ACKNOWLEDGEMENT

- The prestation of this project given me feeling of fulfilment. With immense pleasure we would like to present this report on this project report Website that encrypts and decrypt string. (Uncrackable by anyone).
- We would like to this opportunity to bestow our acknowledgement to the entire person who have directly or indirectly avail in making our project feasible and to turn it up in to successful piece of work.
- We take this opportunity to appeal my profound gratitude to all those who have directly or indirectly help us in our project.

Chauhan JayrajSinh.

Chokshi Jayneel.

Jadhav Yash.

Kaloliya Bhavin.

Ojha Het.

ABSTRACT

Encryption is the encoding of information so that only those who have access to a password or encryption key can access it. Encryption protects data content rather preventing unauthorized interception of or access to data transmission. It is used by intelligence and security organization and in personal security software designed to protect user data. The importance of security in data communications and networking cannot be over-emphasized. Security in networking is based on cryptography, the science and art of transforming messages to make them secure and free from attacks and all sorts of eavesdropping. Cryptography has diverse applications in network security. Encryption algorithms are known to be computationally intensive.

INDEX

CHAPTER - 1

INTRODUCTION

1.1 INTRODUTION OF WEBSITE THAT ENCRYPT AND DECRYPT STRINGS.

Encryption is a process of converting messages, information, or data into a formunreadable by anyone except the intended recipient.

Encryption helps to you protect the privacy of your messages, documents and sensitivefiles.

Encrypted data must be deciphered, or decrypted, before it can be read by the recipient. The root of the word encryption—crypt—comes from the Greek word cryptos, meaninghidden or secret.

In its earliest form, people have been attempting to conceal certain information that theywanted to keep to their own possession by substituting parts of the information with symbols, numbers and pictures. For different reason, humans have been interested in protecting their messages.

Threats to computer and network security increase with each passing day and come from agrowing number of sources. No computer or network is immune from attack.

Encryption, or the ability to store and transmit information in a form that is unreadable toanyone other than intended persons, is a critical element of our defense to these attacks. Indeed, man has spent thousands of years in the quest for strong encryption algorithms.

Data encryption is the conversion of data into a form, called a ciphertext, that cannot beeasily understood by unauthorized people. Decryption is the process of converting encrypted data back into its original form, so it is easily understood.

Encryption is a mechanism for hiding information by turning readable text into a stream ofgibberish in such a way that someone with the proper key can make it readable again.

1.2 PURPOSE : GOALS AND OBJECTIVES.

Goals :-

- Protects reliability of data against tampering.
- Data/resources should be accessible when needed.
- Increases confidentiality.
- Prevention is more important than detection and recovery.
- Protect your text by Encrypting and Decrypting any given text with a key that noone knows.

Objectives :-

- To explore and implement an encryption and digital signature program to use withthe aim of providing the user with a basic knowledge of the fundamental techniques of encryption and key.
- To provide the user with authentication, integrity, confidentiality and non-repudiation of the data.
- To provide the user with an enhanced security of their data.
- To provide the user with a way to easily and conveniently protect the data.

1.3 SCOPE :-

The scope of this project includes the following features :-

- Easy & Secure way of encryption.
- Provide security to the Message.
- UI is optimized so anyone can understand & used website easily.
- Time saving.

1.4 TECHNOLOGIES AND LITERATURES :-

Technologies :-

- Selective data encryption, the traditional method, is costly, resource-intensive andforces risky decisions.

- With our Encryption technique you can protect data and manage privacy bypolicy.

- Historically, various forms of encryption have been used to aid in cryptography. Early encryption techniques were often utilized in military messaging. Since then,new techniques have emerged and become commonplace in all areas of modern computing.

Literatures :-

- To provide security to the database is one of the complicated problems. Basically, encryption keys are used to write data in protected fields. Decryption keys are usedto read the data. So, it provides the access rights for user.

CHAPTER - 2

SYSTEM REQUIREMENTS STUDY

2.1 USER CHARACTERISTICS

- User Friendly website.
- Accessible to All Users.
- Well Planned Information Architecture.
- Well-Formatted Content That Is Easy to Understand.
- Loads Faster.
- Effective & Easy Navigation.
- Does its Job.

2.2 HARDWARE AND SOFTWARE REQUIREMENTS

Hardware :- Not required.

Software :- Any Web browser on Any OS.

2.3 CONSTRAINTS

- If a key is leaked then your Information (Message) Can be Read by someone else.
- If a key or encrypted text is forgotten then the User cannot find the originalmessage.

CHAPTER - 3

SYSTEM ANALYSIS

3.1 STUDY OF CURRENT SYSTEM

- Now there are many encryption techniques now a days. But day by day hackers and experts find a way to crack the techniques. Below Mentioned are some currentTechniques.
    1. One-Time Pad
    2. Pseudo- Random number Generator
    3. Symmetric Key Encryption
    4. Asymmetric Key Encryptions
    5. Diffie-Hellman Key Exchange
    6. RSA Encryption

3.2 PROBLEM AND WEAKNESS OF CURRENT SYSTEM

- Now a days thousands of hacking attacks performed on daily basis.
- There is are many ways of stopping these attacks.
- But it happens by some mistake or by some BUG in some systems.
- Passwords are like underwear's never share with someone. And keep it privateand confidential.
- Security is Myth.

3.3 REQUIREMENT OF NEW SYSTEM

- As we need regular security patches and updates to be safe from attacks, that'swhy we also need update in our encryption algorithms.

3.4 FEASIBILITY STUDY

Eight steps are involved in the feasibility analysis. They are :-

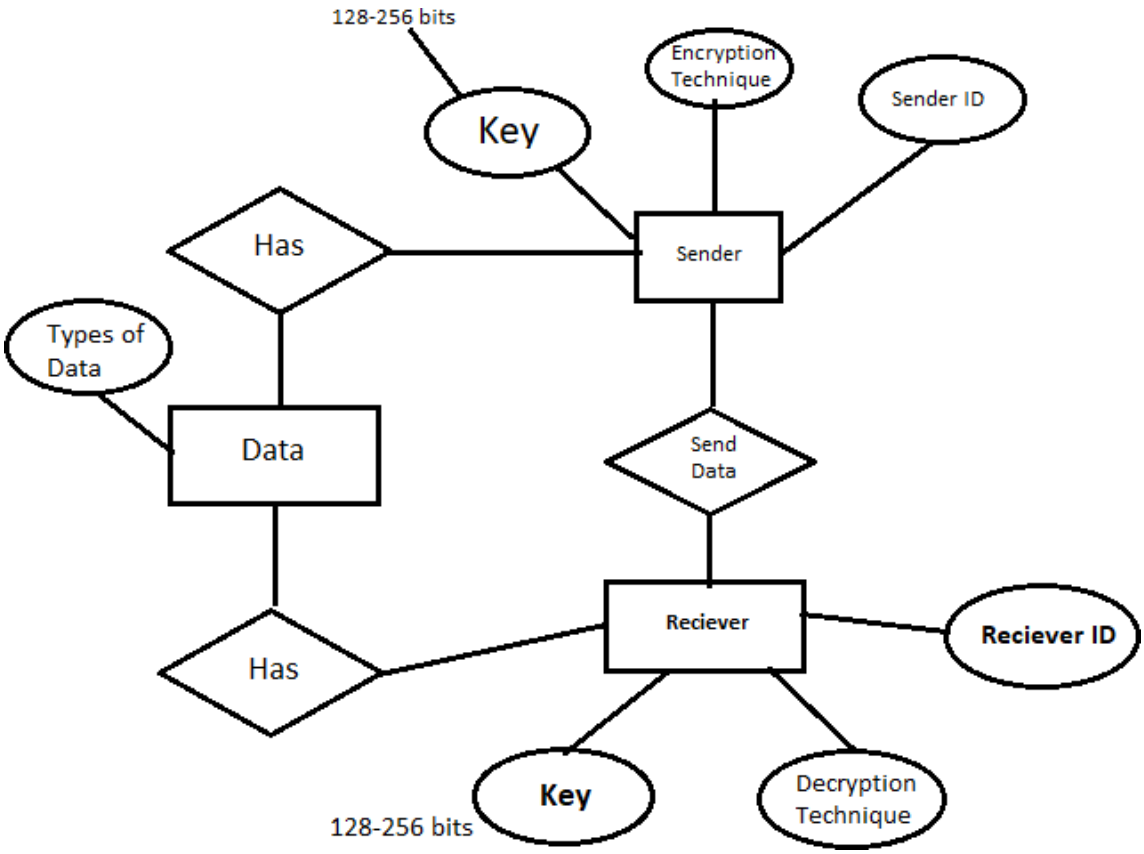
- Form a project team and appoint a project leader.
- Prepare system flowcharts.
- Enumerate potential proposed systems.
- Define and identify characteristics of proposed system.
- Determine and evaluate performance and cost effectiveness of each proposedsystem.
- Weight system performance and cost data.
- Select the best proposed system.
- Prepare and report final project directive to management.

3.5 REQUIREMENT VALIDATION

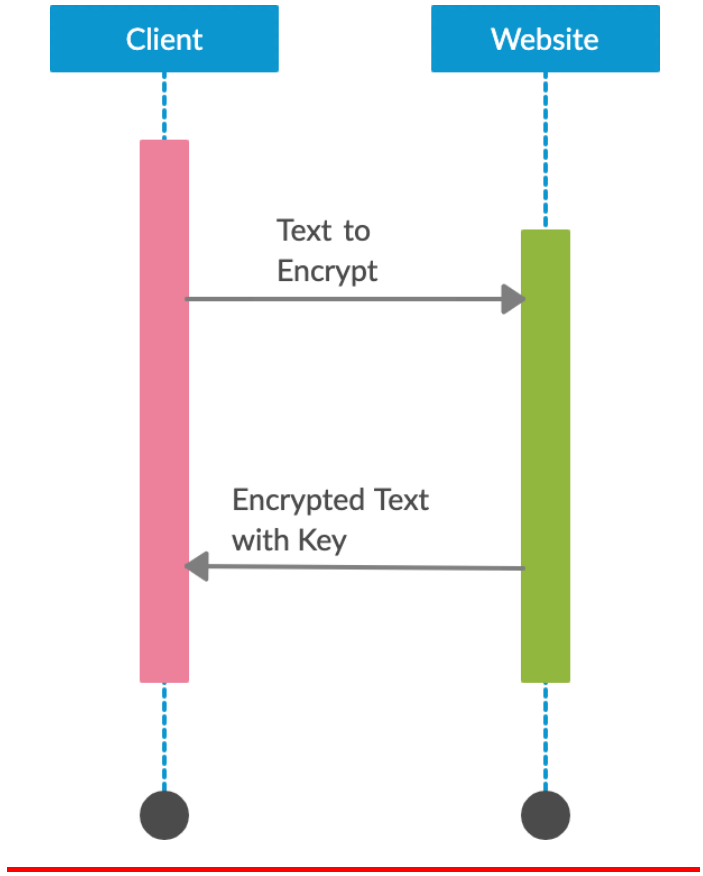
- User friendly layout.
- Best in class security from our side.
- Easy to Use.

3.6 DATA MODELING

3.6.1 Class Diagram/E-R Diagram



3.6.2 System Activity or Object interaction Diagram

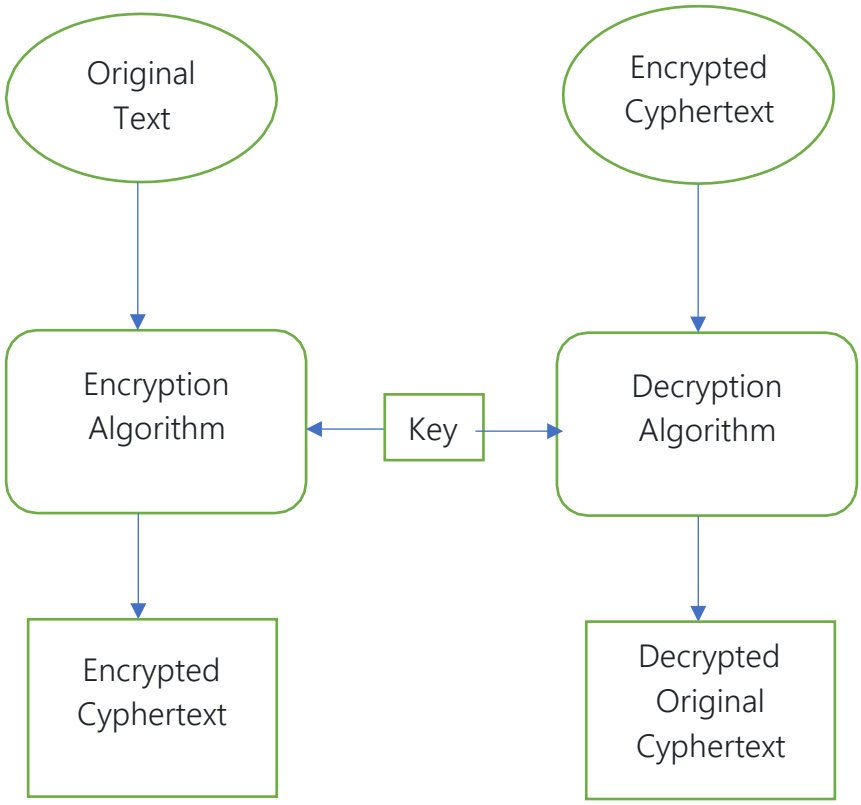


3.6.3 Data Dictionary

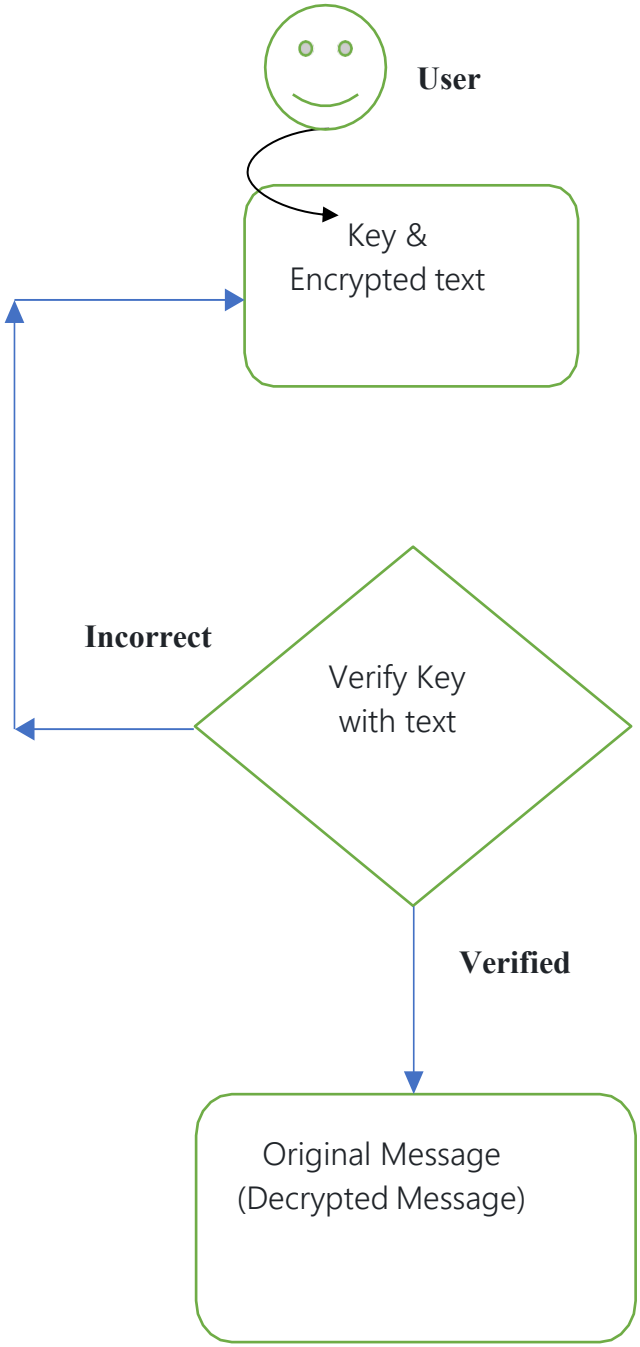
Data dictionary is not applicable in our project as our project doesn't has or performs any type of data related operations.

3.7 FUNCTIONAL AND BEHAVIORAL MODELING

3.7.1 Context Diagram



3.7.2 Data Flow Diagram (o and 1 level)



3.7.3 Process Specification and Decision Table

Process Specification :-

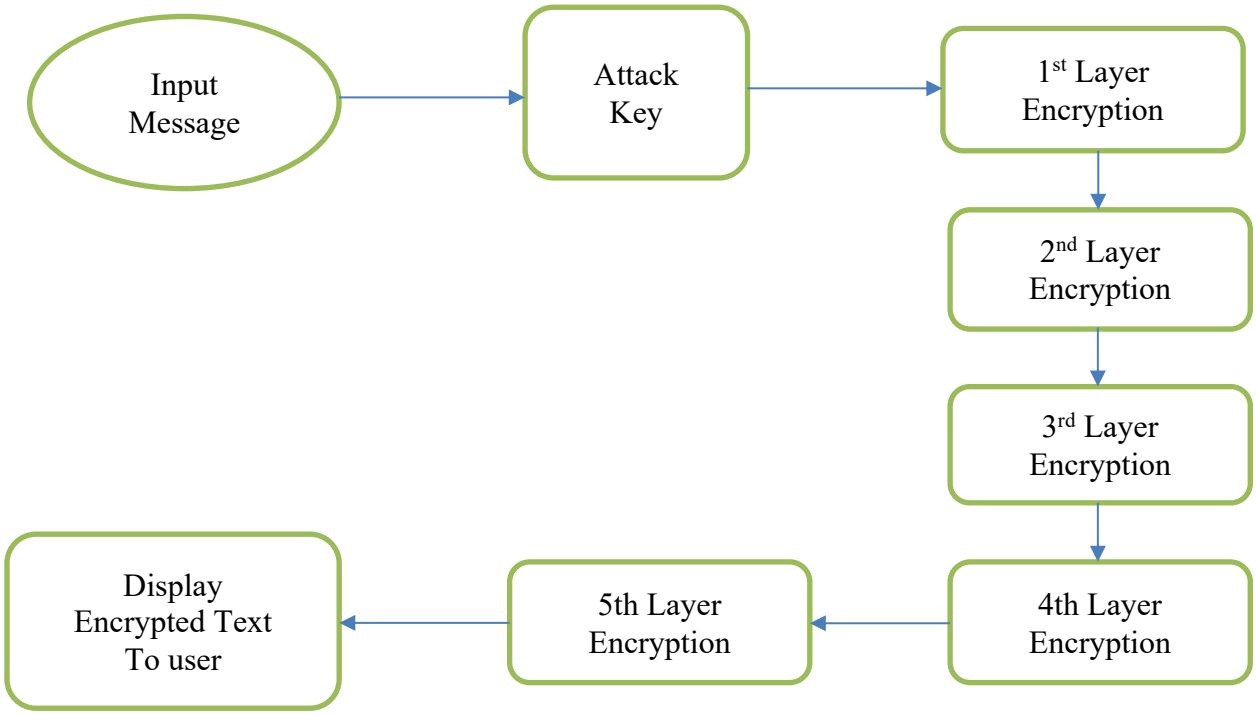
- Process specification is a method used to document, analyze and explain the decision-making logic and formulas used to create. output data from process input data. Its objective is to flow down and specify regulatory/engineering requirementsand procedures. High-quality, consistent data requires clear and complete process specifications.

- Process specification reduces ambiguity, allowing an individual or organization toobtain a precise description of executed tasks and accomplishments and validate system design, including the data dictionary and data flow diagrams.

- Process specifications are created for primitive processes and data flow diagram processes of a higher level (minispecs). Process logic is best represented through structured English, decision tables, decision trees or specified formulas or algorithms and is used to communicate engineering requirements and procedures to businesses involved in the creation of a process. Process descriptions may existon a form or in a computer aided software engineering (CASE) tool repository.

- Process specifications are not created for processes requiring physical input or output, processes representing simple data validation or processes with preexistingand prewritten code.

3.7.4 Control Flow Diagram



3.5 MAIN MODULES OF NEW SYSTEM

- This standard specifies the security requirements that will be satisfied by a cryptographic module utilized within a security system protecting sensitive butunclassified information (hereafter referred to as sensitive information). The standard provides four increasing, qualitative levels of security: Level 1, Level 2,Level 3, Level 4, and Level 5.

- These levels are intended to cover the wide range of potential applications and environments in which cryptographic modules may be employed. The security requirements cover areas related to the secure design and implementation of a cryptographic module. These areas include cryptographic module specification,cryptographic module ports and interfaces; roles, services, and authentication; finite state model; cryptographic key management; electromagnetic interference/electromagnetic compatibility (EMI/EMC); self-tests; design assurance; and mitigation of other attacks.

3.6 SELECTION OF HARDWARE AND SOFTWARE ANDJUSTIFICATION

Hardware Selection Criteria

- Hardware must support current software as well as software planned for procurement over the next planning interval of several years.

- Hardware must be compatible with existing or planned networks.

- Hardware must be upgradeable and expandable to meet the needs of the nextplanning interval.

- Hardware warranties must be of an appropriate length.

- Hardware maintenance must be performed by local vendor.
- Whenever feasible, hardware standards will dictate procurement of like brands andconfigurations to simplify installation and support.
- Routine assessments of installed infrastructure will feed an upgrade/replacedecision process

Software Selection Criteria

- Software must be compatible with current and future hardware over the nextplanning interval.
- Software maintenance and warranties must be of appropriate length and cost
- Software help desk must be maintained by vendor.
- Software must be standardized throughout the business to improve purchasingpower, simplify training, and facilitate support.
- Software must comply with current standards set by technology leadership.
- Software must support and enhance business goals.

In addition to these hardware and software selection criteria, Strat Vantage will evaluatethe proposed vendors on several criteria, including:

Stability — Vendor's attributes such as length of operations, size of customer base, size ofincome and revenue, company size, leadership, stock history and more can affect a technology purchasing decision.

Proven Track Record — A vendor's experience not only in the broader market but in yourbusiness' specific industry can be key.

Business Model Fit — If the vendor is offering, for example, software as a service, but your business isn't always Internet-connected, this business model mismatch could ruleout the vendor.

Mature Technology — You want to see continuity in the vendor's offerings. If the vendorhas been through a series of acquisitions and is just now integrating new technology with an old line of business, you may want to obtain assurances on the longevity of the vendor's solution.

Service Level Agreements — Unfortunately, most vendor Service Level Agreements (SLAs) aren't worth the paper they are printed on. We'll help you understand the vendor'sSLA and negotiate a service level partnership instead.

Conclusion

- There are many other websites for encryption but they may store your data and keyon their servers for recovery purpose. But we promise we never store any of your data with us. As data breaches are occurring day by day that's why our website is created to give you 100% protection to you and your data.

Main Goals :-

- Provide you the best-in-class privacy.
- Save you from breeches and make your data fully Confidential.

CHAPTER - 4

IMPLEMENTATION PLANNING AND DETAILS

4.1 IMPLEMENTATION ENVIRONMENT (Single vs Multi-user, GUI vs Non GUI)

Environment	Discription
Users	Single/Multi user
Compatibility	Website has Universally Compatibility
Programming language	JavaScript
Programming IDE	Visual Studio Code

4.2 PROGRAMS/MODULES SPECIFICATION :-

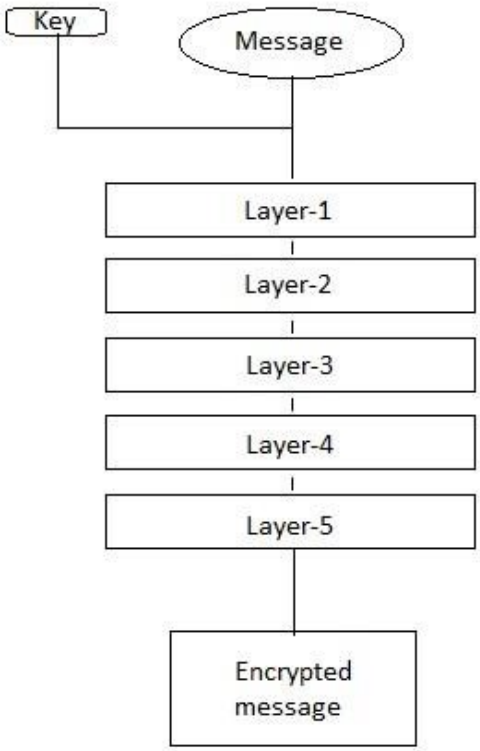
- Our method contains special characters.
- Key generation button make very strong key.
- Every time its generate unique key.
- 5 layer Encryption is used.

4.3 SECURITY FEATURES :-

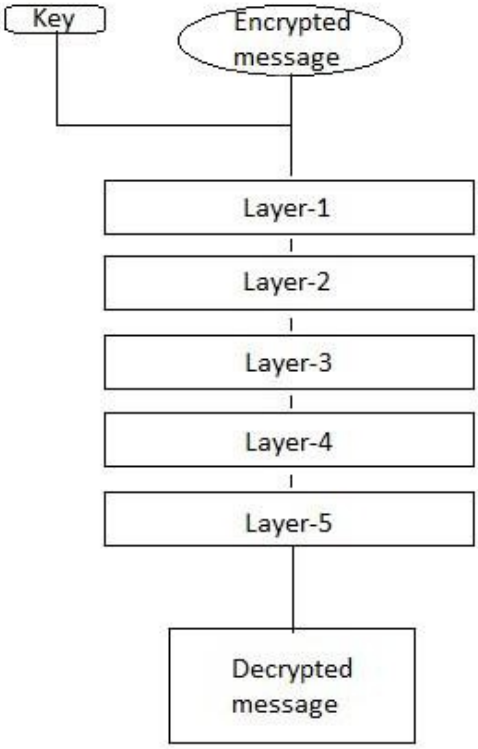
- Five layer protection.
- Key generate (Recommended) option is provided for Highly secure keys.
- No Security Breach is possible if happened u can't suffer because we don't store any of your keys or text on our database.

4.4 CODING STANDARDS :-

Encryption process



Decryption process



4.5 SAMPLE CODING :-

- **THIS IS JAVASCRIPT CODE :-**

```
var caesarShift = function (str, amount) {

    if (amount < 0) {
    return caesarShift(str, amount + 26);

    }

var output = "";

  for (var i = 0; i < str.length; i++) {

  var c = str[i];

  if (c.match(/[a-z]/i)) {
    var code = str.charCodeAt(i);

   if (code >= 65 && code <= 90) {
          c = String.fromCharCode(((code - 65 amount) % 26) + 65);
    }

    else if (code >= 97 && code <= 122) {
        c = String.fromCharCode(((code - 97 + amount) % 26) + 97);
    }

  }

  output += c;
}

return output;

};
```

CHAPTER -5

TESTING

- Security Testing is performed to reveal security flaws in the system in order toprotect data and maintain functionality. This tutorial explains the core conceptsof Security Testing and related topics with simple and useful examples.

5.1 TESTING PLAN :-

- We have planned various types of attacks on website as well as on cipher text, to check that how secure the website and our encryption is

5.2 TESTING STRATEGY :-

- We have planned to attack our website from 2 System co-currently as to check the website is able to maintain its uptime.
- We have planned to do cryptanalysis and other message obtaining method to check how secure the encryption is.
- We have also planned to download the website files from source through various tools and try to crack security algorithm by getting the original encryption algorithm source code.

5.3 TESTING METHODS :-

- We have performed Dos and DDos attack form 2 different system which has 55 mbps of download and 40 mbps of upload speed.

- We also performed cryptanalysis attack , we pasted the cipher text on various websitebs and various tools that are downloaded by us from github that does cryptanalis and no website or no tool was successful to find the encryption cipher as well as the original message.

5.4 TEST CASES (Purpose, Required output, Expected Result)

No.	Test Cases	Expected output	Actual output
1	User click " Encrypt " to encrypt the message using the key.	Message is encrypted.	As expected.
2	Encrypted message obtainable.	Encrypted message is obtained.	As expected.
3	User click " Decrypt " to encrypt the message using the key.	Message is decrypted.	As expected.
4	Decrypted message obtainable.	Decrypted message is obtained.	As expected.

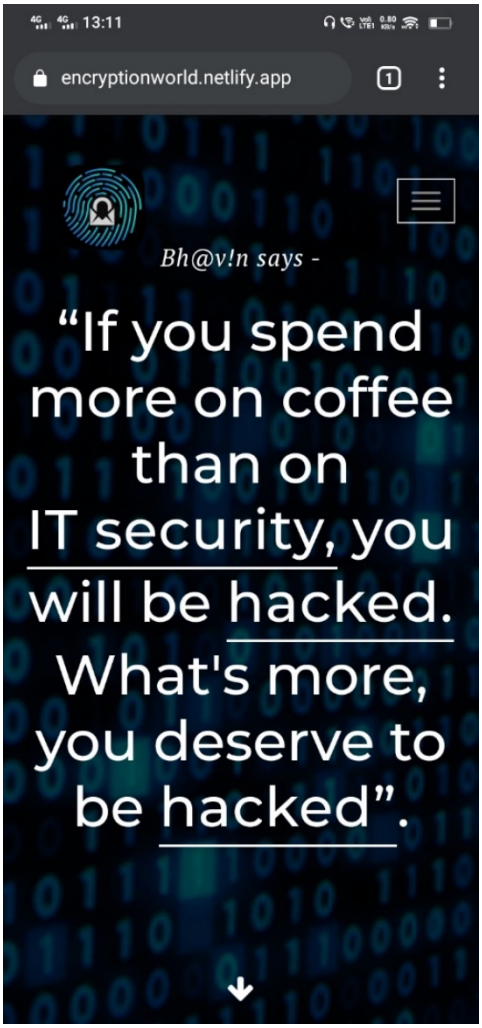
Website that encrypts and decrypts string

CHAPTER - 6

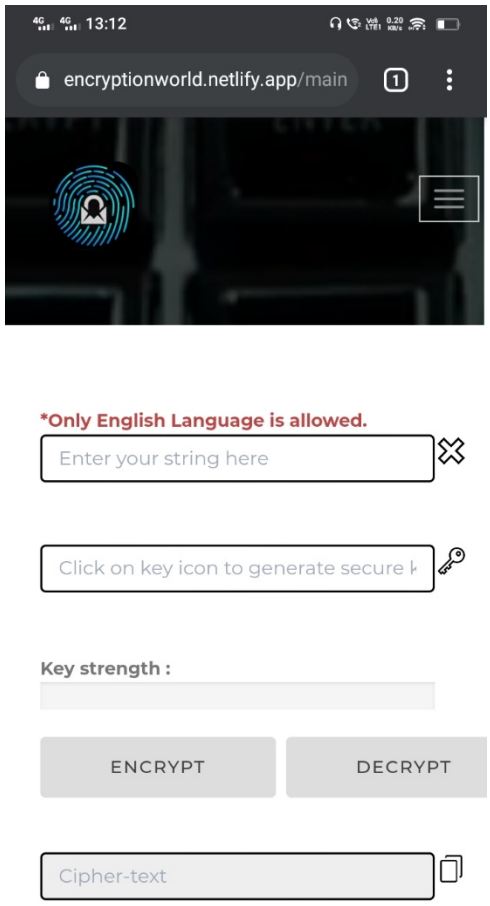
SCREEN SHOTS AND USER MANUAL

• SCREEN SHOTS :-

MOBILE MODE :-



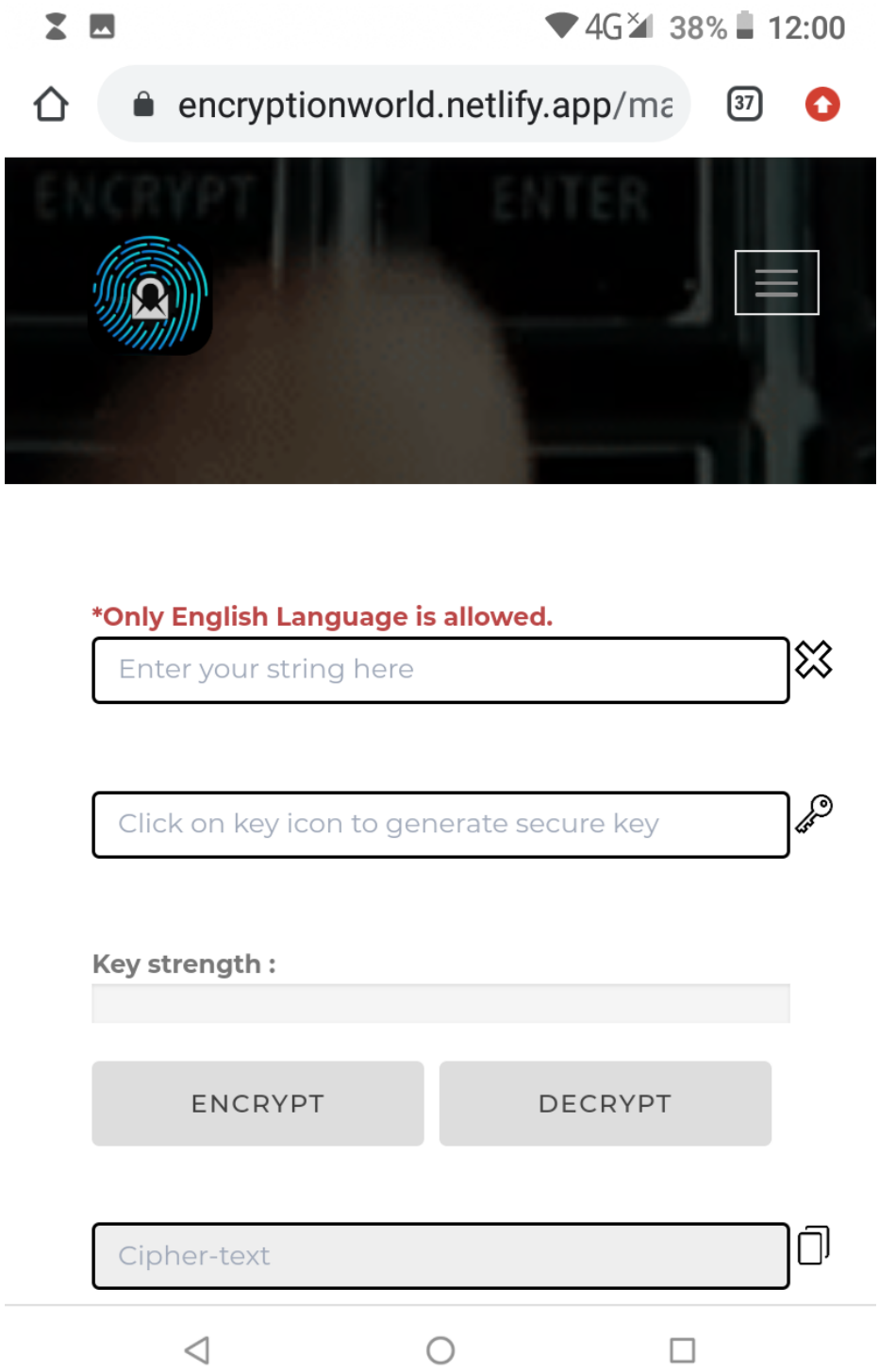
Website that encrypts and decrypts string



Website that encrypts and decrypts string

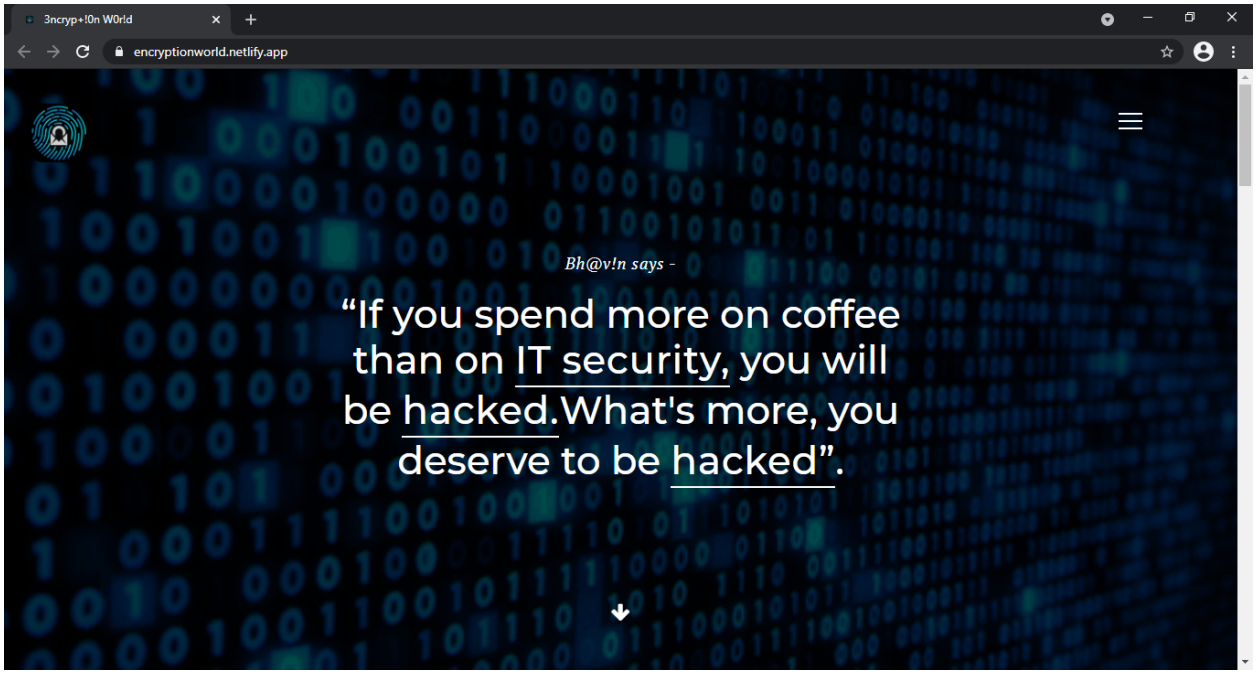
- **TABLET MODE :-**

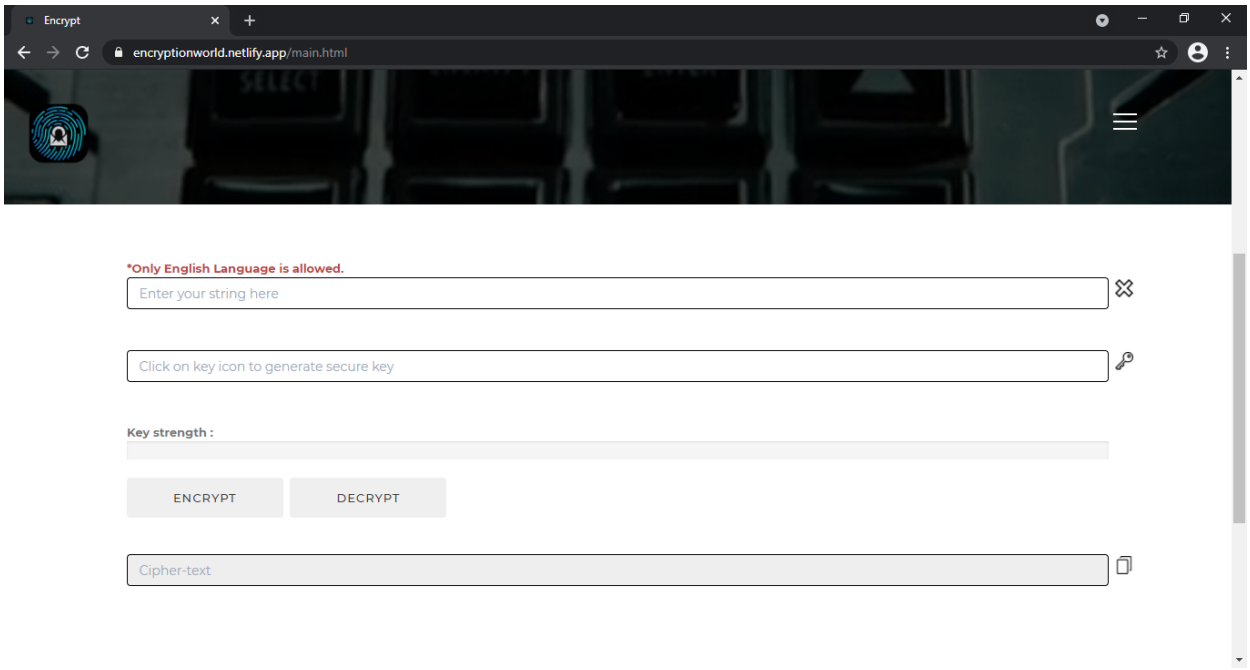
Website that encrypts and decrypts string



Website that encrypts and decrypts string

- **DESKTOP MODE :-**





• USER MANUAL :-

Step 1:- Go to index.html file.

Step 2:- Click on menu button.

Step 3:- Select cryptography. To encrypt and decrypt string.

Step 4:- Enter your string and key, and you can auto generate key using key symbol.

Step 5:- Click on encrypt button to encrypt your string.

Step 6:- Encrypted string shown in below textbox.

Step 7:- Click on copy symbol to copy cipher-text.

Step 8:- Paste this cipher-text in above textbox.

Step 9:- Enter the same key, which you have used to encrypt the string.

Step 10:- Click on decrypt button to decrypt your string. Now we get the original string.

Step 11:- Click on logo for go to main page.

Step 12:- You can also go to encryption page using click on take me to encryption button.

Step 13:- Give feedback on contact page.

CHAPTER - 7

LIMITATIONS AND FUTURE ENHANCEMMENT

- **LIMITATIONS :-**

  - Encryption does not make your data secure. Not using encryption, however, means that any data in transit is as easy to read as the contents of a postcard, sentin regular mail. Encryption at least ensures that anyone who does read your messages has worked hard at it.

- **FUTURE ENHANCEMENT :-**

  - The system can be easily modified to accept any encryption algorithm which would be framed in future. Moreover, currently concentration on the next workwhich adopts Parallelism through multiprocessor system where various encryption algorithms can run in parallel environment which enhances the performance and speed of Encryption/Decryption process.

CHAPTER – 8

CONCLUSION AND DISCUSSION

• CONCLUSION :-

- Information encryption and decryption systems are used to improve information securityto secure information that, thereby providing enhanced level of assurance such that the information that are encrypted cannot be viewed by unauthorized parties in the event of theft, loss or interception

- As we toward a society where automated information resources are increased andcryptography will continue to increase in importance as a security mechanism.

- The information security can be easily achieved by using Cryptography technique.

• DISCUSSION :-

- A cipher is an algorithm for performing encryption or decryption -a siries of well-definedsteps that can be followed as a procedure. An alternative, less common term is encipherment. To encipher or encode is to convert information into encrypted form.