Cryptography System based on Hybrid of Vign'ere Cipher and Polybius Cipher

Khushi
CSE(Hons.)-Information Security
Chandigarh University,Gharuan, Punjab
21BCS8251@cuchd.in

Sorabh kumar
CSE(Hons.)-Information Security
Chandigarh University,Gharuan, Punjab
21BCS4461@cuchd.in

Priyanka jamwal mam
Supervisor
Chandigarh university,Gharuan,Punjab
priyanka.e15553@cumail.in

***Abstract*—The term "cryptography" is derived from a Greek word that refers to the art of securing data by transforming it into a disorganized and unintelligible structure. It combines software engineering and math. The Internet's explosive expansion has increased people's knowledge with curiosity uncertainty difficulties. Despite the fact that security is a major concern on the internet, many apps have been developed and designed without taking into account the secrecy, authentication, and protection of data as their primary focuses. The importance of comprehending such security challenges and problems will rise as our daily activities grow more and more reliant on data networks. Cryptography is necessary to prevent some undesired clients or individuals from accessing the data. By fusing the two most significant ciphers, such as the Vigen'ere and Polybius ciphers, this work develops a new hybrid security cipher. Compared to traditional ciphers, this hybrid encryption cipher offers more security.**

Keywords*—*Vign'ere Ciphers, Polybius Ciphers, Cryptography, Encryption, Hybrid Ciphers

I. Introduction

The vast majority of people today prefer to use the internet as their primary method of moving data from one end of the earth to the other thanks to advancements in technology. Data can be transmitted across the internet in a variety of methods, including messages, chats, and other channels. Data sharing over the internet is incredibly easy, quick, and exact. The "security risk" that comes with sending data via the internet is, in any case, one of the main difficulties; for instance, private or confidential information can be stored or hacked from a variety of perspectives, considering it is among the most crucial factors to take into account when transferring data.

In the open system, security is a crucial element, and cryptography is crucial in this area. An ancient technology that guarantees the security of data in an open system is cryptography. However, the goal of cryptography is used not only to provide classification but also to provide answers to a number of problems, including data reliability, verification, and non-denial. The definition of cryptography is the encapsulation and design of mechanisms that provide crucial data and information to be transmitted in a protected structure so that the only person capable of recovering this data is the conscious recipient.

.

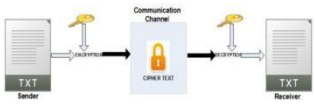

Fig. 1. Enter Caption

Symmetric cryptography and asymmetric cryptography are the two categories of encryption techniques. In symmetric-key cryptography, the same key is used by both sides.

The maintenance of a secure data link In wireless and wired networks, cryptography is used to transform plain text into cipher text and cipher text into plain text. At the transmitter side, encryption takes place when plain text is transformed into cipher text, while at the receiver side, decryption takes place

when cipher text is transformed back into plain text.

This key and an encryption technique are used by the sender to encrypt data, and the recipient uses the same key and the appropriate decryption algorithm to decode the data. Two keys are used in asymmetric or public-key cryptography: a private key and a public key. While the public key is made available to the public, the receiver preserves the private key.

Working figure of Encryption and Decryption :

II. Literature Survey

Content protection in mechanical media is necessary for web security, including password protection for accounts, messages, secret word protection for accounts, etc. It illustrates the pressure for information security in addition to the move encryption standard. The more rounds that are played in a row, the more security that is vulnerable to hacking, intruders, and software developers' active and passive attacks.The Caesarcipher, often known as the shift cipher, is one of the most well-known and least confusing old-style encryption schemes. It functions like a replacement cipher where every letter in the plain text is changed. For example, a move of two would cause A to become C, B to become D, and so on. Caesar ciphers use a combination of encryption techniques that function well together as a disputed and intricate growth plan similar to the Vigen'ere Cipher. As of right now, it also has advantages

in the ROT13 framework and paraphrase system. Similar to how replacement ciphers can be easily and covertly cracked, the Caesar cipher's employment in the current structure lacks security and protection.

One of the earliest and least complicated encryption methods is Caesar Cipher's strategy. It is a type of replacement cipher in which a letter is substituted with another letter a certain number of positions down the alphabetical list. For example, a move of 1 would replace M with N, which would then become O, and so on. Julius Caesar is credited with naming this method since he used it to communicate with his superiors.

Consequently, in order to decipher a particular text, we want a whole number worth, often referred to as a move, which indicates the quantity of positions from which each letter of the text has been derived. The transposition cipher is an adaptive encryption technique that involves moving the location and position of plaintext units using a standard structure or model, resulting in a ciphertext that contains a portion of the original plaintext. The location is the primary stand-in, always occupied, and the pre-location movement by the provided derived metric graph, which can be utilized by the sender's string or message.

Before the message and string are combined using the system Vigenere cipher, a modified version of the Vigenere cipher algorithm was produced as scrabbled and scattering is given by combination and summation of a subjective piece to each byte and bits. The so-called Kasiski attack, which attempts to determine the length of the key by padding the message and string with random bits, fails and burns this process.The primary disadvantage and zero enhancement of this framework is that the combined text and string size will increase by roughly 56%. An alternative approach to implementing the Vigenere algorithm was presented, stating that keys for encryption and message dissemination must be changed repeatedly in a normal, systematic manner. However, in this case, the process's primary keys serve as a continuation of the exchange of substituted keys.

A novel method has been The Virgenere Cipher, which is described in this paper, uses alphabetic numbers and punctuation—colon, comma, semicolon, question marks, underline, full stop, and brackets—as the key instead of characters to make it harder for attackers to launch active and passive attacks. As a result, the message is easily recognizable to literate people who are familiar with the fundamentals of cryptography.

It discusses how the internet's vast association and open structure make it one of the riskiest communication tools. One of the fundamental parametric prerequisites is data assurance.Various security methods are now being proposed to achieve communication security. Each of them makes some excellent arguments and some true assertions. They suggested a hybrid model in an effort to raise the encryption algorithm's level of quality. The suggested paradigm is a hybrid of the DES and AES encryption algorithms. The two methods are particularly good at encryption since they use symmetric key procedures. AES and DES reconciliation would result in a high level of encryption security.

With the suggested arrangement, outcomes have significantly improved.

III. PROBLEM STATEMENT

Encryption: The primary provided letter of the sender and receiver side keys that produces the output as D is the main letter of the plain text, alphabet S, that is in a row combined with alphabet L, that is the key, that is in a column. If E is a row and key I is a column, the crossover of both rows as "Message by sender" and column as the key will produce M. Similar to how other letters are handled, they too will follow the same format and produce an encoded message. The modulus of 26 is increased by the plain text (P) and key (K).

The plain text (P) and key (K) are combined to form the 26-bit modulus.

Ei equals [Pi + Ki]modulus(26) (1)

Decryption: The major letter of the plain text, alphabet S, which is in a row combined with alphabet L, which is the key, which is in a column, is the primary given letter of the sender and receiver side keys that results in the output as D. The crossover of both rows as "Message by sender" and the column as the key, in the case where E is a row and key I is a column, will result in M. They will follow the same syntax and generate an encoded message, just how other letters are treated. The plain text (P) and key (K) raise the modulus of 26.

The 26-bit modulus is the result of combining the plain text (P) and key (K).

Ei is equivalent to [Pi + Ki]modulus (26). (2)

Cipher: A cipher is used to accomplish the encryption and decryption. Merriam-Webster's Collegiate Dictionary defines cipher as —a method of transforming a text in order to conceal its meaning.‖The information that is being hidden is called plain text; once it has been encrypted, it is called cipher text .

A. Vign'ere cipher:

Poly-alphabetic nature: The Vigenère cipher is a poly-alphabetic substitution cipher, which means it uses multiple cipher alphabets. This makes it more secure compared to simple substitution ciphers like the Caesar cipher.

Resistance to Frequency Analysis: Since it uses a keyword to shift the letters, it doesn't exhibit the frequency patterns that can be exploited in mono-alphabetic ciphers.

Limitations of Vign'ere cipher:

Key Distribution: Sharing and managing the key securely can be challenging, especially in a pre-digital era.

Vulnerable to Known-plain-text Attacks: If an attacker knows a portion of the plain-text and the corresponding cipher-text, they can potentially deduce parts of the key and then use it to decrypt the rest of the message.

B. Polybius cipher:

Simplicity: The Polybius cipher is very simple and easy to implement. It's based on a straightforward grid system.

Resistant to Frequency Analysis: Similar to the Vigenère cipher, the Polybius cipher doesn't have frequency patterns that can be exploited.

Limitations of Polybius cipher:

Lack of Security: The Polybius cipher is not very secure, especially against modern cryptographic techniques. It can be easily broken using techniques like frequency analysis or crib-dragging attacks.

Limited Key Space: The key space for the Polybius cipher is relatively small. There are a limited number of arrangements for the grid, which makes it susceptible to brute-force attacks.

IV. METHODOLOGY

The encryption procedure of the technique combines the Vigenere cipher with the Polybius square cipher. The Vigenere cipher will be used to work on the cipher text first.

The process will begin with an arbitrarily selected key. The next cipher text becomes a key for the Polybius Square Cipher procedure towards the end of the process. The message, which is the plain text, is worked on using the key to produce the final cipher text. As a result, the final cipher text will become increasingly difficult to decipher using current crypt-analysis techniques.

The recipient will decrypt in reverse order in order to obtain a message from the sender.

Using Python coding, a product application will be created to demonstrate the calculation's viability, and the cipher text will be subjected to several crypt-analysis techniques.

A. Vign'ere cipher component:

Description:

The Vigenère cipher is a method of encrypting alphabetic text by using a simple form of poly-alphabetic substitution. It uses a keyword to shift letters in a message.

Implementation:

The system will take a keyword (e.g., "FROG") as input.

Extend the keyword to match the length of the plain-text message.

Encrypt the message using the Vigenère cipher algorithm.

Key Generation:

The user provides the keyword.

Encryption Process:

Use the Vigenère cipher algorithm to encrypt the message.

Decryption Process:

Use the Vigenère cipher algorithm with the same keyword for decryption.

CODE:-

function vigenereCipher(key, str, mode) var output = [str.length]; var result = 0;

for (var i = 0; i ¡ str.length; i++) if (mode == 1) result = ((str.charCodeAt(i) + key.charCodeAt(i output[i] = String.fromCharCode(result); else if (mode == 0) if (str.charCodeAt(i) - key.charCodeAt(i result = (str.charCodeAt(i) - key.charCodeAt(i else result = (str.charCodeAt(i) - key.charCodeAt(i output[i] = String.fromCharCode(result); output$_str$ = *output.join*(''); *return output*$_str$;

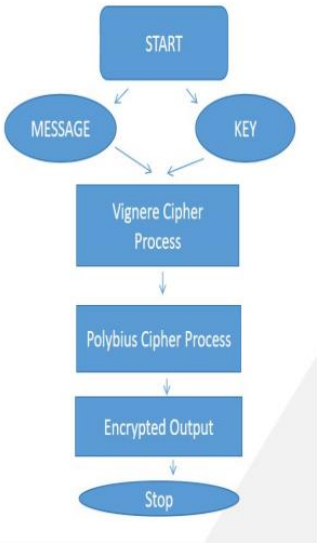

Fig. 2. Enter Caption

B. Polybius Cipher Component:

Description:

The Polybius square is a method for fractionating plaintext characters so that they can be represented by a smaller set of symbols.

Implementation:

Create a 5x5 grid with letters (excluding 'J') and numbers (1-5).

Map each letter of the alphabet and numbers to coordinates on this grid.

Key Generation:

No specific key is required for this component.

Encryption Process:

Replace each letter in the message with its corresponding coordinates.

Decryption Process:

Reverse the process to retrieve the original message.

CODE:-

function polybiusCipher(str) var polybius = ''; for (var i = 0; i ¡ str.length; i++) var charCode = str.charCodeAt(i); if (charCode ¿= 65 charCode ¡= 90) polybius += String.fromCharCode((charCode - 65) / 5 + 65) + String.fromCharCode((charCode - 65) else if (charCode ¿= 97 charCode ¡= 122) polybius += String.fromCharCode((charCode - 97) / 5 + 97) + String.fromCharCode((charCode - 97) return polybius;

A. Hybrid preliminary design of Vign'ere and Polybius Ciphers:

V.RESULT

The method most frequently used to ensure data security, privacy, confidentiality, and dependability is cryptography. Cryptographic systems known as single classic ciphers are said to be the least complex and most vulnerable due to their smooth system, many restrictions, and ease of usage. Vigenere Cipher is a well-known cipher, although it has a few

disadvantages as well. In order to overcome the limitations of the Vigentere cipher, a new method is presented that is an improved version that combines the Vigentere encryption with Polybius cipher and is much more resistant to attacks such as Active, passive, Kasiski, and Friedman assaults (attacks). The usage of product tables for encryption makes cryptanalysis, recurrence analysis, men in the middle attacks, frequency analysis, fault analysis assaults, design expectation, and brute force attacks on the suggested technique extremely problematic. Because of the tremendous degree of complexity, dispersion, spread, and confusion in the technique used to construct them, the modified hybrid combination of the Caesar and Vigenere ciphers is incredibly strong and difficult to crack. Although there are many different cryptographic techniques, the research network must nevertheless give this area serious study in order to improve, upgrade, and strengthen data security and privacy.

Our goal is to validate the suggested methodology in the near future by carrying out message performance analyses and security attacks.

CODE:-

```
function polybiusCipherHybrid(output_str) {
   var polybius = '';
   for (var i = 0; i < output_str.length; i++) {
      var charCode = output_str.charCodeAt(i);
      if (charCode >= 65 && charCode <= 90) {
         polybius += String.fromCharCode((charCode - 65) / 5 +
65) + String.fromCharCode((charCode - 65) % 5 + 1);
      } else if (charCode >= 97 && charCode <= 122) {
         polybius += String.fromCharCode((charCode - 97) / 5
+ 97) + String.fromCharCode((charCode - 97) % 5 + 1);
      }
   }
   return polybius;
```

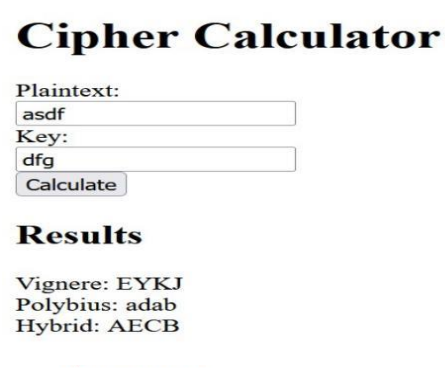

Fig.3: Output of hybrid ciphers.

REFERENCES

[1] [1] 2020 International Conference on Computational Performance Eval- uation (ComPE), North-Eastern Hill University, Shillong, Meghalaya, India. July 2–4, 2020.

[2] [1] (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 8, No. 6, 2017

[3] [1] International Journal of Scientific & Engineering Research Volume 4, Issue3, March-2013 1 ISSN 2229-5518.

[4] [1] Originally published in IEEE Communications Magazine November 1978 — Volume 16, Number 6.

[5] [1] K. Jakimoski, "Security techniques for data protection in cloud computing," International Journal of Grid and Distributed Computing, vol. 9, no. 1, pp. 49–56, 2016.

[6] [1] A. A. Soofi, I. Riaz, and U. Rasheed, "An enhanced vigen'ere cipher for data security," Int. J. Sci. Technol. Res, vol. 5, no. 3, pp. 141–145, 2016. P. Kumar and S. B. Rana, "Development of modified aes algorithm for data security," Optik, vol. 127, no. 4, pp. 2341–2345, 2016.

[7] [1] A. Saraswat, C. Khatri, P. Thakral, P. Biswas et al., "An extended hybridization of vigen´ere and caesar cipher techniques for secure com- munication," Procedia Computer Science, vol. 92, pp. 355–360, 2016