JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

HILL CIPHER AND AFFINE CIPHER SYMMETRIC KEY METHOD

[1] Mrs. Pilla Devi Prasanna, [2]Mokka Harish
[1]Assistant Professor, [2]MCA Final Semester,
[1]Masters of Computer Applications,
[1]Sanketika Vidya Parishad Engineering College, Visakhapatnam, Andra Pradesh, India

Abstract: Cryptography [3] is the study of information encryption and decryption. Attending the process of hiding information from unauthorisedusers accessing it is due to the need to secure information from ancient times till the present. The current technology allows for the creation of ciphers using both symmetric and asymmetric cryptography techniques. The symmetric approach encrypts a plain text at the sender's end to produce a cipher text, which is then decoded at the receiver's end to produce the original plain text. The suggestedmethod makes advantage of a property that fuses the Hill Cipher and Affine Cipher. The third key, which is a matrix, is created throughout the key generation process. The third key matrix format is utilised to convert plaintext to cipher text, and modulo formulation is used to each text form to increase information security and create incredibly effective cipher systems.

***Index Terms*:** Affine Cipher And Hill Cipher, Encryption And Decryption, Three Key-Based Cryptography, Matrix Format.

I. I. INTRODUCTION

Because of it emphasises preventing unauthorised individuals from accessing private information, secrecy and privacy are often synonymous. There are two ways to offer secrecy services, and one of them is called steganography. This technique involves hiding data in another kind of media (for example, writing in visible ink or embedding text in images). The other popular technique for ensuring confidentiality is cryptography, in which data encryption is carried out to produce cyphers (such as Caesar and Substitution cyphers).When algorithms are supposed to be known to the public, the third key is the one that protects cyphers the most. Because of this, robust encryption[1] methods keep a key generator core to generate random keys in their design. The power of all sorts of ciphers can be increased by using the third key generating method to create randomised keys. The system suggests a very difficult encryption technique called modulo formulation and three key creation of matrix format[6]. The Hill cypher uses matrix features such as matrix multiplication and matrix inverse, and the Affine cipher, which combines additive and multiplicative cyphers, requires two keys: one for the additive cypher and another for the multiplicative cypher. Both of these cyphers are used in the symmetric key cryptography technique.So the sender can encrypt the message using the matrix format and the receiver can decrypt the message with the randomized keys and inverse of matrix modulation.

II. EXISTING SYSTEM

Any of the two primary types of encryption techniques symmetric or asymmetric can be used to create ciphers. In symmetric approaches, a secret key must be held by both the broadcaster and the receiver of secret information. A plain text is encrypted at the sender's end using a secret key[8] to create cipher text, which is then decoded at the receiver's end to reveal the original plain text. The guiding principles state that keys are crucial for cipher security against cryptanalytic attacks.

LIMITATION OF EXISTING SYSTEM

1. Keys are not updated.
2. Low capacity.
3. Keys are given by the user.

III. PROPOSED SYSTEM

The suggested symmetric key[7] cryptography system uses a property that combines both the Affine cipher[4] and the Hill cipher[5] for improved data security in order to address the short comings of the current system. The third key, which is in matrix format, is generated during the key generation process for encryption or decryption[2]. The matric format and modulo formulation are applied toeach text format through out the process of transforming plain text to cipher text. Both symmetric and asymmetric cryptography approaches can be used to create ciphers under the current system. In the symmetric method, a plain text is encrypted at the sender's end to create the cipher text, and at the receiver's end, the cipher text is decoded to generate the original plain text. the sender can encrypt the message using the matrix format and the receiver can decrypt the message with the randomized keys and inverse of matrixmodulation.

ADVANTAGES OF PROPOSED SYSTEM

The following are the benefits of the proposed system. They are:

1) More Secure: Both the Hill cipher and the affine cipher are efficient and reliable data encryption techniques. They are harder to crack than basic substitution ciphers, and by employing a bigger key and a more complicated encryption algorithm, they can be made even more secure.

2) Keys are generated randomly: Both the Hill cipher and the affine cipher are symmetric ciphers, which means they both encrypt and decrypt messages using the same key. The Hill cipher key is an integer square matrix, and the affine cipher key is an integer pair.

3) High Complexity: Using a larger key can enhance the complexity of data encrypted using the affine ciphers and hill ciphers. The matrix or linear transformation that is used to encrypt the data is created using the key. An attacker will find it more challenging to crack the cipher with a larger key.

IV. FEASIBLITY STUDY

Goal definition triggers the start of the feasibility analysis. It begins by coming up with broad potential solutions that could serve asa general guide for how the new system should be designed. Users should be able to determine how the new system will fit into the organization and create accurate cost estimations using the information provided by the solution. It's crucial to avoid making a major effort at this point just to discover that the project is pointless or that the initial purpose needs to be considerably changed. A new system must be feasible in order for us to execute it, and it must also be effective and economical.

IV(a)Economically Feasibility

The Hill and Affine ciphers can be combined to provide a more powerful encryption scheme. This is because using cryptography to safeguard information is becoming increasingly crucial in today's digital environment. The recommended plan should not be too expensive to adopt, making it a viable alternative for the majority of businesses. The usage of electronic payment systems is also growing, which raises the necessity for safe encryption solutions.

IV(b)Technical feasibility

The most challenging aspect of a feasibility study is evaluating the technical feasibility. This is because there are currently not many systems with precise designs, making it challenging to access issues like performance, prices, etc. While performing a technical analysis, a variety of factors must be taken into account.

1. Recognise the various technologies utilised in the proposed system: We must be extremely clear on the technologies that will be needed for the creation of the new system before we start the project.

2. Find out whether the organization currently possesses the required technologies: Is the required technology available with the organization? If so is the capacity sufficient? For instance -

"Will the current printer be able to handle the new reports and forms required for the new system?

IV(c)Operational Feasibility

Only if proposed ideas can be transformed into information systems that satisfy the operational needs of the organisation are they beneficial. This feasibility test, put simply, inquires as to whether the system will function after development and installation. Exist significant obstacles to implementation? Here are some queries to gauge a project's operational viability. Is there enough management and user support for the project? There may be opposition if the current system is so well-liked and widely used that people find it difficult to understand why it needs to change. Are the user-friendly existing commercial practises? Users may embrace a change that results in a more functional and useful system if they are not currently, though. Has the user been a part of the project's planning and development? Early involvement raises the likelihood of a successful project and lowers the possibility of system and ingenuity opposition. Given that the proposed system was intended to lessen the difficulties faced. The new approach was thought to be operationally practicable with the manual system that was already in place.

V. SPECIFICATION

Processor : Intel i3 & Above
1.RAM : 2 GB
2.Hard disk : 250 GB 3.Keyboard
: Standard 102 Keys 4.Mouse :
Standard
5.Operating system : Windows 7 & Above
6.Front-end/GUI tool : Python & Tkinter
7.moduleProgramming language : Python Programming
8.Version : 3.10.6

VI. SYSTEM ANALYSIS

Attending the process of hiding information from unauthorised users accessing it is owing to the requirement to safeguard information from ancient times to the present. We suggested the purpose of cryptography, a discipline of computer science, is to safeguard senders and receivers while transmitting and receiving sensitive information through an insecure channel[9]. This includes both the encryption and decryption operations. Ciphers can be created using either of the two main types of encryption techniques symmetric or asymmetric. In symmetric techniques, a secret key must be possessed by both the broadcaster and the receiver of secret information. At the sender's end, plain text is encrypted using a secret key to form cipher text, which is then decoded at the receiver's end to exposethe original plain text. According to the guiding principles, keys are critical for cypher security against cryptanalytic assaults. The proposed symmetric key cryptography system employs a characteristic that combines the Hill and Affine cyphers to increase data security[10]. During the key creation procedure, a third key in matrix format is created for encryption or decryption. Throughout the process of converting plain text to cipher text[11], the matric format and modulo formulation are applied to each text format.

VII. DEVELOPMENT TOOLS AND TECHNOLOGIES:

VII(a)PYTHON:

Python is an interpreter, interactive, object-oriented programming language. It incorporates modules, exceptions, dynamic typing, very high level dynamic data types, and classes. Python combines remarkable power with very clear syntax. It has interfaces to manysystem calls and libraries, as well as to various window systems, and is extensible in C or C++.

VII.a.(1):Python is portable

It runs on many Unix variants, on the Mac, and on Windows 2000 and later. When he began implementing Python, Guido van Rossum was also reading the published scripts from "Monty Python's Flying Circus", a BBC comedy series from the 1970s. Van Rossum thought he needed a name that was short, unique, and slightly mysterious, so he decided to call the language Python.

Python is one of those rare languages which can claim to be both simple and powerful. You will find yourself pleasantly surprised to see how easy it is to concentrate on the solution to the problem rather than the syntax and structure of the language you are programming in. Python is simple and minimalistic language. Reading a good Python program feels almost like reading English, although very strict English! This pseudo- code nature of Python is one of its greatest strengths. It allows you to concentrate on the solution to the problem rather than the language itself. Due to its open-source nature, Python has been ported to (i.e., changed to makeit work on) many platforms. All your Python programs can work on any of these platforms without requiring any changes at all if youare careful enough to avoid any system-dependent features.

VIII. LIBRARY USED

VIII.a(1)TKINTER: Tkinter is a Python standard library for creating desktop application graphical user interfaces[12] (GUIs). It makesit simple to create desktop applications. Our primary GUI toolkit will be Tk, which is Python's default GUI framework. Tkinter, a Python interface, will be used to access Tk (short for Tk interface). Running python -m Tkinter from the command line should displaya simple Tk interface, indicating that Tkinter is properly installed on your system and also indicating what version of Tcl/Tk is installed,allowing you to browse the documentation for that version. Tkinter works with various Tcl/Tk versions, both with and without threadsupport. Tcl/Tk 8.6 threaded is included in the official Python binary distribution[13]. More information about supported versions canbe found in the _tkinter module's source code. Tkinter is not a light wrapper, but it does contribute some logic to make the experiencemore pythonic. The documentation will focus on these additions and updates, with aspects that remain unchanged being referred to as the standard Tcl/Tk documentation.

Features

Displaying Text and Images.
Displaying Clickable Buttons.
Getting User Input.
Getting Multiline User Input.
Assigning Widgets to Frames.
Adjusting Frame Appearance.

VIII.a(2) Tkinter Message box

The message box module in Python is used to show message boxes in programs that use them. A variety of functions are used,depending on the application's requirements, to display the pertinent messages.

There are seven functions in the Tkinter Message box there are listed below

a. showinfo(): When we need to provide the user with some pertinent information, we use the showinfo() message box
b. showwarning(): The warning is shown to the user using this technique.
c. showerror(): This technique is used to show the user the error notice.
d. askquestion(): This approach is used to pose questions to users that they can respond to with a simple yes or no.
e. askokcancle(): This technique is employed to verify the user's participation in an application activity.
f. askyesno(): Using this technique, a question concerning action is posed
g. askretrycancel(): Using this technique, the user is asked whether they would like to perform a specific task again.

IX. DATA FLOW DIAGRAMS

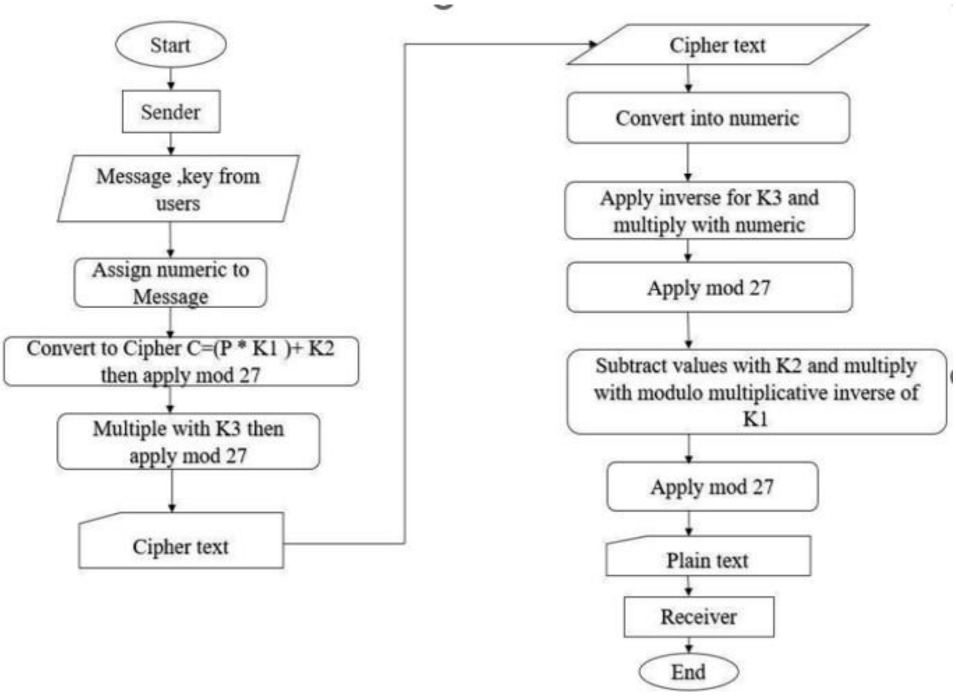


FIGURE IX:This reflects data flow diagram

IX.a) STATE CHART DIAGRAM

The state machine diagram, also known as a state chart or state transition diagram, depicts the sequence of states that a system item passes through. It logs the software system's behaviour. It replicates the behaviour of a class, a subsystem, a package, and an entire system. It is frequently used to represent how the system and external entities interact and collaborate. It uses event-based systems to manage an object's state. It also specifies the number of distinct states in which a system component can reside. Each item or component is in a certain state.

A state machine diagram, also known as a state chart or state transition diagram, is a sort of Unified Modelling Language (UML) behavioural diagram that depicts transitions between distinct objects. It specifies the sequence of events that an item goes through over its existence in reaction to events, modelling the behaviour of a single object.A state machine diagram depicts the many states of an object and is used to describe the dynamic nature of a system. It is widely used to illustrate the interaction and collaboration between the systemand external entities.A state machine diagram has the following important characteristics.

IX.a.1) STATE CHART DIAGRAM FOR SENDER

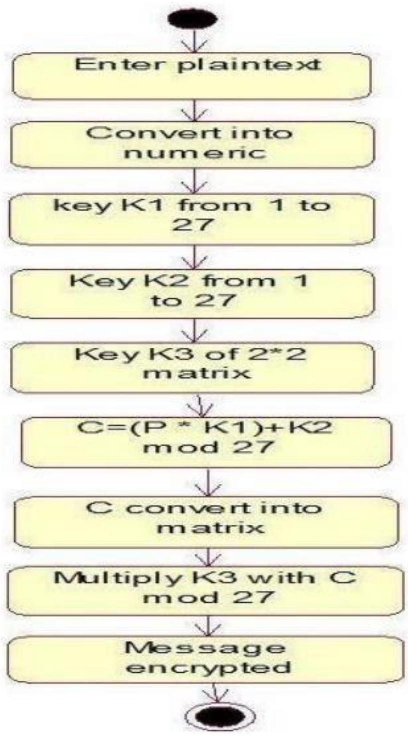


FIGURE **1:**This reflects sender chat diagram

IX.a.2) STATE CHART DIAGRAM FOR RECEIVER

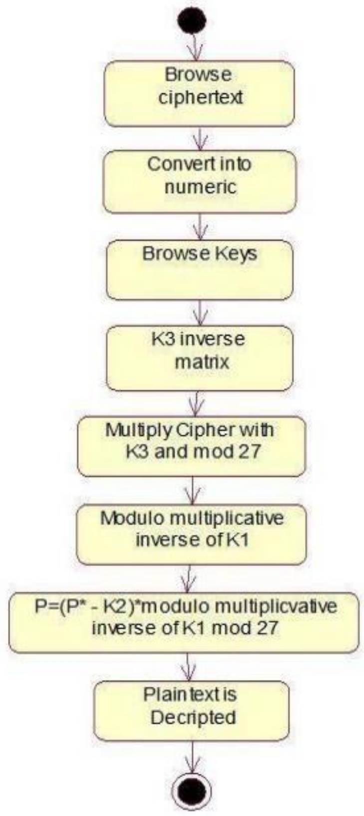


FIGURE 2: This reflects receiver chat diagram

X. SYSTEM IMPLEMENTATION

Encryption is the process of converting plaintext into ciphertext, where plaintext is the input to the encryption process and ciphertextis the result. Decryption is the process of converting cypher text into plain text, where cypher text is the input to the decryption processand plain text is the result. There are two types of encryption algorithms: symmetric and asymmetric encryption methods. This projectemploys a method for data encryption and decryption that is based on the ASCII of plaintext characters. This technique is used to encrypt data by utilising the data to be encrypted's ASCII values[14].

Encryption and Decryption

Data that can be read and understood by anyone without any special knowledge about it is called plaintext or clear text. The method of disguising the plaintext in such a way as to hide the information is called encryption. Encrypting plaintext results in unreadable gibberish called cipher text. You use encryption to ensure that information is hidden from anyone for whom it is not intended, even those who can see the encrypted data. The process of reverting ciphertext to its original plaintext is called decryption.

Conventional Cryptography

In conventional cryptography, also called secret-key or symmetric-key encryption, one key is used to both encrypt and decrypt the data. The famous Caesar's Cipher is an example of this technique. Only the person who knew the "shift by 3" rule could understand the message. While sending the encrypted data, the key is shared through another secure channel to make it possible for the receiver to decrypt the cipher text into the original plaintext. Which makes it a bit insecure?

Public Key Cryptography

In this technique, there are two keys involved, one for encryption and the other for decryption. The receiver already has a private key which is never used in any communications. Only the public key is sent along with the cipher text. No one without having the private decrypt.

Encryption Method

Plain text is converted into respected numerics and select keys which are k1,k2,k3 from 0-27 and k3 which is matrix format n*n .compute the encryption formulae and apply modulo to the output then the plain text is encrypted to cipher text.

The Encryption process involves these steps:

Step 1: We should first enter the Keys k1, k2 and also plain text.Step 2:
Convert plain text to numeric values .
Step 3: Select third key K3 of $m * m$ matrix type. Determine the determinant of the matrix $|A|$.
Step 4: Compute $C* = (P * K1) + K2$. Where $C*$ is the intermediate encrypted message and P is the plaintext.
Step 5: Divide the $C*$ into n blocks matrix. Put padding if necessary. Padding is usually indicated by zero (0) in the symbol set. Step 6: Multiply K3 with every block and apply MOD27 to get the finest result .Then the result is the final encrypted message as
$C = (C * * K3)$.
Step 7: Repeat till the last block.
Step 8: Now Plain text is converted into cipher text with the randomized keys.Step 9:
We must save Ciphertext, keys.

Decryption Method

The keys and cipher text are browsed and the cipher text is converted into respected numerics . Perform inverse modulo multiplicative inverse[15] of k2 and add mod27 to that values. Apply k2 and perform decryption to the cipher text which is converted to the plain text which the sender given.

The Decryption process involves these steps:
Step 1: Browse Cipher Text
Step 2: Convert into digits.
Step 3: Add multiplicative inverse of k2 and inverse of k3.Step
4: Apply mod27 to the given values.
Step 5: Select random keys.
Step 6: Perform P ∗ = (C ∗ K3 ∗−1) to the cipher text.Step
7: Repeat till last block of cipher text.
Step 8: The resultant plain text.

XI. UNIT TESTING

During this first stage of testing, the programmer is subjected to tests that focus on distinct units or components of the software to evaluate whether each one is fully functional. The major purpose of this project is to determine whether or not the application performs. At this stage, a unit can refer to a function, an individual programmer, or even a method, whereas a White-box[16] can refer to anything.To finish the assignment, the testing approach is usually used. One of the most notable benefits of this testing phase is that it may berun whenever a piece of code is modified, allowing problems to anticipated be rectified as soon as feasible[18]. programmer engineersmust do formal testing[17] on their programmer before presenting it to testers.

Test Case ID	Test Case Name	Expected output	Observed output	Status
01	Encryption and Decryption using upper case	Cipher text and Plain text	Cipher text and Plain text	Pass
02	Encryption and Decryption using lower case	Cipher text and Plain text	Cipher was hidden and Plain text	Fail
03	Encryption and Decryption using even letters	Cipher text and Plain text	Cipher text and Plain text	Pass
04	Encryption and Decryption using odd letters		Cipher text and Plain text	Pass

TABLE 1 This reflects unit test tableXII.OUTPUT

SCREENS

In the below output screen shows, how the data is changes from plain text to cipher text by using encryption and decryption methods. The below models can shows how the data is inserting for encryption, and after that will generates the cipher text. And after that data is inserting for decryption.

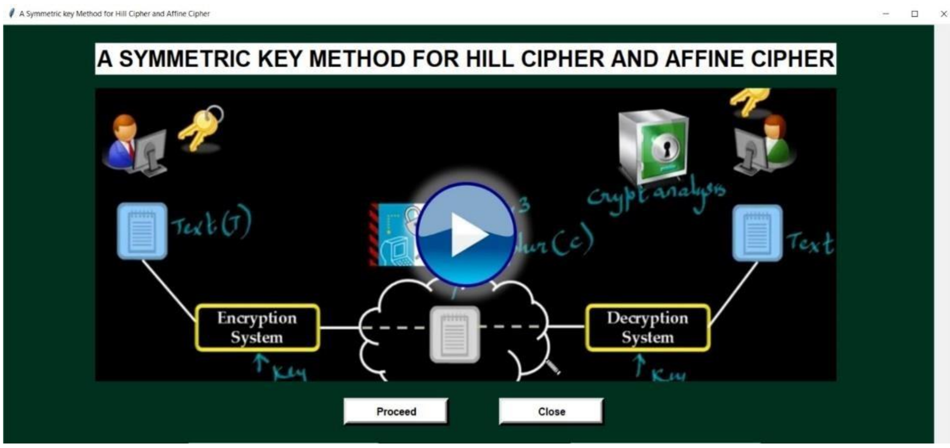
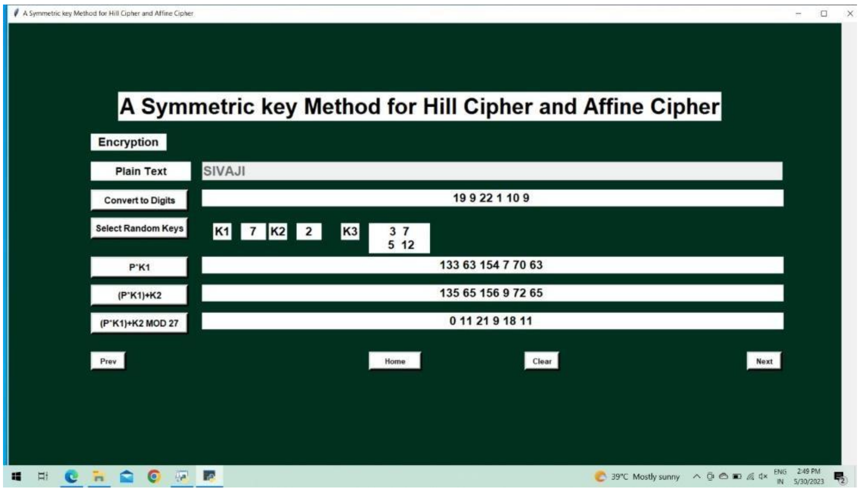
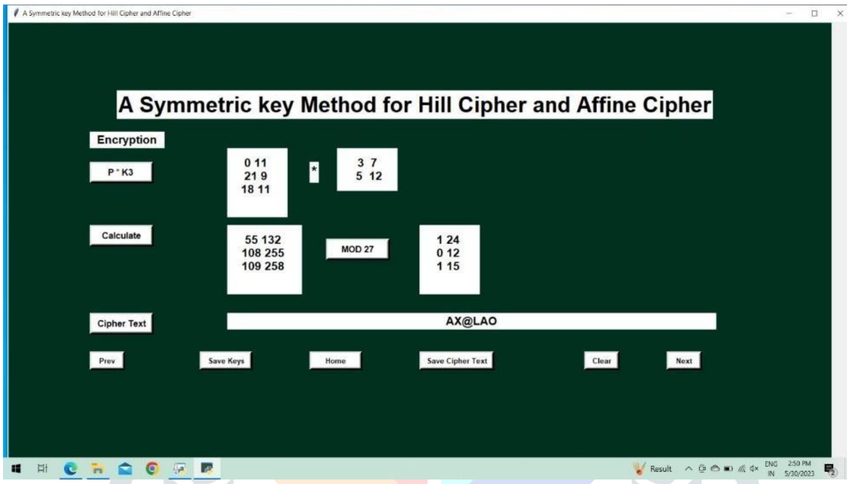


FIGURE XII.a: This reflects output screen



XII.b INSERTING DATA FOR ENCRYPTIONFIGURE XII.b: This reflects insertion data for encryption



XII. c:GENERATING CIPHER TEXT

FIGURE XII.c: This reflects generating cipher text

XII.d :INSERTING DATA FOR DECRYPTION

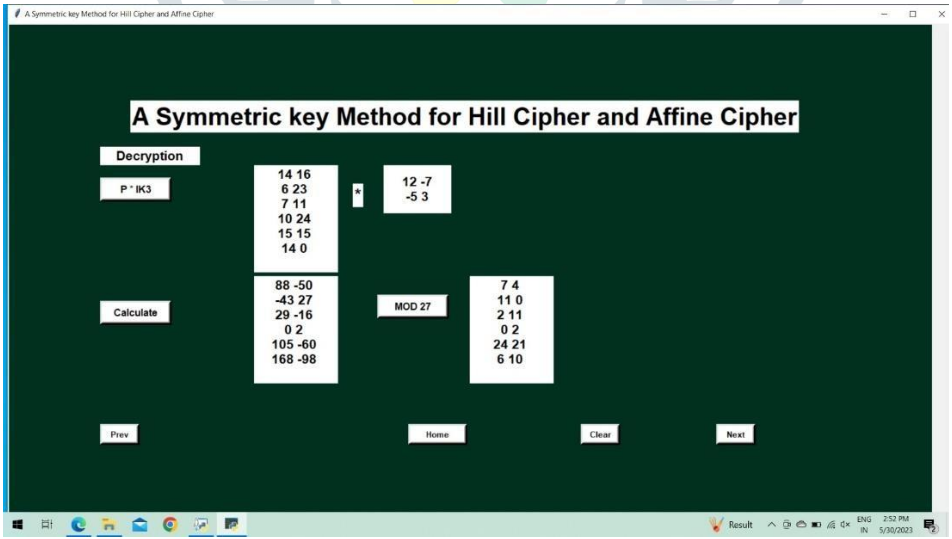


FIGURE XII.d: This reflects inserting data for decryption

XII.e: OUTPUT

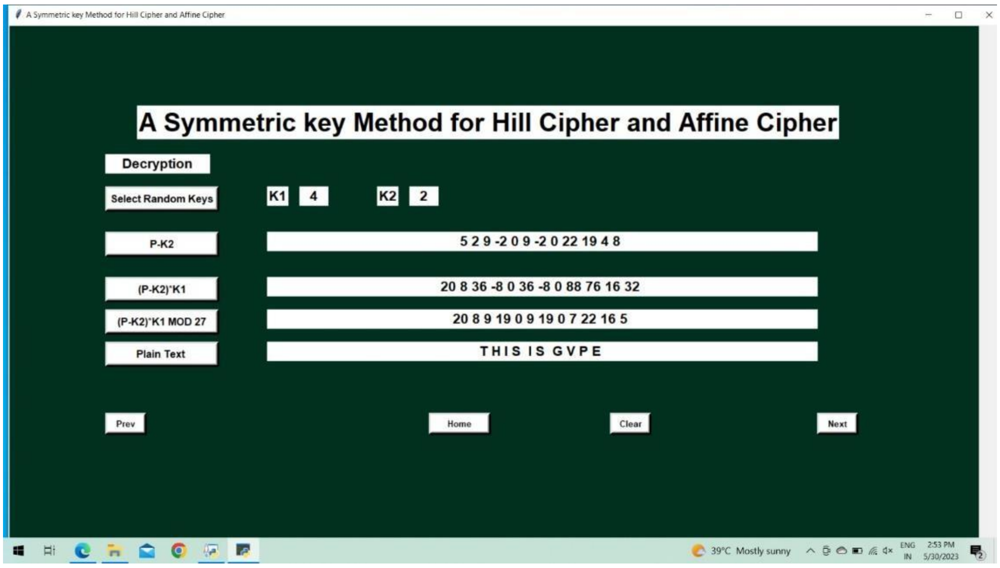


FIGURE XII.e: This reflects final output screen

XIII.CONCLUSION

Cryptography is a procedure that combines encryption and decoding. Because of its fast processing[19], the symmetric key cryptography approach is frequently preferred for encrypting large messages. In this case, the suggested system makes advantage of the Affine cypher and the Hill cypher properties to improve data security. The method is straightforward to grasp and of average complexity. It can be used on a variety of systems, resulting in speedier text conversion.

10.1. SCOPE FOR FUTURE DEVELOPMENT

In the future, the project will have a very broad reach. The project can be implemented in the future. Because it is quite adaptable in terms of extension, the project may be upgraded in the near future as and when the need arises. We can protect the data using this hill cypher and affine cypher project. These can be beneficial for users to communicate data in a conference setting.

11.REFERENCES

[1] An Article Reference of Encryption
https://ieeexplore.ieee.org/abstract/document/8713449
[2] An Article Reference of Decryption
https://ieeexplore.ieee.org/abstract/document/9429920
[3] An Article Reference of Cryptography
https://www.emerald.com/insight/content/doi/10.1108/JFRC-06-2020-0062/full/html
[4] An Article Reference of Affine cipher
https://www.sciencedirect.com/science/article/abs/pii/S0030402622002704
[5] An Article Reference of Hill cipher
https://www.sciencedirect.com/science/article/abs/pii/S0030402622002704
[6] An Web Reference of Matrix format
https://link.springer.com/chapter/10.1007/978-1-5041-2940-4_9
[7] An Web Reference of Symmetric key
https://link.springer.com/article/10.1007/s12652-021-02980-w
[8] An Web Reference of Secret key
https://ieeexplore.ieee.org/abstract/document/9346002
[9] An Web Reference of Insecure channel
https://link.springer.com/chapter/10.1007/11535218_19
[10]An Web Reference of Data security
https://link.springer.com/chapter/10.1007/978-3-319-93417-4_31
[11] A Book Reference Of the cipher text
https://www.tandfonline.com/doi/abs/10.1080/0161-110091888745
[12] A Book Reference Of the graphical user interface
https://www.sciencedirect.com/science/article/abs/pii/S0010465504002115
[13] A Book Reference on binomial distribution
https://www.sciencedirect.com/science/article/abs/pii/S0304407616301610
[14] A Book Reference on ASCII Values
https://link.springer.com/article/10.1007/s11042-021-11741-y
[15] A Book Reference Of multiplicative inverse
https://link.springer.com/article/10.1007/s00605-007-0479-z
[16]AN Article Reference of white-box
https://ieeexplore.ieee.org/abstract/document/8314681
[17] A Book Reference of Formal testing
https://www.nature.com/articles/nature09014
[18] AN Article Reference of the Feasible
https://bmjopen.bmj.com/content/8/9/e022233.abstract
[19]An Web Reference of Fast Processing

https://www.science.org/doi/abs/10.1126/science.1066893
[20] AN Article Reference of Conference Setting
https://www.sciencedirect.com/science/article/abs/pii/S0950584908001390
BIBILIOGRAPHY

Pilla Devi Prasanna Currently working as Professor from Department of Computer Science and Engineering at Sanketika Vidya Parishad Engineering College, affiliated to Andhra University, accredited by NAAC. Madam is currently working as Head of The Department , Published Papers in Various National & International Journals.her Subjects of interests are Machine Learning, Data Mining & Warehousing.

Mokka Harish is studying his 2nd year, Master of Computer Applications in Sanketika Vidya Parishad Engineering College, affiliated to Andhra University,accredited by NAAC. With his interest in python, cryptography and as a part ofacademic project, he choose encryption and decryption with hill cipher and affine cipher using python. As a result of a desire to comprehend the flaws in conventional reporting and to preserve timely and high-quality report output in hill and affine ciphersymmetric key method. A completely developed project along with code has been submitted for Andhra University as an Academic Project. In completion of her MCA.