SECURE MESSENGER ANDROID APP

Project report submitted in partial fulfillment of the requirement for the degree of Bachelor of Technology

in

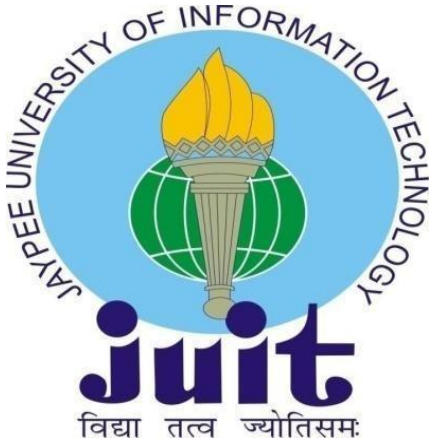
Computer Science and Engineering

By

VISHNU (181385)

Under the supervision of

DR. SHUBHAM GOEL



Department of Computer Science & Engineering and Information Technology

Jaypee University of Information Technology Waknaghat, Solan-173234, Himachal Pradesh

Table of Content

Certificate

Candidate's Declaration

I hereby declare that the work presented in this report entitled **"SECURE MESSENGER ANDROID APPLICATION"** in partial fulfillment of the requirements for the award of the degree of **Bachelor of Technology in Computer Science & Engineering and Information Technology** submitted in the department of Computer Science & Engineering and Information Technology**,** Jaypee University of Information Technology Waknaghat is an authentic record of my own work carried out over a period from January 2022 to May 2022 under the supervision of **(DR. SHUBHAM GOEL(PROFESSOR OF ,Computer Science & Engineering).**The matter embodied in the report has not been submitted for the award of any degree or diploma.

(Student Signature)

VISHNU KUMAR
(181385)

This is to certify that the above statement made by the candidate is true to the best of my knowledge.

Supervisor Signature:
DR SHUBHAM GOEL
Department of Computer Science & Engineering
Jaypee University of Information Technology

ACKNOWLEDGEMENT

First and foremost, I offer my heartfelt gratitude to almighty God for His heavenly grace, which has enabled me to successfully finish the project work.

I am extremely grateful and like to express my deep gratitude to Supervisor Dr. Mrityunjay Singh**,** Designation, Department of CSE Jaypee University of Information Technology, Wagnaghat & keen interest of my supervisor in the field of **cryptography** to carry out this project. His never-ending patience, intellectual direction, persistent encouragement, constant and energetic supervision, constructive criticism, helpful suggestions, and reading numerous poor versions and revising them at all stages allowed this project to be completed.

I'd like to thank **Dr. SHUBHAM GOEL** of the Department of CSE for his invaluable assistance in completing my project.

I'd also like to convey my gratitude to everyone who has backed me in making this project a success, whether directly or indirectly. In this unique situation, I might want to thank the various staff individuals, both educating and non-instructing, which have developed their convenient help and facilitated my undertaking.

Finally, I must acknowledge with due respect the constant support and patients of my parents.

Vishnu kumar 181385

ABSTRACT

Android revolutionized the smartphone industry. Thanks to an open model backed by Google, there are many options to embrace and take use of the prospects given by smartphones. Exiting the smartphone app market was also helpful to end users since, while most apps achieved their goals without violating users' privacy, an open and popular platform like Android served as a perfect location to employ and propagate security

assaults.

We've created a request for safe communication between two or more persons with strong security to avoid the inconvenience of chats and communication in the Android app.

When encrypting and segregating data with a secret key, our application provides data connection protection using various cryptography algorithms, where transmission is done in two ways. If the file / data is public, a file is selected and delivered to a specific recipient; if the file / data is confidential, a password verification key is requested and sent to the receiver, resulting in a safe transfer of information (file / data).

CHAPTER 1: INTRODUCTION

1.1 Introduction:-

When information is being shared in a secure manner, they really do not want each other to recognize what they're communicating. Organizations must converse in such a way that they are unable to listen or just become dissatisfied in order to accomplish this. Apart from face-to-face conversation without the possibility of listening in, no interaction can be considered to be safeguarded in this fashion, despite technical constraints such as law, economics, performance difficulties (login and encrypting), and multicast transmission aimed at minimizing surveillance.

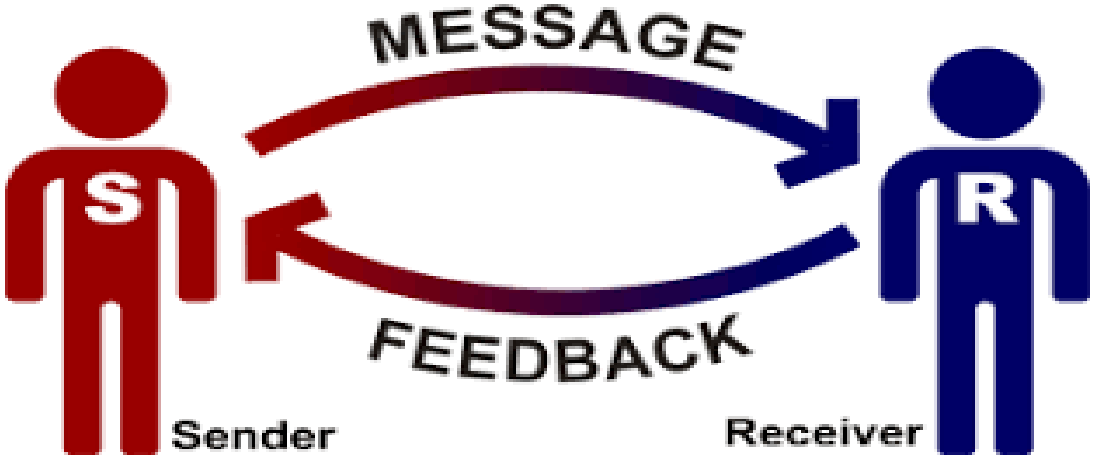


fig 1.communication between two people

Technology and its adaptability are at the core of this argument as more communication takes place in remote places and electronic interventions, as well as greater awareness

regarding the significance of cross-cutting concerns. As a result, the focus of this article is mediated or practically included.

Types of security

The following headings can be used to characterize security in general, with illustrations:

● Protecting a communication's substance or character.

Code - the law of converting a piece of information (for example, a letter, word, phrase, or touch) into another type or representation (one symbol into another symbol), not the same type. In communication and Information processing, coding is the process by which information from a source is converted into symbols to be transmitted. Coding is a reversible process, turning these code symbols back into the recipient's comprehensible information. Another reason for coding is to facilitate communication in areas where common spoken or written language is difficult or impossible. For example, semaphore, where the configuration of flag-held flags or arms of the semaphore tower includes parts of a message, usually single letters and numbers. Someone standing at a distance can interpret flags and generate sent words.

1. Ambiguity
2. Cryptographic
3. Asymmetric encryption
4. Identifiable

Keeping the characteristics of the parties involved in a transmission hidden - restricting detection and fostering concealment .

fig 2. shows secure communication

"Audiences" and other forms of anonymous grouping – When information originates from a "community," it's difficult to know who said what. ○ Unregistered cell phones and Internet cafes are examples of anonymous cellular networks.

Proxies that are anonymous

Routing methods that are difficult to trace – such as relays or unapproved third-party systems Keeping the fact that a conversation is taking place a secret

"Security by obscurity" – similar to needle in a haystack

Random traffic – To make the existence of genuine communication considerably more difficult and dynamic routing less precise, random data flow is created.

1.2 PROBLEM STATEMENT:-

Our project's objectives are as follows:-

1.build the good interface for communication

2.most of the communication is done through smartphones so it is a good application.

fig 3 shows encryption

3.secure communication between different peoples across the android platform.

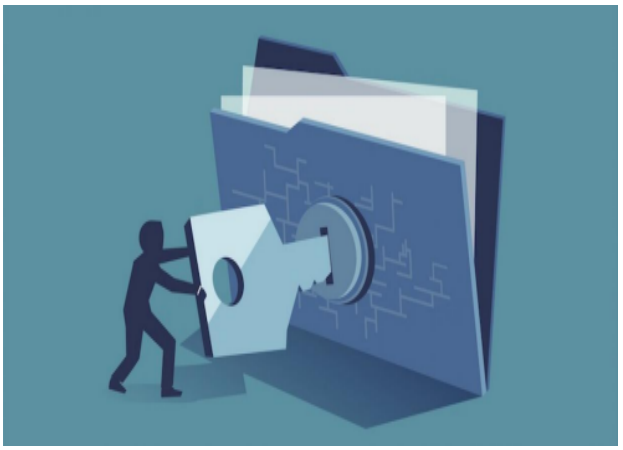


fig 4. Shows decryption

5. Users must have the option and the way to encrypt the data and also has the way to decrypt the text or data. 6. The most private way to connect with others is in person, without the use of computers or phones at all. Because this isn't always attainable, end-to-end encryption is the next best option.

1.3 OBJECTIVES:-

The main purpose of this activity is to achieve the safest and best communication between two people communicating in any language or any other form such as file or anything. There must be a mechanism so that no third party or persons can interfere with any form of communication and thus secure communication must be established between the communication persons. It should be very advanced and should end up encrypting based on.only speaking people should be able to decode. People should have the ability to change the level of encryption. They should adjust the level of communication based on what they are talking about.

1.4 METHODOLOGY :- Types and Methods of Encrypting

Asymmetric Encryption

The secret key is disclosed for everyone to use and write messages in public key encryption systems. The encryption key that allows communications to be read is only accessible to the receiving group. In 1973, a confidential document described public key encryption for the first time.

Prior to it, symmetric key encryption was the only option (also called secret key).

Symmetric encryption

Encryption keys and decryption keys are the same in symmetric key configurations. To make a secure connection, both parties must use the same key.

Encryption Algorithms

Triple DES Encryption

The DES Triple algorithm was created to replace the original Data Encryption Standard (DES) algorithm, which hackers have readily cracked. Triple DES was once a recommended standard and the industry's most extensively utilized symmetric algorithm.

DES Triple employs three separate keys, each of which is 56 bits long. Although the overall key length can go to 168 bits, experts believe that 112 bits with the same critical power is sufficient.

Triple DES remains a reliable hardware encryption solution for financial services and other industries, despite its delayed completion.

RSA encryption

RSA is an online data encryption standard and public key encryption method. It's also possible that it's one of the ways used in PGP and GPG packages.

Because it uses a key pair, RSA is classified as an asymmetric encryption algorithm, unlike Triple DES. The message is encrypted with the public key, and the encryption is decrypted with the private key. It takes a long time and a lot of computing power for an attacker to crack this encryption scheme.

Advanced Encryption Levels (AES)

The Advanced Encryption Standard (AES) is a cryptographic method that the US government and a number of other corporations trust. AES encryption uses 192 and 256 bit

keys for heavy-duty encryption, despite the fact that it works extremely well in 128-bit forms.With the exception of brute-force attacks, which seek to decrypt texts using all possible combinations of 128-, 192-, or 256-bit ciphers, AES is regarded to be immune to all attacks. However, security analysts expect that in the private sector, AES will ultimately become the standard for data protection.

Following are some cryptographic algorithms:-

IDEA encryption algorithm

MD5 encryption algorithm

Twofish encryption algorithm

HMAC encryption algorithm

Blowfish encryption algorithm

1.5 LANGUAGE USED:-

1. JAVA for backend coding internal working of the application.

2. XML for designing the layout of the various activities.

1.5 Technical Requirements (Hardware part)

* *To Run :*

Android Based Smartphone / Tablet Based
On or Above Android 4.4+ (KitKat And Above).

* For Development :

intel Core i3 laptop or desktop for testing purpose 4 GB RAM DDR4 (min)

Technical Requirements (Software part)

1. Android studio Software for development environment for a good environment.

2.Android emulator for testing purposes or normal smartphone or tablet for debugging purposes.

3. used a volleyball library to interact with the remote host basically used for connecting local database servers to our android application.

1.6 Deliverables of the Major Project =

1.A secure communication between two people should be established.

2.Provide easy access for the people.

● CHAPTER 2: LITERATURE SURVEY

Today, data security is a critical component of military hardware. It also necessitates prompt action in terms of securely transmitting and receiving statistical information. We will cover how to communicate photographs and data in a safe, effective, and timely manner in this paper. Data is encrypted for secure transmission using Identity-Based Cryptography and Visual Cryptography. This method can be used in MANET, particularly for military monitoring. Because of its simplicity and efficiency, the cryptographic visual approach is an excellent choice for transmitting and receiving images and becoming used to exchanging encrypted images.

To make the system more secure, private and public key pairs are employed in these tactics. A single-channel system with several cellular networks, such as Mobile Ad hoc Network, is represented by the proprietary cryptographic algorithm (MANET).

For system configuration, encoding, and data extraction, identity-based cryptography steps are used. The deceptive and rapid functioning of Indian Ancient Vedic Mathematics to calculate crucial quantities has made it famous. In comparison to modern calculations, Vedic calculations take less time to complete. Modern statistics employ the RSA cryptography approach to generate a public and

private key. The public and private keys are generated using RSA Vedic statistical technology.

2.1 THE RSA ALGORITHM :-

The RSA algorithm was first made public in 1977, and their surnames are derived from the letters RSA (RivestShamirAdleman). The most flexible and extensively used public key algorithm today is RSA, which is an asymmetric key encryption scheme. The inclusion of a long value module to the RSA is required. Upgrades to the public/private key system are made to ensure better data security.

As a result, quick module duplication becomes the key to real-time encryption and decryption, which is necessary for high data throughput [3]. RSA is the most frequently used cryptosystem, with applications in both encryption and digital signatures. It's commonly used to secure e-commerce and e-mail, as well as to run secure, transparent networks that ensure the validity of electronic documents. It is present in many commercially available security products and is utilized on many Web servers and browsers. Indeed, the RSA's widespread use has positioned it at the forefront of modern information security. It is not an exaggeration to suggest that the RSA cryptosystem's security assets are critical to Internet security.

'Veda' is a Sanskrit word that signifies 'knowledge.' The Vedas contain dozens of texts; it is estimated that India has thousands of such texts, many of which have yet to be translated and which are highly ordered both internally and in connection to one another. The 16 sutras of Vedic Mathematics deal with arithmetic, algebra, and geometry. Direct and indirect repetition are terms used to describe the Urdhva Tiryakbhyam style of Vedic repetition.

Sutras help students enhance their math skills in a variety of situations, ensuring both speed and accuracy. Sutras help students enhance their arithmetic skills in a variety of situations, ensuring both speed and precision while relying heavily on logical and logical reasoning. Vedic methods are straightforward, and their simplicity and simplicity are simply astonishing.

● CHAPTER 3: SYSTEM DEVELOPMENT

This chapter discusses the origin of the data set, the collection process, the strengths, and the constraints. In addition, the data set analysis was performed to provide a clear picture of all past data sets available in the form of a table. Finally, the algorithm launch process.

3.1 DESIGN:-

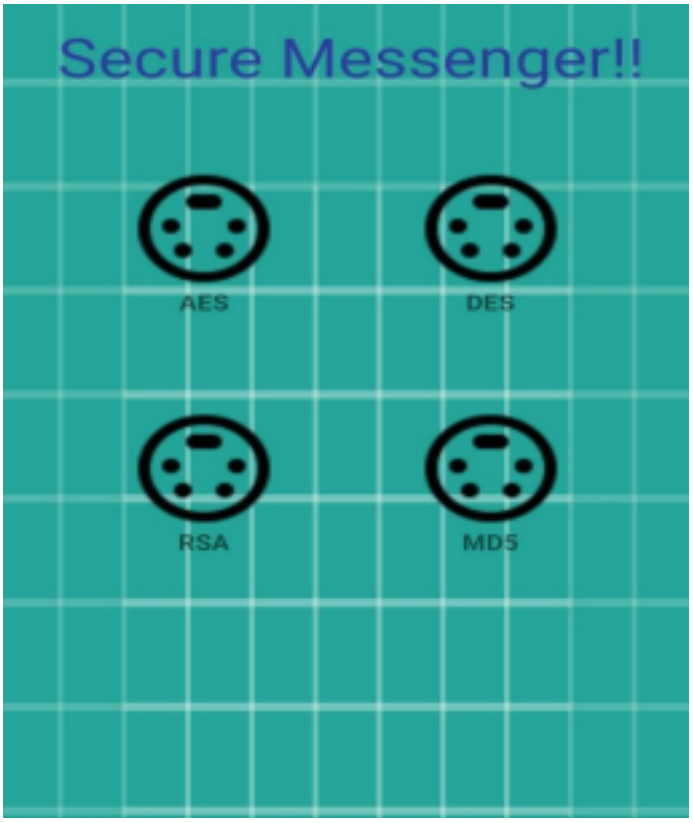


fig 5 show main app ui design of app

We have use four major cryptography algorithms for encryption purpose namely

i. The Advanced **Encryption** Standard (**AES**)

ii. The Data **Encryption** Standard (**DES**)

iii. **RSA** (Rivest–Shamir–Adleman)

iv.The **MD5** message-digest algorithm

then we combined it into our app and implemented in the backend connected all the necessary stuff needed for working.

3.2 Analysis on the Project

Possible research is a thorough examination of all important project aspects, such as economic, technical, legal, and planning issues, in order to establish the feasibility of completing a project effectively. Before investing a lot of time and money into a project, project managers utilize feasibility studies to see what the benefits and drawbacks are. Program managers may not be the ones doing the feasibility study, they can be important guidelines as the project progresses. Project managers can use feasibility studies to understand project boundaries, business objectives and risk factors in play .

.

3.3 Requirements on Major Project SDLC

3.3.1 Functional Requirements

**** To Run :***

1.Android studio software using gradle script
2.Android Based Smartphone / Tablet Based On or Above Android 4.4+ (KitKat And Above) .

*** For Development :**

Laptop or computer having intel Core i3 4 GB RAM DDR4 min

3.3.2 Non-Functional Requirements:

1.Security:- the data is securely communicated to the other people without any third party interference.

Performance:- the application will process the information as fast as possible from the moment the data is inserted .

3.4 ALGORITHM:-

3.4.1 The Advanced Encryption Standard (AES):-

Encryption works by transforming a blank text into a ciphertext, which is composed of seemingly random letters. The encryption can only

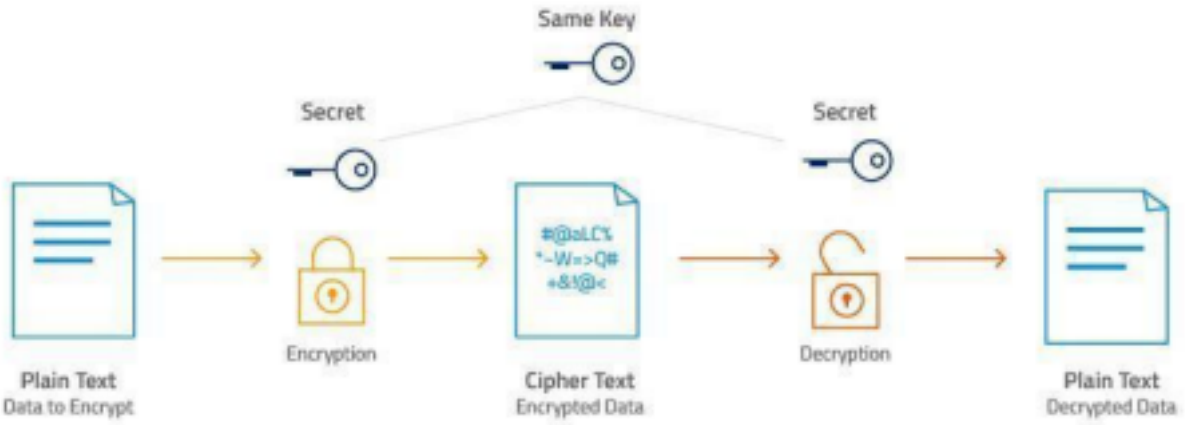


fig 6 shows aes algorithm working

be broken by those who have a specific key. AES employs symmetric key encryption, in which just one secret key is used to cypher and decrypt data.

The AES Encryption algorithm (also known as the Rijndael algorithm) is a block cipher algorithm that uses a 128-bit block size / chunk. The keys 128, 192, and 256 bits are used to convert these individual blocks. They combine these pieces to generate a ciphertext text while encrypting them.

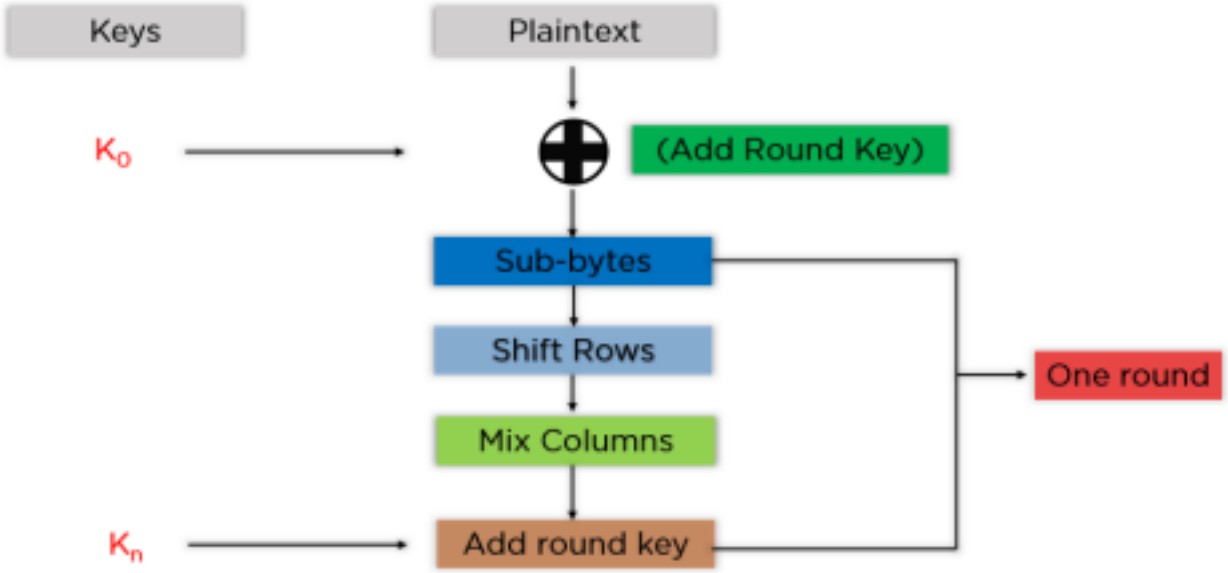
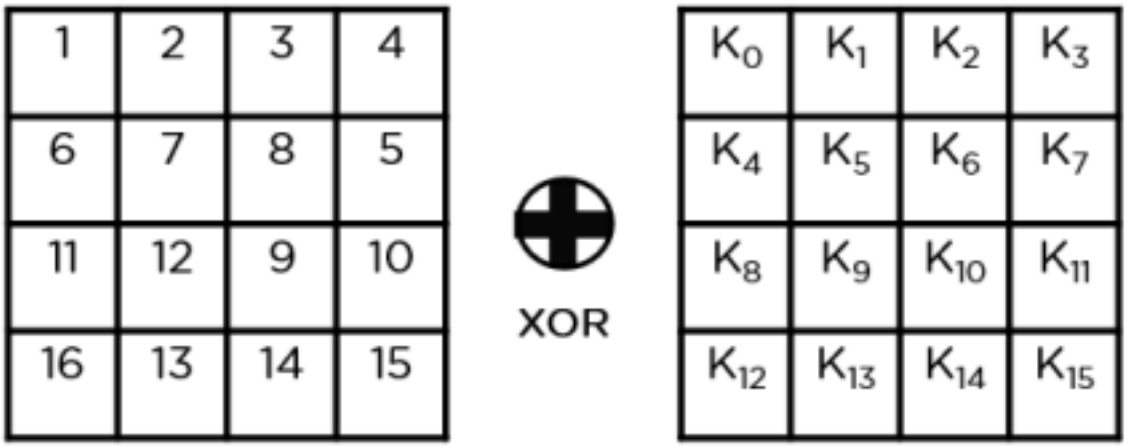


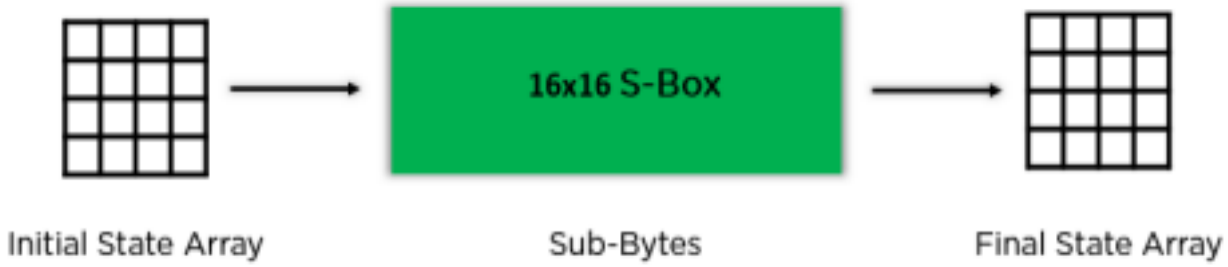
FIG 7. The steps to follow in AES are shown in the graphic below:

The steps listed above should be followed in order in each block. He connects the separate blocks together to make the final secret code after successfully installing them one by one. The procedure is as follows:

Add Rotate Key: Uses the XOR function with the first produced key to transfer blo**cking data held in the state system (K0). Inputs the state outcome system in the next stage.**



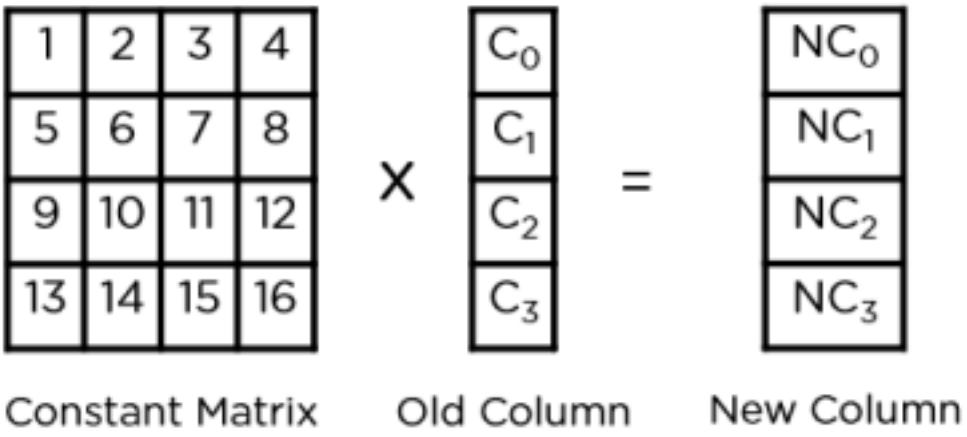
● **Sub-Bytes:** This phase divides each plot of land into two equal portions and turns it to a hexadecimal. These sections are rows and columns that have been mapped with an S-Box to provide new values for the final state system.



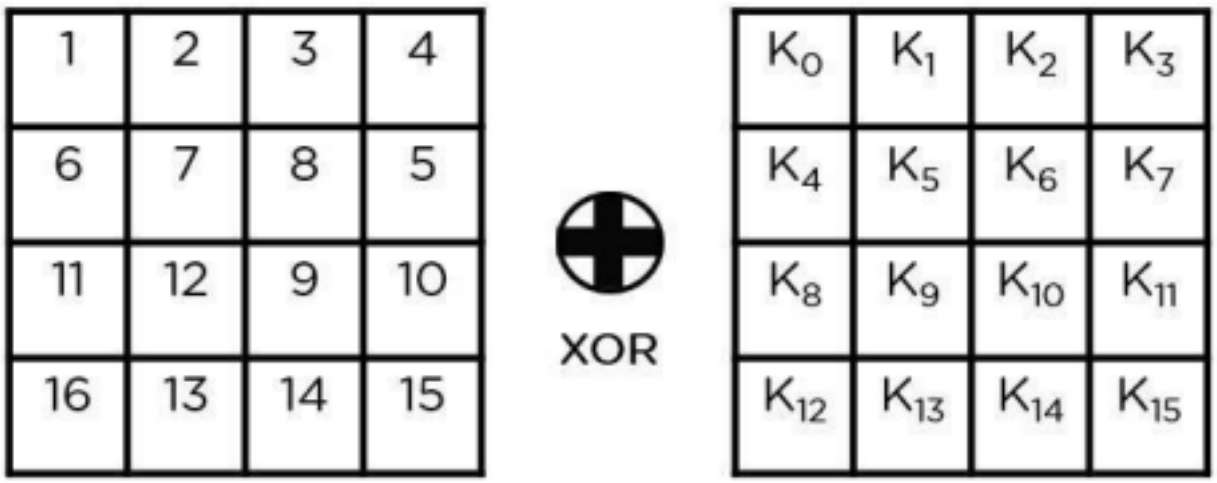
● **Shift Rows:** It swaps the items in the row with one another. The first line should be skipped. The items are moved to the second row, one space to the left. It also moves pieces from the third row to the left in two consecutive positions, as well as the last

three vertical lines.

- **Mix Columns:** For each column in the region system, the unmodified matrix is repeated to produce a new column for the same comparable district members. You'll have your next step plan after you've repeated all of the columns with the same constant matrix. In the final round, this step should be skipped.



Add Round Key: The appropriate round key says XOR'd and state array are located in the previous step. If this is the last cycle, the resulting state system becomes the cipher text of a particular block; if not, it goes as far as the inclusion of a new regional plan for the next round.



Now that you have a basic understanding of the procedures involved in the encryption process, you can follow along with this example

.

Plaintext – Two One Nine Two

T	w	o		O	n	e		N	i	n	e		T	w	o
54	77	6F	20	4F	6E	65	20	43	69	6E	25	20	54	77	6F

Plaintext in Hex Format
54 77 6F 20 4F 6E 65 20 43 69 6E 25 20 54 77 6F

Encryption Key – Thats my Kung Fu

T	h	a	t	s		m	y		K	u	n	g		F	u
54	68	61	74	73	20	6D	79	20	4B	75	6E	67	20	46	75

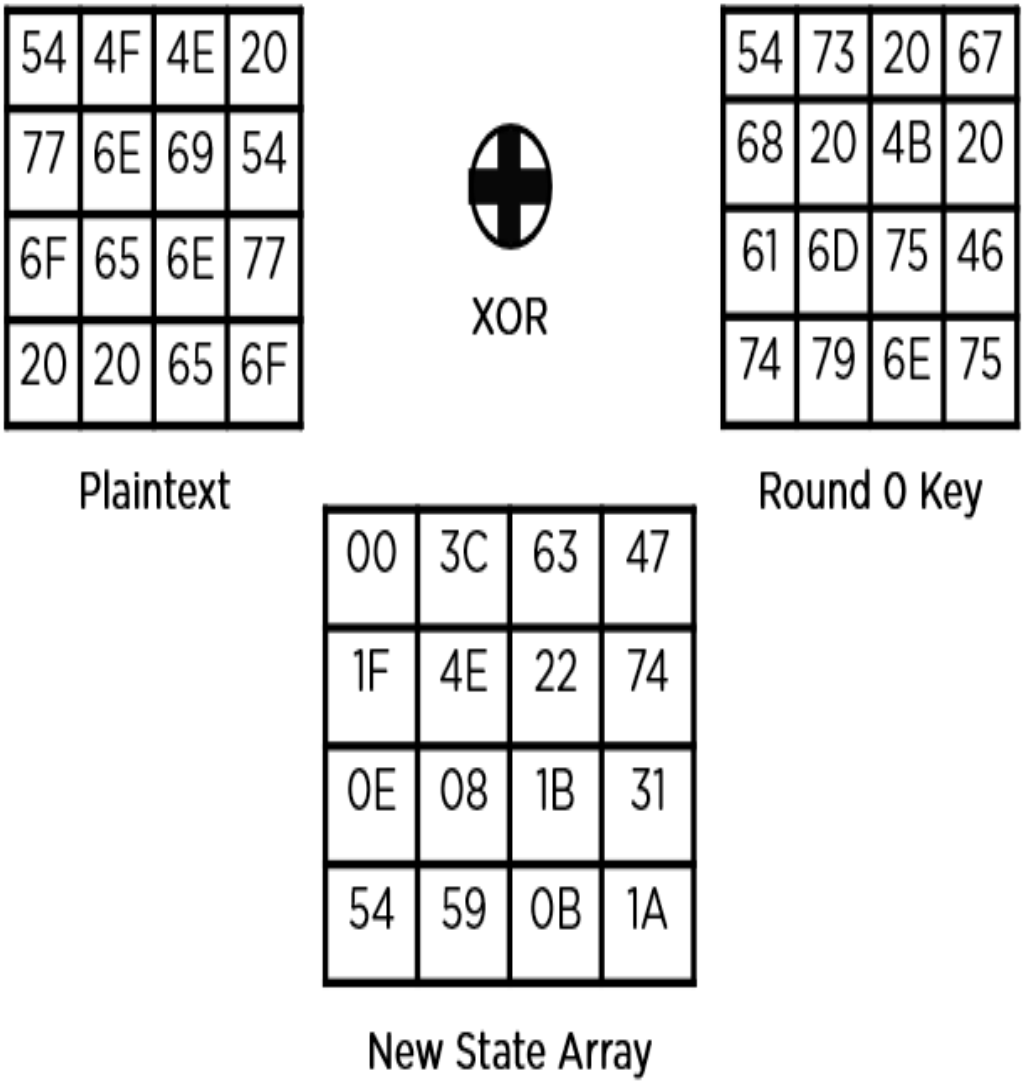
Encryption Key in Hex Format
54 68 61 74 73 20 6D 79 20 4B 75 6E 67 20 46 75

fig 8 plain text conversion

Plain text and encryption transform buttons into hex format before activation, as shown in the image above. As shown below, you should be able to produce the keys for the next ten rounds.

You must repeat the processes outlined above, extracting the state array in order and sending it on as input to the next round. The procedure is as follows:

- Add Round Key:



- **Sub-Bytes: It generates an entirely new state array by passing the items through a 16x16 S-Box.**

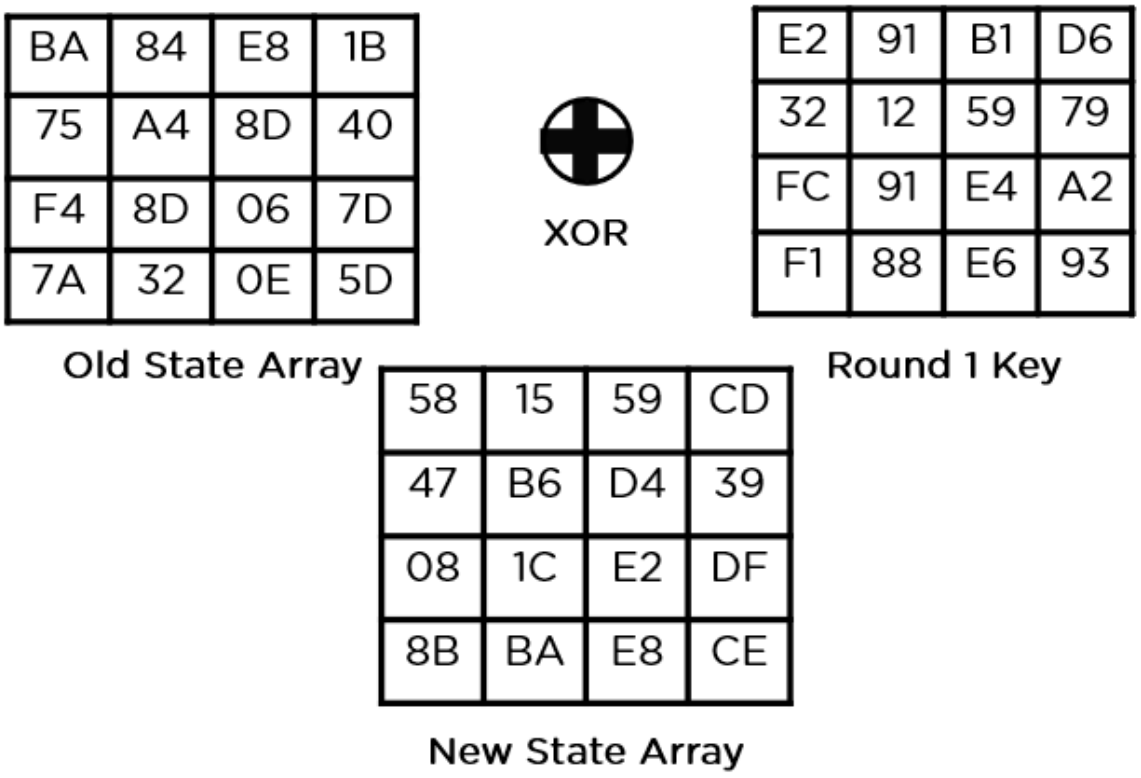
Final State Array after Round 10

29	57	40	1A
C3	14	22	02
50	20	99	D7
5F	F6	B3	3A

AES Final Output

29 C3 50 5F 57 14 20 F6 40 22 99 B3 1A 02 D7 3A

Ciphertext



This regional group currently serves as the cycle's final document. This becomes the next cycle's input. Repeat the processes above until you reach round 10, after which you will get the final ciphertext, depending on the length of the key.

This regional group currently serves as the cycle's final document. This becomes the next cycle's input. Repeat the processes above until you reach round 10, after which you will get the final ciphertext, depending on the length of the key.

3.4.2 The Data Encryption Standard (DES)-

The DES (Data Encryption Standard) algorithm is a symmetric-key block cipher developed by IBM and authorized by the National Institute of Standards and Technology in the early 1970s (NIST). Using 48-bit keys, the technique collects blank text in 64-bit blocks and turns it to ciphertext.

Because it's a symmetric key algorithm, the same key is used for both encryption and decryption. If it were an asymmetrical algorithm, the encryption and decryption keys would be different.

○ **DES Algorithm Steps -**

To put it another way, DES converts a 64-bit blank text into a 64-bit ciphertext text. While it comes to asymmetric algorithms, the same key is used when removing text writing.

The following steps make up the algorithm process:

The first permutation (IP) function is applied to a 64-bit blank text block to start the process.

After that, the initial authorisation (IP) is done in plain text.

Following that, initial access (IP) creates two parts of the authorized block, referred to as Left Blank Text (LPT) and Right Blank Right (RBR) (RPT).

Each LPT and RPT undergoes a 16-round encryption procedure.

LPT and RPT were eventually rejoined, and Final Permutation (FP) was applied to a newly merged block.

As a result of this procedure, the required 64-bit text is generated.

Step 4 of the encryption process is further broken into five stages:

An important change

Permission extension

S-Box Permission

P-Box Permission

XOR and change

We utilize the same approach to decrypt encryption and undo the layout of 16 round keys. Next, let's look at the various ways that DES operates in order to gain a better understanding of what it is.

3.4.3 RSA (Rivest–Shamir–Adleman)-

The RSA (Rivest-Shamir-Adleman) algorithm is the foundation of a cryptosystem - a collection of cryptographic algorithms used for specific applications or security purposes - that generates public key encryption and is widely used to protect sensitive data sent over an insecure network like the Internet.

How does RSA work?

RSA customers can choose between private or public key encryption, which provides a wide range of services. If you utilize a public key for encryption, you should also use a private key. This is great for delivering sensitive data via a network like the internet, where the data receiver sends the data sender their data key. The data sender then uses the public key to encrypt sensitive information before sending it to the recipient. Because a public key encrypts data, only the owner of the private key has the ability to decrypt sensitive data.

As a result, even if the data was intercepted during transit, only the intended recipient of the data may decrypt it.

Encrypting a message with a secret key is another method of asymmetric encryption with RSA. The data sender encrypts the data with his secret key and delivers the encrypted data together with their public key to the data recipient in this example. The recipient of the data can then use the sender's public key to erase the data recorder, thus confirming the sender's identity. Data can be stolen and read in transit this way, but the main goal of this sort of encryption is to prove the sender's identity. If the data was stolen and altered while in route, the recipient would be able to tell since the public key was unable to decrypt the new message.

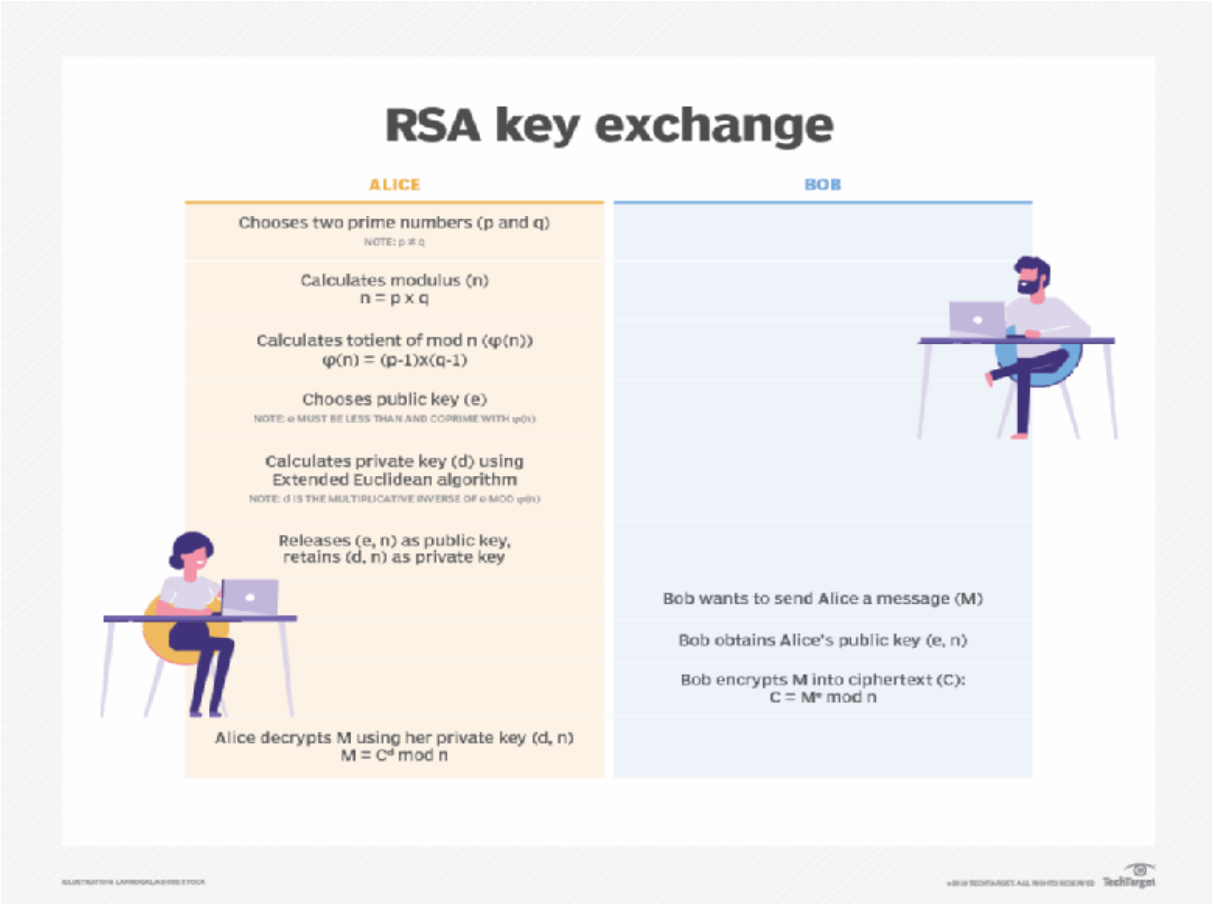


fig 9 shows rsa algorithm working

3.4.4 MD5 (Message-Digest algorithm 5)

MD5 (Message-Digest algorithm 5) is a 128-bit symmetric block cipher that is commonly used in cryptography. MD5 is monitored or improved for a number of security applications, and is frequently used to evaluate the integrity of files or products, since it is utilized at the web level (RFC 1321). A 32-character hexadecimal integer is used to represent an MD5 hash. MD5 is the most recent or enhanced version of MD4. Similarly to MD4, the MD5 hash was created by MIT University's "Professor Ronald Rivest." MD5 has also been used as a SHA-1 model because they share numerous similarities. MD5 and SHA-1 are the two most extensively used hash algorithms today, although MD5's use will decline over time as it is currently deemed broken.

Algorithm

"RFC 1321" describes the MD5 hash algorithm, as well as the use of C. The MD5 hash is comparable to the MD4 hash. The cushioning is identical.

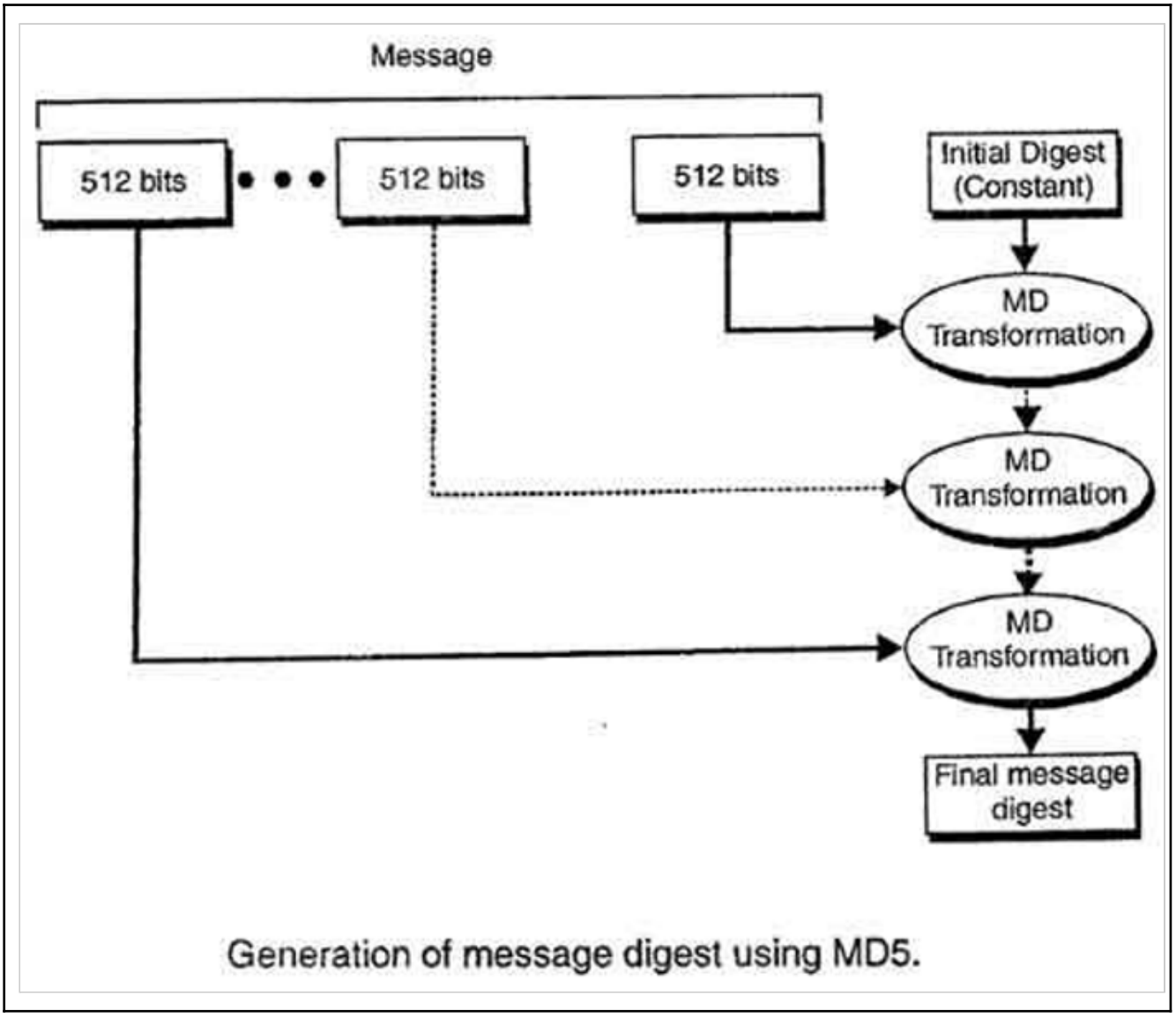
MD5 only works with words that are 32 bits long. Allow "M" to be used for the required message.

The message "M" is attached in such a way that its length in bits equals 448 modulo 512, i.e. the total message length is less than 64 bits of 512 multiples.

The padding starts with a single bit in the first column, followed by enough zeros to browse the message to the required length of 512 bits. Even though the actual length of M is equal to 448 mod 512, padding is always used. As a result, at least one bit of attachment and 512 bits stuffing is present. After that, a 64-bit block is appended to represent the length of the message parts you utilize before attaching them.

In addition to being a multiple of 512 bits, the connected message is also a multiple of 32 bits.

Let M stand for the required message, and N for the number of 32-bit words in the appended message. N is a factor of 16 bits because of finish.



Generation of message digest using MD5.

The message digest is generated using a four-word buffer (A, B, C, D). A, B, C, and D are each a 32-bit buffer for use. The following hexadecimal values are used to initialize these buffer words:

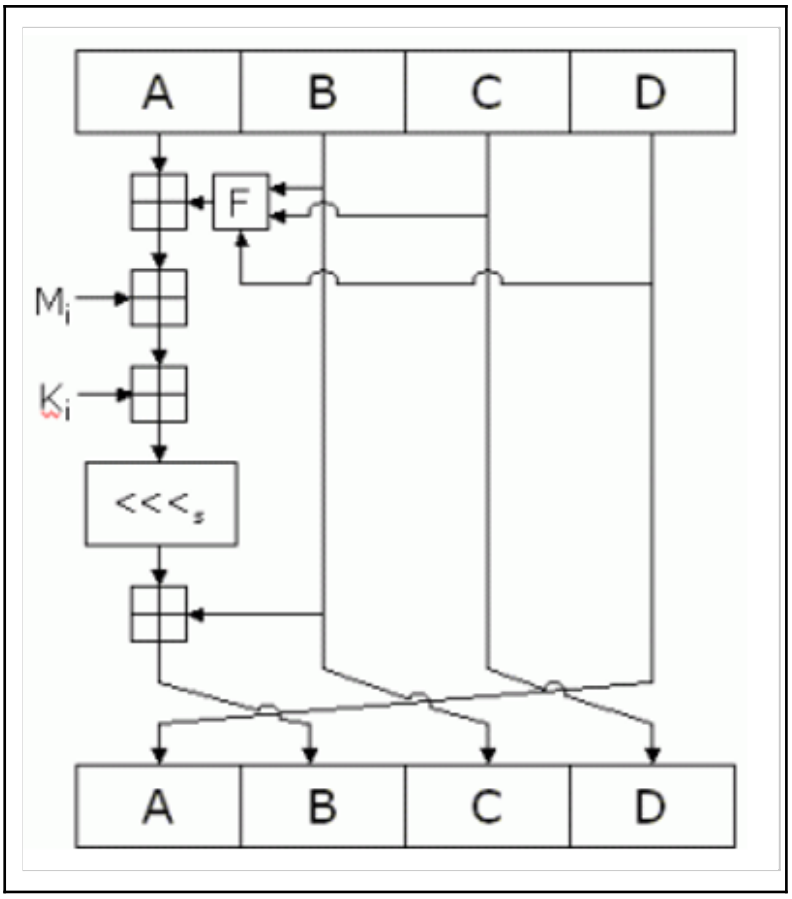
```
word A: 01 23 45 67

word B: 89 ab cd ef

word C: fe dc ba 98

word D: 76 54 32 10
```

We begin by defining the four auxiliary functions that are used in the buffer, each of which accepts three 32-bit words as input and outputs one 32-bit word.

$$F(X,Y,Z) = (X \wedge Y) \vee (\neg X \wedge Z)$$
$$G(X,Y,Z) = (X \wedge Y) \vee (Y \wedge \neg Z)$$
$$H(X,Y,Z) = X \oplus Y \oplus Z$$
$$I(X,Y,Z) = Y \oplus (X \vee \neg Z)$$

Here $\vee$ it is logical "**or**" , $\wedge$ it is logical "**and**", and $\oplus$ is logic.

Using the four auxiliary functions, the uses of the four buffers (A, B, C, and D) are now merged with the words of the input (F, G, H and I). There are four rounds in all, each with 16 basic procedures to complete. In the diagram below, one operation is depicted.



The diagram depicts how the auxiliary function works "The message word "M(i)" and the constant "K" are used to communicate with the four buffers (A, B, C, and D) (i). "n" is the item "n" is the item "n" is the item " "denotes an n-bit binary left shift.

The output

After we've completed all rounds, the MD5 digest of the original input is stored in buffers A, B, C, and D.

MD5 consists of five phases and four rounds of calculations that compute the hash of the input value and output the buffer.

- **CHAPTER 4: analysis stages,screenshots of project 4.1**

screenshot of stages

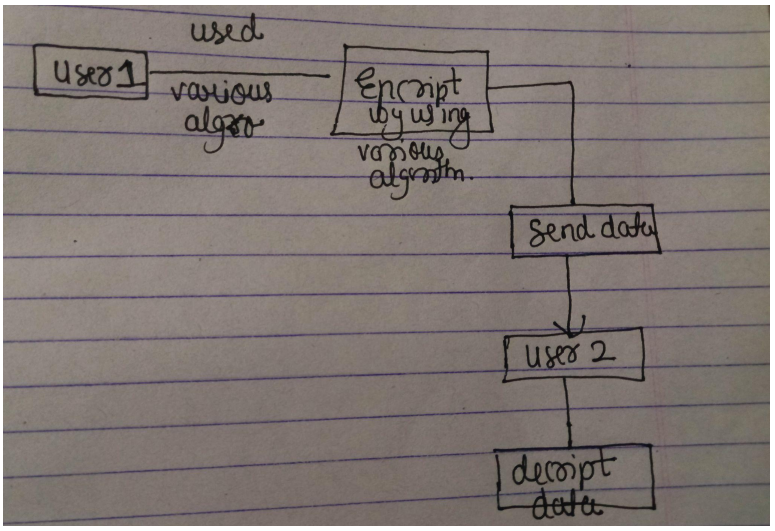


fig 10 user case diagram

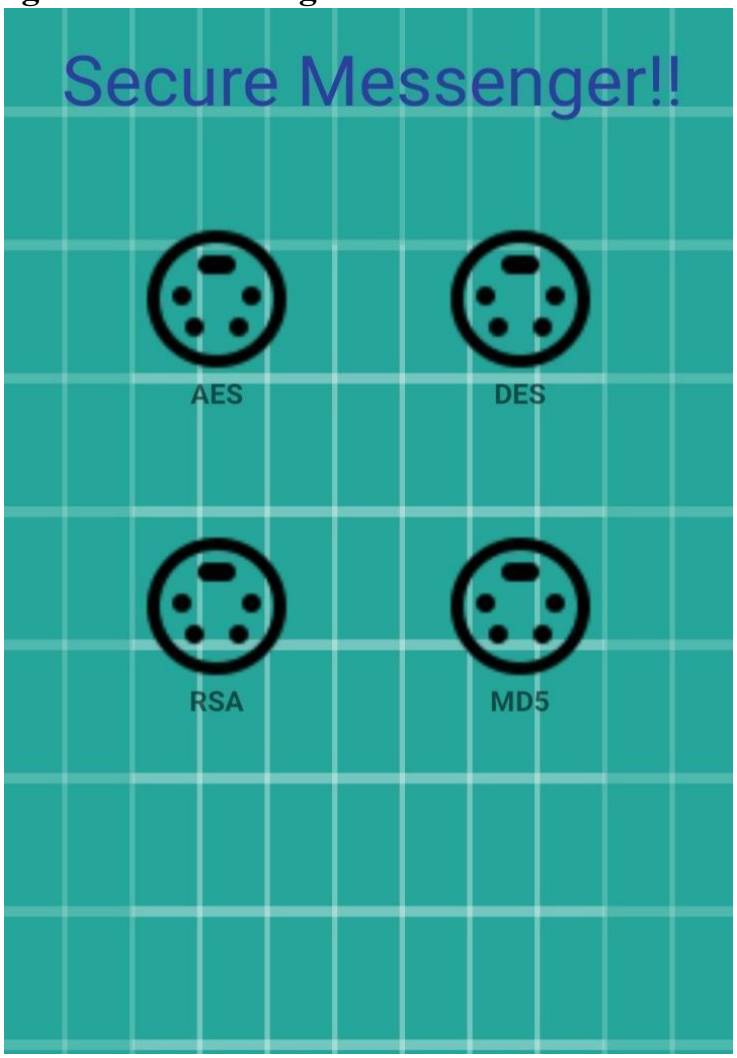


fig 11 home screen of app

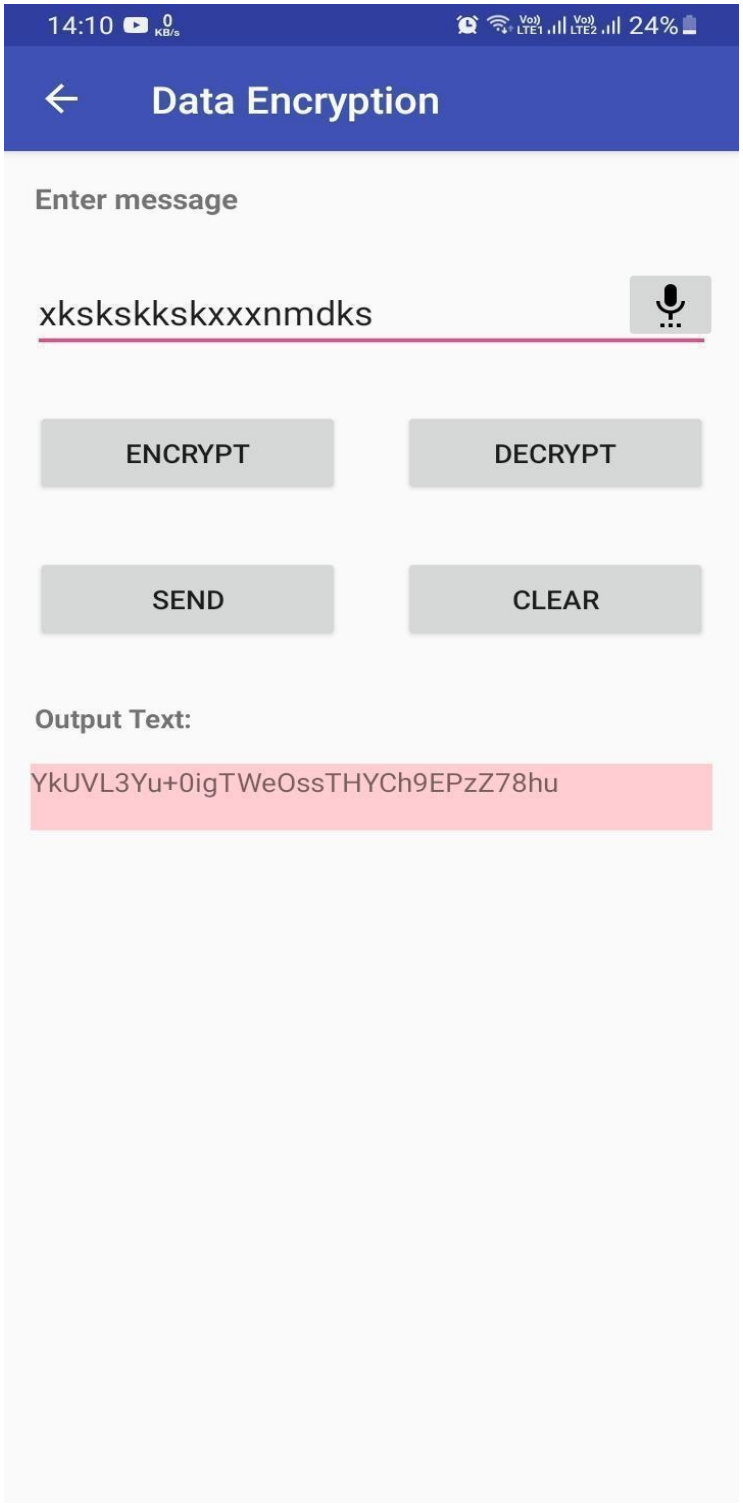


fig 12 des encryption

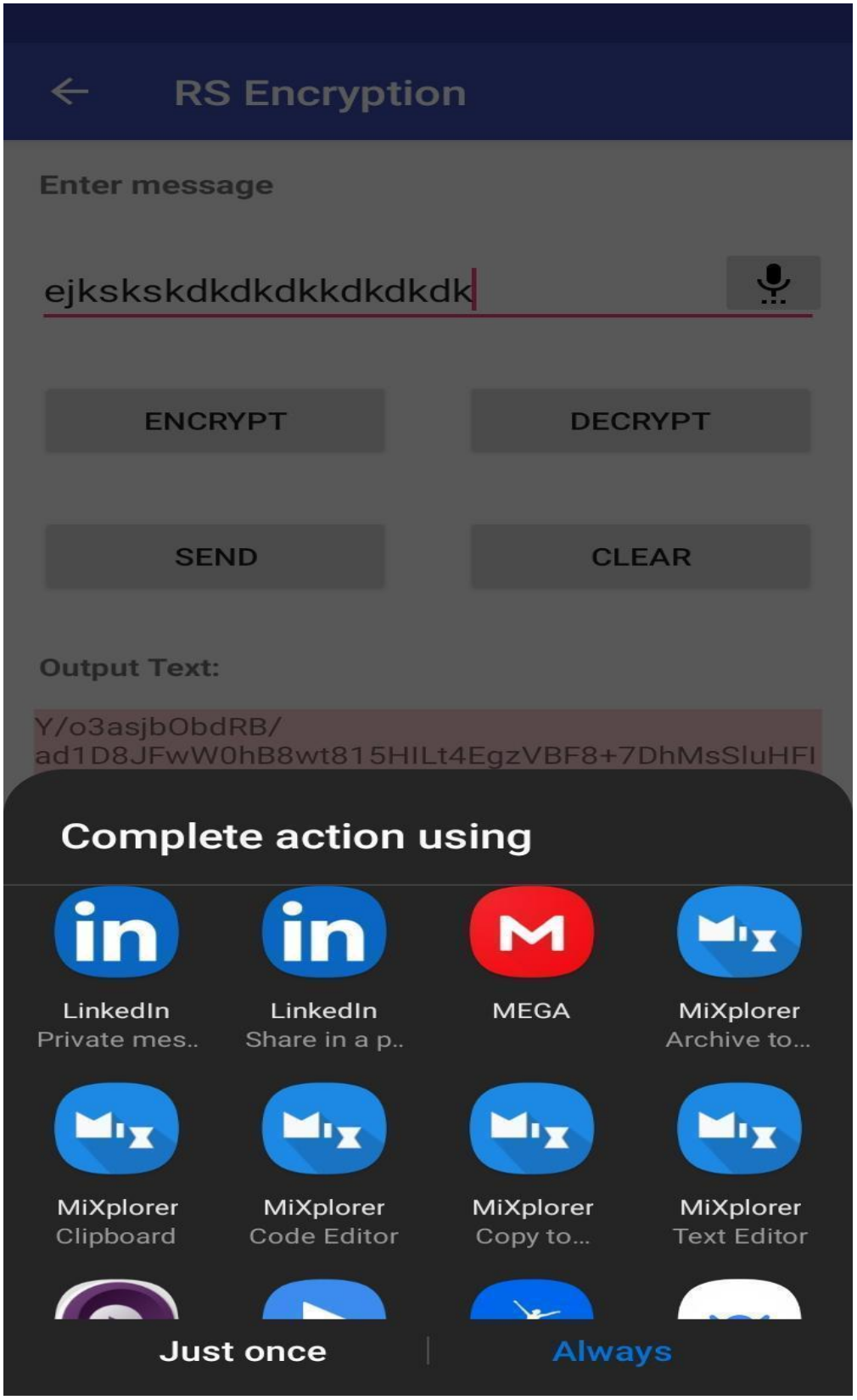


fig 13 sending message to someone

CHAPTER 5: application,future work conclusion

4.1 Application of the major Project

This is a professional encrypted based secure communication and thus used for communicating with others .

4.2 conclusion

therefore by using all the 4 above cryptography algorithms we can encrypt the data with high level of encryption and thus able to communicate easily and thus a secure communication is established between any two individuals

4.3 Future Work

we can make the communication between the two people in our app itself so that no third party app will be used and thus more secure communication is established.

REFERENCE

more info at

https://developer.android.com/

https://en.wikipedia.org/wiki/Cryptography

https://www.simplilearn.com/what-is-des-article

https://www.encryptionconsulting.com/education-center/what-is-rsa/

https://www.proofpoint.com/us/threat-reference/encryption