International Journal of Engineering Applied Sciences and Technology, 2021
Vol. 6, Issue 2, ISSN No. 2455-2143, Pages 39-42
Published Online June 2021 in IJEAST (http://www.ijeast.com)

A CRYPTO SYSTEM USING VIGENERE AND POLYBIUS CIPHER

Bhavana K V, Banushree D J, Bhumika D, Chaitanya K B
Department of CS&E
BIET, Davangere, Karnataka, India

Prof. Raghu B R
Asst. Professor,
Department of CS&E
BIET, Davangere, Karnataka, India.

Abstract—The Cryptography is a Greek word which implies the craft of ensuring data by changing it into a muddled organization and unreadable format. Cryptography is a method to secure sensitive data for storage and communication in the presence of third parties called adversaries. It is a mix of arithmetic and software engineering. The drastic growth of the Internet over a period of time made an unintentional security. Even though security is the measure worries over the internet, numerous applications have been created and structured without considering fundamental destinations of data security that is confidentiality, authentication, and protection. To gain some undesirable clients or individuals to gain admittance to the data, cryptography is required. This paper introduces a new hybrid security cipher by combining the two most important Ciphers such as Polybius Cipher and Vigenere Cipher. This hybrid encryption cipher provides greater security as compared to classic ciphers.

Keywords— **Cryptography, Security, confidentiality, Polybius Cipher, Vigenere Cipher.**

I. INTRODUCTION

Cryptography is the art of creating written or generated codes that allow information to be kept secret. Cryptography converts data into a format that is unreadable for an unauthorized user, allowing it to be transmitted without unauthorized entities decoding it back into a readable format, thus compromising the data. Information security uses cryptography on several levels. The information cannot be read without a key to decrypt it. Cryptography is technique of securing information 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 prefix "crypt" means "hidden" and suffix graphy means "writing". Enhancing the privacy, confidentiality and reliability of the work requires a lot work to strengthen the current methods. Accordingly, it was proven that encoding is one of the most reliable strategies used to secure information. Ancient people, who used similar methods to enable security on their valued information and documents. Data encoding is the process of changing the form of the data into certain symbols through the use of meaningless or mixture of codes.

II. LITRATURE SURVEY

In paper [1], they have combined vigenere cipher with the stream cipher as vigenere cipher is the simplest, more vulnerable and it can be easily attacked by hackers and intruders. So, the paper says that the proposed algorithm hides the relationship between the plaintext and the cipher text, which makes the cryptanalysis more difficult. This increases or enhance the security of vigenere cipher and also it shows that stream cipher is really hard to break. But this was complex method and it was taking more time to encrypt and decrypt the messages.

In paper [2], a modified version of Polybius cipher was proposed using music notes and magic squares, where magic square is a game of puzzles having n/n grids with numbers along column s and rows and music notes consists of 6/6 matrix using the latin letters A, B, C, D, E, F, G. They also used Medjig method to construct magic square. It was a unique magic square having integers arranged from 1 to 36 and alphabets from 1 to 26. So by looking into the rows and columns, and magical notes numbers, encryption and decryption were done. Sender also can change the keys frequently. But it was only safe for small texts during communication. It was not suitable for large communication.

In paper [3], vigenere cipher was enhanced for security purpose. In this, their proposed method was having a table consists of 26 columns and 8 rows. Here, they used formula for encryption and decryption. For encryption, plain text and key character were added and modulo 27 of the resultant was calculated. Similarly for decryption, numeric value was subtracted from the table and resultant was calculated from modulo 27. In this proposed technique every combination of key phrase character and plain text character could replace

International Journal of Engineering Applied Sciences and Technology, 2021
Vol. 6, Issue 2, ISSN No. 2455-2143, Pages 26-30
Published Online June 2021 in IJEAST (http://www.ijeast.com)

with many other cipher characters. This technique was very secure against Friedman and kasiski attacks.

In paper [4], they have used signature that is basic tool used for security that can be used in banking, password, Email. Where signature is the compressed data with Advanced Encryption Standard (AES). AES is a symmetric algorithm then the secret key can be of any size and uses same key for encryption and decryption the key is very secret it's hard to guess by the hackers and it is generated by Polybius square. In modified AES key size of 320 bits is used. Along with AES Triple Data Encryption Standard (TDES) and Data Encryption Standard (DES) also used. Here time can be calculated by time taken by algorithm conversion. As number of round increase to 16 the system is more secure. But it's a very complex process.

In paper [5], they have used Vigenere cipher which is poly-alphabetic cipher technique by using Vigenere table but in this they have also extended this table by using numbers so that numbers also can be encrypted. And it combines both vigenere and Caesar cipher and encrypt plane text with given key.in tis it will break down the disadvantage of poly-alphabetic cipher by adding numbers. So cryptanalysis will be complex to hack to make cryptanalysis more complex they also added special symbols. Although after all this vigenere still considered as less secure.

In paper [6], they have used Goldbach algorithm, it is used for compression as we know vigenere is less secure to overcome weakness of vigenere they have used Goldbach algorithm. So the output from vigenere can be taken to Goldbach algorithm that compressed data is called as Goldbach code. Goldbach reduce the size of file and eliminates some redundant data such that humans can not recognize. If key size is smaller than the number of character in plaintext, the key will be repeated as times many as plaintext.

In paper [7], they used Gronsfeld cipher for the protection of important data and important information. Here 2 equations were used, which were the formulas for encrypting and decrypting the text. Formula contains addition of the plain text to be encrypted and the key, following mod 26 or mod 256 for encryption. Similarly subtracting the encrypted text and key following mod 256 or 26 for decryption. This was done using the Gronsfeld map. It has noerrors, as it was a mathematical computation. But its weakness is that the key could be rotated to produce the plaintext and Modulus can be done up to 256 characters.

In paper [8], a hybrid algorithm was designed using polybius and vigenere cipher. Here, encryption and decryption were done 2 times. So it was a kind of double encryption and double decryption. First encryption was done using vigenere cipher with the key which outputs alphabets. Next encryption was done using Polybius which converts alphabets to numbers. In the same manner decryption was done in the reverse process. But this was taking only alphabets as input with limited size.

III. SYSTEM DESIGN

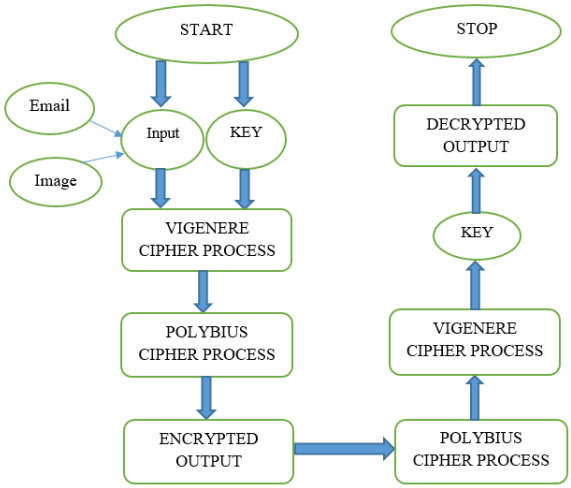

Fig. 1. Flow diagram of crypto system

The figure shows the flow of our model which consists of sending an email and an image, encryption of the message and image through vigenere and polybius cipher, and then decryption using the Polybius and vigenere cipher by using the same key to obtain the original contents

IV. IMPLEMENTATION

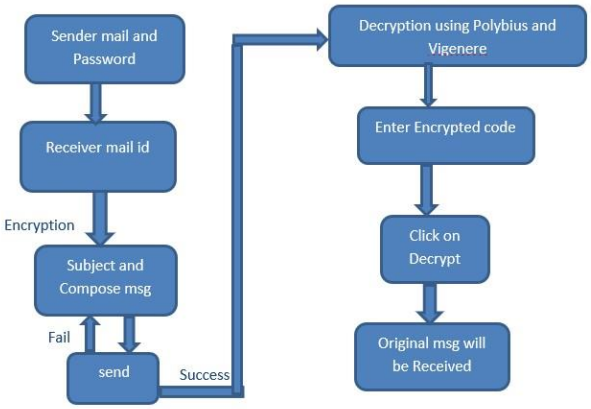

Fig. 2. Model design

The input as email and an image having any size and Key is send through sender in two phase for execution and working of System as in first phase it will proceed through Vigenere Cipher and then the new instructed and disputed encrypted cipher comes and then in second phase it became the input of Polybius cipher which result as output as Numerical encrypted Cipher that is confusing and scrambled mix numerical. This Output from Polybius at last phase is numerical and the Input that proceed in first phase was alphabetic letters this all confuses and doesn't allow the intruders, detectors, thefts, hackers and cybercrime to

International Journal of Engineering Applied Sciences and Technology, 2021
Vol. 6, Issue 2, ISSN No. 2455-2143, Pages 26-30
Published Online June 2021 in IJEAST (http://www.ijeast.com)

commit any assaults and attacks on system and doesn't allow them to steal Information. In the same way decryption is first done through polybius cipher and then with vigenere cipher. So Original contents will be received. We have applied 2 algorithms:

1. Encryption and decryption using vigenere cipher.
2. Encryption and decryption using Polybius cipher.

V. OBJECTIVES

To form a Hybrid cipher using Vigenere and Polybius cipher.

To send text and image using hybrid cipher for encryption and decryption.

To achieve this action by developing desktop application.

To complete the action in less time using same key (Private key).

VI. RESULTS

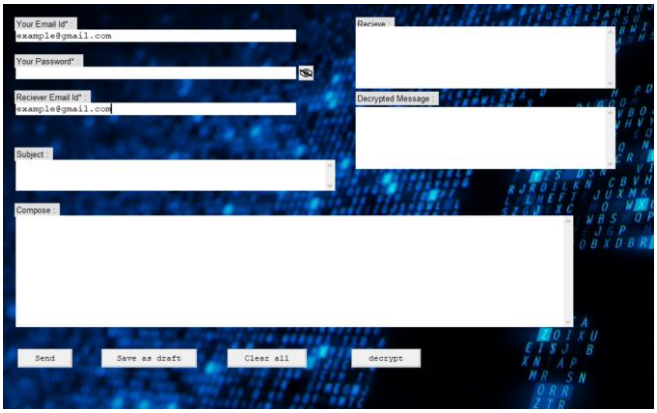

Fig. 3. UI design of crypto system

This is the UI application of our project. It has fields like Gmail address, password, subject, compose, receive, decrypted message. It also has buttons like send, save as draft, clear all, decrypt. Here message will be encrypted and decrypted using Vigenere and Polybius cipher.

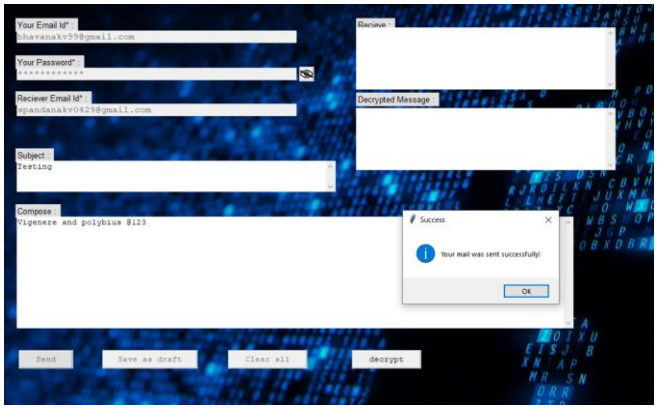

Fig. 4. Sending encrypted message through email.

The above figure shows composing message and sending email to the recipient.

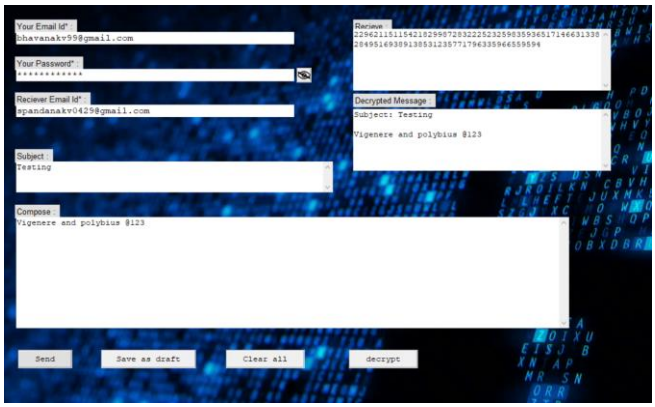

Fig. 5. Decryption of message.

The above figure shows decryption of the encoded message using Polybius and vigenere cipher to obtain the original message.

VII. CONCLUSION

Cryptography is the generally utilized technique for the security, privacy, confidentiality and reliability of data. Single classic ciphers are cryptographic techniques that are viewed as least complex and most vulnerable because of numerous impediments, restriction, and smooth system. One of the famous ciphers is Vigenere Cipher but it also has few drawbacks. To conquer the impediments of Vigenere cipher, In 2020 a new technique was shown an upgraded variant as a combination of Polybius cipher and Vigenere that is a lot more secure against attacks like Active, passive and Friedman assaults (attacks), but it was taking only the text as inputs. In our proposed system, we are sending message through email as input and image which will be encrypted and decrypted to original content by using python programming language. This system can be used by intelligence agencies, militaries for sending their secret data. Even though there are numerous cryptographic strategies yet this space still requires genuine consideration of the research

network for the up-gradation and enhancement of data privacy and security.

VIII. FUTURE WORK

- In future our point is to give approval of proposed approach by performing security and performance analysis on messages.
- Using audios and videos for input.
- Developing web application.

IX. REFERENCES

[1] F. M. S. Ali and F. H. Sarhan, "Enhancing security of vigenere cipher ` by stream cipher," International Journal of Computer Applications, vol. 100, no. 1, pp. 1–4, 2014.

[2] M. Maity, "A modified version of polybius cipher using magic square and western music notes," International Journal For Technological Research In Engineering, ISSN, pp. 2347–4718, 2014.

[3] A. A. Soofi, I. Riaz, and U. Rasheed, "An enhanced vigenere cipher for ` data security," Int. J. Sci. Technol. Res, vol. 5, no. 3, pp. 141–145, 2016.

[4] P. Kumar and S. B. Rana, "Development of modified aes algorithm for data security," Optik, vol. 127, no. 4, pp. 2341–2345, 2016.

[5] A. Saraswat, C. Khatri, P. Thakral, P. Biswas et al., "An extended hybridization of vigenere and caesar cipher techniques for secure com- ´ munication," Procedia Computer Science, vol. 92, pp. 355–360, 2016.

[6] S. D. Nasution, G. L. Ginting, M. Syahrizal, and R. Rahim, "Data security using vigenere cipher and goldbach codes algorithm," ` Int. J. Eng. Res. Technol, vol. 6, no. 1, pp. 360–363, 2017.

[7] A. P. U. Siahaan, "Protection of important data and information using gronsfeld cipher," 2018.

[8] Shivam Vatshayan, "Design of Hybrid Cryptography system using vigenere cipher and Polybius cipher", International Conference on Computational Performance Evaluation (ComPE), 2020.