Cryptography Techniques Encryption and Decryption

Akash G Gaikwad
Student, MCA Department,
MGM's Jawaharlal Nehru Engineering College Aurangabad
akashgaikwad4260@gmail.com

Arundhati A Dudhgaonkar
Assistant Professor,
MCA Department, MGM's Jawaharlal Nehru Engineering College Aurangabad
dudhgaonkar.arundhati@gmail.com

Abstract- Cryptography is used to secure and protect information throughout communication. Encryption is a method that transforms the initial data into associate degree unidentifiable kind. decoding could be a method of changing encoded/encrypted information during a kind that's legible and understood by a person's or a laptop. Secret writing and decoding algorithmic rule's security depends on the algorithm whereas the interior structure of the rigor of arithmetic, it additionally depends on the key confidentiality.

1. INTRODUCTION

Secret writing methodology helps you to safeguard your confidential information like passwords and login id. Public, Private, Pre-Shared and satellite square measure necessary keys employed in cryptography. An worker square measure causing essential documents to his/her manager is associate degree example of associate degree secret writing methodology. Cryptography is used to secure and protect information throughout communication. Encryption is a method that transforms the initial data into associate degree unidentifiable kind. decoding could be a method of changing encoded/encrypted information during a kind that's legible and understood by a person's or a laptop. Secret writing and decoding algorithmic rule's security depends on the algorithm whereas the interior structure of the rigor of arithmetic, it additionally depends on the key confidentiality. The manager is receiving the essential encrypted documents from his/her worker associate degreed decrypting it's an example of a decoding methodology. Key within the secret writing algorithmic rule incorporates a crucial position, once the key was leaked, it means anyone will be within the secret writing system to inscribe and decode info, it means that the secret writing algorithmic rule is useless. Therefore, what quite information you select to be a key, a way to distribute the personal key, and the way to save lots of each information transmission keys square

measure important problems within the secret writing and decoding algorithmic rule. This paper planned associate degree implementation of a whole and sensible RSA encrypt/decrypt resolution supported the study of RSA public key algorithmic rule. Additionally, the inscribe procedure and code implementation is provided in details.

2. LITERATURE REVIEW:

2.1 IN paper

Cryptography is the ability of encryption methods where the "original text" (plaintext) is encrypted using an encryption key into "random text that is difficult to read" (cipher text) by somebody who doesn't have a decryption key decoding using the decryption key can recover the original information. The original of retrieving the first manuscript by somebody who doesn't have the decoding key for a brief time is extremely tiny. The encoding technique utilized in classical cryptography is isosceles encryption, wherever the decryption key is identical because the secret writing key. For public key cryptography, uneven secret writing techniques square measure required wherever the decoding secret's not identical because the secret writing key. Encryption, decryption, and key generation for uneven secret writing techniques need additional intensive computation than isosceles secret writing as a result of uneven secret writing uses immense numbers.

2.2 IN paper2

Encryption is that the method of scrambling a message so that only the intended recipient will read it. Encoding encryption a means of securing info. As a lot of and a lot of information is hold on computers or communicated via computers, the necessity to insure that this info is invulnerable to snooping and/or change of state becomes a lot of relevant. With the quick progression of digital information exchange in electronic manner, info Security is changing into way more important in information storage and evolution of human intelligence, the art of cryptography has become a lot of complicated so as to form info a lot of secure. Arrays of coding systems square measure being deployed in the world of data Systems by varied organizations. In this paper, a survey of varied coding Algorithms is presented.

3. MEATHODOLOGY

- **Encryption Algorithms**
  3.1 Rivest-Shamir-Adleman (RSA)
  3.2 Data Encryption Standard (DES)
  3.3 Advanced Encryption Standard(AES)
  3.4 Triple DES (3DES)
  3.5 Blowfish
  3.6 Twofish

3.1 Rivest-Shamir-Adleman (RSA)

RSA (Rivest–Shamir–Adleman) may be a public-key cryptosystem that's wide used for secure information transmission. it's additionally one amongst the oldest. The form RSA comes from the surnames of West Chadic Rivest, Adi Shamir, and Elmore John Leonard Adleman, UN agency in public delineated the algorithmic rule in 1977. identical system was developed on the QT, in 1973 at GCHQ (the British SIGINT agency), by English scientist Clifford Cocks. That system was unclassified in 1997.

In a public-key cryptosystem, the secret writing key's public and distinct from the cryptography key, that is unbroken secret (private). associate degree RSA user creates and publishes a public key supported 2 giant prime numbers, in conjunction with associate degree auxiliary price. The prime numbers area unit unbroken secret. Messages may be transmission. Info Confidentiality features a distinguished significance within the study of ethics, law and last in info Systems. With the

The security of RSA relies on the practical difficulty of factoring the product of two large prime numbers, the "factoring problem". Breaking RSA encryption is known as the RSA problem. Whether it is as difficult as the factoring problem is an open question.[3] There are no published methods to defeat the system if a large enough key is used.

RSA is a relatively slow algorithm. Because of this, it is not commonly used to directly encrypt user data. More often, RSA is used to transmit shared keys for symmetric key cryptography, which are then used for bulk encryption-decryption.

3.1.1 Key distribution

Suppose that Bob wants to send information to Alice. If they decide to use RSA, Bob must know Alice's public key to encrypt the message and Alice must use her private key to decrypt the message.

To enable Bob to send his encrypted messages, Alice transmits her public key (n, e) to Bob via a reliable, but not necessarily secret, route. Alice's private key (d) is never distributed.

3.1.2 Encryption

After Bob obtains Alice's public key, he can send a message M to Alice.

To do it, he first turns M (strictly speaking, the un-padded plaintext) into an integer m (strictly speaking, the padded plaintext), such that $0 \leq m < n$ by using an agreed-upon reversible protocol known as a padding scheme. He then computes the ciphertext c, using Alice's public key e, corresponding to.

This can be done reasonably quickly, even for very large numbers, using modular exponentiation. Bob then transmits c to Alice.

encrypted by anyone, via the public key, but can only be decoded by someone who knows the prime numbers.

Given m, she can recover the original message M by reversing the padding scheme.

3.1.3 Decryption

Alice can recover m from c by using her private key exponent d by computing

5. into two 32-bit blocks, called *left* and *right*, respectively. The initial values of the left and right blocks are denoted L_0 and R_0.

6. There are then 16 rounds of operation on the L and R blocks. During each iteration (where n ranges from 1 to 16), the following formulae apply:

$$L_n = R_{n-1}$$
$$R_n = L_{n-1} \oplus f(R_{n-1},K_n)$$

At any given step in the process, then, the new L block value is merely taken from the prior R block value. The new R block is calculated by taking the bit-by-bit exclusive-OR (XOR) of the prior L block with the results of applying the DES cipher function, *f*, to the prior R block and K_n. (K_n is a 48-bit value derived from the 64-bit DES key. Each round uses a different 48 bits according to the standard's Key Schedule algorithm.)

The cipher function, f, combines the 32-bit R block value and the 48-bit subkey in the following way. First, the 32 bits in the R block are expanded to 48 bits by an expansion function (E); the extra 16 bits are found by repeating the bits in 16 predefined positions. The 48-bit expanded R-block is then ORed with the 48-bit subkey. The result is a 48-bit value that is then divided into eight 6-bit blocks. These are fed as input into 8 selection (S) boxes, denoted $S_1,...,S_8$. Each 6-bit input yields a 4-bit output using a table lookup based on the 64 possible inputs; this results in a 32-bit output from the S-box. The 32 bits are then rearranged by a permutation function (P), producing the results from the cipher function.

1. are moved to the 58th, 50th, and 42nd position, respectively.

2. The 64-bit permuted input is divided

7. The results from the final DES round — i.e., L_{16} and R_{16} — are recombined into a 64-bit value and fed into an inverse initial permutation (IP^{-1}). At this step, the bits are rearranged into their original positions, so that the 58th, 50th, and 42nd bits, for example, are moved back into the 1st, 2nd, and 3rd positions, respectively. The output from IP^{-1} is the 64-bit ciphertext block.

Consider this example using DES in CBC mode with the following 56-bit key and input:

Key: **1100101 0100100 1001001 0011101 0110101 0101011 1101100 0011010 = 0x6424491D352B6C1A**

3.2 DES Operational Overview

Data Encryption Standard (DES) is a block cipher algorithm that takes plain text in blocks of 64 bits and converts them to ciphertext using keys of 48 bits. It is a symmetric key algorithm, which means that the same key is used for encrypting and decrypting data.

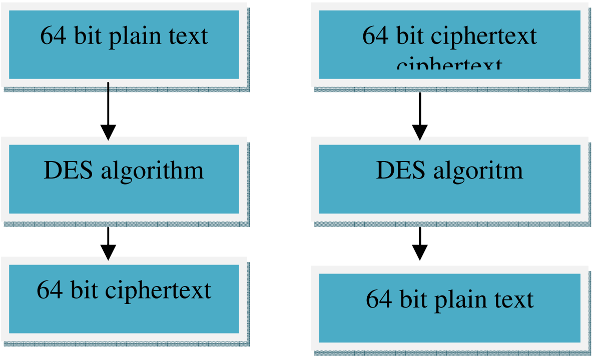


Fig. Encryption and Decryption using the DES algorithm

DES then acts on 64-bit blocks of the plaintext, invoking 16 rounds of permutations, swaps, and substitutes, as shown in Figure 8. The standard includes tables describing all of the selection, permutation, and expansion operations mentioned below; these aspects of the algorithm are not secrets.

3.3 The Advanced Encryption Standard (AES)

AES or Advanced Encryption Standard is a cipher, i.e., a method for encrypting and decrypting information. Whenever you transmit files over secure file transfer protocols like HTTPS, FTPS, SFTP, WebDAVS, OFTP, or AS2, there's a good chance your data will be encrypted by some flavor of AES ciphers - either AES 256, 192, or 128. We'll discuss more about these AES encryptions shortly.

Different secure managed file transfer software may be equipped with varying selections of encryption algorithms. Some ciphers may be included in certain selections but absent in others. Not AES. AES will almost certainly be present in all but a few. Why is this so? It all started when the US government began looking for a new encryption algorithm that would be used to protect sensitive data.

secure file transfer protocols like FTPS, HTTPS, SFTP, AS2, WebDAVS, and OFTP. But what exactly is its role?

Because symmetric and asymmetric encryption algorithms each have their own strengths, modern secure file transfer protocols normally use a combination of the two. Asymmetric key ciphers a.k.a. public key encryption algorithms are great for key distribution and hence are used to encrypt the session key used for symmetric encryption.

Symmetric key ciphers like AES, on the other hand, are more suitable for encrypting the actual data (and commands) because they require less resources and are also much faster than asymmetric ciphers. The article Symmetric vs Asymmetric Encryption has a more thorough discussion regarding these two groups of ciphers.

Here's a simplified diagram illustrating the encryption process during a typical secure file transfer secured by SSL/TLS (e.g. HTTPS, FTPS, WebDAVS) or SSH (e.g. SFTP). AES encryption operates in step 3.

3.4 Triple DES (3DES)

In cryptography, **Triple DES** (**3DES** or **TDES**), officially the **Triple Data Encryption Algorithm** (**TDEA** or **Triple DEA**), is a symmetric-key block cipher, which applies

3.5 Twofish

In cryptography, **Twofish** is a symmetric key block cipher with a block size of 128 bits and key sizes up to 256 bits. It was one of the five finalists of the Advanced Encryption Standard contest, but it was not selected for standardization. Twofish is related to the earlier block cipher Blowfish.

A. How is the AES encryption algorithm used in secure file transfers?

As mentioned earlier, AES is implemented in

the DES cipher algorithm three times to each data block. The Data Encryption Standard's (DES) 56-bit key is no longer considered adequate in the face of modern cryptanalytic techniques and supercomputing power. However, an adapted version of DES, Triple DES (3DES), uses the same algorithm to produce a more secure encryption.

While the government and industry standards abbreviate the algorithm's name as TDES (Triple DES) and TDEA (Triple Data Encryption Algorithm),[1] RFC 1851 referred to it as 3DES from the time it first promulgated the idea, and this namesake has since come into wide use by most vendors, users, and cryptographers.

3.5 Blowfish

Blowfish is a symmetric-key block cipher, designed in 1993 by Bruce Schneier and included in many cipher suites and encryption products. Blowfish provides a good encryption rate in software and no effective cryptanalysis of it has been found to date. However, the Advanced Encryption Standard (AES) now receives more attention, and Schneier recommends Twofish for modern applications.

Schneier designed Blowfish as a general-purpose algorithm, intended as an alternative to the aging DES and free of the problems and constraints associated with other algorithms. At the time Blowfish was released, many other designs were proprietary, encumbered by patents or were commercial or government secrets. Schneier has stated that, "Blowfish is unpatented, and will remain so in all countries. The algorithm is hereby placed in the public domain, and can be freely used by anyone."

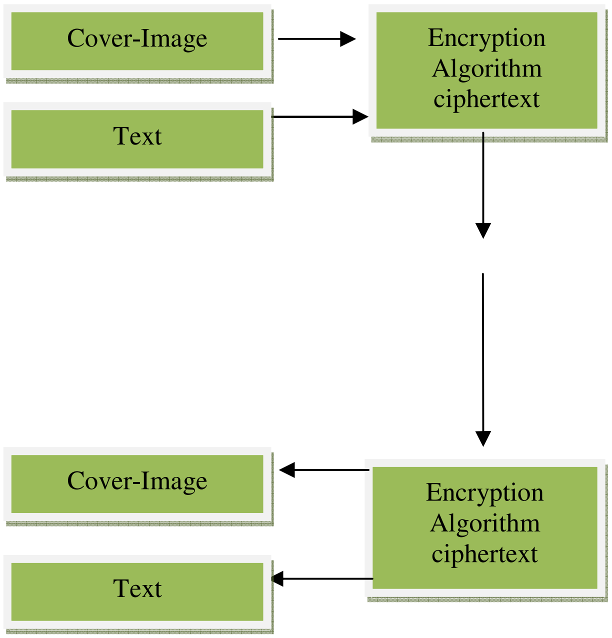
Twofish's distinctive features are the use of pre-computed key-dependent S-boxes, and a relatively complex key schedule. One half of an n-bit key is used as the actual encryption key and the other half of the n-bit key is used to modify the encryption algorithm (key-dependent S-boxes). Twofish borrows some elements from other designs; for example, the pseudo-Hadamardtransform (PHT) from the SAFER family of ciphers. Twofish has a Feistel structure like DES. Twofish also employs a Maximum Distance Separable.

3.7 Steganography

Steganography comprises of the two terms that is the message and the cover picture in which the information is to be hided . Message is the secret data and the cover image act as the carrier for hiding the data. Together the cover media and the embedded message creates a stego-carrier. For example , when a crucial data(secret message) is hidden within a cover image, the resulting product is the stego-image.

The possible formula of the process is represented asCover media + embedded message + stego key = stego-medium

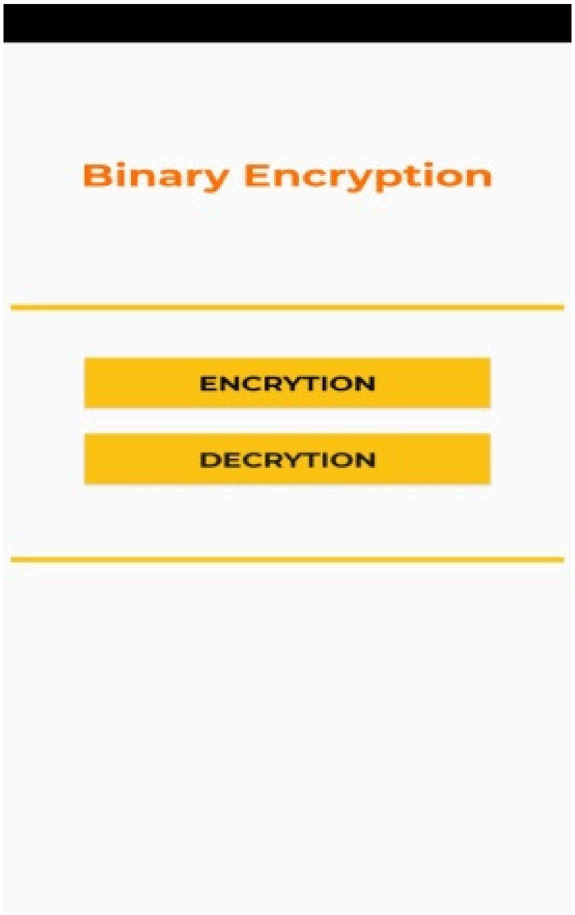
Notable features of the design include key-dependent S-boxes and a highly complex key schedule.

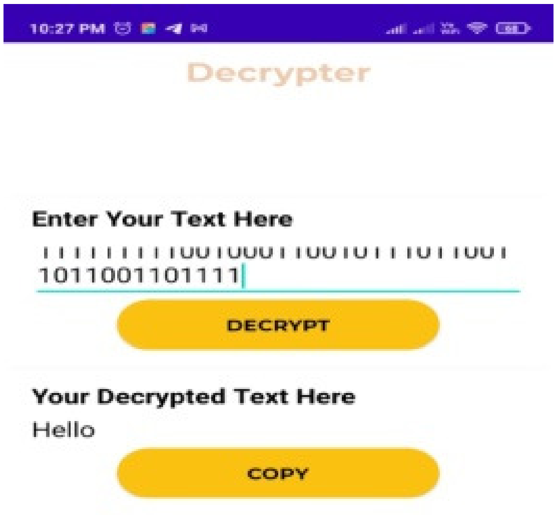

Cover-Image
Text
Encryption Algorithm ciphertext
Cover-Image
Text
Encryption Algorithm ciphertext

ISSN: 0017-2294

Fig: Stego-image

User Side



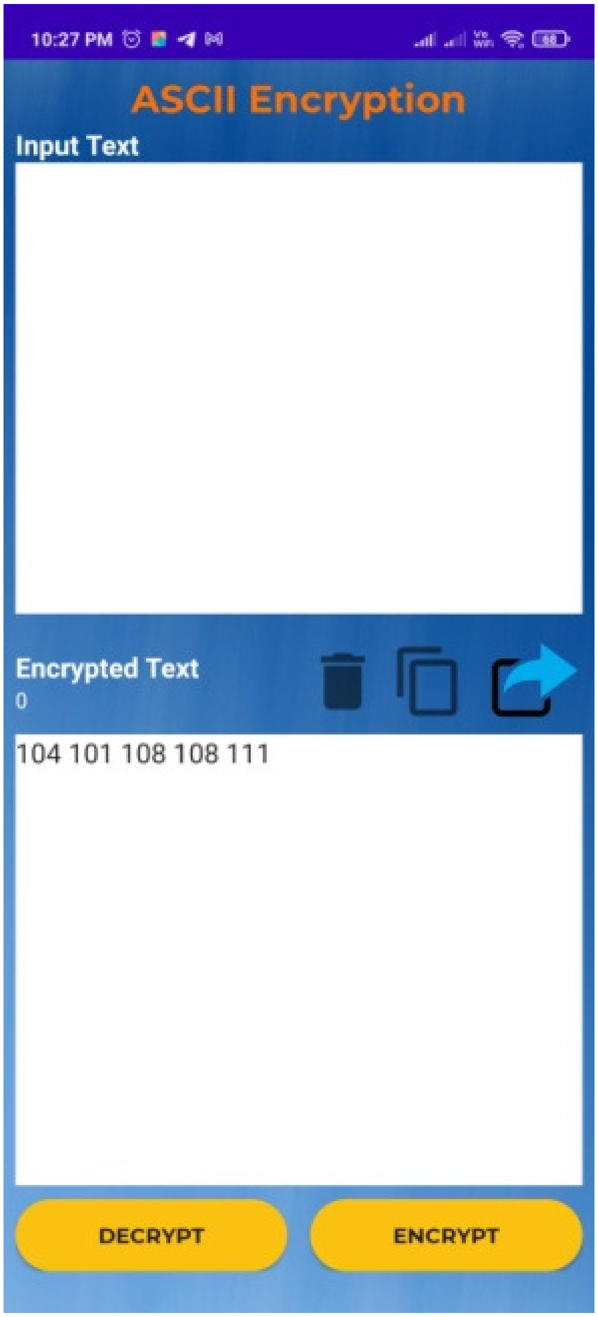


Enter Your Text Here

1111111110010001100101111011001
1011001101111

Your Decrypted Text Here

Hello

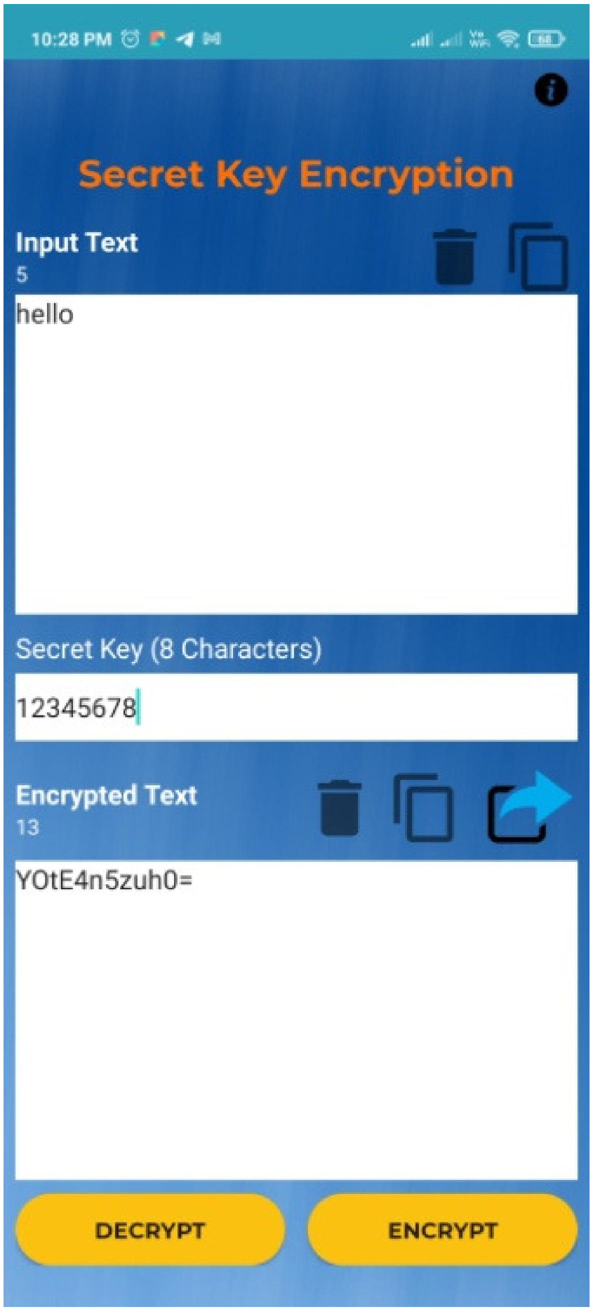


ASCII Encryption

Input Text

Encrypted Text
0

104 101 108 108 111



Secret Key Encryption

Input Text
5

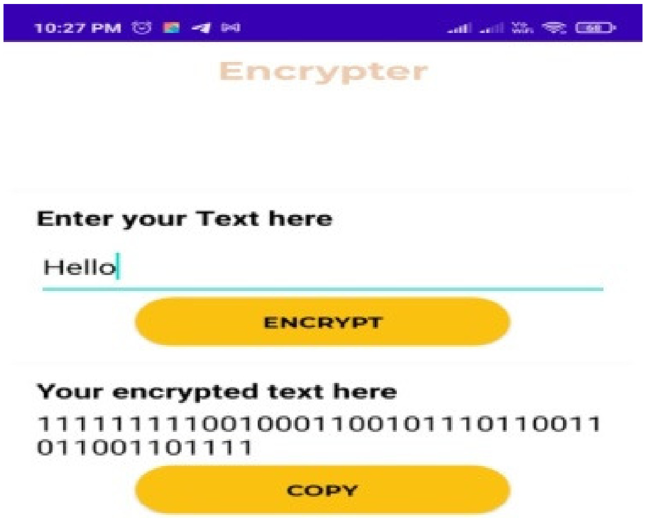
hello

Secret Key (8 Characters)

12345678

Encrypted Text
13

YOtE4n5zuh0=

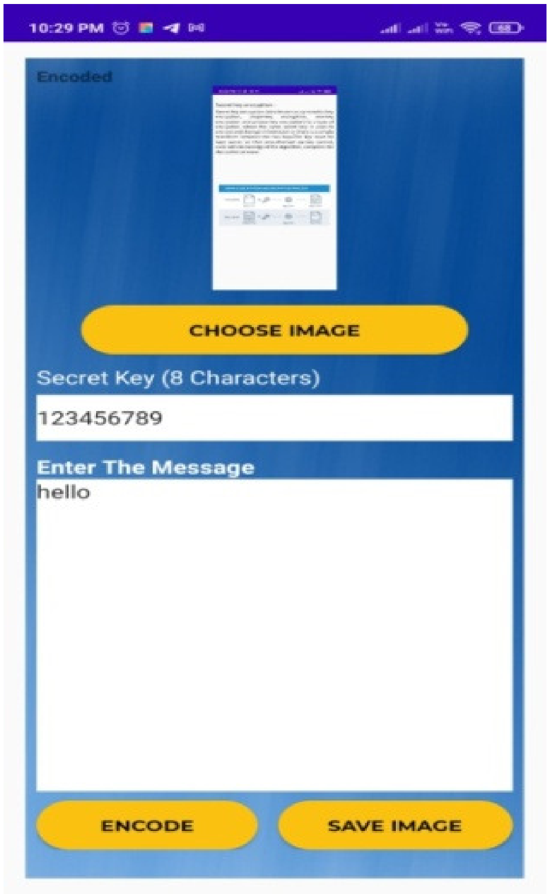


Enter your Text here

Hello

Your encrypted text here

1111111110010001100101110110011
011001101111

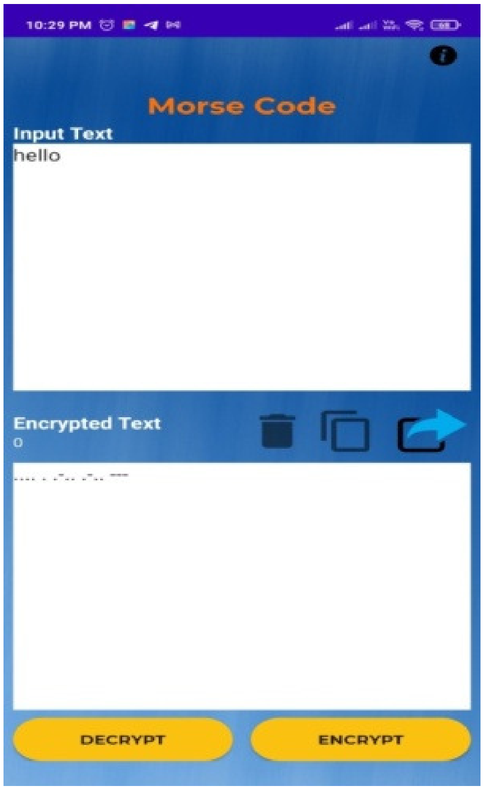


Secret Key (8 Characters)

123456789

Enter The Message

hello



Input Text

hello

Encrypted Text

0

.... . .-.. .-.. ---

5.CONCLUSION

This paper describes the short survey on steganography , Binary encryption, secret key encryption . Different techniques for image, text steganography are also explained in it. These techniques are very helpful for detecting the stego- images and the image media relating to the security of the information. Binary encryption is helpful to text encryption. The proposed method is used for message communication. Short message can be send securely using encryption techniques.

6. REFERENCE

1] Dr. Fadhil Salman Abed ―A Proposed Method of Information Hiding Based on Hybrid Cryptography and Steganography‖, IJAIEM, Volume 2, Issue 4, April 2013

2] William "Cryptography and Network Security Principles and Practice", Fifth Edition, Pearson Education, Prentice Hall, 2011.

3] Schneier B, "Applied Cryptography", John Wiley& Sons Publication, New York, 1994.

4] Bobade S and Goudar R 2015 Secure Data Communication Using Protocol Steganography in IPv6 IEEE 2015 International Conference on Computing Communication Control and Automaton.