encoded as the letter W.

- Transposition ciphers.

Unlike substitution ciphers that replace letters with other letters, transposition ciphers keep the letters the same, but rearrange their order according to a specific

algorithm. For instance, in a simple columnar transposition cipher, a message might be read horizontally but would be written vertically to produce the cipher text.

- Polygraphic ciphers. Substituting one letter for another letter, a polygraphic cipher performs substitutions with two or more groups of letters. This masks the frequency distribution of letters, making frequency analysis attacks much more difficult.
- Permutation ciphers. In this cipher, the positions held by plaintext are shifted to a regular system so that the ciphertext constitutes a permutation of the plaintext.
- Private-key cryptography . In this cipher, the sender and receiver must have a pre-shared key. The shared key is kept secret from all other parties and is used for encryption, as well as decryption. This cryptography is also known as "symmetric key algorithm."
- Public-key cryptography. In this cipher, two different keys -- public key and private key -- are used for encryption and decryption. The sender uses the public key to perform the encryption, but the private key is kept secret from the receiver. This is also known as "asymmetric key algorithm."
- Pen and paper ciphers. These types of ciphers are also known as the “classical ciphers” and include the following methods.

SOFTWARE AND HARDWARE REQUIREMENTS

Software Requirements:

- Windows
- Linux
- Java compatible platform

Hardware Requirements:

- RAM - 512 MB
- Monitor, Keyboard, Mouse
- ROM - 4GB

SOFTWARE REQUIREMENTS ANALYSIS

The two basic building blocks of all encryption techniques are:

SUBSTITUTION

- Letters of plain texts are replaced by other letters or by numbers or symbols.
- If the plain text is viewed as a sequence of bits, then substitution involves replacing plain text bit patterns with cipher text patterns.

TRANSPOSITION/PERMUTATION

- The letters/ bytes /bits of plain text are rearranged without altering the actual letters used.
- Can be easily recognized since these ciphertext have the same frequency distribution as the original plain text.

OBJECTIVES

CONFIDENTIALITY OF THE MESSAGE

· Only the authorized recipient should be able to extract the content of the ciphertext.

· In addition, obtaining information about the content of the message should not be possible once the cryptographic analysis becomes easier.

MESSAGE INTEGRITY

·The recipient must be able to determine if the message was altered during transmission.

AUTHENTICATION OF THE SENDER

·The recipient should be able to identify the sender and verify if it was him who sent the message.

IRREVOCABILITY OF THE SENDER

· It should not be possible to deny the authorship of the message.

ASCII TABLE

ASCII TABLE

Decimal	Hex	Char	Decimal	Hex	Char	Decimal	Hex	Char	Decimal	Hex	Char
0	0	*[NULL]*	32	20	*[SPACE]*	64	40	@	96	60	`
1	1	*[START OF HEADING]*	33	21	!	65	41	A	97	61	a
2	2	*[START OF TEXT]*	34	22	"	66	42	B	98	62	b
3	3	*[END OF TEXT]*	35	23	#	67	43	C	99	63	c
4	4	*[END OF TRANSMISSION]*	36	24	$	68	44	D	100	64	d
5	5	*[ENQUIRY]*	37	25	%	69	45	E	101	65	e
6	6	*[ACKNOWLEDGE]*	38	26	&	70	46	F	102	66	f
7	7	*[BELL]*	39	27	'	71	47	G	103	67	g
8	8	*[BACKSPACE]*	40	28	(	72	48	H	104	68	h
9	9	*[HORIZONTAL TAB]*	41	29	)	73	49	I	105	69	i
10	A	*[LINE FEED]*	42	2A	*	74	4A	J	106	6A	j
11	B	*[VERTICAL TAB]*	43	2B	+	75	4B	K	107	6B	k
12	C	*[FORM FEED]*	44	2C	,	76	4C	L	108	6C	l
13	D	*[CARRIAGE RETURN]*	45	2D	-	77	4D	M	109	6D	m
14	E	*[SHIFT OUT]*	46	2E	.	78	4E	N	110	6E	n
15	F	*[SHIFT IN]*	47	2F	/	79	4F	O	111	6F	o
16	10	*[DATA LINK ESCAPE]*	48	30	0	80	50	P	112	70	p
17	11	*[DEVICE CONTROL 1]*	49	31	1	81	51	Q	113	71	q
18	12	*[DEVICE CONTROL 2]*	50	32	2	82	52	R	114	72	r
19	13	*[DEVICE CONTROL 3]*	51	33	3	83	53	S	115	73	s
20	14	*[DEVICE CONTROL 4]*	52	34	4	84	54	T	116	74	t
21	15	*[NEGATIVE ACKNOWLEDGE]*	53	35	5	85	55	U	117	75	u
22	16	*[SYNCHRONOUS IDLE]*	54	36	6	86	56	V	118	76	v
23	17	*[END OF TRANS. BLOCK]*	55	37	7	87	57	W	119	77	w
24	18	*[CANCEL]*	56	38	8	88	58	X	120	78	x
25	19	*[END OF MEDIUM]*	57	39	9	89	59	Y	121	79	y
26	1A	*[SUBSTITUTE]*	58	3A	:	90	5A	Z	122	7A	z
27	1B	*[ESCAPE]*	59	3B	;	91	5B	[	123	7B	{
28	1C	*[FILE SEPARATOR]*	60	3C	<	92	5C	\	124	7C	|
29	1D	*[GROUP SEPARATOR]*	61	3D	=	93	5D	]	125	7D	}
30	1E	*[RECORD SEPARATOR]*	62	3E	>	94	5E	^	126	7E	~
31	1F	*[UNIT SEPARATOR]*	63	3F	?	95	5F	_	127	7F	*[DEL]*

PROGRAM

```
import java.io.*;
import java.applet.*;
import java.awt.event.*;
import java.applet.Applet;
import java.awt.*;


public class cipher extends Applet implements ActionListner {
    Label l;
    Button b1, b2, b3;
    TextFeild t1, t2, t3;
    String str, str1 = "", msg, s = "", str2, str3 = "";
    char c, d;
    int k, h;


    public void in() {
        l = new Lable("Enter the text:");
        t1 = new TextFeild(50);
        t2 = new TextFeild(50);
```

```
        t3 = new TextFeild(50);
        b1 = new Button("Getcihper");
        b2 = new Button("clear");
        b3 = new Button("Decrypt");
        add(l);
        add(t1);
        add(b1);
        add(t2);
        add(b3);
        add(t3);
        add(b2);
        t1.addActionListener(this);
        t2.addActionListener(this);
        t3.addActionListener(this);
        b1.addActionListener(this);
        b2.addActionListener(this);
        b3.addActionListener(this);
    }

    public void actionPerformed(ActionEvent ae){
        str=ae.getActionCommand();
        if(str.equals("Getcipher")){
```

```
        int count=0;
        s=t1.getText();
        for(int i=0;i<s.length();i++){
            c=s.charAt(i);
            k=c;
            if(k%2==0)
            k=k+4;
            else
            k=k+16;
            d=(char)k;
            str1+=d;
        }
        t2.setText(str1);
        str1="";
        t1.setText(str1);
    }
    if(str.equals("clear")){
        str1="";
        t1.setText(str1);
        str2="";
        t2.setText(str2);
        str3="";
```

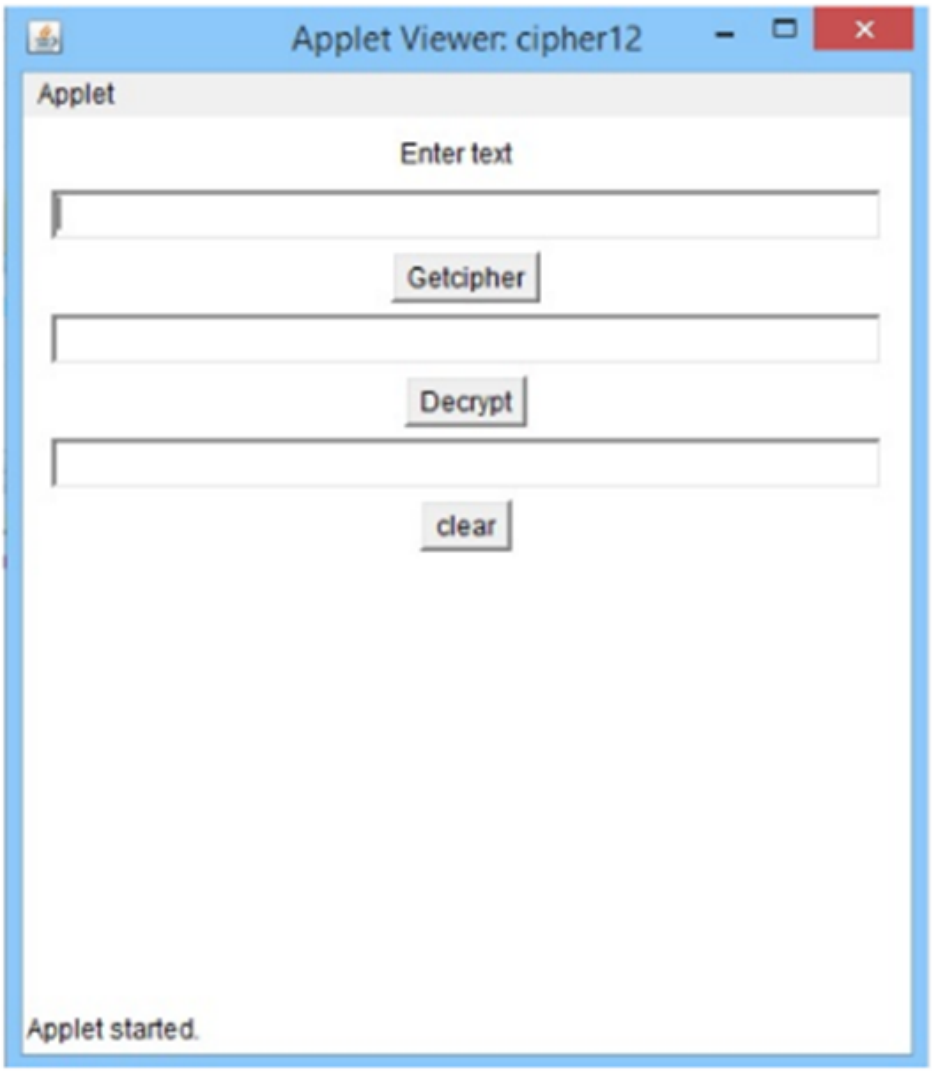
```
            t3.setText(str3);
        }
        if(str.equals("Decrypt")){
            int count=0;
            s=t2.getText();
            for(int i=0;i<s.length();i++){
                c=s.charAt(i);
                k=c;
                if(k%2==0)
                k-k-4;
                else
                k=k-16;
                str3+=(char)k;
            }
            t3.setText(str3);
            str3="";
        }
    }


    public void paint(Graphic g) {
        msg = "";
        g.drawString(msg, 10, 100);
```

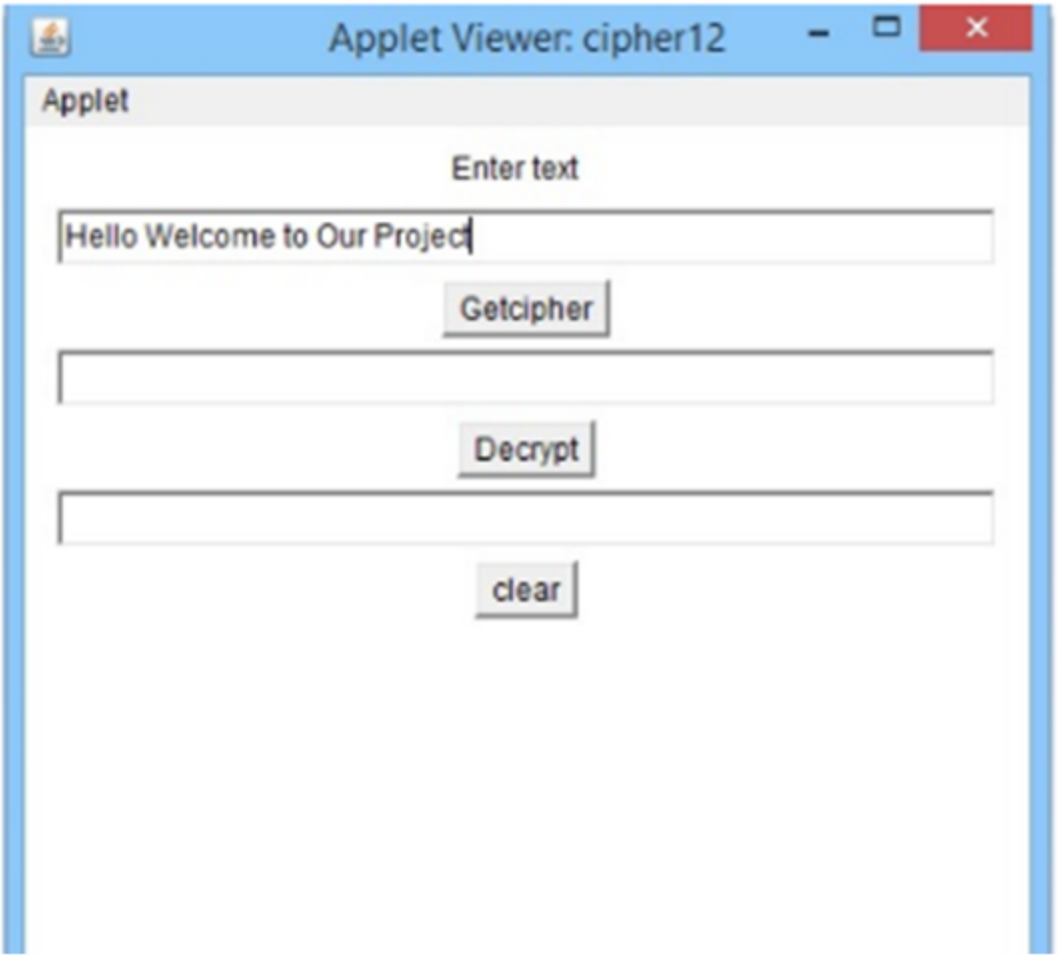
```
    }

}
```

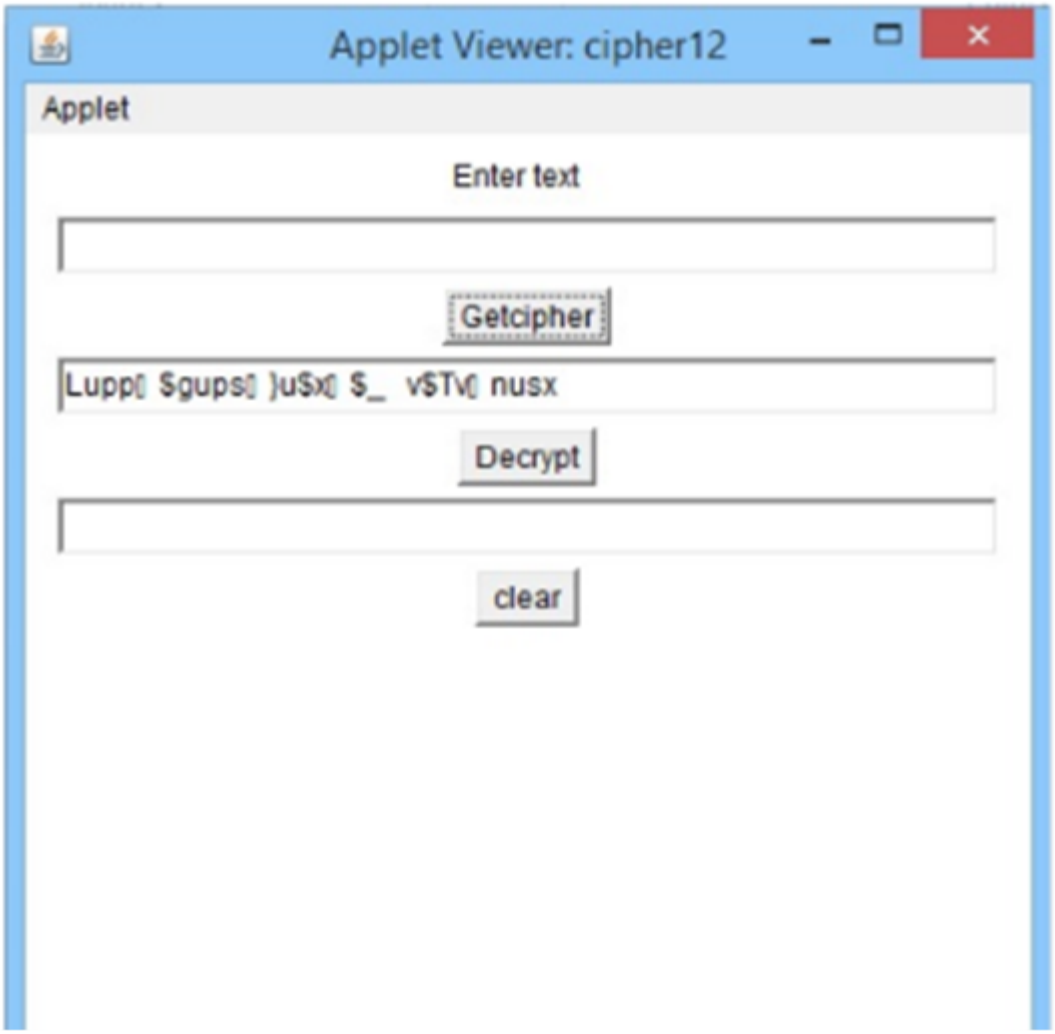
OUTPUT



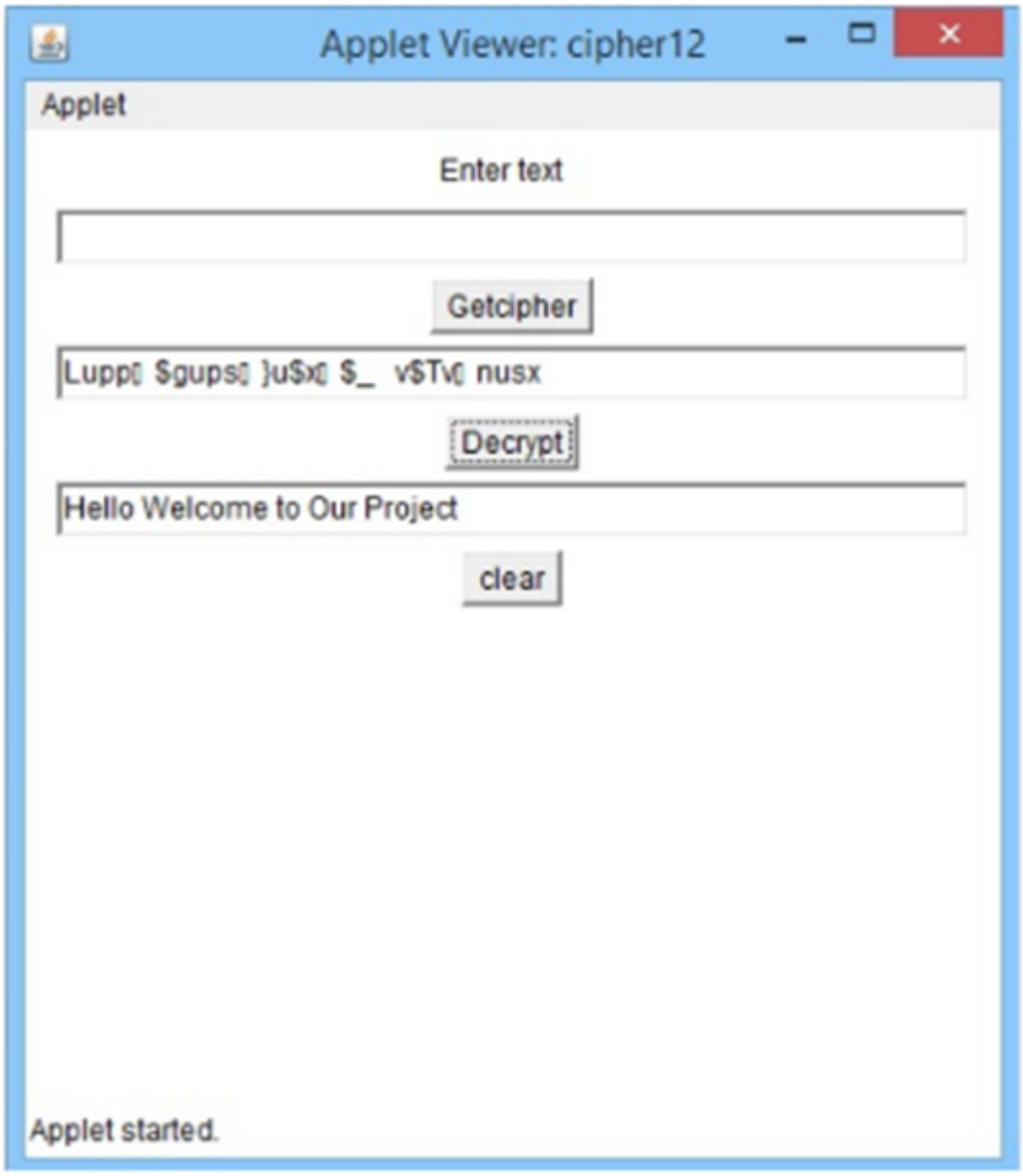
Applet Window


Applet Viewer: cipher12
Applet
Enter text
Hello Welcome to Our Project
Getcipher
Decrypt
clear

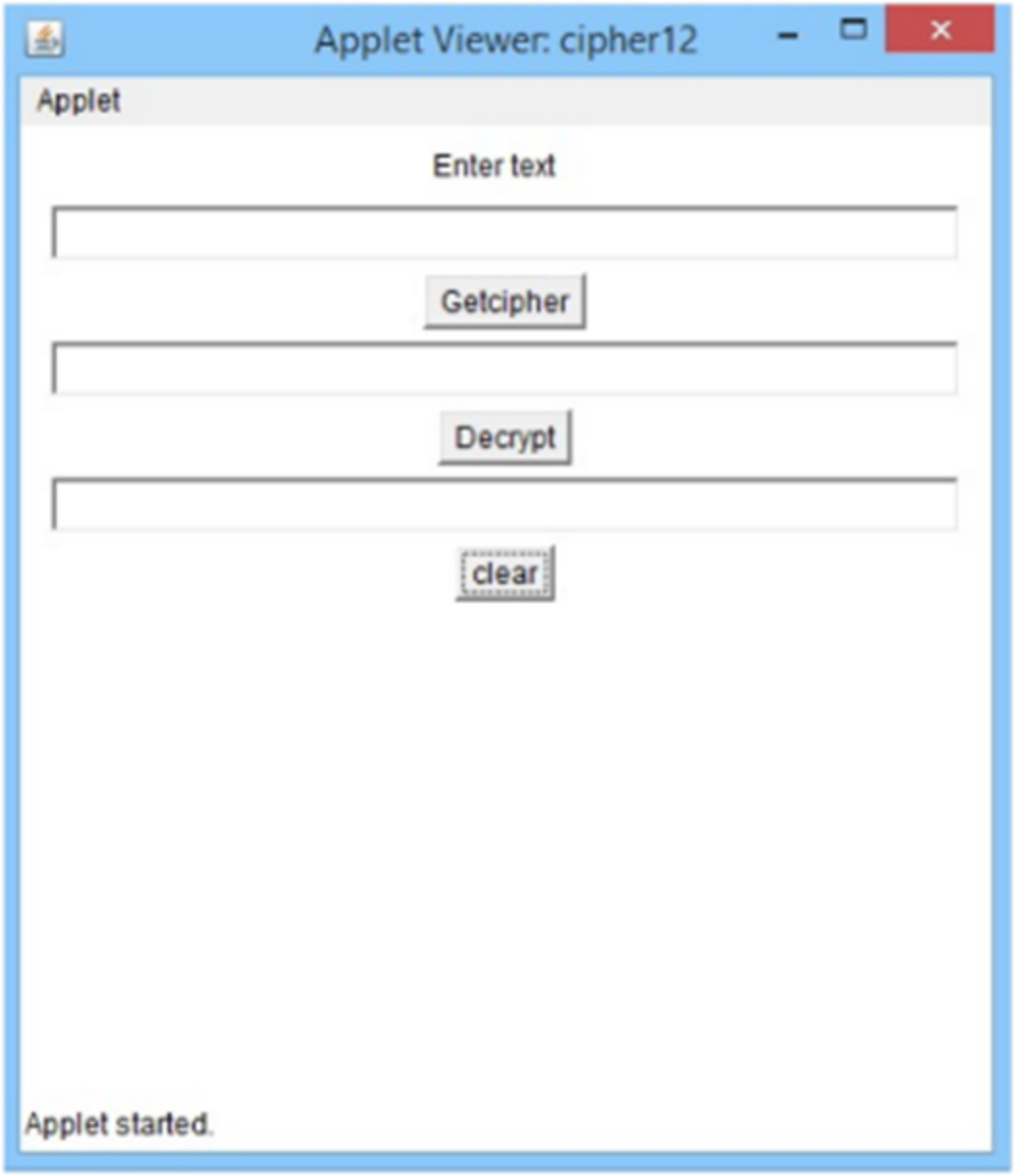
User Input



Output when Getcipher Button is clicked



Output when Decrypt Button is clicked



Output when clear Button is clicked

BIBLIOGRAPHY

- www.studocu.com
- https://www.sciencedirect.com
- www.cs.cmu.edu
- WIKIPEDIA