DYNAMIC KEY GENERATION FOR SECURE INFORMATION TRANSMISSION USING ENCODING

[1]Sadhana Kodali,[2]P.Leela Pavani, [3]M.Meghana, [4]K.Kiran Kumar Singh,[5]M.Ramji.

[1]Associate Professor, [2,3,4,5]Student -8th Semester
Department of CSE,
Lendi Institute of Engineering & Technology, Vizianagaram, India

***Abstract*: In modern security models, cryptography plays a fundamental role in protecting data integrity and confidentiality for secure information transmission. The data encryption techniques used in cryptography are still vulnerable to attacks. To reduce the cryptanalysis attack risk, a dynamic key generation model is proposed, because the key generated in this model is dynamic and this can improve the security in cryptographic system can provide better secure information transmission. The dynamic key generation scheme and key update mechanism are formally analyzed to demonstrate balance between security and performance. This project uses a key generation process which works similar to symmetric cryptography by using text processing. And this method of dynamic key generation is very difficult for the attacker to break the key. This project encodes the cipher text before transmission in order to secure the information.**

***Keywords*: Authentication, Dynamic Key Generation, Symmetric Cryptography, Encoding, Decoding.**

1. INTRODUCTION

With the evolution of computer technology, computer networking, and the Internet, the digital information transfer has rapidly increased. An additional challenge was that the increase in the transfer of digital information, has given rise to the unauthorized parties (i.e., eavesdroppers) intercepting and interpreting transmitted digital information that is not intended for them. Thus, techniques, such as encryption, have been developed to secure the information so that only the intended parties are able to understand the substance of the message. The concept behind encryption is quite simple—make the digital information illegible for everyone except the intended parties. Cryptography plays an important role in secured data communication over the network using unknown, untrusted mediums. In the fast digital transformation, traffic on network increasing rapidly where users are always connected, being online, anytime anywhere. As part of data, extortions like altering, spoofing and snooping of are quite common over the network by unauthorized access. Cryptography is well known mechanism where asymmetric or symmetric algorithms using public or private keys provide secure data communication. There are many more cryptography algorithms existing but with emerging technologies and diverse application domains seeking consistent enhancement and better performance with resource restriction. In this paper, we present a novel symmetric cryptography technique based on Caesar cipher symmetric cryptography technique to transform the original text/message into secret text/message. In this technique, the sender transmits message into cipher text and provides a secret keyto thereceiver to decrypt the message of a sender.

The dynamic key generation scheme and key update mechanism which are used in this project are formally analyzed to demonstrate balance between security and performance. This project uses a dynamic key generation process which works similar to symmetric cryptography by using text processing. The dynamic key generation scheme and key update mechanism which are used in this project are formally analyzed to demonstrate balance between security and performance. This project uses a dynamic key generation process which works similar to symmetric cryptography by using text processing. And this method of dynamic key generation is very difficult for the attacker to break the key. This project encodes the cipher text even before transmission in order to secure the transmitted information.

CRYPTOGRAPHY

In every sector, security for confidential data is the biggest concern for everyone , mainly in online banking and reservation system, so that no one can change and access the data for illegal use. To prevent such circumstances, the preferred technique is cryptography that converts the data into an indescribable code form (cipher) at sender side and decode into readable form at receiver side. The main objective of cryptography technique is to convert the data into non-readable form so that only authorized user can access the data, and in any situation the attacker should not have

any chance to access the database server or secrete data. Cryptography is carried out into two different phases' encryption and decryption. Encryption as well as decryption both are important aspects of security. In encryption process, plain text or secret message converted into a weird message or scrambled one known as cipher text with the help of secret key and, in the decryption process, cipher text is converted back to plain text with the help of same secret key used in encryption process.

In the fast digital transformation, traffic on network increasing rapidly where users are always connected, being online, anytime anywhere. As part of data, extortions like altering, spoofing and snooping are quite common over the network by unauthorized access. Cryptography is well known mechanism where asymmetric or symmetric algorithms using public or private keys provide secure data communication. There are many more cryptography algorithms existing but with emerging technologies and diverse Cryptography plays an important role in secured data communication over the network using unknown, untrusted application domains seeking consistent enhancement and better performance with resource restriction. Encryption as well as decryption both are important aspects of security. In encryption process, plain text or secret message converted into a weird message or scrambled one known as cipher text with the help of secret key and, in the decryption process, cipher text is converted back to plain text with the help of same secret key used in encryption process mediums.

Caesar Cipher:

The Caesar Cipher technique is one of the earliest and simplest methods of encryption technique. It's simply a type of substitution cipher, i.e., each letter of a given text isreplaced bya letter with a fixed number of positions down the alphabet.

For Example, A = 0, B = 1, Z = 25. Encryption of a letter by a shift n can be described mathematically as.

$E_n(x)=(x+n) \bmod 26$ (Encryption Phase with shift n)

$D_n(x)=(x-n) \bmod 26$

(Decryption Phase with shift n)

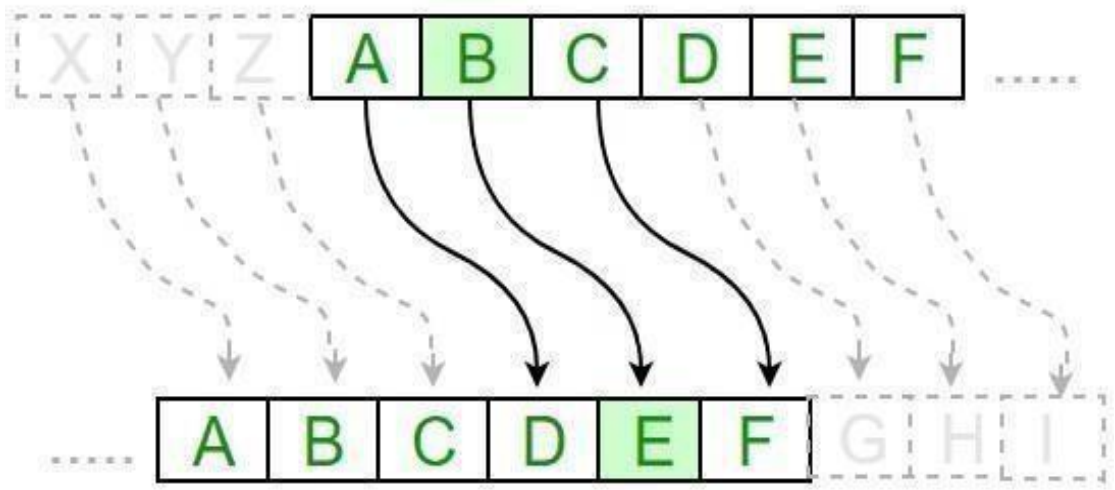

Fig 1: Encryption for Caesar Cipher

Figure 1 indicates the encryption for Caesar cipher where we historically consider three right shifts for normal Caesar cipher.

Text : ABCDEFGHIJKLMNOPQRSTUVWXYZ

Shift: 23

Cipher: XYZABCDEFGHIJKLMNOPQRSTUVW

In this paper, we present a novel symmetric cryptography technique based on Caesar cipher symmetric cryptography

technique to transform the original text/message into secret text/message. In this technique, the sender transmits message into cipher text and provides a secret key to the receiver to decrypt the message of a sender. This method of dynamic key generation is very difficult for the attacker to break the key. This project encodes the cipher text before transmission in order to secure the transmitted information.

2. LITERATURE SURVEY

The Author (Sanjeev Kumar,et.al) in [1], performed the encryption and Decryption process using modular arithmetic considering the concept of Caesar cipher . Inspiring from Caesar
cipher technique, a novel symmetric cryptography technique proposed in this work to provide more secure transition over the network and complement the ever-demanding enhancement in cryptography.
Introducing (Sourabh Chandra,et.al), the encryption and decryption depending upon the data and the channel through which data is being communicated in [2] drawn a comparison analysis of the proposed mechanisms based on their basic features, advantages, drawbacks and applications.
Summary by the author in [3] performed A Modified Symmetric Key Cryptography Method for Secure Data Transmission as the transmission of information is in a secure way is possible by introducing a method using symmetric key cryptography. A method had been drawn from the basis of symmetric key cryptography in order to transmit the data in a secure way.
Caesar cypher substitution was used by the author in [4] for more security purposes. The author had used the randomized approach for the method substitution in encrypting the information. By randomizing the method for Encryption does enhance the security of Caesar cipher for more secure information.
As the Caesar cipher substitution method using a randomized approach for secure information transmission doesn't reach the level of tight security. The writer in [5] introduced a double substitution method in order to provide more security in the transmission of information. The securitycan be enhanced by the double substitution method in transmission.
In order to obtain robustness, transparency, security, imperceptibility, possibility of verification the author in [6] believed the digital watermarking scheme and public key certification and revocations are found to be highly efficient. The watermarking scheme is based on Steganographic systems, where the information is directly embedded into media data. The public key certification and revocation techniques ensure the validation of public keys, which is essential for data privacy.
Hash code is used in symmetric key according to the author in [7]. As the Adoption of emerging technologies in view of rapid digital transformation, number of web users and connected devices are increasing promptly which leads to heavy network traffic over internet and underlying infrastructure. The proposed technique generates cipher text which is more difficult to decode for hackers/unauthorized users. It also provides secure key(symmetric) transmission over the network.

With the development of computer technology, computer networking, and the Internet, the transfer of digital information has rapidly increased. Additionally, with the increase in the transfer of digital information, there has been an increase in unauthorized parties (i.e., eavesdroppers) intercepting and interpreting transmitted digital information that is not intended for them. Thus, techniques, such as encryption, have been developed to secure the information so that only the intended parties are able to understandthe substance of the message. The concept behind encryption is quite simple make the digital information illegible for everyone except the intended parties.

3. METHODOLOGY

The data encryption techniques used in cryptography are still vulnerable to attacks. To reduce the cryptanalysis attack risk, a dynamic key generation model is proposed, because the key generated in this model is dynamic and this can improve the security in cryptographic system can provide better secure information transmission. The dynamic key generation scheme and key update mechanism are formally analyzed to demonstrate balance between security and performance. This project uses a key generation process which works similar to symmetric cryptography by text processing. And this method of dynamic key generation is very difficult for the attacker to break the key. This project encodes the cipher text before transmission to secure the information. Moreover keys will be generated dynamically based on the text in our system.

Here we had introduced four methods for the encryption process. These four methodologies are namely normal Caesar cipher with encoding, encryption based on the length of the word, encryption with corresponding letter position, Encryption based onthe additionof position and the letter of the word. These four methods will be generated randomly by the system. The method which is used for the encryption process will be used for the decryption process. After the encryption is done then the encrypted text will undergo to the encoding process to secure the information. The same

process will be done in the reverse order for the decryption process.

Here we Introduced four Encryption Techniques In order to secure the information.

Methodology 1: Normal Caesar Cipher with Encoding

Here In figure 3.1 Normal Caesar Cipher with Encoding we are encrypting the text based on the normal Caesar. forexample,when we take the plain text as ABC
PT->ABC where A,B,C haspositions 0,1,2then we encrypt it as followsA+2=CB+2=D
C+2=E Here we got the cipher text as CT->CDE

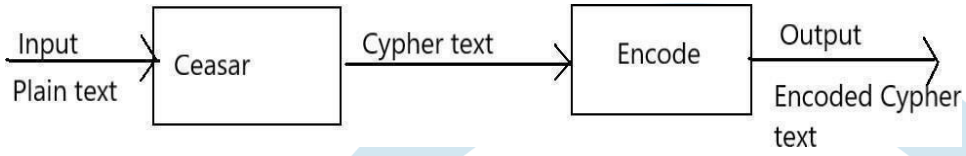

Fig 3.1: Normal Caesar Cipher with Encoding

Methodology 2: Length of the word

Here in figure 3.2 the Length of the word encryption technique we are encrypting the text based on the length of the word. Forexample when we take the plain text as ABCD
PT->ABCD where the word length is |W|=4A+4=EB+3=EC+2=ED+1=E
Where we got the CT->EEEE and generate the morse code.

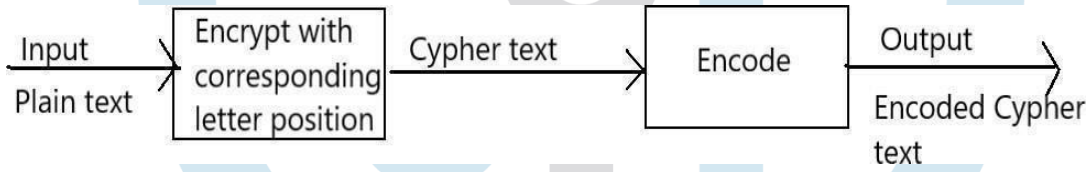

Fig 3.2: Length of the Word

Methodology 3: With corresponding letter position

Here in figure 3.3 this technique the encryption does takes place with corresponding letter position. The position and the placement of the letter will be added together with the position of the letter in the word which is going to be encrypted. Here the position of the letter will be different to every word and the position of the word will be same to that particular word but if the word changes to other then the position of the letter will be depend on that word.
By the following example we can clearly understand the concept of encrypting using the method encrypting with the corresponding letter position.
Position +Placement ofthe letter
For example, when we takethe plain text as How Are You PT->How Are You
As thereare three letters in the word the words take the positions as How,Are, You ->0,1,2
The word length is |W|=3
For the word How: For the word Are:

Pos+'H'+3-> 0+H+3 = KPos+'O'+2-> 0+O+2 = Q
Pos+'W'+1-> 0+W+1 = X

The above steps are clearly explained in figure 3.3

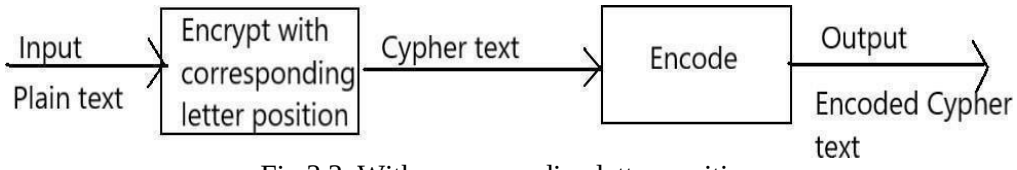

Fig 3.3: With corresponding letter position

Methodology 4: Key+ Position of word

Here the encryption technique is based on the Keyand Position of the word.

Constant key+ Position of the word

Here the key is generated automatically bythe system itself. The formula for the keygeneration is Key=Position +Key
For example in the figure 3.4 where we take the plain text as PT->How Are You each word has three letters in each so they take the positions as HOW as 0 , ARE as 1 and You as 2.After that they internally divide the letters as H,O,W as 0,1,2 likewise A,R,E as 0,1,2follows.
Therandomly generated key constant key will be added to the position to be encrypted.

If the system generated key is taken as 3 then theprocess of encryption will be doneas followsFor How: 0+3=3

1+3=4

2+3=5

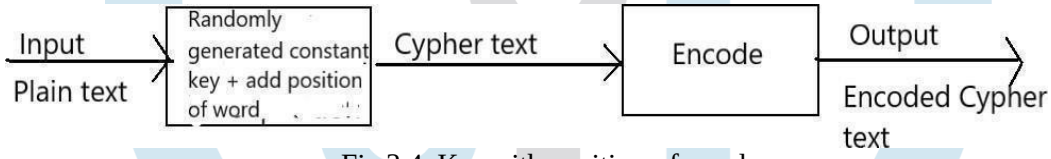

Fig 3.4: Key with position of word.

4. EXPERIMENT

Many systems were using different encryption and decryption techniques for their security Ex: Substitution ciphers-Caesar Cipher, mono alphabetic cipher...
This process hides the data from third parties. The Caesar Cipher technique is one of the ancient and easiest method of encryption technique. It's simply a type of substitution cipher, i.e., each letter of a given text is replaced by a letter with a fixed number of positions down the alphabet historically the number of positions moved are three. For example, with a shift of 2, A would be replaced by C, B would become D, and so on but historically we use three shifts. The method is apparently named after Julius Caesar, who apparently used it to communicate with his officials.
Thus, cipher a given text we need an integer value, known as a shift which indicates the number of positions each letter of the text has been moved down.
Cryptography is carried out into two different phases encryption and decryption. Encryption as well as decryption both are important aspects of security. In encryption process, plain text or secret message converted into a weird message or scrambled one known as cipher text with the help of secret key and, in the decryption process, cipher text is converted back to plain text with the help of same secret key used in encryption process. This system is designed to provide security based on encryption and decryption. Unlike other encryption techniques, we use dynamic key generation techniques. For every word or for every text the key differs and makes it difficult for the unauthorized person to crack the key.

ALGORITHM:

Step 1: Take input

Step 2: Declare encryptionPattern1(),
encryptionPattern2(), encryptionPattern3(), encryptionPattern4(), encode()
Step 3: Declare decryptionPattern1(),
decryptionPattern2(), decryptionPattern3(), decryptionPattern4(), decode()

Step 4: Generate random number from 0 to 4Step 5: making random number as choice
Case 1: call encryptionPattern1() Case 2: call encryptionPattern2() Case 3: call encryptionPattern3() Case 4: call encryptionPattern4()
Step 6: call encode()
Step 7: display Encoded text returned by encode functionStep 8: call decode()
Step 9: take encrypted text and analyze patten using last characterStep 10: making last character as choice
Case 1: call decryptionPattern1() Case 2: call decryptionPattern2() Case 3: call decryptionPattern3() Case 4: call decryptionPattern4()
Step 11: display plain text

System Design

System design is a process of defining system elements such as architecture, modules and components, the various interfaces ofthese components and the data that passes through the system. It is intended to satisfy needs and business organization requirements by engineering a coherent and well functioning system.

System design focuses primarily on defining the architecture, components, modules, interfaces and data for the system to meet the specified requirements. System design can be understood as the application of systems theory to product development. System design means a systematic approach to system design. It may require a bottom –up or top-down approach, but either way the process is systematic, taking into account all related systems to be created from the architecture, the required hardware and software to the data and how it moves and transform along the way through the system. System design then overlaps with system analysis, system engineering and system architecture. The system design approach first appeared just before world war II when engineers were trying to solve complex control and communications problems. They needed to be able to a standardized their work into a formal discipline with the right methods especially for new fields such as information theory, operation research and computer science in general. With development computer technology, computer networks and the internet, the transfer of digital information has increased rapidly.

In addition, with increase in the transmission of digital information, the number of unauthorized parties(i.e eavesdropping) capturing and interpreting transmitted digital information that is not intended for them. That is, techniques such as encryption, were developed to secure information so that only the intended parties can understand it's essence message. The concept of encryption is quite simple-it renders digital information unreadable to all but the user intended parties.

The main objective of cryptography technique is to convert the data into non-readable form so that only authorized user can access the data, and in any situation the attacker should not have any chance to access the database server or secrete data. Cryptography is carried out into two different phases encryption and decryption. Encryption as well as decryption both are important aspects of security. In encryption process, plain text or secret message converted into a weird message or scrambled one known as cipher text with the help of secret key and, in the decryption process, cipher text is converted back to plain text with the help of same secret key used in encryption process.

This system is designed to provide security based on encryption and decryption. Unlike other encryption techniques, we use dynamic key generation techniques. For every word the key differs and makes it difficult to crack the key. In encryption process, plain text or secret message converted into a weird message or scrambled one known as cipher text with the help of secret key and, in the decryption process, cipher text is converted back to plain text with the help of same secret key used in encryption process.

Data Flow Diagram:

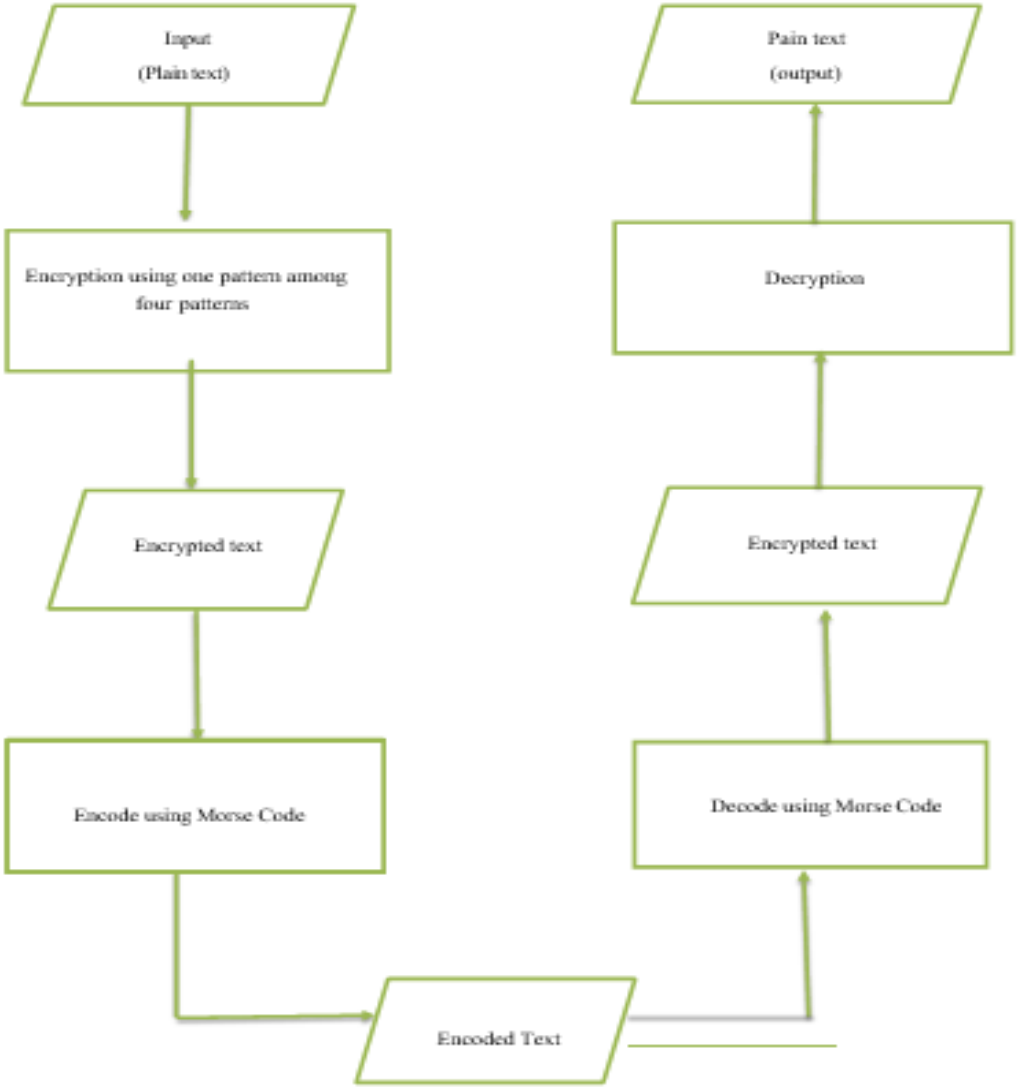

Fig 4.1: Data Flow Diagram

Figure 4.1 represents the data flow diagram for the methodoly followed for generating the encoding.The Input has been taken as a plain text and the text will be encrypted using one pattern among the four patterns (Patterns are: NormalCaesar cipher with encoding, Length of the word, with corresponding letter position, key with position of word) . Now we will obtain encrypted text. The encryptedtext will encode using morse code and we will get encoded text. Now the encoded text will be decoded using morse code then we willget encrypted text, this encrypted text will go through the decryption process then we get a plain text asa desired output.

EXPERIMENT RESULTS

Landing Page

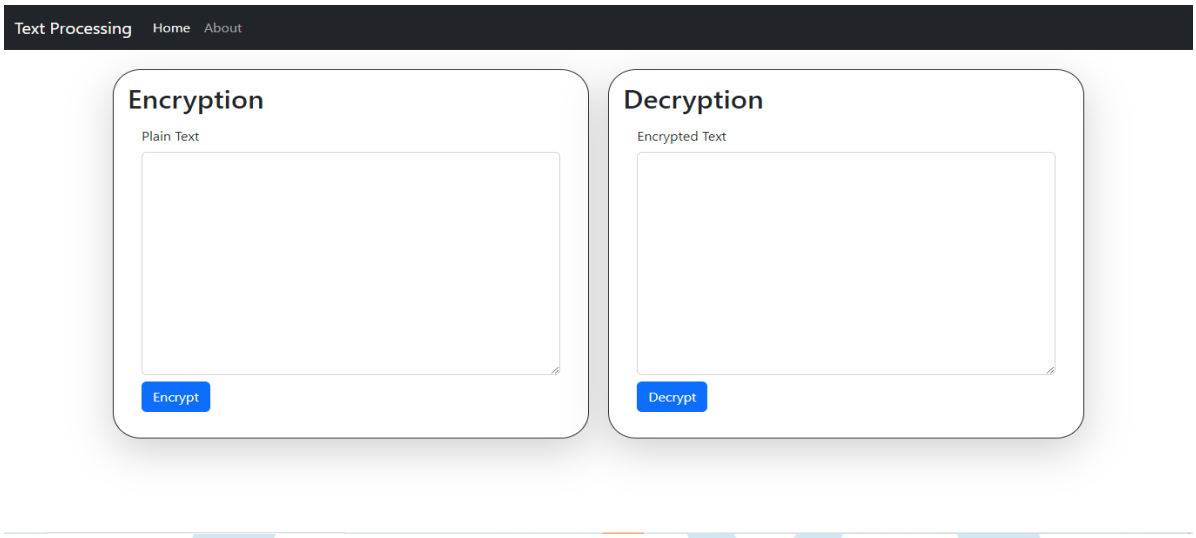

Fig 4.2: Landing Page

The figure 4.2 will be the home page for our application it is developed for generating the encoding for the cipher text

Encryption and Decryption ofword

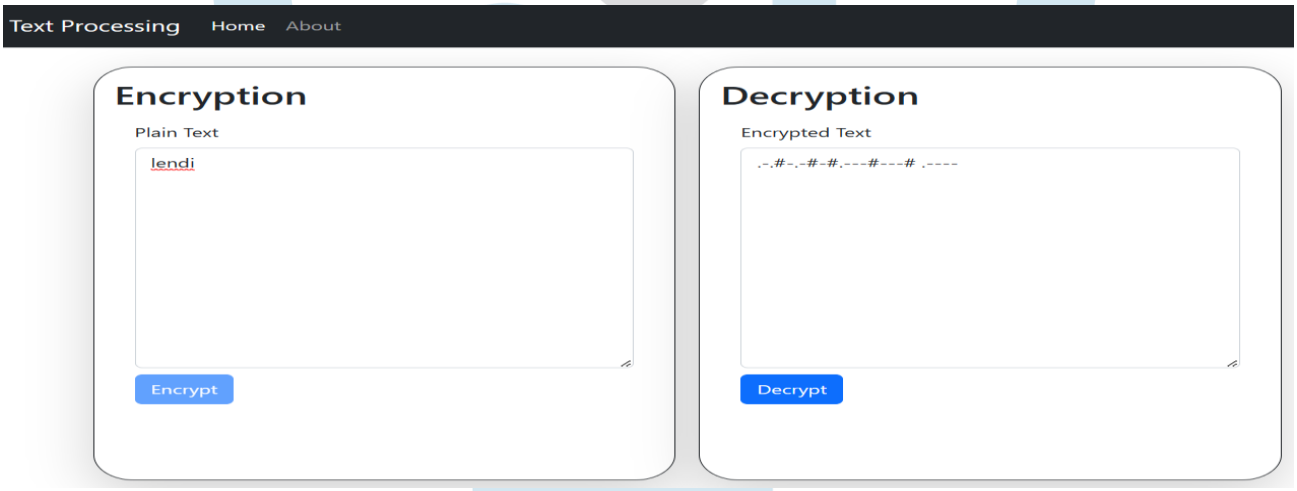

Fig 4.3:Encryption and decryption of word

Here from 4.3 when we considered plain text as lendi the encrypted text obtained is ‘qiqfj’ by using one of theencrypted methods discussed above. Now the encrypted text will be encoded using morse code and we will getencoded text.

Encryption and Decryption ofa Sentence

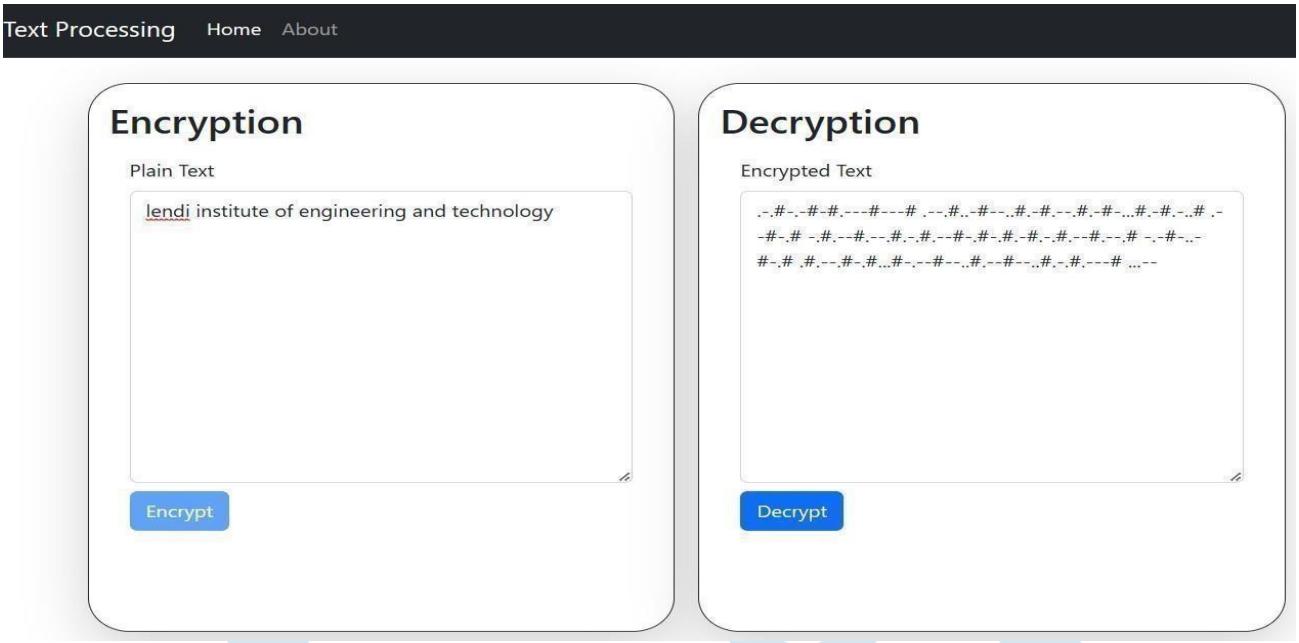

Fig 4.4: Encryption and decryption of a sentence

Here we considered plain text as 'lendi institute of engineering and technology' the encrypted text obtained is 'qiqfj rvzznxxvf qg pxpqukjvlph dpe nkottpriz' by using one of the encrypted methods discussed above. Now the encrypted textwill be encoded using morse code and we will get encoded text.

These are some ofthe results of our proposed system**.**

5. CONCLUSION

Information security can be easily achieved by using Cryptography techniques. Symmetric cryptography is more efficient and therefore more suitable for encrypting/decrypting large volumes of data. Cryptography is well known mechanism where asymmetric or symmetric algorithms using public or private keys provide secure data communication. There are many more cryptography algorithms existing but with emerging technologies and diverse Cryptography plays an important role in secured data communication over thenetwork.
The goal of symmetric encryption isto secure sensitive, secret, or classified information.

The data encryption techniques used in cryptography are still vulnerable to attacks. To reduce the cryptanalysis attack risk, a dynamic key generation model is proposed, because the key generated in this model is dynamic and this can improve the security in cryptographic system can provide better secure information transmission. The dynamic key generation scheme and key update mechanism are formally analyzed to demonstrate balance between security and performance. This project uses a key generation process which works similar to symmetric cryptography by text processing. And this method of dynamic key generation is very difficult for the attacker to break the key. This project encodes the cipher text before transmission in order to secure the information.

REFERENCES

[1] Sanjeev Kumar.et.al." Approach of Symmetric Key Cryptography" Int. J. Computer. Appl.vol.57.pp.128-234,2015.
[2] Sourabh Chandra, et.al." A study and analysis on Symmetric Cryptography". IEEE design and test of computers, Dec 1991pp.6-17,IEEE.
[3] M. Sohal and S. Sharma. "BDNA-A DNA inspired symmetric key cryptographic technique to secure cloud computing," J. King Saud Univ. – Computer . Inf. Sci., 2018
[4] S. Chandra, "A Studyand Analysis on Symmetric Cryptography," in International Conference onScience, Engineering andManagement Research (ICSEMR 2014), 2014, no. November.
[5] A. Mohammed, A. Argabi, and I. Alam, "A new Cryptographic Algorithm AEDS (Advanced Encryption and DecryptionStandard) for data security." Int. Adv. Res. J. Sci. Eng. Technol., vol. 6, no. 10, pp. 1-7, 2019.
[6] A. Balogun, P. Sadiku, and H. Mojeed, "Multiple Caesar Cipher Encryption Algorithm."ABACUS, (Mathematics

Sci. Ser..vol. 44, no. December 2017, 2017.
[7] S. B. Dar, "Enhancing The Security of Caesar Cipher Using Double Substitution Method." Int. J. Computer Science. Eng.Technol. Enhancing, vol. 5, no. 07, pp. 772-774, 2014.
[8] S. B. Dar, "Enhancing The Security of Caesar Cipher Using Double Substitution Method." Int. J. Computer Sci. Eng. Technol.Enhancing, vol. 5, no. 07, pp. 772-774, 2014.
[9] S. Gowda, "Innovative Enhancement Of The Caesar Cipher Algorithm For Cryptography," in International Conference onAdvances in Computing, Communication, & Automation (ICACCA), 2017.
[10] D. S. Ginting, K. Sitompul, J. Simanulang, R. W. Sembiring, and M. Zarlis, "Modification of Symmetric Cryptography with Combining Affine Chiper and Caesar Chiper which Dynamic Nature in Matrix of Chiper Transposition by Applying Flow Pattern in the Planting Rice," Adv. Sci. Technol. Eng. Syst. Journa, vol. 2, no. 5, pp. 6–12, 2017.
[11] F. I. Lubis, H. Fachri, S. Simbolon, T. P. Batubara, and R. W. Sembiring, "Combination of Caesar Cipher Modification with Transposition Cipher," Adv. Sci. Technol. Eng. Syst., vol. 2, no.5, pp. 22–25, 2017