**Abstract:**

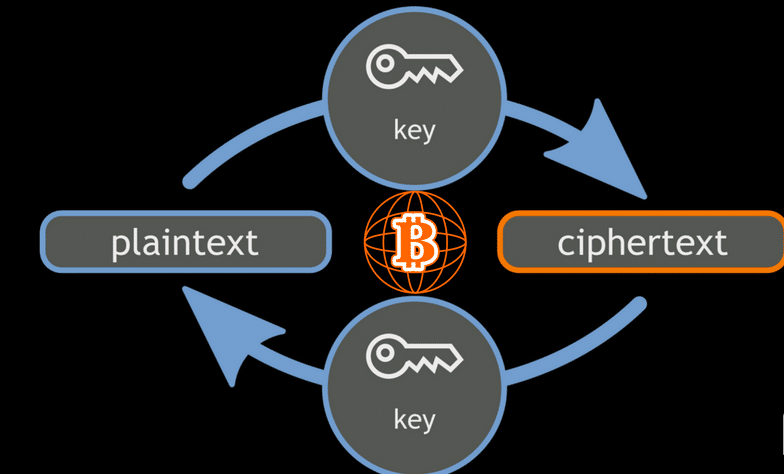
Many Ciphers have been developed to provide data security. We made this project to contribute to the general body of knowledge in the area of classical cryptography by developing a new modified hybrid way of encryption of plaintext. The Caesar Cipher and Vigenere Cipher have been modified and expanded so as to include alphabets, numbers and symbols and at the same time introduced a complete confusion and diffusion into the modified cipher developed. Classical ciphers can be made effective and used for providing security by adding the properties possessed by the modern ciphers.

In today’s world the amount of data that is exchanged has increased in the last few years so securing the information has become a crucial task. Cryptography is an art of converting plain text message into unreadable message. Encryption algorithms play an important role in information security systems. Encryption is considered as one of the most powerful tool for secure transmission of data over the communication network. Vigenere technique is an example of polyalphabetic stream cipher; it has various limitations such as Kasiski and Friedman attack to find the length of encryption key. In this project an enhanced version of traditional vigenere cipher has been proposed that provides better security against cryptanalysis and pattern prediction.

**Introduction:**

Privacy is one of the key issues information Security addresses. Through encryption one can prevent a third party from understanding raw data during signal transmission. The encryption methods for enhancing the security of digital contents has gained high significance in the current era of neglect of security and misuse of the confidential information intercepted and misused by the unauthorized parties. We made this project to contribute to the general body of knowledge in the area of cryptography application and by developing a new way of implementing Vigenere cipher encryption algorithm by automatically changing the cipher key after each encryption step. The new method will use successive keys that will be dependent on the initial key value during the encryption process. The algorithm ultimately makes it possible for encryption and decryption of the text. The ciphertext will have different encryption key pattern and the Vigenere cryptosystem will be more difficult to decipher using frequency attack.

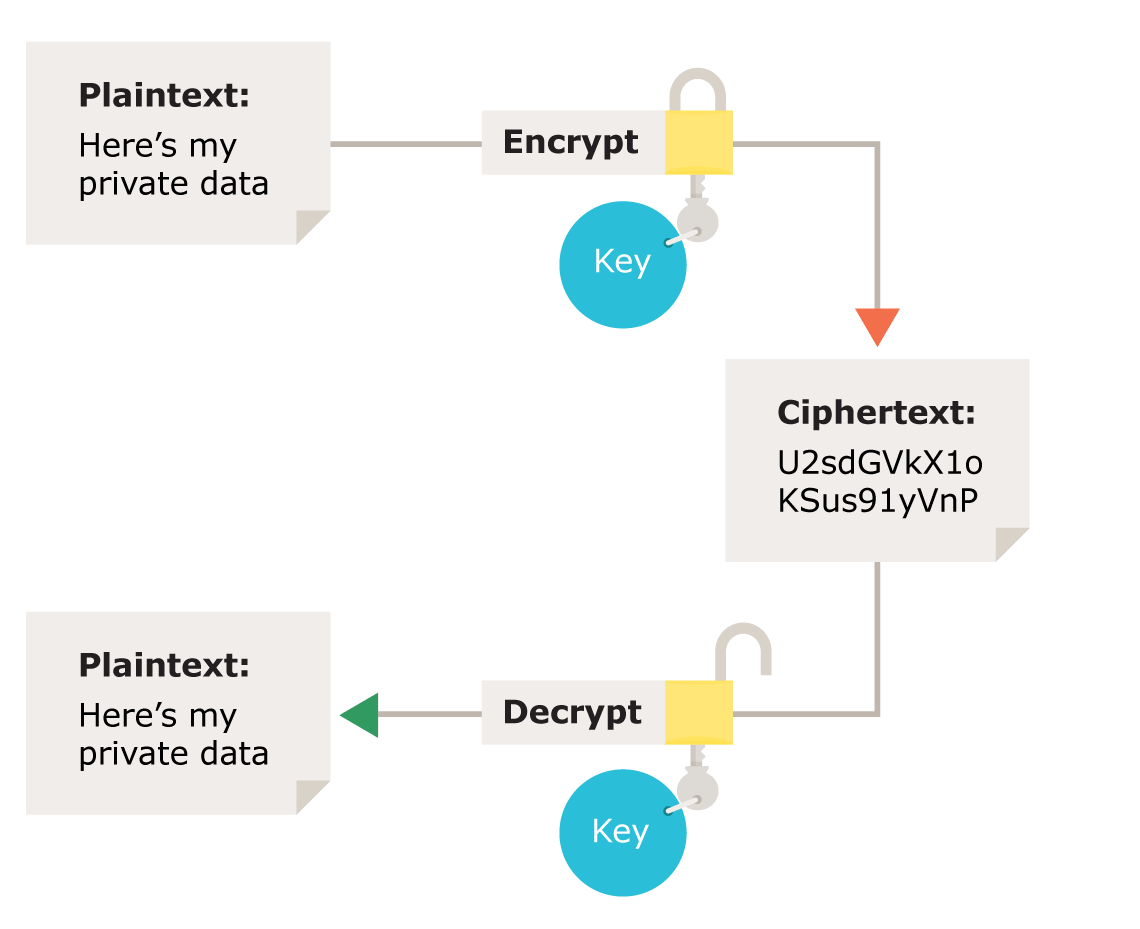
Secured communication involves encryption process at the sending end and decryption process at the receiving end of the communication system. Over the years, there are many aspects to security solutions on many applications, ranging from secure commerce and payments to private communications and protecting passwords. Cryptography is the practice and study of hiding information. That is cryptography is the science of using mathematics to encrypt and decrypt data. Thus cryptography enables someone to store sensitive information or transmit it across unsecure networks (like the Internet) so that it cannot be read by anyone except the intended recipient. In modern times, cryptography is considered a branch of both mathematics and computer science, and is affiliated closely with information theory, computer security, and engineering.



Cryptography is used in applications present in technologically advanced societies; examples include the security of ATM cards, computer passwords, and electronic commerce, which all depend on cryptography. Cryptography refers to encryption, the process of converting ordinary information (plaintext) into unintelligible cipher text. Cryptography is divided into two types, Symmetric Key Cryptography and Asymmetric Key Cryptography. In Symmetric Key Cryptography a single key is shared between sender and receiver. The sender uses the shared key and encryption algorithm to encrypt the message.

The receiver uses the shared key and decryption algorithm to decrypt the message. In Asymmetric Key Cryptography each user is assigned a pair of keys, public key and private key. The public key is announced to all members while the private key is kept secret by the user. The sender uses the public key of the receiver to encrypt the message. The receiver uses his own private key to decrypt the message. The process of converting plain text into Cipher text is called enciphering or encryption while restoring the plain text from the Cipher text is called deciphering or decryption. Decryption is the reverse, moving from unintelligible cipher text to plaintext. A cipher is a pair of algorithms which creates the encryption and the reversing decryption. The detailed operation of a cipher is controlled both by the algorithm and, in each instance, by a key. This is a secret parameter for a specific message exchange context. Keys are important, as ciphers without variable keys are trivially breakable and therefore less than useful for most purposes. Historically, ciphers were often used directly for encryption or decryption, without additional procedures such as authentication or integrity checks. Encryption has long been used by militaries and governments to facilitate secret communication.

**THE PROCESS OF ENCRYPTION AND DECRYPTION:**



We have implemented 3 ciphers in our project

1. Vigenere Cipher
2. Caesar Cipher
3. Permutation Cipher

The implementation was done using C# programming.

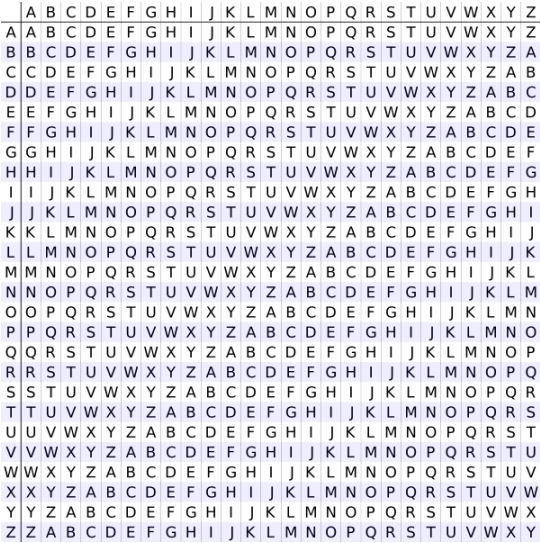
1. **VIGENERE CIPHER:**

Vigenere cipher is one of the earliest known polyalphabetic cipher which was considered secure for a very long time until 1917 when Friedman and Kasiski were able to break it by determining repeating segments of the ciphertext and using it to determine the length of the key. Once the length of the key is known, the ciphertext could be grouped in columns and treated as a separate caesar cipher which can be solved. Over the years, a lot of modification has been done to improve the security of the vigenere cipher. In cryptography, a Vigenere cipher is a method of encrypting alphabetic text by using a series of differentCaesar ciphers based on the letters of a keyword. It is a simple form of polyalphabetic substitution.

**Working:**

Vigenere Cipher is a method of encrypting alphabetic text. It uses a simple form of polyalphabetic substitution. A polyalphabetic cipher is any cipher based on substitution, using multiple substitution alphabets .The encryption of the original text is done using the Vigenere square or Vigenere table.

* The table consists of the alphabets written out 26 times in different rows, each alphabet shifted cyclically to the left compared to the previous alphabet, corresponding to the 26 possible Caesar Ciphers.
* At different points in the encryption process, the cipher uses a different alphabet from one of the rows.
* The alphabet used at each point depends on a repeating keyword.



**Example:**

INPUT : Plaintext: GEEKSFORGEEKS

Keyword: MOIZ

OUTPUT: Cyphertext: GCYCZFMLYLEIM

For generating key, the given keyword is repeated in a circular manner until it matches the length of the plaintext.

The keyword “MOIZ” generates the key “MOIZMOIZMOIZM” the plaintext is then encrypted using the process explained below:

**Encryption:**

The first letter of the plaintext, G is paired with M, the first letter of the key. So use row G and column M of the Vigenere square, namely S. Similarly, for the second letter of the plaintext, the second letter of the key is used, the letter at row E and column O is S. The rest of the plaintext is enciphered in a similar fashion.

**Decryption:**

Decryption is performed by going to the row in the table corresponding to the key, finding the position of the ciphertext letter in this row, and then using the column’s label as the plaintext. For example, in row M (from MOIZ), the ciphertext G appears in column G, which is the first plaintext letter. Next we go to row O (from MOIZ), locate the ciphertext C which is found in column E, thus E is the second plaintext letter.

**Vigenere Cipher Implementation/Logic:**

**Public Class Cipher:**

In this class we globally declared some data-types, an array with all alphabets, and a 2-D Array for Vigenere Table implementation:

**Constructor Cipher:**

Then we made a default constructor, for initializing the Vigenere table on making object of the class:

**Encryption Method:**

After that, we made a method with three parameters, firstly input (Plain Text), secondly Key and finally t3 (Cipher Text). Then inside the method we converted both Plain Text and Key into the CharArray in order to find the value in 2=D Array on the the indexes [Input,Key] (Inside loop ). In nested loops we replaced the char value of plain text by the value Output[c]=[I,j]. (“I is the index refers to the Plain Text”,“J is the index refers to the Key”.

And finally we converted the stored Cipher Text CharArray into the String and saved in a variable declared in main class Program.cs(Program.enc).

**Decryption Method:**

For Decryption Process we also use a method likely, with three parameters but here the input (I.e Plain Text) is replaced by the Cipher Text and the t3 is used for Output (I.e Plain Text). Same we declared three CharArrays which converted the three strings into the arrays.

In nested loops we just only used [0] index of J(plain text), and again and again replaced the value of Key I(Key) in order to find the given character, once the character is found, the Output[c] will save the Character of Plain Text that is obtained by searching the Vigenere Table.

Finally, after obtaining the Plain Text in a CharArray we converted the Array into the String named newstg.

**Method CopyKey:**

As we know in Vigenere Cipher the length of Plain Text and the length of Key must be kept same. In our implementation we did an extra work in order to reduce complexity. If the length of the Key is smaller then the length of Plain Text, the method shown below is able to Copy the key again and again to complete the required length.

Basically it is an internal Function which contains two parameters key and the length of Plain Text required to compare both lengths.

1. **CEASAR CIPHER:**

The Caesar Cipher algorithm for cryptography is one of the oldest algorithms. Now much newer algorithms have arrived that are much more secure, however in terms of speed of execution Caesar cipher algorithm is still the fastest owing to its simplicity. However the algorithm is extremely easy to crack. This is because in this algorithm each character of a message is always replaced by the same fixed character that has been predetermined. Caesar used to encrypt messages using a very simple algorithm, which could be easily decrypted if you know the key. It would take each letter of the alphabet and replace it with a letter a certain distance away from that letter. When it got to the end, it would wrap back around to the beginning.

Example with a shift of 3:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **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 |

**Working:**

* When using a Caesar cipher, you assign each letter to an index starting from 0.
* You would then compute the following:

plain letter index + key) mod (total number of letters)

* This will give you the index of the encrypted letter!
* As you can see, the modulus is the total number of letters in the alphabet. For English, this modulus is 26.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **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** |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |

**Example:**

* Let’s say we have a 5 letter alphabet with only the letters A-E
* First, we assign each letter an index, starting from 0.
* We then have to choose a key. For this example, we’ll use 2.
* Let’s try encoding the word BEAD using the formula.
* The index of the letter B is 1. The key is 2. The modulus is 5, since the alphabet is 5 letters.
* Let’s use the algorithm: (1+2) = 3. 3 mod 5 = 3. The index of D is 3, so B would become the letter D.
* Using algorithm on each letter, can you encode the full word?

**DBCA**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **A** | **B** | **C** | **D** | **E** |
| **0** | **1** | **2** | **3** | **4** |

**WORKING OF DECODING:**

To decode, you do the following:

* (cipher letter index – key + total number of letters) mod (total number of letters)

**Encryption:**

Encryption with Caesar code is a monoalphabetical substitution, i.e. a same letter is replaced with only one other. Caesar code is defined on an alphabet shift: a letter further in the alphabet.

Plain Alphabet : ABCDEFGHIJKLMNOPQRSTUVWXYZ

Caesar Alphabet (+3) : DEFGHIJKLMNOPQRSTUVWXYZABC

Example: Crypt DCODEX with a shift of 3.

To encrypt D, take the alphabet and look 3 letters after : G. So D is crypted with G.

To encrypt X, loop the alphabet: after X : Y, after Y : Z, after Z : A. So X is coded A.

DCODEX is coded GFRGHA

Another way to crypt, more mathematical, note A=0, B=1, ..., Z=25, and add a constant (the shift), then the result modulo 26 (alphabet length) is the coded text.

Example: To crypt D (of value 3), add the shift 3: 3+3=6 and find the letter for 6 : 6=G, so D is crypted with G.

To crypt X=23, 23+3=26 and 26 mod 26 = 0, 0=A, so X is crypted with A, etc.

DCODEX is coded GFRGHA.

**Decryption:**

Caesar code decryption replaces a letter another with an inverse alphabet shift : a previous letter in the alphabet.

Example: Decrypt GFRGHA with a shift of 3.

To decrypt G, take the alphabet and look 3 letters before : D. So G is decrypted with D.

To decrypt X, loop the alphabet: before A: Z, before Z: Y, before Y: X. So A is decrypted X.

GFRGHA is decrypted DCODEX.

Another way to decrypt, more mathematical, note A=0, B=1, ..., Z=25, subtracts a constant (the shift), then the result modulo 26 (alphabet length) is the plain text.

Example: Take G=6, subtract the shift 6-3=3 and 3=D, so G is decrypted with D

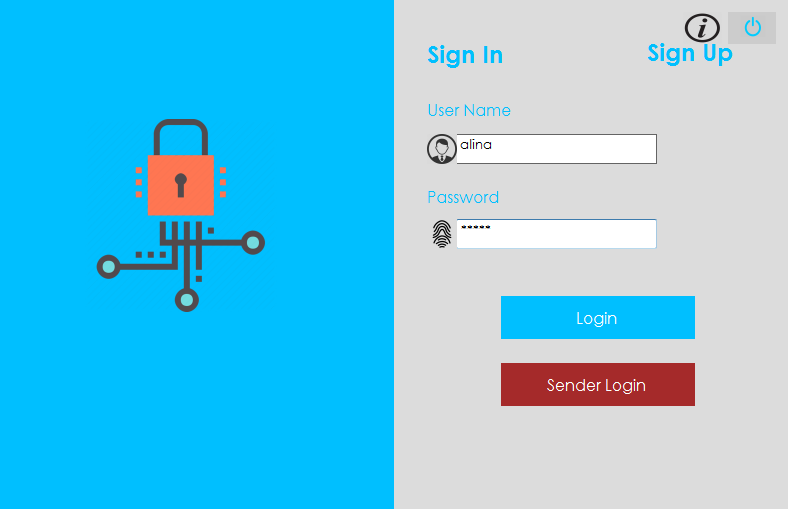
Take A=0, 0-3=-3 and -3 mod 26 = 23, 23=X, so A is decrypted with X, etc.

GFRGHA is decrypted DCODEX.

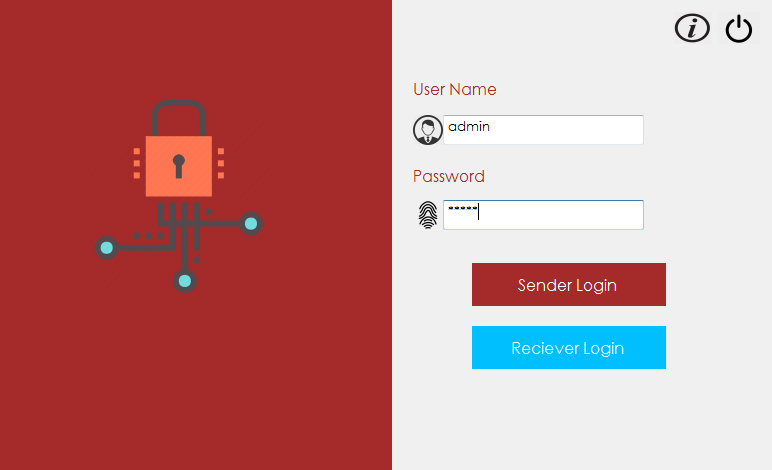
**Screenshots of Project:**

Following are the screenshots of our project:

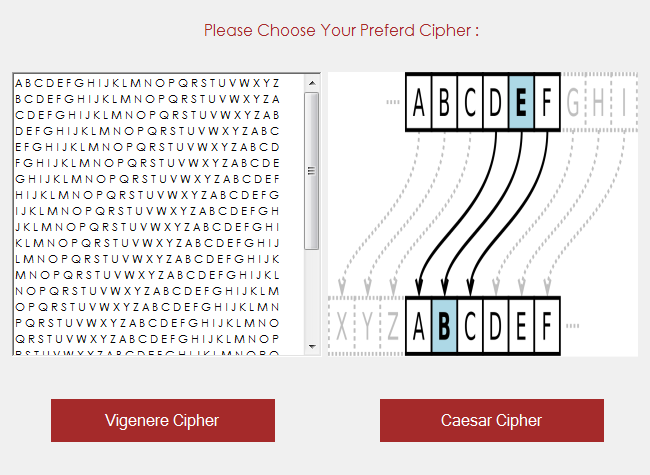
**Sign Up Form:**



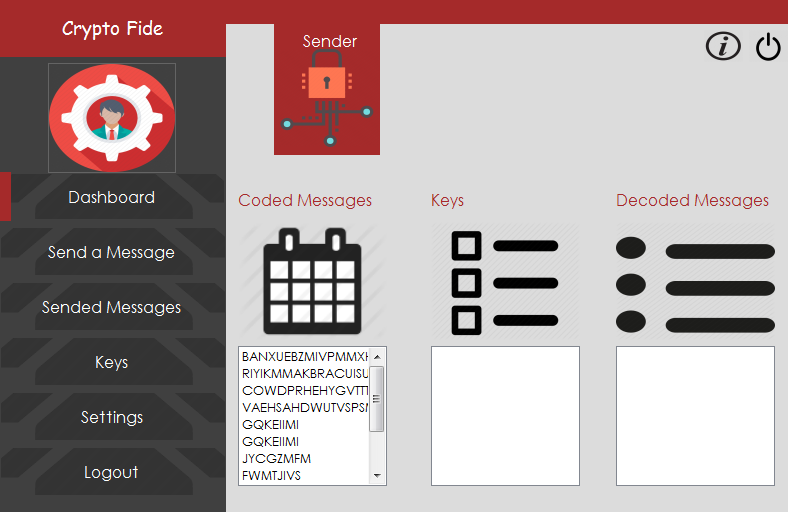
**User Login Form:**



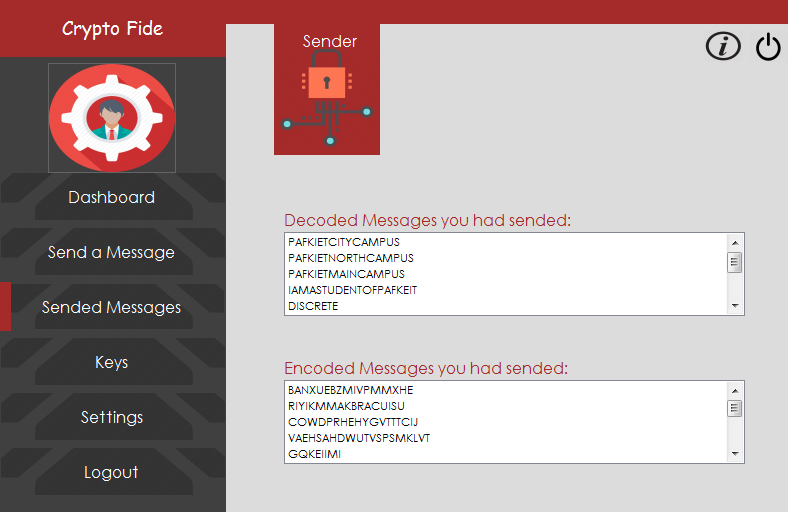
**Choice Form:**



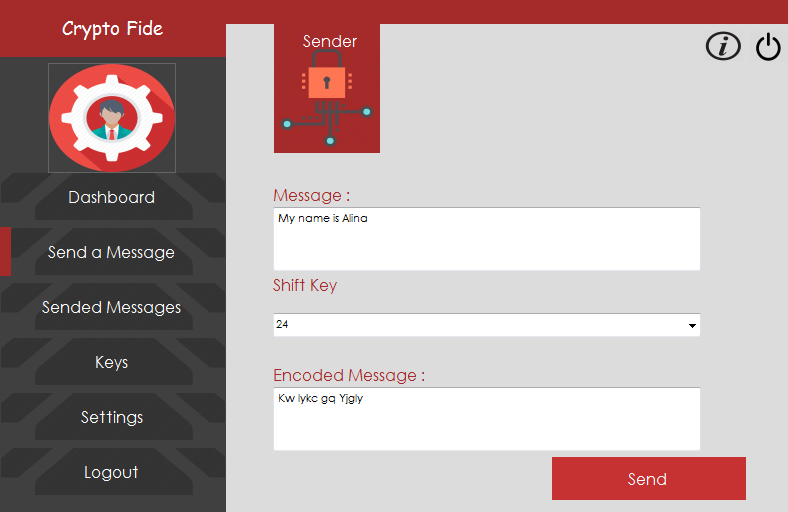
**Vigenere Cipher:**



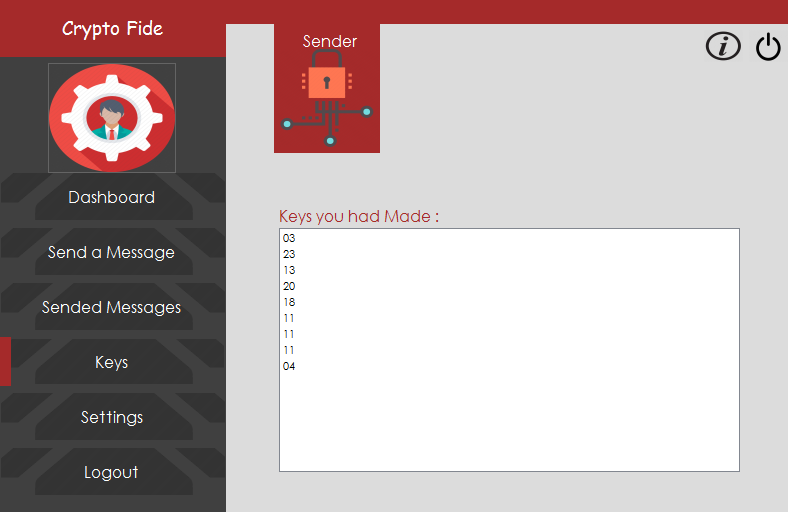
**Sended Messages:**



**Caesar Cipher:**



**Keys:**



**Benefits of Project:**

Various benefits of our project include:

**Authentication:**

Authentication is verification of the identity of the sender at receiver end. A user or system can prove their identity to another who does not have personal knowledge of their identity.

**Confidentiality:**

Confidentiality is most commonly addressed goal. It refers that transmitted message is only received by authorized party.

**Integrity:**

Integrity is making it sure that the received message is in same form as it was sent. Only authorized users have privileges to modify the data.

**Access control:**

Access control is making it sure that only authorized parties have privileges to access the given information.

**Non repudiation:**

Non repudiation is a method of guaranteeing message transmission between parties via digital signature or encryption. It helps to protect against the denial of authentication attempt.

**Summary/Conclusion:**

A generalized model of Vigenere cipher is proposed in which any matrix whose rows or columns are unique can be used in place of Vigenere square. The matrix may be random or regular. Once such a matrix is obtained, its corresponding reversible matrix can be easily derived. Either of the two reversible matrices can be used for encryption or decryption. Use of random matrices in place of Vigenere square will increase the difficulty level of cracking the cipher. An improved random key stream generation method is also suggested to enhance the security level of the Vigenere cipher.

In summary modified hybrid of Caesar cipher and Vigenere cipher algorithm was to test data security on communicated message and it was found to be most secure compared to data security test on Caesar cipher and Vigenere cipher algorithm or that of hybrid Caesar cipher and Vigenere cipher algorithm. It was discovered that originally, cipher text generated with Caesar cipher algorithms and Vigenere algorithms are prone to be broken easily using brute force, exhaustive search, searching by frequency and many other methods because they lack diffusion and confusion in the algorithms that generate them but with the modified hybrid of both the Caesar cipher and Vigenere cipher, there is now a high percentage of diffusion and confusion in the algorithm that generates them making it a very strong cipher and difficult to break.