

A MEDICAL DATA ENCRYPTING USING GENERATIVE ADVERSARIAL NETWORK ALONG WITH HASH FUNCTION

Submitted in partial fulfillment of the requirements for the award of

Bachelor of Engineering Degree in

Electronics and Communication Engineering

By

ANJALI M (Register No. 38130011)

BHARATHI L (Register No. 38130031)



**DEPARTMENT OF ELECTRICAL AND ELECTRONICS ENGINEERING
SCHOOL OF ELECTRICAL AND ELECTRONICS ENGINEERING**

SATHYABAMA

**INSTITUTE OF SCIENCE AND TECHNOLOGY
(DEEMED TO BE UNIVERSITY)**

Accredited with Grade "A" by NAAC

JEPPIAAR NAGAR, RAJIV GANDHI SALAI, CHENNAI – 600 119

APRIL 2022



SATHYABAMA

**INSTITUTE OF SCIENCE AND TECHNOLOGY
(DEEMED TO BE UNIVERSITY)**

Accredited "A" Grade by NAAC | 12B Status by UGC | Approved by AICTE

www.sathyabama.ac.in

DEPARTMENT OF ELECTRICAL AND ELECTRONICS ENGINEERING

BONAFIDE CERTIFICATE

This is to certify that this Project Report is the bonafide work of **ANJALI M** (Reg.No. 38130011) and **BHARATHI L** (Reg.No. 38130031) who carried out the project entitled **"A MEDICAL DATA ENCRYPTING USING GENERATIVE ADVERSARIAL NETWORK ALONG WITH HASH FUNCTION"** under our supervision from December 2021 to April 2022.

Miss. Yogalakshmi

Internal Guide

Dr. T. Ravi

(Head of the Department)

Submitted for Viva voce Examination held on _____

Name:

Signature:

Internal Examiner

External Examiner

DECLARATION

We **ANJALI M** (Reg. No. 38130011) and **BHARATHI L** (Reg. No. 38130031) hereby declare that the project Report entitled “**A MEDICAL DATA ENCRYPTING USING GENERATIVE ADVERSARIAL NETWORK ALONG WITH HASH FUNCTION**” done by us under the guidance of **Miss. Yogalakshmi** is submitted in partial fulfillment of the requirements for the award of Bachelor of Engineering degree in Electronics and Communication Engineering.

DATE:

PLACE:

SIGNATURE OF THE CANDIDATES

1.

2.

ACKNOWLEDGEMENT

We are pleased to acknowledge our sincere thanks to the Board of Management of **SATHYABAMA** for their kind encouragement in doing this project and completing it successfully. We are grateful to them.

We convey our thanks to **Dr. N. M. Nanditha., Dean, School of Electrical and Electronics Engineering** and **Dr. T. Ravi, Head of the Department, Dept of Electronics and Communication Engineering** for providing us necessary support and details at the right time during the progressive reviews.

We would like to express our sincere and deep sense of gratitude to our Project Guide **Miss. Yogalakshmi** Assistant Professor for her valuable guidance, suggestions and constant encouragement paved the way for the successful completion of our project work.

We wish to express our thanks to all Teaching and Non-teaching staff members of the Department of Electronics and Communication Engineering who were helpful in many ways for the completion of the project.

ABSTRACT

In recent years, there is a tremendous demand for healthcare systems that establishes a framework to reduce the time required to complete the work and the expensive procedures used to recover a patient's medical report, along with the constant integration of sets of medical data to furnish it to the healthcare industry. EHRs (Electronics Health Records) widely permit the insurance companies, patients and healthcare providers to launch, manage and process the healthcare information of the patients from anywhere at any time. We propose an efficient cryptosystem for data encryption and authentication. Some of data might be transmitted through insecure channel from sender to receiver. Cryptography is the process of encrypting messages and other data in order to transmit them in a form that can only be accessed by the intended recipients. It was initially applied to written messages. With the introduction of modern computers, cryptography became an important tool for securing many types of digital data. Cryptography is one of the most significant and popular techniques to secure the data from attackers by using two vital processes that is Encryption and Decryption. Cryptography algorithms uniquely define the mathematical steps required to encrypt and decrypt messages in a cryptographic system. Shortly, they protect data from unauthorized access. Advanced Encryption Standard (AES) is the most commonly used algorithm for data encryption and widely symmetric block cipher algorithm. In this project, AES algorithm can be applied on text file, it perception of binary coded form and generating of cipher keys is used to encrypt the data file. Encryption is the process of encoding data to prevent it from intruders to read the original data (Plaintext) into unreadable format known as cipher text using a key. In this system **GAN** used to provide both security and safe to encrypted and decrypted of the data efficiently. After a brief literature review, we compared and analyzed the complexity of several existing methods in order to provide efficient results. Various studies regarding this concern have been performed to ensure these requirements by hybridizing different domains, such as spatial and transform domains. The results indicate that the proposed cryptosystem provides high performance and enhanced security.

Keywords: Foundation of cryptography, composable security, GAN network

TABLE OF CONTENTS

CHAPTER NO	TITLE	PAGE NO
1	Introduction	1-2
	1.1 Overview	1
	1.2 Objective	2
2	Literature Survey	3-4
3	Aim and Scope of the Project	6-7
	3.1 Scope of the Project	5
	3.2 Existing System	6
	3.3 Proposed System	7
4	System Function	8-9
	4.1 Block Diagram	8
	4.2 Working Explanation	9
5	System specification	10-22
	5.1 Hardware Specification	10
	5.2 Software Specification	10
	5.3 AES Algorithm	10
	5.3.1 Choosing the Rjindael cipher	11
	5.3.2 Attacks on AES	12
	5.3.3 Advantages of AES	12
	5.3.4 Disadvantages of AES	12
	5.4 Encryption	13
	5.4.1 How encryption works	14

	5.4.2	Types of encryption	15
	5.4.3	Encryption Challenges	15
	5.4.4	Benefits of encryption	15
	5.5	Decryption	16
	5.5.1	Decryption used	16
	5.5.2	Types of Decryption	16
	5.5.3	Advantages and Disadvantages of Decryption	17
	5.5.4	Image of Encryption and Decryption	17
	5.6	Cryptography	18
	5.6.1	Features of Cryptography	18
	5.6.2	Types of Cryptography	19
	5.7	Generative Adversarial Network	21
	5.7.1	GANs Network	21
	5.7.2	Types of GANs	22
6	Matlab		23-40
	6.1	Matlab	23
	6.1.1	The Matlab System	24
	6.1.2	Matlab's power of computational Mathematics	25
	6.1.3	Features of Matlab	25
	6.1.4	Uses of Matlab	26
	6.1.5	Local Environment Setup	26

	6.1.6 Understanding the Matlab environment	27
	6.1.7 The M file	29
	6.1.8 Application of Matlab	30
	6.2 PYQT5	33
	6.2.1 Supporting Environment	34
	6.2.2 Advantages of PyQt	39
	6.2.3 Disadvantages of PyQt	39
	6.3 Python	40
7	Hardware specification	41-47
	7.1 I5 Processor	41
	7.1.1 About-Core I5	41
	7.1.2 Technical specification of I5 Processor	42
	7.2 RAM	43
	7.2.1 Functions of RAM	43
	7.2.2 Types of RAM	46
	7.2.3 RAM vs Virtual Memory	46
	7.2.4 RAM vs Flash Memory	47
8	Result	48
	8.1 Original data	48
	8.2 Encrypted data	48
9	Conclusion	49
10	References	50-53

CHAPTER 1

INTRODUCTION

1.1 OVERVIEW

Internet communication is playing the important role to transfer large amount of data in various fields. Some of the data may be transmitted insecurely through channel from sender to receiver. Now a days wireless communication systems are facing the issues of a data security and privacy. Establishing a highly reliable and secure means of wireless communication for the transfer of digital data (in the form of text, image, and video) from source to destination is becoming an essential requirement. With the development of computers, electronics, modern communication technologies, issue of security and confidentiality of information transmission and storage has become an important research field. Such data processes are implemented in either legal or illegal manner and different approaches are used to hide data such as key generation, it can be considered as an enhanced method that can provide protection to the ownership of the digital media against digital piracy. Various types of techniques and methods have been using by private and public sectors to protect the sensitive data from intruders because of the security of electronics data is crucial issue. Cryptography is one of the most efficient and popular techniques to secure the data from attackers by using two vital processes that is called Encryption and Decryption. Encryption is the process of encoding data to prevent it from third parties. This encryption process has the ability to convert the original data (Plaintext) into unreadable format known as Cipher text. The next process that has to carry out by the authorized person is Decryption. Decryption is contrary of encryption. It is the process to convert cipher text into plain text without missing any words in the original text. To perform these process cryptographies relies on mathematical calculations along with some substitutions and permutations with a key. Generative adversarial networks (GAN) using to security purpose. GAN used to provide both security advances and attack scenarios, in order to bypass detection systems.

1.2 OBJECTIVE

- The main objective of this project is encrypted and decrypted the data file safely and secure.
- A key should be established between the sender and receiver for encryption and decryption process.
- Secures data from being accessed by any malicious user.
- Only authorized users are provided to access these data.
- Ensure that private data is not accessed by other users.
- Improves security of internet
- No one would be able to know what it says unless there's a security key to the code

CHAPTER 2

LITERATURE SURVEY

[1] Moustafa Mamdouh, Rowayda Sadek.” A new dynamic secured IEEE802.11e AES based system”, 2017 9th International Conference on Computational Intelligence and Communication Networks.

Advanced Encryption Standard (AES) is a symmetric block cipher which uses same key for encryption and decryption. It is also an iterative cipher as the initial input block and the key undergoes multiple rounds of transformation before producing the output. The computation is performed on bytes unlike any other algorithms that performs computation on bits.

[2] Padate, R., & Patel, A. (2018). Encryption and decryption of text using AES algorithm. International Journal of Emerging Technology and Advanced Engineering, 4(5), 54-9.

AES algorithm is based on AES key expansion to encrypt and decrypt data. It is another most important step in AES structure. Each round has a new key. In this section concentrates on AES Key Expansion technique. The key expansion routine creates round keys word by word, where a word is an array of four bytes. The routine creates $4 \times (Nr+1)$ words.

[3] Monika Agrawal, A Comparative Survey on Symmetric Key Encryption Techniques, International Journal on Computer Science and Engineering (IJCSE), Vol. 4 No. 05 May 2017.

” Cryptography” derives from the Greek word *kryptos* which means” hidden”. Cryptography is an area of computer science which is developed to provide security for the senders and receivers to transmit and receive confidential data through an insecure channel.

[4] Neetesh Saxena and Narendra S. Chaudhari, EasySMS: A Protocol for End-to-End Secure Transmission of SMS, IEEE Transactions on Information Forensics and Security, Vol. 9, No. 7, July 2019.

The algorithms used in the project are EasySMS protocol, Blowfish encryption algorithm and MD5 hashing algorithm. The protocol aims to achieve authentication, the Blowfish encryption algorithm is used to achieve confidentiality and MD5 is used to achieve integrity to the message. The protocol includes two Mobile Stations (MS1 and MS2), Authentication Server (AS) and a certified authority (CA). The AS stores all the symmetric keys shared between AS and the respective MS. CA stores all the information related to the mobile subscribers. We assume that every subscriber has to register his/her mobile number with CA entity and only after the verification of identity, the SIM card gets activated by this entity. Thus, this entity is responsible to validate the identity of the subscribers. We also assume that a symmetric key is shared between the AS and the CA which provides the proper security to all the transmitted information between AS and CA.

[5] Rammohan, S. R., Jayashri, N., Bivi, M. A., Nayak, C. K., & Niveditha, V. R. (2020). High performance hardware design of compressor adder in DA based FIR filters for hearing aids. International Journal of Speech Technology, 1-8

The ABE techniques leverage encrypts all the patient's PHR report to achieve scalable and fine-grained data access control of the PHRs [19]. The owner of the data updates their data into the arbitrary cloud data centers.

[6] Hui Yin, Jixin Zhang, Yinqiao Xiong, Lu Ou, Fangmin Li, Shaolin Liao & Keqin Li (2019), "CP-ABSE: A Ciphertext-Policy Attribute-Based Searchable Encryption Scheme, IEEE vol. 7, pp.5682-5694.

Exploiting a secured path for data exchange has become the major obstacle in the healthcare industry. PHR is an online, patient-centric algorithm for the safe exchange of healthcare information. It allows the patients to coordinate and access their lifelong healthcare data with other users.

CHAPTER 3

AIM AND SCOPE OF THE PROJECT

3.1 SCOPE OF PROJECT

While talking about information system, cryptography in computer science takes major roles. In modern days, cryptography is considered to be technical practice of converting any readable text or message to a code which is an unintelligible one. However, this coded message can be converted to its readable format with the help of cryptography. As computer system is becoming too complex, cryptography holds much importance and the skill of cryptography is deeply rooted in a subjected matter of computer science. Here are few scopes for cryptography students in computer science subject.

Cryptography holds four fundamental pillars which include authenticity, integrity, non-repudiation and confidentiality. Cryptography maintains the confidentiality of the data transferred through computer network by restricting audience except for the intended one. Cryptography can allow the user's identification before transmitting any data. Cryptography allows non-repudiation by restricting the option where the user can deny to the actions.

Cryptography ensures integrity of the user by analyzing the authentication of the same. For example; electronic signature is based on cryptographic tool which is considered to be a public key. One of the most important functions of cryptography is to maintain the integrity of the user in computer network. After completing studies in computer science with cryptography, you can opt for several career opportunity and some of them are listed below.

NSA (National Security Agency)

National Security agency focuses on computer network security, encryption, protection and coding. NSA contributes to protect the government and the entire country by supplying military and armed forces. NSA also protects national data with its highest security. Any student after completing computer science degree course can join NSA serve national data security by the skill of cryptography.

Security Consultant

After completing education in computer science, one can choose the job role of a security consultant. Being a security consultant, you need to suggest the best way to protect computers, software and network. You need to take early protection from possible threats to information system. Computer science teaches you the way of coding the essential data and also makes you understand the ways of recording the same. In order to ensure the surety of those vulnerable data, you need to make vulnerability testing, risk analysis and security assessment of the entire data.

Apart from the job role of a security consultant, you may opt for the career path of security auditor, security engineer, security analyst and security administrators. The major responsibility of these job roles is to maintain the standard security and authenticity of entire network system. Technical supervision is required for furnishing these job role. After completing your study in computer science you must possess knowledge and excellence in robust security architect and corporate security policy.

Other job opportunities available in market for computer science student with the skill of cryptography are security architect, IT project manager and security manager. Hence, your study in computer science can embrace your career in technical field with cryptography knowledge

3.2 EXISTING METHOD

- This existing system contains a technique for secret communication using cryptography. This is the technique which is used to protect the sensitive data.
- The secret message is encrypted by a block of cipher text based on two cryptographic algorithms, the Data Encryption Standard (DES) and the Triple Data Encryption Algorithm (TDEA) which may be used by Federal organizations to protect important data.
- This algorithm uniquely defines the mathematical steps required to transform data into a cryptographic cipher text and also to transform the cipher text back to the original data form with block length of 128 bits and key length of 256 bits.

- Data Encryption Standard was not designed for software and hence runs relatively slowly.
- In a new technology it is improving a lot of possibility to break the encrypted code, so that Advanced Encryption Standard (AES) is preferred than DES.

3.3 PROPOSED SYSTEM

- In this project, the text file data can be encrypted and decrypted based on the security key.
- Encryption is a process of coding information which could either be a file into cipher text a form unreadable without a decoding key in order to prevent anyone except the intended recipient from reading that data.
- Decryption is the reverse process of converting encoded data to its original un-encoded form, plaintext. A key in cryptography is a long sequence of bits used by encryption / decryption algorithms.
- Advanced Encryption Standard (AES) is the most commonly used algorithm for data encryption and widely symmetric block cipher algorithm.
- The AES algorithm can be applied on text file and generating of cipher keys is used to encrypt the data file.
- This stage has the ability to convert the original data (Plaintext) into unreadable format known as Cipher text.
- The decryption is the process to obtain the original data that was encrypted. This process is based on the key that was received from the sender of the data.
- The decryption processes of an AES is similar to the encryption process in the reverse order and both sender and receiver have the same key to encrypt and decrypt data
- In this project by using GAN network for securely transferring the data file without hacking of the data.

CHAPTER 4

SYSTEM FUNCTION

4.1 BLOCK DIAGRAM

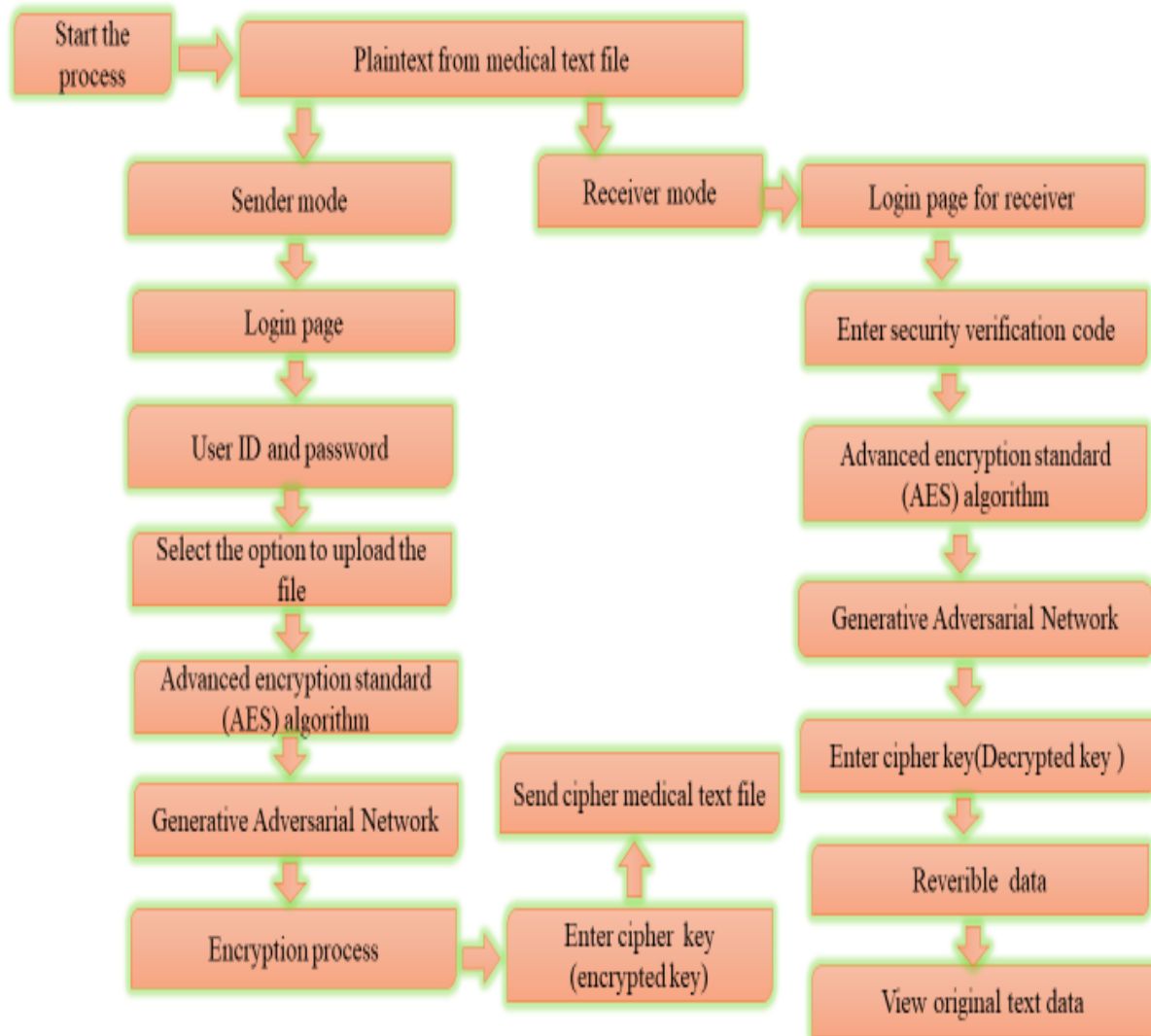


Fig.no:4.1 Block Diagram

4.2 WORKING EXPLANATION

- The above block diagram represents the encrypted and decrypted the text data based on the security key.
- Cryptography algorithms uniquely define the mathematical steps required to encrypt and decrypt messages in a cryptographic system.
- Shortly, they protect data from unauthorized access. Advanced Encryption Standard (AES) is the most commonly used algorithm for data encryption and widely symmetric block cipher algorithm.
- In this project, AES algorithm can be applied on text file .The text data are processed using effective image processing technique.
- This system has two modes sender and receiver mode.
- The sender can login with user ID and password.
- Encryption is the process of encoding data to prevent it from intruders to read the original data easily.
- This stage has the ability to convert the original data (Plaintext) into unreadable format known as Cipher text.
- Encryption is the process of converting the plaintext into cipher text using a key. The patient text data can be send to receiver with the security key.
- In the receiver side the receiver also having login page for login, after a login the receiver enter the security code for that encrypted text file.
- Then the receiver decrypted the text data. The results indicate that the proposed cryptosystem provides high performance and enhanced security.
- In this system **GAN** used to provide both security and safe to encrypted and decrypted of the data effectively.

CHAPTER 5

SYSTEM SPECIFICATION

5.1 HARDWARE SPECIFICATION

- Processor: INTEL i5 (7th generation)
- RAM: 8 GB RAM
- Hard disk: 1TB
- Monitor: 20' colour monitor

5.2 SOFTWARE SPECIFICATION

- Software used: MATLAB
- Platform: Windows 8

5.3 AES ALGORITHM

- The **AES algorithm** (also known as the **Rijndael algorithm**) is a symmetrical block cipher algorithm that takes plain text in blocks of 128 bits and converts them to cipher text using keys of 128, 192, and 256 bits. Since the Advanced Encryption Standard algorithm is considered as secure and safety, it is in the worldwide standard.
- An AES algorithm uses a substitution-permutation, or SP network, with multiple rounds to produce cipher text. The number of rounds based on the key size being used. A 128-bit key size dictates ten rounds, a 192-bit key size dictates 12 rounds, and a 256-bit key size has 14 rounds. Each of these rounds requires a round key, but since only one key is inputted into the algorithm, this key needs to be expanded to get the keys for each round, including round 0.

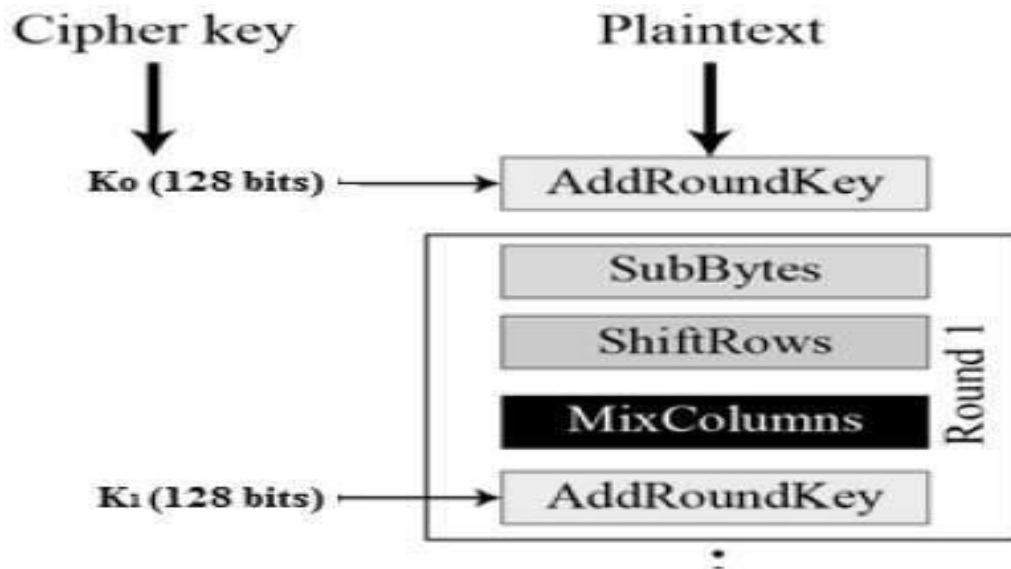


Fig no 5.1 AES Image

5.3.1 CHOOSING THE RJINDAEL CIPHER

To create the AES algorithm, a competition was held, which initially had 15 different encryption algorithms in the running. It was eventually narrowed down to just 5 algorithms:

- MARS
- Rivest Cipher 6 (RC6)
- Rjindael
- Serpent
- Two fish

This encryption algorithms were extensively analysed by both the National Institute of Standard Technology (NIST) and the National Security Agency (NSA), to determine the most secure one to use in the Advanced Encryption Standard. After rigorous testing of these algorithms, the Rjindael cipher was selected to be used in AES. The use of a 256-bit key gives the Rjindael cipher strong security and safety, while maintaining its interoperability with existing hardware and software. Stronger ciphers exist, but they do not have the ability to be implemented into existing systems easily, like the Rjindael cipher can.

5.3.2 ATTACKS ON AES

- Related-key attack
- Distinguished key attack
- Side channel attack
- Key compromise
- Quantum computing

5.3.3 BENEFITS OR ADVANTAGES OF AES

- As it is implemented in both the hardware and software, it is most strong security protocol.
- It uses higher length key sizes such as 128, 192 and 256 bits for encryption. Hence it makes Advanced Encryption Standard algorithm strong against hacking.
- It is most common safety and security protocol used for wide different type of applications such as wireless communication, financial transactions, e-business, encrypted data storage, signal processing etc.
- This is one of the most spread commercial and open source solutions used throughout the world.
- No attackers can hack your personal information.
- For 128 bits, approximately 2^{128} attempts are needed to break. This makes it very difficult to hack it as a result it is very safe and secure protocol.

5.3.4 DRAWBACKS OR DISADVANTAGES OF AES

- It uses very simple algebraic structure.
- Every block should always encrypted in the same way.
- It is very hard to implement with software.
- AES algorithm in counter mode is complex to implement in software taking both performance and security into considerations.
- Remembering or recording key/passwords when accessing the data.
- Consumes plenty of resources.
- Issue of compatibility

5.4 ENCRYPTION

Encryption is the process of securing digital data using one or more mathematical techniques, along with a password or "key" used to decrypt the encrypted information. The encryption process translates information using some algorithms such as AES, DES that makes the original information into unreadable. The process can convert an original text, known as plaintext into an alternative form (unreadable text) known as cipher text. When an authorized user needs to access the data, they may decrypt the data using a binary key (cipher key). This will convert cipher text back to plaintext so that the authorized user can access the original information.

Encryption is an important way for individuals and companies to protect sensitive information from hacking. For example, websites that transmit credit card and bank account details should always encrypt this information to prevent it from theft and fraud. The mathematical study and application of encryption is known as cryptography.

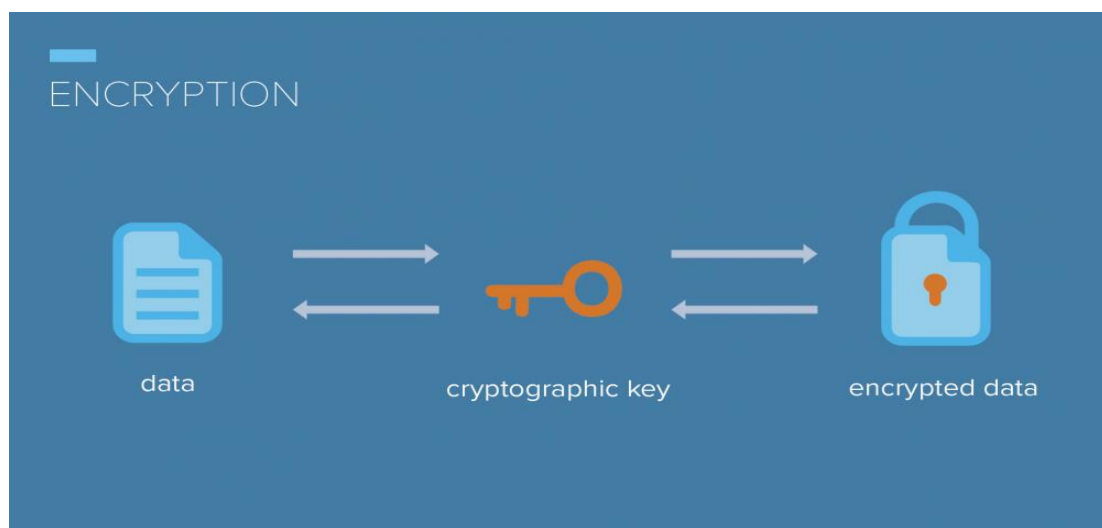


Fig No: 5.2 Encryption Image

5.4.1 HOW ENCRYPTION WORKS

Original information, or plain text, might be something as simple as "Hello, world!" As cipher text, this might appear as something confusing like 7*S1\$0+gvU2x something seemingly random or unrelated to the original plaintext.

However encryption is a logical process, whereby the party receiving the encrypted data but also in possession of the security key can simply decrypt the information and turn it back to an original text.

For decades, attackers have tried by brute force essentially, by trying over and over again to figure out such security keys. Cyber criminals increasingly have access to stronger computing power such that sometimes, when vulnerabilities exist, they can be able to gain access.

Data needs to be encrypted when it is in two different states: "at rest," when it is stored, such as in a database; or "in transit," while it is being accessed or transmitted between authorized users.

An encryption algorithm is the mathematical formula used to transform plaintext (data) into unreadable text. An algorithm will use the security key to alter the data in a predictable way. Even though the encrypted data appears to be random, it can actually be turned back into plaintext by using the security key again. Some commonly used encryption algorithms include Blowfish, Advanced Encryption Standard (AES), Data Encryption Standard (DES), Triple Data Encryption Standard (TDES) Rivest Cipher 4 (RC4), Rivest Cipher 5 (RC5), Rivest Cipher 6 (RC6), Blowfish Encryption and Two fish Encryption.

Encryption has evolved over time, from a protocol that was used only by only governments for top-security purpose (operation) to an everyday must-have for organizations to ensure the security and privacy of their data.

5.4.2 TYPES OF ENCRYPTION

- Symmetric Encryption
- Asymmetric Encryption
- Data Encryption Standard (DES)
- Triple Data Encryption Standard (3DES)
- Rivest-Shamir-Adleman (RSA)
- Two fish Encryption
- Blowfish Encryption
- Advanced Encryption Standard (AES)
- Encryption in the Cloud
- End-to-End Encryption

5.4.3 ENCRYPTION CHALLENGES

The attackers will still try to access the data even though when they knows that data or devices are encrypted. They would figure that with some effort, they may get through. For many years, weak passwords served as the impetus for attackers to keep trying, as some sophisticated software could sooner or later figure out passwords.

Such brute force attacks have become more sophisticated, as attackers hope that by making thousands or even millions of guesses, they will figure out the key for decryption. However, most modern encryption methods, coupled with Multi-Factor Authentication (MFA), is helping an organizations to become more resistant to brute force attacks.

5.4.4 BENEFITS OF ENCRYPTION

- Privacy and Security
- Regulations
- Secure Internet Browsing
- Encryption Keeps Sensitive Data Safe

5.5 DECRYPTION

- The conversation of encrypted data into its original data is known as decryption. It's generally a reverse process of encryption.
- Decryption decodes the encoded or encrypted text and converting it back to text which is encrypted by you that is original information. This term could be used to describe a method of unencrypting the data manually or unencrypting the data using the proper codes or security keys.
- Data might be encrypted to make it much difficult to attackers to steal the information easily. Companies also encrypt the data for general protection of company data and trade secrets. If this data needs to be viewable, it must require decryption process. If a decryption passcode or security key is not available, special software might be needed to decrypt the data using algorithms to crack the decryption and make the data readable.

5.5.1 DECRYPTION USED

- It helps you secure sensitive info, such as passwords (Security key) and login IDs.
- It Provides confidentiality of private information
- It helps you ensure that the record or file is still unchanged and un attacked.
- Encryption also avoids plagiarism and protects IP.
- Beneficial for network communication such as the internet and where the hacker can quickly obtain unencrypted data.
- It's an essential method because it lets you protect data safely that you don't want someone else to access.

5.5.2 TYPES OF DECRYPTION

- Triple DES
- RSA
- Blowfish
- Two fish
- AES

5.5.3 ADVANTAGES AND DISADVANTAGES OF DECRYPTION

- While the reason for using decryption process might vary, adequate protection is one of the advantages and purposes that it serves. The company can have smooth management with the help of decryption. The Cyber security professionals use this method to prevent the exfiltration of confidential information.
- The primary concern with decryption, however is the matter of data security. Decryption would operates on the risk of separating an essential part of the workforce. Take the example of an employee who by chance logged into their email or bank account details. This might at any time, trigger a firewall incident, if the keywords are inadequately selected.
- Hence privacy for the end consumers is renounced when decryption is underway. An innocent employee with no intention of exposing sensitive organizational information might find their network traffic observed as a result of triggering the firewall involuntarily.

5.5.4 IMAGE OF ENCRYPTION AND DECRYPTION

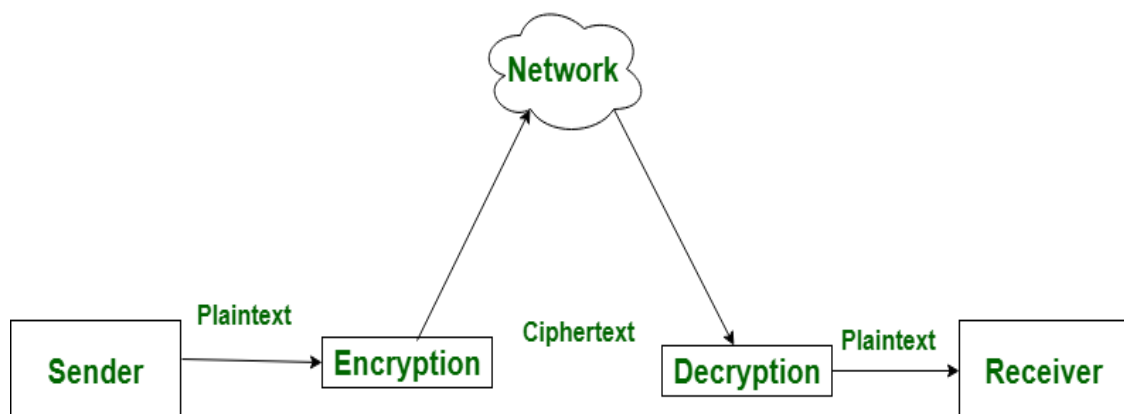


Fig.no: 5.3 Encryption and Decryption image

5.6 CRYPTOGRAPHY

Cryptography is the technique of protecting sensitive data and communications through use of codes so that only those people for whom the information is intended can understand it and process it. Thus, preventing unauthorized access to information. The meaning of cryptography is “hiding the sensitive data”. The prefix “crypt” means “hidden” and suffix “graphy” means “writing”.

In Cryptography the techniques which are used to protect information are obtained from mathematical concepts and a set of rule-based calculations known as algorithms to convert messages in ways that make it hard to decode it. These algorithms are used for cryptographic security key generation, digital signing, and verification to protect data privacy, web browsing on internet and to protect confidential transactions such as credit card and debit card transactions.

5.6.1 FEATURES OF CRYPTOGRAPHY

Confidentiality

The information can only be accessed by the authorized person for whom it is intended and no other person can access except the authorized users.

Integrity:

Information cannot be modified in storage or transition between sender and intended receiver without any addition to information being detected.

Non-repudiation:

The creator or sender of the information cannot deny his or her intention to send information at later stage.

Authentication:

The identities of sender and receiver are confirmed. As well as destination or origin of information is confirmed.

5.6.2 TYPES OF CRYPTOGRAPHY

There are three types of cryptography. They are,

- Symmetric key cryptography
- Asymmetric key cryptography
- Hash function

Symmetric key cryptography

Symmetric key cryptography is also known as **Private-key cryptography**. Symmetric key cryptography is an encryption system where the sender and receiver of message use a single common security key to encrypt and decrypt information. Symmetric Key Systems are faster and much simpler but the problem is that the sender and receiver have to somehow exchange security key in a secure manner. The most popular symmetric key cryptography system is Data Encryption System (DES).

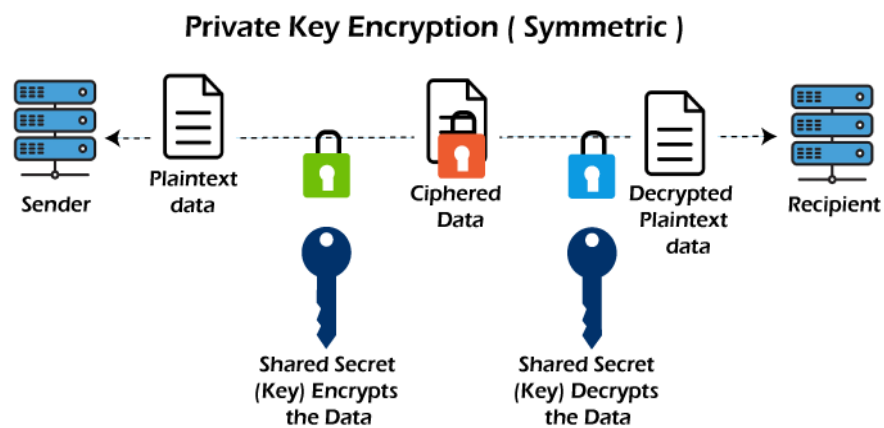


Fig No: 5.4 Private Key Encryption

Asymmetric key

Asymmetric key cryptography is also known as **Public-key cryptography**. Asymmetric key cryptography is a cryptographic system that uses pairs of security keys. Each pair consists of a public key and a private key. The generation of such

key pairs depends on cryptographic algorithms which are based on mathematical problems termed one-way functions.

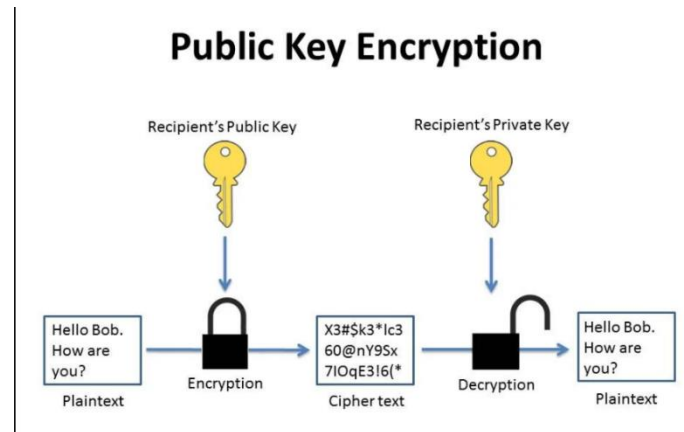


Fig no: 5.5 Public key Encryption

Hash Function

A hash function is any function that can be used to map data of arbitrary size to fixed-size values. The value returned by a hash function are called hash values, hash codes, digests or simply hashes. The values are usually used to index a fixed-size table called a hash table.

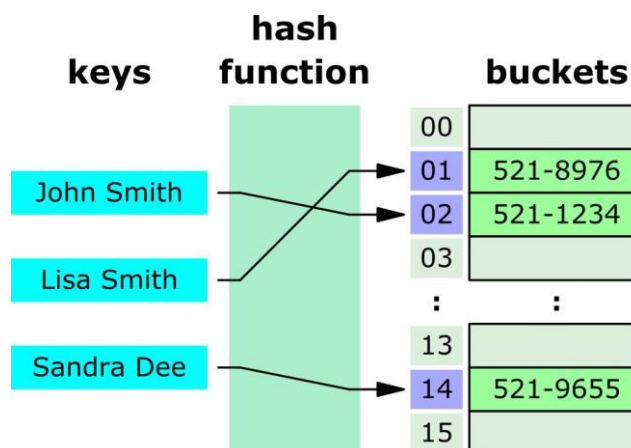


Fig No: 5.6 Hash function

5.7 GENERATIVE ADVERSARIAL NETWORK (GAN)

A generative adversarial network is a class of machine learning frameworks designed by Ian Goodfellow and his colleagues in June 2014. A Generative adversarial networks is a type of neural network that can generate new images from the given set of samples that are similar to the given dataset, yet individually different. They are composed of two neural network models, a generator and a discriminator. The generator learns to develop new samples, whereas the discriminator learns to differentiate the generated examples from the real ones. These two models work together for training the GAN network to generate and distinguish new plausible samples from the existing dataset. Since GAN networks learn to recognize and distinguish images, they are used in photography, image editing, gaming etc. And also Generative adversarial networks can be used for translating data from images. GANs can be utilized for image-to-image translations, semantic image-to-photo translations, and text-to-image translations.

5.7.1 GANS WORK

Generative: To learn a generative model, which describes how data is generated in terms of a probabilistic model.

Adversarial: The training of a model is done in an adversarial setting.

Networks: Use deep neural networks as the artificial intelligence (AI) algorithms for training purpose

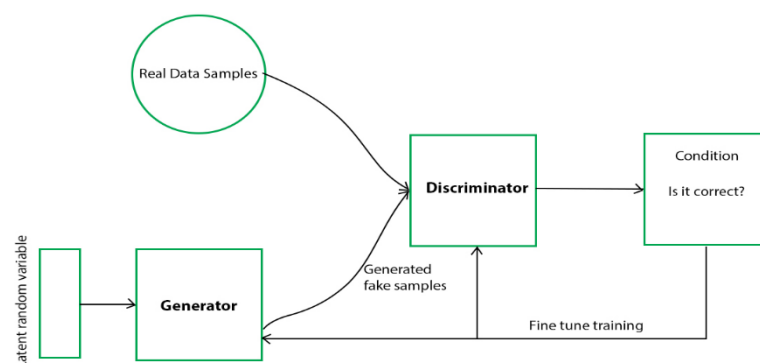


Fig no: 5.7 GAN Network

5.7.2 TYPES OF GAN NETWORKS

Vanilla GAN: This is the simplest type GAN. Here, the Generator and the Discriminator are simple multi-layer perceptron's. In this GAN network, the algorithm is really simple, it tries to optimize the mathematical equation using stochastic gradient descent.

Conditional GAN (CGAN): Conditional GAN can be described as a deep learning method in which some conditional parameters are put into place. In CGAN, an additional parameter 'y' is added to the Generator for generating the corresponding data. Labels are also put into the input to the Discriminator in order for the Discriminator to help distinguish the real data from the fake generated information.

Deep Convolutional GAN (DCGAN): Deep convolutional GAN network is one of the most popular and also the most successful implementation of GAN network. It is composed of ConvNets in place of multi-layer perceptron's. The Convolutional Nets are implemented without max pooling, which is in fact replaced by convolutional stride. Also, the layers are not fully connected.

Laplacian Pyramid GAN (LAPGAN): This laplacian pyramid network is a linear invertible image representation consisting of a set of band-pass images, spaced an octave apart, plus a low-frequency residual. This approach uses multiple numbers of Generators and Discriminators and different levels of the Laplacian Pyramid networks. This approach is mainly used because it produces more high-quality images. An image is down-sampled at first at each layer of the pyramid and then it is again up-scaled at each layer in a backward pass where the image acquires some noise from the Conditional GAN network at these layers until it reaches its original size.

Super Resolution GAN (SRGAN): The SRGAN as the name suggests is a way of designing a GAN in which a deep neural network is used along with an adversarial network in order to produce higher resolution images. This type of GAN is particularly useful in optimally up-scaling native low-resolution images to enhance its details minimizing errors while doing so.

CHAPTER 6

SYSTEM SOFTWARE

6.1 MATLAB

MATLAB is a high-performance and proprietary multi-paradigm programming language for technical computing. Matlab was developed by MathWorks.it allows matrix manipulations, computation, plotting of functions and data, visualization, implementation of algorithms, creation of user interfaces and interfacing with programs written in other languages. Typical uses include:

- Math and computation
- Algorithm development
- Modeling, simulation, and prototyping
- Data analysis, exploration, and visualization
- Scientific and engineering graphics
- Application development, including Graphical User Interface building

MATLAB is an interactive system whose basic data element is an array that does not require dimensioning. This allows us to solve many technical computing problems, especially those with matrix and vector formulations, in a fraction of the time it would take to write a program in a scalar non-interactive language such as C or Fortran.

The name MATLAB stands for matrix laboratory. MATLAB was originally written to provide easy access to matrix software developed by the LINPACK and EISPACK projects, which together represent the state-of-the-art in software for matrix computation.

MATLAB has evolved over a period of times with input from many users. In university environments, it is the standard instructional tool for introductory and advanced courses in mathematics, engineering, and science. In industry, MATLAB is the tool of choice for high-productivity research, development, and analysis.

MATLAB features is a family of application-specific solutions called toolboxes. Very important to most users of MATLAB, toolboxes allows us to learn and apply

specialized technology. Toolboxes are comprehensive collections of MATLAB functions (M-files) that extend the MATLAB environment to solve particular classes of technical problems. Areas in which toolboxes are available include signal processing, control systems, neural networks, fuzzy logic, wavelets, simulation, and many others.

6.1.1 THE MATLAB SYSTEM

The MATLAB system consists five major parts:

THE MATLAB LANGUAGE.

The MATLAB language is a high-level matrix or array language with control flow statements, functions, data structures, input or output and object- oriented programming features. It allows the pair "programming in the small" to rapidly create fast and dirty throw-away programs and "programming in the large" to create finish large and complex application programs.

THE MATLAB WORKING ENVIRONMENT.

The MATLAB working environment is the set of tools and facilities that you work with as the MATLAB user or programmer. It includes facilities for control the variables in your workspace and importing and exporting data. It as well as includes tools for developing, managing, debugging and profiling M-files, MATLAB's applications.

HANDLE GRAPHICS

Handle Graphics is the MATLAB graphics system. It comprise high-level commands for two-dimensional and three-dimensional data visualization and image processing and animation and presentation graphics. It as well as includes low-level commands that allow you to fully customize the appearance of graphics .It also to build finish Graphical User Interfaces on your MATLAB applications.

THE MATLAB MATHEMATICAL FUNCTION LIBRARY

The MATLAB mathematical function library is a huge group of computational algorithms ranging from elementary functions like sum, sine, cosine and

complex arithmetic, to more sophisticated functions like matrix inverse and matrix eigenvalues and Bessel functions and fast Fourier transforms.

THE MATLAB APPLICATION PROGRAM INTERFACE (API)

This is a library .It allows you to write C and Fortran programs that interact with MATLAB. It includes amenity for calling routines from MATLAB (dynamic linking), calling MATLAB as a computational engine and for reading and writing MAT-files.

6.1.2 MATLAB'S POWER OF COMPUTATIONAL MATHEMATICS

MATLAB is used in each and every facet of computational mathematics. Following are some commonly used mathematical calculations where it is used most commonly –

1. Dealing with Matrices and Arrays
2. 2-D and 3-D Plotting and graphics
3. Linear Algebra
4. Algebraic Equations
5. Non-linear Functions
6. Statistics
7. Data Analysis
8. Calculus and Differential Equations
9. Numerical Calculations
10. Integration
11. Transforms
12. Curve Fitting
13. Various other special functions

6.1.3 FEATURES OF MATLAB

Following are the basic features of MATLAB –

- MATLAB is a high-level language for numerical computation, visualization and application development.

- MATLAB provides also an interactive environment for iterative exploration, design and problem solving.
- MATLAB provides huge library of mathematical functions for linear algebra, statistics, Fourier analysis, filtering, optimization, numerical integration and solving ordinary differential equations.
- MATLAB provides built-in graphics for visualizing data and tools for creating custom plots.
- MATLAB's programming interface gives development tools for improving code quality maintainability and maximizing performance.
- MATLAB provides tools for building applications with custom graphical interfaces.
- MATLAB provides functions for integrating MATLAB based algorithms with external applications and languages such as C, Java, .NET and Microsoft Excel.

6.1.4 USES OF MATLAB

MATLAB is widely used as a computational tool in science and engineering encompassing the fields of physics and chemistry and math and all engineering streams. MATLAB is used in a range of applications including –

- Signal Processing and Communications
- Image and Video Processing
- Control Systems
- Test and Measurement
- Computational Finance
- Computational Biology

6.1.5 LOCAL ENVIRONMENT SETUP

Setting up MATLAB environment is a matter of just few clicks to install. The installer will be downloaded from [here](#).

Math Works provides the licensed product, a trial version as well a student version. You need to log into the site and wait a couple of minutes or seconds for their approval.

After downloading the installer and the software can be installed through just few clicks

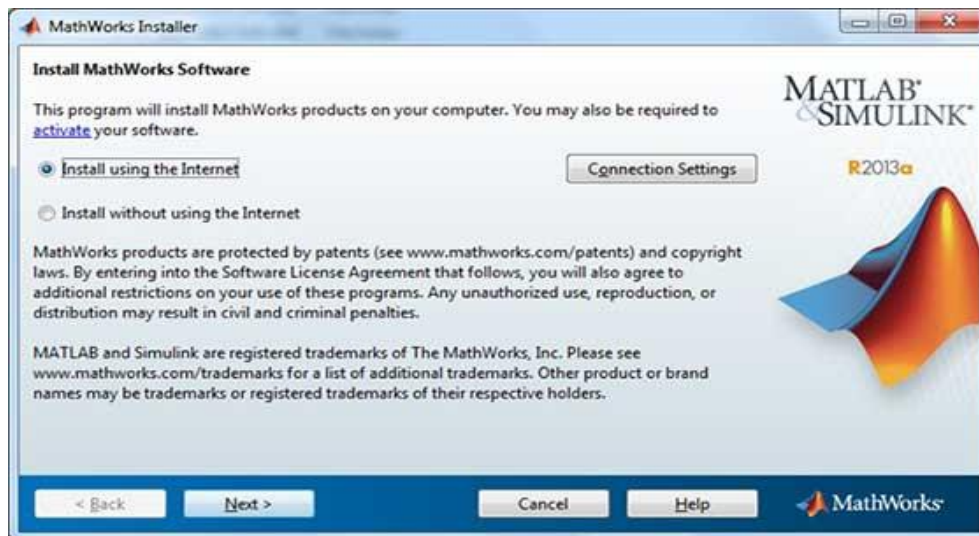


Fig.No:6.1 Matlab Install Page

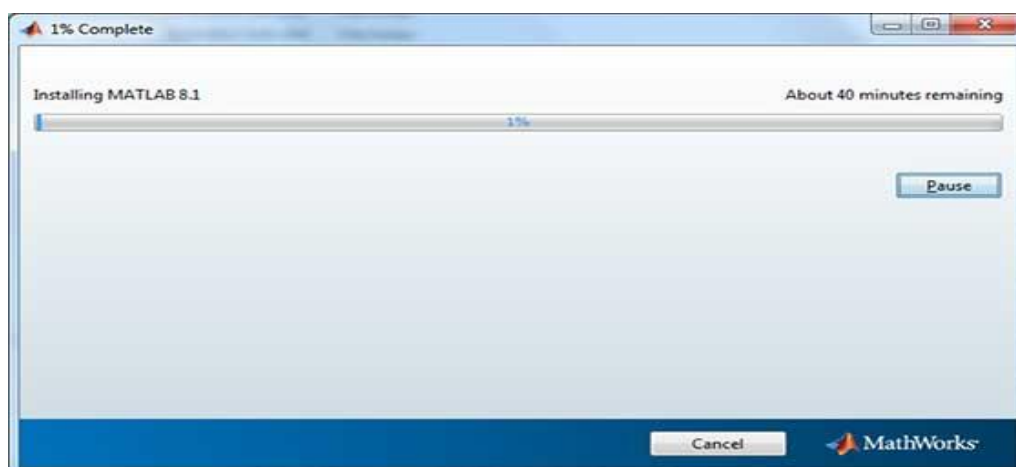


Fig.No:6.2 Installing Page

6.1.6 UNDERSTANDING THE MATLAB ENVIRONMENT

MATLAB development IDE could be launched from the icon created on the desktop. The major working window in MATLAB is called the desktop. Whenever MATLAB is started, the desktop appears in its default layout –

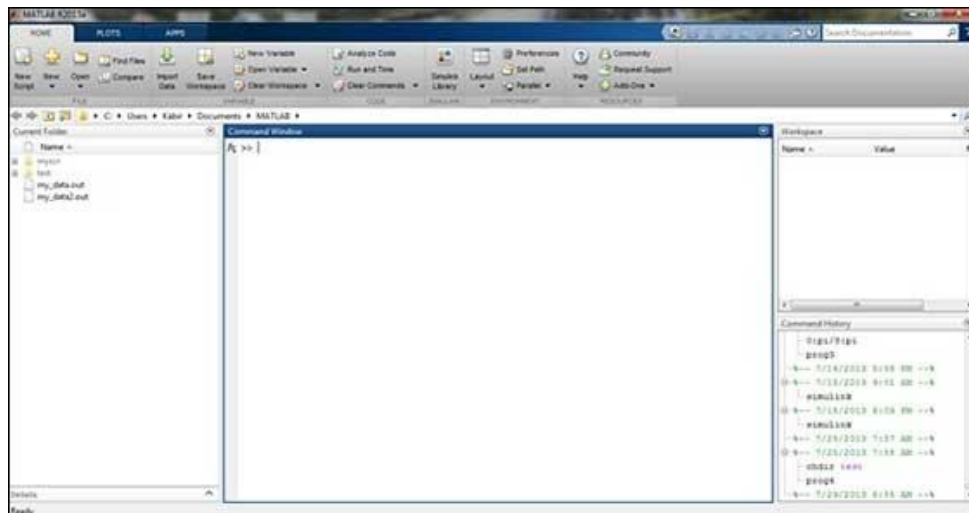


Fig.No:6.3 Matlab Window

The desktop has the following panels –

- **Current Folder** – This panel allows you to access the project folders and files.



Fig.No:6.4 Folder Page

- **Command Window** – This is the major area where commands can be entered at the command line. Command Window is indicated by the command prompt (>>).

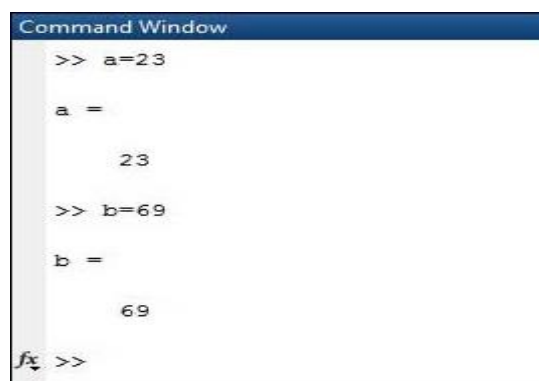
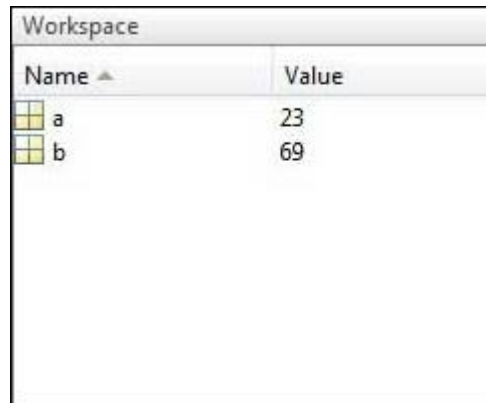


Fig.No:6.5 Command Window

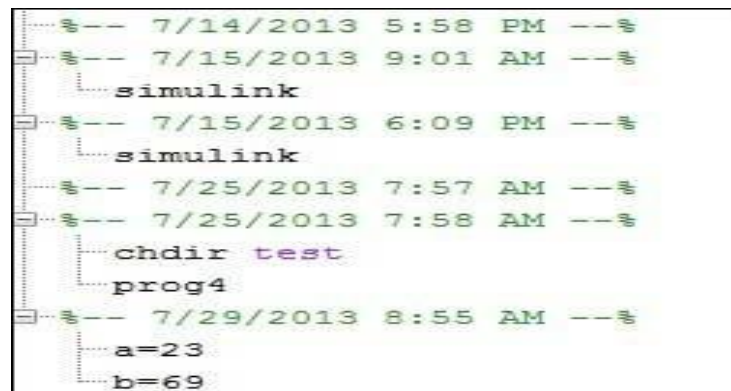
- **Workspace** –It shows all the variables created and/or imported from files.



Workspace	
Name ▲	Value
a	23
b	69

Fig.No:6.6 Workspace

- **Command History** – The Command History panel shows or return commands that are entered at the command line.



```

$-- 7/14/2013 5:58 PM --$
$-- 7/15/2013 9:01 AM --$
simulink
$-- 7/15/2013 6:09 PM --$
simulink
$-- 7/25/2013 7:57 AM --$
$-- 7/25/2013 7:58 AM --$
chdir test
prog4
$-- 7/29/2013 8:55 AM --$
a=23
b=69

```

Fig.no:6.7 program window

Set up GNU Octave

If you are interest to use Octave on your machine (Linux, BSD, OS X or Windows), then warmly download latest version from Download GNU Octave. You could check the given installation instructions for your machine.

6.1.7 THE M FILES

MATLAB allows writing two Types of program files –

Scripts – this files are program files with .m extension. Script files, you write series of commands, which you want to execute together in program. Scripts

do not accept inputs and do not return any outputs. They operate on data in the workspace.

Functions – these files are also like program files with .m extension. Functions could accept inputs and return outputs. Internal variables are local to the function file.

You can use the MATLAB editor or any further text editor to create your m-files. In this section, we will discuss about the script files. A script file contains more sequential lines of MATLAB commands and function calls. You could run a script by typing its name at the command line.

6.1.8 APPLICATIONS OF MATLAB

MATLAB could be used as a tool for simulating various electrical networks but the recent developments in MATLAB make it a very competitive tool for Artificial Intelligence, Robotics, Image processing, Wireless communication, Machine learning, Data analytics and whatnot. Though it's mostly used by circuit branches and mechanical in the engineering domain to solve a basic set of problems its application is broad. MATLAB is a tool that enables computation, programming and graphically visualizing the results.

The basic data element of MATLAB as the name suggests is the Matrix/array. MATLAB toolboxes are professionally built. It enables you to turn your imaginations into reality. MATLAB programming is somewhat similar to C programming and just requires a little brush up of your basic programming skills to start working with.

Below are a few applications of MATLAB –

Statistics and machine learning (ML)

This toolbox in MATLAB could be very handy for the programmers. Statistical methods such as descriptive/inferential can be easily implemented. So is the case with machine learning. Various models could be employed to solve modern-day problems. The algorithms used can also be used for big data applications.

CURVE FITTING

This toolbox helps to analyze the pattern of occurrence of data. After a particular trend which could be a curve or surface is obtained, its future trends could be predicted. Further plotting and calculating integrals and derivatives and interpolation, etc. can be done.

Control systems

Systems nature could be obtained. Factors such as closed-loop and open-loop and its controllability and observability and bode plot, Nyquist plot, etc. can be obtained. Various controlling techniques such as PD and PI and PID could be visualized. Analysis could be done in the time domain or frequency domain.

Signal Processing

Signals and systems, digital signal processing are taught in various engineering streams but MATLAB provides the opportunity for proper visualization of this. Various transforms such as Laplace and Z, etc. could be done on any given signal. Theorems could be validated. Analysis could be done in the time domain or frequency domain. There are multiple built-in functions that could be used.

Mapping

Mapping has multiple applications in various domains. For example, in Big data and the MapReduce tool is quite important which has multiple applications in the real world. Theft analysis or financial fraud detection and regression models and contingency analysis and predicting techniques in social media and data monitoring, etc. could be done by data mapping.

Deep learning

Deep learning is a subclass of machine learning which can be used for speech recognition, financial fraud detection and medical image analysis. Tools such as time-series, Artificial neural network (ANN) and Fuzzy logic or combination of such tools can be employed.

Financial analysis

An entrepreneur before starting any endeavor needs to do a proper survey and the financial analysis in order to plan the course of action. The tools needed for this are all available in MATLAB. Elements such as profitability and solvency and liquidity and stability can be identified. Business valuation, capital budgeting and cost of capital, etc. can be evaluated.

Image processing

The most common application that we observe almost every day are bar code scanners and selfie (face beauty, blurring the background, face detection), image enhancement, etc. The digital image processing also plays quite an important role in transmitting data from far off satellites, receiving, decoding it in the same way. Algorithms to support all such applications are available.

Text analysis

Based on the text, sentiment analysis could be done. Google gives millions of search results for any text entered within a fraction of second. All this is viable because of text analysis. Handwriting comparison in forensics could be done. No limit to the application and just one software which could do this all.

Electric vehicles designing

Used for modelling electric vehicles, analyse their performance with a change in system inputs. Speed torque comparison and designing and simulating of a vehicle, whatnot.

Aerospace

This toolbox in MATLAB is used for analysing the navigation, to visualize flight simulator.

Audio toolbox

Provides tools for audio processing and speech analysis and acoustic measurement. It as well as provides algorithms for audio and speech feature extraction and audio signal transformation.

6.2 PYQT5

This is the latest version of a GUI widgets toolkit developed by Riverbank Computing. PYQT5 is a Python interface for Qt, one of the most powerful and popular cross-platform GUI libraries. It is a blend of Python programming language and the Qt library. This introductory tutorial will assist you in creating graphical applications with the help of PyQt.

PyQt is a GUI widgets toolkit. It is a Python interface for Qt, one of the most powerful, and popular cross-platform GUI libraries.. The latest version of PyQt could be downloaded from its official website – riverbankcomputing.com

PyQt API is a set of modules containing a more number of classes and functions. While QtCore module contains non-GUI functionality for working with file, directory etc., QtGui module contains all the graphical controls. In addition, there are modules for working with XML (QtXml) and SVG (QtSvg) and SQL (QtSql), etc.

Regularly/Frequently used modules is given below –

- QtCore – Core non-GUI classes used by other modules
- QtGui – Graphical user interface components
- QtMultimedia – This Classes for low-level multimedia programming
- QtNetwork – Classes for network programming
- QtOpenGL – OpenGL support classes
- QtScript – This Classes for evaluating Qt Scripts
- QSql – This Classes for database integration using SQL
- QtSvg – This Classes for displaying the contents of SVG files
- QtWebKit – This Classes for rendering and editing HTML
- QtXml – Classes for handling XML
- QtWidgets – This Classes for creating classic desktop-style UIs

- QtDesigner – Classes for extending Qt Designer

6.2.1 SUPPORTING ENVIRONMENTS

PyQt is compatible with all the popular operating systems including Windows and Linux and Mac OS. It is dual licensed and available under GPL as well as commercial license. The latest stable version is PyQt5-5.13.2.

Windows

Wheels for 32-bit or 64-bit architecture are provided that are more compatible with Python version 3.5 or later. The recommended way to install is using PIP utility –**pip3 install PyQt5**. To install development tools such as Qt Designer to support PyQt5 wheels and following is the command –**pip3 install pyqt5-tools**

You can as well as build PyQt5 on Linux/macOS from the source code www.riverbankcomputing.com/static/Downloads/PyQt5



Fig No 6.8 Qmain Window

The PyQt installer comes with a GUI builder tool called Qt Designer. Using its simple drag and drop interface and a GUI interface could be quickly built without having to write the code. It is however, not an IDE such as Visual Studio. Hence, Qt Designer does not have the facility to debug and build the application.

Start Qt Designer application which is a portion of development tools and installed in scripts folder of the virtual environment.

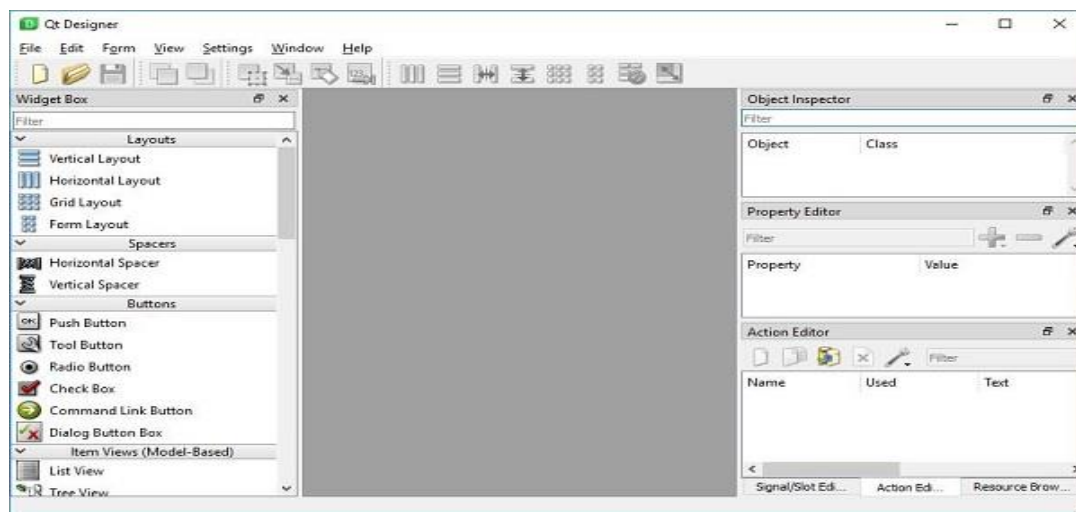


Fig No 6.9 PYQT5 Main Window

Start designing GUI interface by choosing File → new menu.

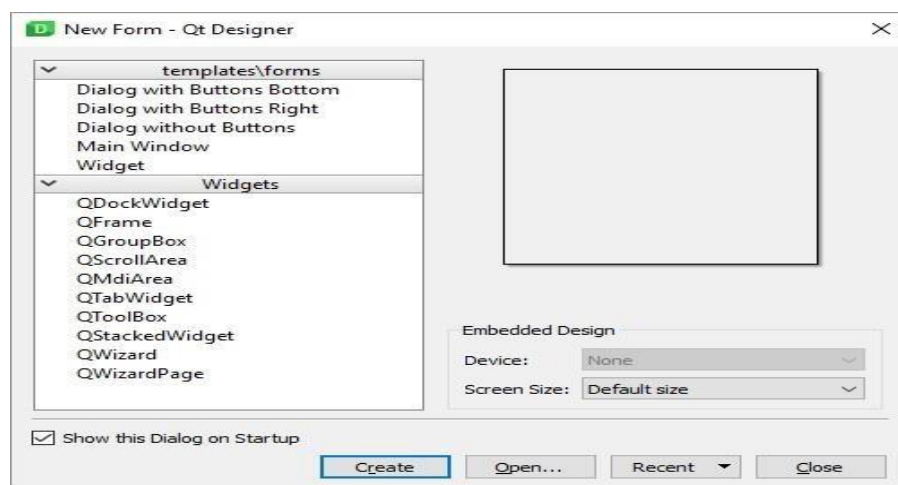


Fig no 6.10 dialog box

You could then drag and drop required widgets from the widget box on the left pane. You can as well as assign value to properties of widget laid on the form.

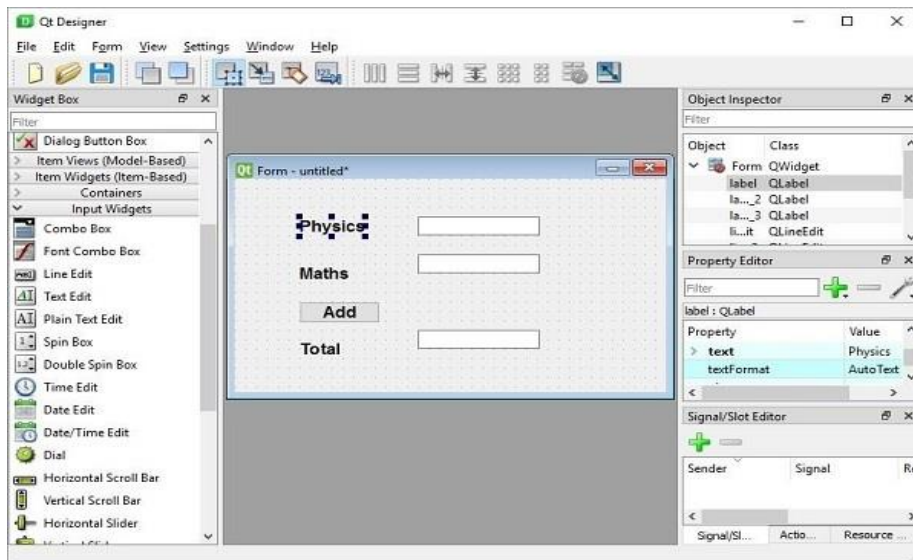


Fig No 6.11 Form Page

The designed form is saved as demo.ui. This ui file contains XML representation of widgets, their properties in the design. This design is changed into Python equivalent by using pyuic5 command line utility. This utility is a wrapper for uic module of Qt toolkit. The use of pyuic5 is as follows **-pyuic5 -x demo.ui -o demo.py**

In the above command, -x switch adds a little amount of additional code to the generated Python script (from XML) so that it becomes a self-executable standalone application.

```
if __name__ == "__main__":
```

```
    Import sys
```

```
    App = QtGui.QApplication(sys. argv)
```

```
    Dialog = QtGui.QDialog()
```

```
    ui = Ui_Dialog()
```

```
    ui. setupUi(Dialog)
```

```
    Dialog. Show ()
```

```
    sys. exit (app. exec_ ())
```

The resultant python script is executed to show the following dialog box –

Python demo.py

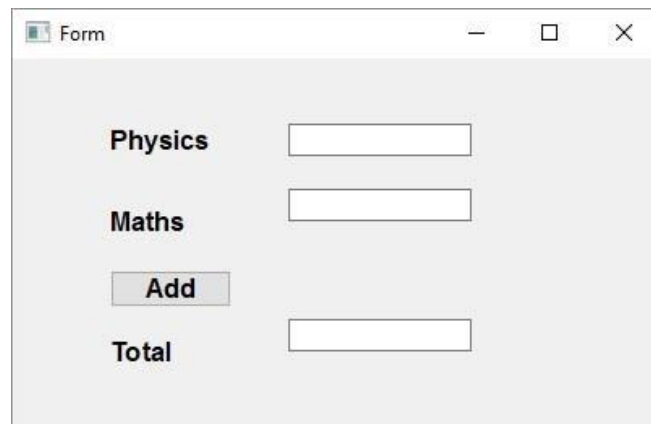


Fig no 6.12 form window

The user could input data in input fields but clicking on Add button will not generate any action as it is not associated with any function. Reacting to user-generated response is called as event handling.

Unlike a console mode application, which is executed in a sequential manner and a GUI based application is event driven. Functions /methods are executed in response to user's actions like clicking on a button and selecting an item from a collection or a mouse click etc., called events.

Widgets used to build the GUI interface act as the source of such events. Each PyQt widget, which is derived from QObject class and is designed to emit 'signal' in response to one or more events. The signal on its own does not perform any movement. Instead, it is 'connected' to a 'slot'. The slot could be any callable Python function.

Using Qt Designer's Signal/Slot Editor

First design a simple form with a Line Edit control and a Pushbutton.

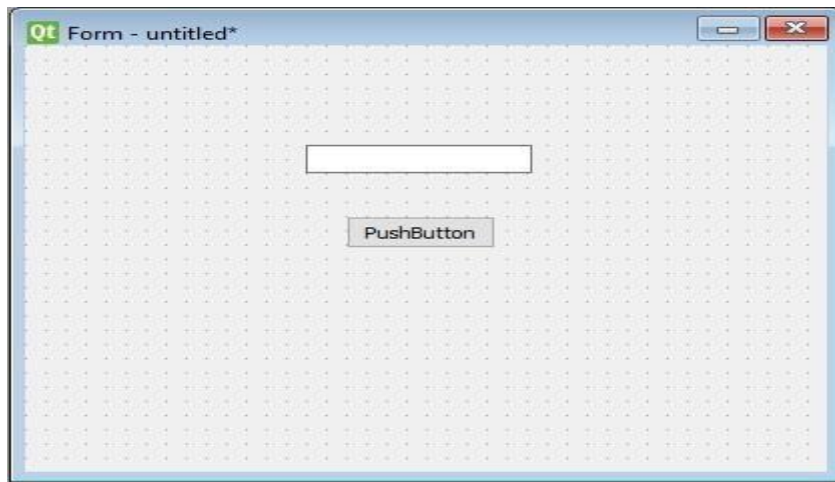


Fig No 6.13 Design Page

It is desired that if button is pressed, contents of text box should be erased. The QLineEdit widget has a `clear ()` method for this purpose. Hence, the button's clicked signal is to be connected to `clear ()` method of the text box.

To start with, choose Edit signals/slots from Edit menu or press F4. Then highlight the button with mouse, drag the cursor towards the textbox

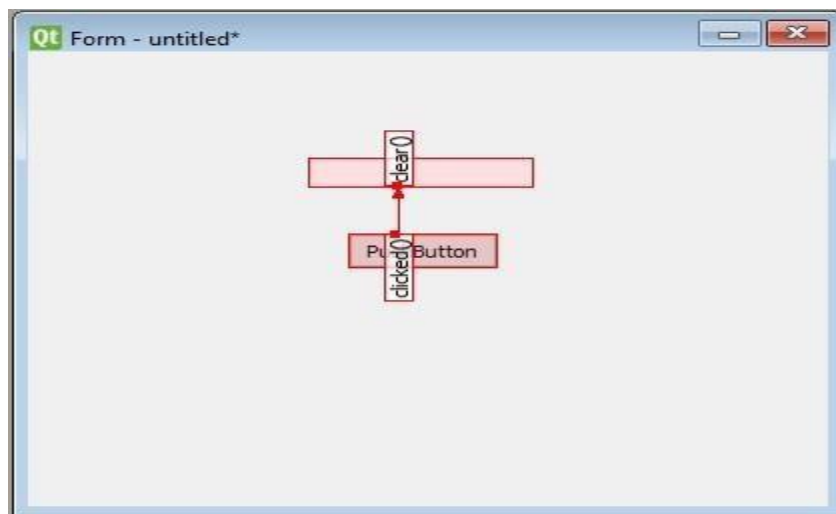


Fig no: 6.14 Form design page

As the mouse is released, a dialog showing signals of button and methods of slot will be displayed. Select clicked signal and `clear ()` method

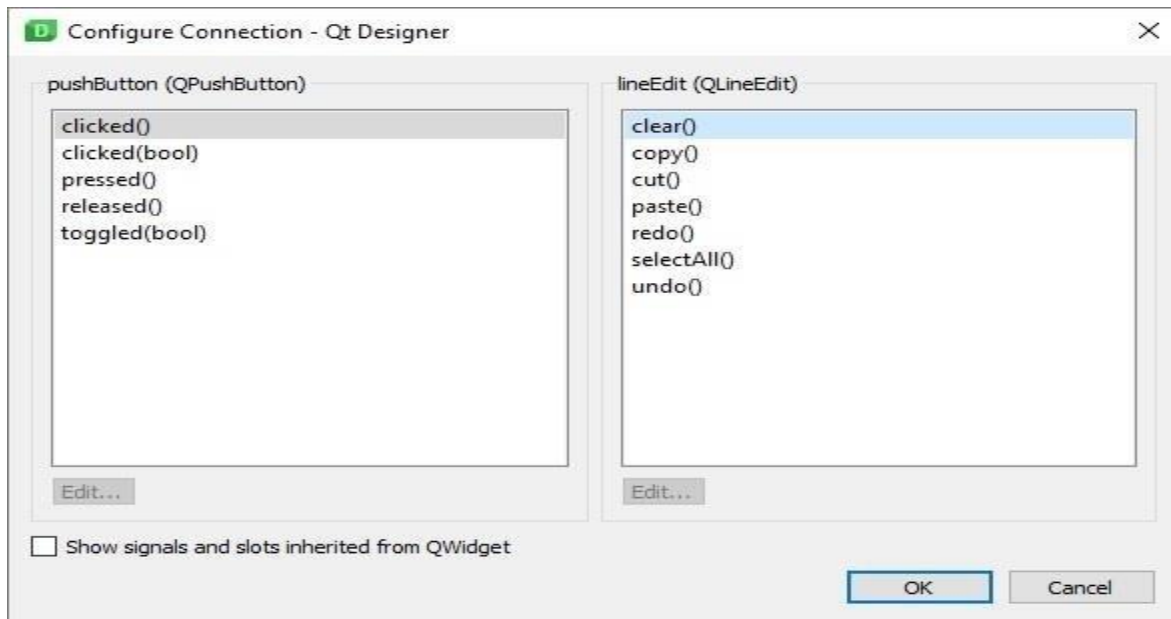


Fig No 6.15 Editing Page

6.2.2 ADVANTAGES OF USING PYQT

Coding versatility –GUI programming with Qt is built around the idea of signals, slots for creating contact between objects. It allows versatility in dealing with GUI incidents which results in a smoother code base.

More than a framework: Qt uses a broad variety of native platform APIs for networking and database development and more. This provides primary access to them through a special API.

Various UI components: Qt provides multiple widgets and such as buttons or menus and all designed with a basic interface for all compatible platforms.

Various learning resources: As PyQt is one of the most commonly used UI systems for Python, you can conveniently access a broad variety of documentation.

6.2.3 DISADVANTAGES OF USING PYQT

- Lack of Python-specific documentation for classes in PyQt5
- It takes a lot of time to grasp all the specifics of PyQt, meaning it's a pretty steep learning curve.

- If the application is not open-source, you must pay for a commercial license.

6.3 PYTHON

- Python is currently the most widely used multi-purpose, high-level programming language.
- Python allows programming in Object-Oriented and Procedural paradigms.
- Python programs generally are smaller than other programming languages like Java. Programmers have to type relatively less and indentation requirement of the language, makes them readable all the time.
- Python language is being used by almost all tech-giant companies like – Google, Amazon, Facebook, Instagram, Dropbox, and Uber... etc.
- The biggest strength of Python is huge collection of standard library which can be used for the following:
 - Machine Learning
 - GUI Applications (like Kivy, Tkinter, and PyQt etc.)
 - Web frameworks like Django (used by YouTube, Instagram, and Dropbox)
 - Image processing (like OpenCV, Pillow)
 - Web scraping (like Scrapy, BeautifulSoup, and Selenium)
 - Test frameworks
 - Multimedia
 - Scientific computing
 - Text processing and many more.

CHAPTER 7

HARDWARE SPECIFICATION

7.1 I5 PROCESSOR

As we all know that Intel is the renowned company that manufactures the processors since 1940s. Every year they introduce different versions of the processors that have more advanced, the new features as compared to the previous one. After the introducing i5 processors, Intel introduced i5 core processors and increases the family members of I series of the processors. It was invented in 2009 as a result of the advanced theories, for the sake to meet the challenges of the modern, latest technologies.

7.1.1 ABOUT-CORE I5

Developed and manufactured by Intel, the Core i5 is a computer processor and available as dual-core or quad-core. It could be used in both desktop and laptop computers and is one of four types of processors in the "i" (Intel Core family) series. The first i5 processor was released in September 2009, new generations of the i5 continue to be released (2020).

The Core i5 processor is available in multiple speeds and ranging from 1.90 GHz up to 3.80 GHz and it features 3 MB and 4 MB or 6 MB of cache. The Core i5 utilizes either the LGA 1150 or LGA 1155 socket on a motherboard. Core i5 processors are most often found as quad-core and having four cores. However, a select few high-end Core i5 processors feature six cores.

The most common type of RAM used with a Core i5 processor is DDR3 1333 or DDR3 1600. However, higher performance RAM could be used as well if it's supported by the motherboard.



Fig No 7.1 Core I5 Processor

Power usage varies for the Core i5 processors:

- Slower speeds (1.90 gigahertz to 2.30 gigahertz) use 11.5 W of power
- Medium speeds (2.60 gigahertz to 3.10 gigahertz) use 15 W, 25 W, 28 W or 37 W of power
- Faster speeds (3.20 gigahertz to 3.80 gigahertz) use 35 W, 37 W, 45 W, 47 W, 65 W or 84 W of power

Core i5 processors are commonly found in desktop computers for most everyday use, some higher performance needs. Some laptop computers feature Core i5 processors also to provide improved performance for heavier usage needs. At the lower speeds and battery usage is pretty conservative and can reach up to five hours or usage on a single charge. However, at higher speeds, battery usage is higher and may result in up to three hours or so of usage per charge.

7.1.2 TECHNICAL SPECIFICATIONS OF I5 PROCESSORS:

I5 processors basically introduced to manage the different strategies between the low and the advanced working. Some of the technical specifications of the i5 processors that deal with the performing or working capacity and the technicalities of operation of the i5 processors in the computer system are listed below.

1. i5 processors have ability to work with integrated memory and can enhance the performance of the applications. The increase the memory up to 1333 MHz
2. As i5 processors have high speed performing rate so they are able to perform at the maximum CPU rate of 3.6 GHz
3. Turbo technology is present in the device that boosts up the working speed of the computational systems.
4. It also provides the 64-bit architecture for the users for the reliable and much faster working.
5. Micro architecture for the i5 processors was presented by the Nehalem and these processors have a cache rate up to 8 MB.

7.2 RAM

RAM (Random Access Memory) is the hardware in a computing device where the operating system (OS), application programs, data in current use are kept so they could be quickly reached by the device's processor. RAM is the major/important memory in a computer. It is much faster to read from and write to than other kinds of storage, such as a hard disk drive (HDD) and solid-state drive (SSD) or optical drive. RAM is volatile. That means data is retained in RAM as long as the computer is on, but it is lost when the computer is turned off. When the computer is rebooted and the OS and other files are reloaded into RAM, usually from an HDD or SSD.

7.2.1 Functions of RAM

Because of its volatility, RAM could not store permanent data. RAM could be compared to a person's short-term memory and a hard disk drive to a person's long-term memory. Short-term memory is focused on immediate work but it could only keep a limited number of facts in view at any one time. When a person's short-term

memory fills up, it could be refreshed with facts stored in the brain's long-term memory.

A computer also works this way. If RAM fills up, the computer's processor must repeatedly go to the hard disk to overlay the old data in Random Access Memory with new data. This process slows the computer's operation.

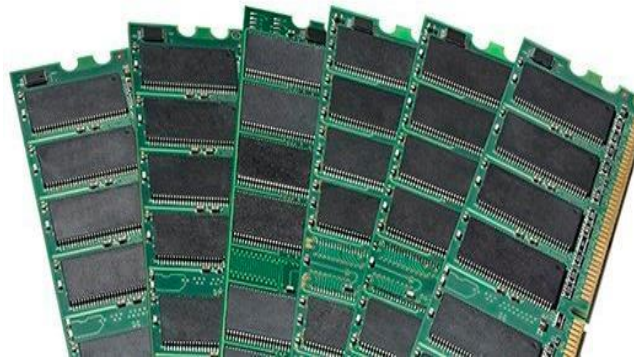


Fig.No:7.2 RAM Modules

A computer's hard disk could become completely full of data and unable to take any more, but RAM won't run out of memory. However, the combination of RAM and storage memory could be completely used up.

How does RAM work

The term random access as applied to RAM comes from the fact that any storage location, also known as any memory address, could be accessed directly. Originally, the term Random Access Memory was used to distinguish regular core memory from offline memory.

Offline memory typically referred to magnetic tape from which a specific piece of data could only be accessed by locating the address sequentially and starting at the beginning of the tape. RAM is organized and controlled in a way that enables data to be stored and retrieved directly to and from specific locations.

Other types of storage — such as the hard drive, CD-ROM—are also accessed directly or randomly, but the term random access is not used to describe these other types of storage.

RAM is similar in concept to a set of boxes in which each box could hold a 0 or a 1 and each box has a unique address that is found by counting across the columns, down the rows. A set of RAM boxes is called an array, each box is known as a cell.

To find a specific cell, the Random Access Memory controller sends the column, row address down a thin electrical line etched into the chip. Each row and column in a Random Access Memory array has its own address line. Any data that's read flows back on a separate data line.

Random Access Memory array is physically small .It stored in microchips. Random Access Memory array also small in terms of the amount of data it could hold. A typical laptop computer may come with 8 gigabytes of RAM, while a hard disk could hold 10 terabytes.

A hard drive, on the other hand and stores data on the magnetized surface of what looks like a vinyl record. Alternatively, an SSD stores data in memory chips that, unlike Random Access Memory, are nonvolatile. They don't depend on having constant power and won't lose data once the power is turned off data won't lose . Random Access Memory microchips are gathered together into memory modules. These plug into slots in a computer's motherboard. A bus, or a set of electrical paths, is used to connect the motherboard slots to the processor.

Most PCs enable users to add Random Access Memory modules up to a certain limit. Having more Random Access Memory in a computer cuts down on the number of times the processor must read data from the hard disk, an operation that takes longer than reading data from RAM. Random Access Memory access time is in nanoseconds, while storage memory access time is in milliseconds.

7.2.2 TYPES OF RAM

RAM comes in two primary forms:

- **Dynamic Random-Access Memory (DRAM)** makes up the typical computing device's Random Access Memory and as was previously noted, it needs that power to be on to retain stored data.

Each Dynamic Random-Access Memory cell has a charge or lack of charge held in an electrical capacitor. This data must be constantly refreshed with an electronic charge every few milliseconds to compensate for leaks from the capacitor. A transistor serves as a gate and determining whether a capacitor's value could be read or written.

- **Static Random-Access Memory (SRAM)** also needs constant power to hold on to data, but it doesn't need to be continually refreshed the way Dynamic Random-Access Memory does.

In Static Random-Access Memory, instead of a capacitor holding the charge and the transistor acts as a switch, with one position serving as 1 and the other position as 0. Static Random Access Memory requires several transistors to retain one bit of data compared to dynamic Random Access Memory which needs only one transistor per bit. As a result, SRAM chips are much larger and more expensive than an equivalent amount of DRAM.

However, Static Random Access Memory is significantly faster and uses less power than DRAM. The price and speed differences mean static Random Access Memory is mainly used in small amounts as cache memory inside a computer's processor.

7.2.3 RAM VS VIRTUAL MEMORY

A computer could run short on memory and especially when running multiple programs simultaneously. Operating systems could compensate for physical memory shortfalls by creating virtual memory.

With virtual memory and data is temporarily transferred from Random Access Memory to disk storage and virtual address space is increased using active memory in RAM and inactive memory in an HDD to form contiguous addresses that hold an application and its data. Using virtual memory, a system could load larger programs/ multiple programs running at the same time, letting each operate as if it has infinite memory without having to add more Random Access Memory.

Virtual memory is able to handle twice as many addresses as Random Access Memory. A program's instructions, data are initially stored at virtual addresses and once the program is executed, those addresses are turned into actual memory addresses.

One downside to virtual memory is that it could slow a computer because data must be mapped between the virtual and physical memory. With physical memory alone, programs work directly from Random Access Memory.

7.2.4 RAM VS FLASH MEMORY

Flash memory and Random Access Memory are both comprised of solid-state chips. However, they play different roles in computer systems because of differences in the way they're made, their performance specifications and cost. Flash memory is used for storage memory. Random Access Memory is used as active memory that performs calculations on the data retrieved from storage.

8.1 ORIGINAL DATA

Vaccine Name : Covishield
Date of Dose : 15 March 2021 (1st Dose) & 15 June 2021(2nd Dose)
Vaccinated by : R Gayathri
Vaccination at : Begarahalli APHC, Dharmapuri, Tamil Nadu

8.2 ENCRYPTED DATA

[illegible]

CHAPTER 9

CONCLUSION

Using internet and network are increasing rapidly. Everyday a lot of digital data have been exchanging among users. Some of the data is more sensitive that need to protect from intruders. Cryptography is one of the study of secure communications technique that uses mathematics to encrypt and decrypt data. In cryptography we can store information and also we can transmit it over the internet and only the recipient can read this. Pretty Good Privacy (PGP) is data encryption and decryption technique that presents the cryptographic privacy and the verification for data delivery. It is also used to lock up the email communication. PGP is also used for the security purposes. The usage of PGP is mostly in encrypting and decrypting the texts. Security of DES is good. It uses subroutines. There are two permutations which are used in encryption method with starting and final permutation. There are 16 Festal round in the structure of DES. It is used to lock up almost all types of data. Triple DES is based on the DES Encryption algorithms play vital roles to protect original data from unauthorized access. But the advanced version of DES algorithm is AES algorithm that is Advanced Encryption Standard. DES is now considered to be insecure for some applications like banking system. There are also some analytical results which demonstrate theoretical weaknesses in the cipher. For that purpose we are using AES algorithm. It is an efficient algorithm to secure the data. Various kind of algorithms are existing to encrypt data. Advanced encryption standard (AES) algorithm is one of the efficient algorithm and it is widely supported and adopted on hardware and software. This algorithm enables to deal with different key sizes. According to the results shows that AES has the ability to provide much more security compared to other algorithms like DES, 3DES etc.

We conclude this section, the AES algorithm computes much faster than RSA in execution and implementation. RSA algorithm is reliable for key exchange management but it's not very efficient in terms of performance and cost factor. RSA's strengths and weaknesses remain in the factoring large integers. AES's strength remains in the possible key permutations using Rijndael finite field method.

CHAPTER 10

REFERENCES

- [1] Abdullah, A. M., & Aziz, R. H. H. (2019, June). New Approaches to Encrypt and Decrypt Data in Image using Cryptography and Steganography Algorithm., International Journal of Computer Applications, Vol. 143, No.4 (pp. 11-17).
- [2] Singh, G. (2018). A study of encryption algorithms (RSA, DES, 3DES and AES) for information security. International Journal of Computer Applications, 67(19).
- [3] Gaj, K., & Chodowiec, P. (2017, April). Fast implementation and fair comparison of the final candidates for Advanced Encryption Standard using Field Programmable Gate Arrays. In Cryptographers' Track at the RSA Conference (pp. 84-99). Springer Berlin Heidelberg.
- [4] Stallings, W. (2018). Cryptography and network security: principles and practices. Pearson Education India.
- [5] Yenuguvanilanka, J., & Elkeelany, O. (2020, April). Performance evaluation of hardware models of Advanced Encryption Standard (AES) algorithm. In Southeastcon, 2020. IEEE (pp. 222- 225).
- [6] Niveditha, V. R., and T. V. Ananthan. "Improving Acknowledgement in Android Application." Journal of Computational and Theoretical Nanoscience 16.5-6 (2019): 2104-2107.
- [7] Sundaram, P. S. S., Basker, N. H., & Natrayan, L. (2019). Smart Clothes with Bio-sensors for ECG Monitoring. International Journal of Innovative Technology and Exploring Engineering, 8(4), 298-301
- [8] Magesh, S., et al. (2020) "Concepts and Contributions of Edge Computing in Internet of Things (IoT): A Survey." 146 –156. DOI: 10.22247/ijcna/2020/203914
- [9] Paranthaman V, K. Shanmuga Sundaram, and L. Natrayan. Influence of SiC Particles on Mechanical and Microstructural Properties of Modified Interlock Friction Stir Weld Lap Joint for Automotive Grade Aluminium Alloy. Silicon (2021): 1-11.

- [10] Rammohan, S. R., Jayashri, N., Bivi, M. A., Nayak, C. K., & Niveditha, V. R. (2020). High performance hardware design of compressor adder in DA based FIR filters for hearing aids. *International Journal of Speech Technology*, 1-8.
- [11] Renu Mary Daniel, Elijah Blessing, Rajsingh & SalajaSilas (2017), "Analysis of hierarchical identity based encryption schemes and its applicability to computing environments ", *Journal of Information Security and Applications*", Vol. 36, pp. 20-31.
- [12] Natrayan L, and M. Senthil Kumar. "An integrated artificial neural network and Taguchi approach to optimize the squeeze cast process parameters of AA6061/Al₂O₃/SiC/Gr hybrid composites prepared by novel encapsulation feeding technique." *Materials Today Communications* 25 (2020): 101586.
- [13] Magesh, S., et al. (2020) "Pervasive computing in the context of COVID-19 prediction with AI-based algorithms. " *International Journal of Pervasive Computing and Communications*, 15(5); 477-487.
- [14] Maithilee Joshi, Karuna P. Joshi & Tim Fin in (2018), Attribute Based Encryption for Secure Access to Cloud Based EHR Systems, *IEEE 11th International Conference on Cloud Computing*, pp. 932-935.
- [15] Snehal Pise(2018) Security of Personal Health Records through Attribute Based Encryption in Cloud Computing, *International Journal Of Engineering Research & Technology*, Vol. 03, No. 01, pp. 1952-1954.
- [16] Livinus Obiora Nweke, Prosper Yeng, Stephen D. Wolthusen & Bian Yang (2020), "Understanding Attribute-based Access Control for Modelling and Analysing Healthcare Professionals' Security Practices", *(IJACSA) International Journal of Advanced Computer Science and Applications*, Vol. 11, No. 2, 2020, pp. 683-690.
- [17] A. Akhtar, M. Zia, and U. Baig, "Enhancing the security of simplified DES algorithm using transposition and shift rows," *International Journal of Computer Science and Software Engineering*, 6(5), 2017, pp. 115-119.
- [18] U. Gupta, S. Saluja, and T. Tiwari, "Enhancement of cloud security and removal of anti-patterns using multilevel encryption algorithms," *Int. J. Recent Res. Asp.*, 5(1), 2018, pp. 55-61.

- [19] S. Singh and S. Kumar, "Analysis of various cryptographic algorithms," *Int. J. Advanced Research in Science, Engineering and Technology*, 5(3), pp. 5341-5348, 2018.
- [20] M. Mohan, and J. Prakash, "Analysis of various cryptographic algorithms," *International Journal of Engineering Technology, Management and Applied Sciences*, 2(3), 201, pp. 51-61.
- [21] M. A. Hameed, A. I. Jaber, J. M. Alobaidy, and A. Alaa, "Design and simulation DES algorithm of encryption for information security," *American Journal of Engineering Research*, 7(4), 2018, pp. 13-22.
- [22] S. N. Habib, R. Awan, and W. Haider, "A modified simplified data encryption standard algorithm," *International Journal of Computer Science and Software Engineering*, 6(7), pp. 152-154, 2017.
- [23] M. Mushtaq Faheem, S. Jamel, A. Hassan Disina, Z. A. Pindar, N. Shafinaz Ahmad Shakir, and M. Mat Deris, "A survey on the cryptographic encryption algorithms," *Int. J. Adv. Comput. Sci. Appl.*, 8(11), 2017, pp. 333-344.
- [24] N. Sharma , Prabhjot and H. Kaur, " A Review of Information Security using Cryptography Technique" *International Journal of Advanced Research in Computer Science*, vol.8, no. Special Issue, pp.323-326, 2017.
- [25] S. Tayal, N. Gupta, P. Gupta, D. Goyal and M. Goyal, "A Review paper on Network Security and Cryptography," *Advances in Computational Sciences and Technology* , vol. 10, no. 5, pp. 763-770, 2017.
- [26] N. Varol, F. Aydoğan and A. Varol, "Cyber Attacks Targeting Android Cellphones," in *The 5th International Symposium on Digital Forensics and Security (ISDFS 2017)*, Tirgu Mures, 2017.
- [27] J. P. Aumasson, *SERIOUS CRYPTOGRAPHY A Practical Introduction to Modern Encryption*, San Francisco: No Starch Press, Inc, 2018.
- [28] A. Gupta and N. K. Walia, "Cryptography Algorithm: A Review," *INTERNATIONAL JOURNAL OF ENGINEERING DEVELOPMENT AND RESEARCH*, vol. 2, no.2, pp.1667-1672, 2014.

- [29] H. Orman, "Recent Parables in Cryptography," IEEE Internet Computing vol. 18, no.1, pp.82-86, 2014.
- [30] S. D. Rihan, S. E. F. Osman, and A. Khalid, "A performance comparison of encryption algorithms AES and DES," International J. Eng. Res. Technol., 4(12), 2015, pp. 151-154.
- [31] M. T. Bemila, K. Kundar, L. Jain, S. Sharma, and N. Makasare, "Comparative study of various security algorithms applicable in multi-cloud environment," Int. J. Advanced Research in Computer and Communication Engineering, 5(3), 2016, pp. 460-463.
- [32] K. P. Karule and N. V Nagrale, "Comparative analysis of encryption algorithms for various types of data files for data security," International Journal of Scientific Engineering and Applied Science, 2(2), 2016, pp. 495-498.
- [33] S. J. Aboud, "Secure e-exam scheme," International Journal of Science and Research, 3(9), 2014, pp. 2200-2203.
- [34] M. M. Al-Laham, "Reducing security concerns when using cloud computing in online exams case study: General Associate Degree Examination (Shamel) in Jordan," Int. J. Comput. Sci. Inf. Technol., 7(6), 2015, pp. 131-144.