Cryptography Analysis Through Hybrid Model Algorithm

Nitya Veeran* and S. Sheeja†
Dept. of Computer Science, Karpagam Academy of Higher Education, Coimbatore, India

Keywords: Vigenere Ciphers, Polybius Ciphers, Cipher Key, Cryptography, Encryption, Decryption.

Abstract: Cryptography is derived from a Greek word that means the technique to safeguard information by transforming to an unintelligible form. It is a combination of mathematics and computer s-cience. With the rapid growth of the internet, concerns over security and privacy have increased. However, numerous applications have been created without taking into account the fundamental goals of data security, including protection, confidentiality, and authentication. As we become more reliant on information networks for our daily activities, it is important to understand these security issues to prevent unauthorized access to data. Cryptography is needed to prevent undesired users or individuals from accessing the data. In order to offer more security than traditional ciphers, the article suggests a novel hybrid security cipher that combines two of the most significant ciphers, the Polybius Cipher and the Vigenere Cipher.

1 INTRODUCTION

Today's world, technology has advanced to the point where people prefer using the internet as their basic means of exchange information throughout the globe. The internet offers various ways to communicate information quickly and accurately, such as emails and chats. However, sending data over the internet also poses a security risk, as personal and private information can be intercepted or hacked in different ways (Timothy & Santra 2017). However, there are highly sophisticated methods that Attacker may use to achieve their goals such as:

Advanced Persistent Threats (APTs): APTs are highly targeted attacks that are specifically designed to infiltrate a network or system and remain undetected for a long time to gather sensitive information.

Zero-Day Exploits: These are susceptibility in software or hardware that are not known to manufacturer or developer. Hacker can exploit these vulnerabilities to access the systems.

Advanced Malware: Advanced malware such as rootkits, Trojans, and backdoors are highly sophisticated and difficult to detect. These malwares can be used to gather sensitive information or unauthorized person can access to a system.

As it is crucial to emphasize data security as one of the pivotal factors during the process of transferring data. cryptography plays a vital role in ensuring it. Cryptography is an ancient and secure method of protecting information in the public system. The Greek words "kryptos" and "graphein," which both mean "hidden" or "secret," are where the word "cryptography" originates. So, writing and deciphering secret codes or messages is the art and science of cryptography. It involves techniques that transform readable messages into unintelligible or encrypted text to secure the information from an unauthorized access or interception. However, the objective of cryptography is not only to provide confidentiality but also to provide solutions to other issues such as non-repudiation, authentication, and data integrity. Such security can be achieved by use of digital signatures and time stamping and by encrypting the data using a symmetric or asymmetric encryption algorithm. Cryptography is a term used to encompass techniques that allow important information and transmitted of data in a encrypted format, to avoid for an unauthorized person to access the information (Qadir & Varol 2019).

Encryption is the process of transforming plain text into cipher text, an unintelligible format. The main purpose of encryption is to protect once's

* Final Year PG Student
† Professor

Veeran, N. and Sheeja, S.
Cryptography Analysis Through Hybrid Model Algorithm.
DOI: 10.5220/0012611700003739

In *Proceedings of the 1st International Conference on Artificial Intelligence for Internet of Things: Accelerating Innovation in Industry and Consumer Electronics (AI4IoT 2023)*, pages 227-233
ISBN: 978-989-758-661-3

information from unauthorized access, theft, and manipulation. In encryption, a key and an encryption algorithm are used to transform the original plaintext into an encrypted representation. The encryption algorithm uses a mathematical function to transform the plaintext into cipher text (Soofi et al 2016). The key is a sequence of bits that determines how the encryption algorithm will transform the plaintext. The cipher text is converted back into plaintext using the key. Different methods of encryption, including symmetric and asymmetric encryption, are available. In symmetric encryption, the same key is used for both encryption and decryption, whereas in asymmetric encryption, a public key is used for encryption and a private key is used for decryption. Encryption is used widely in various applications, such as secure communication over the internet, data protection, digital signature, and access control. Cryptography uses encryption as one of its main tools to protect information from unauthorized access, interception, or modification.

However, cryptography also includes other techniques, such as digital signatures, message authentication codes (MACs), and key management protocols, to ensure data integrity, authentication, and non-repudiation (Qadir & Varol 2019). These techniques collectively help to secure data transmission and storage in various applications such as online banking, e-commerce, electronic voting, and communication.

Symmetric key encryption and asymmetric key encryption are the two main types of key-based cryptography employed. The same key is utilised in symmetric key encryption (Verma et al 2012) for both the encryption and decryption processes. This is a straightforward and effective encryption technique, however the key distribution problem needs to be resolved first. Asymmetric key encryption, on the other hand, utilizes two mathematically related keys: a public key and a private key. Everyone has access to the public key, which is used to encrypt data. However, the private key of an authorized recipient is the only way to decrypt the encrypted data. Overall, both symmetric and asymmetric key encryption are important techniques in cryptography for securing data and ensuring confidentiality, integrity, and authenticity of information.

2 LITERATURE REVIEW

In today's world, the security of online transactions and personal information such as bank account passwords, email account passwor---ds, etc. is crucial. This requires the use of encryption techniques to ensure the confidentiality of the information. The encryption standard used determines the level of security provided, and the rounds of calculation to be performed during the encryption process determines, level of resistance to attacks by intruders, hackers, and software engineers. The Caesar cipher, a substitution cipher that substitutes the plaintext of each letter with a fixed number of locations across the alphabet, is one of the simplest and most well-known encryption methods. However, this encryption technique is easily broken and provides no confidentiality and security in modern times.

To provide better security, a combination of encryption techniques such as the Vigenere Cipher and ROT13 framework can be used to create a more complex and secure encryption plan.Vigenere Cipher is a polyalphabetic substitution cipher based on a keyword that employs a variety of Caesar ciphers. The Vigenere Cipher requires the user to choose a keyword and repeat it until it is the same length as the plaintext message in order to encrypt a message. Then, a numerical value is given to each letter in the keyword based on where it appears in the alphabet (A = 0, B = 1, C = 2, etc.).

These numerical values are used to change the plaintext message's letters, resulting in a new, more secure cipher message than the Caesar cipher.The ROT13 framework, commonly referred to as the "rotate by 13 places" cipher, is a straightforward replacement cipher that changes every letter in the plaintext message to the letter that is 13 alphabetical positions further up. As an illustration, A would be changed to N, B to O, C to P, and so on. This method is frequently used for straightforward encryption of innocuous data, such online forums or crossword puzzles. However, because it is so easily cracked, it is not a reliable encryption method for sensitive data.

By combining the Vigenere Cipher and ROT13 framework, a more secure encryption plan can be created. The Vigenere Cipher can be used as the primary encryption technique, while ROT13 can be used to obscure the underlying cipher. This would make it more difficult for an attacker to crack the cipher, as they would first need to understand that ROT13 is being used and then use more advanced techniques to break the Vigenere Cipher(Mandal et al 2016). Overall, combining encryption techniques can help to create a more secure encryption plan by leveraging the strengths of each technique while minimizing their weaknesses.

A message could be encrypted by Vigenere Cipher with a keyword as "SECURE" and then further encrypted using ROT13. The resulting cipher

text would be difficult to break as an attacker would first need to determine that ROT13 is being used, and then use more advanced techniques to break the Vigenere Cipher.

For instance, let's say we want to encrypt the message "ATTACK AT DAWN" using the Vigenere Cipher with a keyword of "SECURE". First, we would repeat the keyword until it matched the message's length.

The next step would be to encrypt each letter of the message with the matching letter of the keyword using the Vigenere Cipher.

The resulting ciphertext can be "SXVUSRSSFUUFV", which can be further encrypted using ROT13 to obscure the underlying Vigenere Cipher.

The final ciphertext, "FKHIHEFFHSHSI", is a combination of the Vigenere Cipher and ROT13 framework and would be more difficult for an attacker to break than using either cipher alone.

The transposition cipher is a type of encryption system that involves changing the positions of units of plaintext based on a standard structure or model. This results in a ciphertext that contains a phase of the original plaintext. In a modified version of the Vigenere cipher algorithm, instinctive piece is added to every byte and bit before encryption using the Vigenere cipher. This helps to prevent Kasiski attacks aimed at finding the length of the key. However, the drawback of this approach is that it increases the size of the encrypted text by approximately 56%. New technique for implementing the Vigenere Cipher algorithm, which involves using a combination of alphabetic, numerical, and punctuation marks as the key instead of just characters. An attackers face problem to crack the encryption word. The sentence emphasises the significance of data security in the public internet infrastructure and refers to the suggested hybrid architecture, which combines the AES and DES algorithms for more robust encryption. The integration of these two algorithms would favour,high level of security in encryption format. The proposed technique has shown significant improvement in results compared to other encryption algorithms.

However vigenere square ciphere on the other hand was considered more secure than the vignere cipher with ROT13 because it used more complex encryption process.In addition ,the longer the key used in the cipher,the more difficult it was to break.Before the advent of Modern computer and algorithm,the vigenere square cipher was often used for important communication such as military orders and diplomatic messages.

3 THEORIES

The internet poses a significant risk to computer security as it is a global network that is vulnerable to viruses and malware that can compromise personal information. To maintain the security of a computer and its network, various aspects of computer security need to be considered. These include privacy, confidentiality, non- repudiation, data integrity, authentication, and availability.

Privacy involves keeping confidential information away from unauthorized individuals. Encryption technology can be used to ensure that only the data owner can access the data.

Confidentiality, on the other hand, involves implementing rules or agreements to limit access to certain types of information.

Non-repudiation ensures that the authenticity of a signature or message cannot be denied by those involved in the communication.

Data Integrity refers to the reliability and accuracy of data throughout its lifecycle.

Authentication is the method to identity the user who is willing to gain access to a system or message.

Finally, System, application, and data accessibility is ensured via **Availability.**

Cryptography is an important tool for ensuring computer security and has four fundamental components: plaintext, ciphertext, key, and algorithm.

1) Plaintext refers to the readable message, while
2)ciphertext is the unreadable message created through encryption.
3)The cryptography procedure uses the key and both symmetric and asymmetric encryption methods.
4)The method by which encryption and decryption techniques are carried out is known as an algorithm.

Cipher

It is a set of rules and processes used to convert plaintext (unencrypted data) into ciphertext (encrypted data) that is unreadable to unauthorized parties. Cryptography, the science of secret writing,

has been used since ancient times to ensure the confidentiality and privacy of communications
Symmetric and asymmetric ciphers are the two main categories.
The same secret key is used for both encryption and decryption in symmetric ciphers.

The three most popular symmetric ciphers are Advanced Encryption Standard (AES), Blowfish, and Twofish.Data Encryption Standard (DES), RC4, Triple DES (3DES), Polybius Square Cipher, and Vigenere Cipher are all types of encryption.

AES, commonly referred to as Rijndael, is a popular and extremely secure symmetric cipher. It was chosen as the encryption standard for sensitive information by the (NIST) or National Institute of Standards and Technology of the United States. It is no longer advised to utilise DES, an outdated symmetric cipher that is less secure than AES.

Asymmetric Ciphers:
Asymmetric ciphers employ two distinct keys, one of which is a public key for encryption and the other of which is a private key for decryption. Asymmetric ciphers like

Rivest-Shamir-Adleman (RSA),
Elliptic Curve Cryptography (ECC), and
Diffie-Hellman Key Exchange (DH) are among the most widely utilised.

Asymmetric cipher RSA is frequently used and is regarded as being very secure. It is utilized for encryption, key sharing, and digital signatures. The algebraic structure of elliptic curves serves as the foundation for ECC, a more recent asymmetric cipher. It is more trustworthy than RSA and helpful in applications with constrained computational resources. A shared secret key can be established between two parties using the key exchange protocol known as DH via an unsecured channel.

In this paper our focus will be on *Polybius and Vigenere cipher system for the Implementation of Hybrid cipher*.

A. The Polybius Square Cipher
Is a substitution cipher that encrypts plaintext using a square grid. The row and column of the letter in the grid are represented by a two-digit number for each letter of the alphabet. For instance, the number "11" may stand in for the letter "A," indicating that it is located in the grid's first row and first column. Each letter in a message is replaced with its corresponding two-digit number to encrypt it. The ciphertext is created by pairing the resulting numbers together.

Here is an example of how the Polybius Square Cipher works:

Suppose we have a Polybius Square with the following arrangement of letters:

1	2	3	4	5
A	B	C	D	E
F	G	H	I/J	K
L	M	N	O	P
Q	R	S	T	U
V	W	X	Y	Z

Figure 1: Polybius.

To encrypt the message "HELLO", we would first find the row and column of each letter in the grid, and then write the corresponding pair of numbers:

H - > 2 3
E - > 1 4
L - > 3 1
L - > 3 1
O - > 4 2
So the encrypted message would be
"23 14 31 31 42".
To decrypt the message, we simply reverse the process by looking up the letters corresponding to each pair of numbers in the grid.

3.1 The Algorithm for Polybius Square Cipher Is as Follows

- Create a 5x5 grid and fill it with letters or numbers in a specific order.
- Split the plaintext into individual characters.
- Find the row and column of each character in the grid.
- Write the corresponding pair of numbers.
- Repeat for each character in the plaintext.
- The resulting ciphertext is the sequence of number pairs.
- To decrypt, look up the letters corresponding to each pair of numbers in the grid.

B. Vigenere Cipher
A polyalphabetic replacement cipher called Vigenere uses a variety of Caesar ciphers based on a keyword. Blaise de Vigenère popularised it after Giovan Battista Bellaso created it in the middle of the 16th century.
The earlier ceaser cipher, a straightforward substitution cipher that swaps out each letter in the plaintext with a letter a predetermined number of

positions down the alphabet, has been updated to a highly secure form. The keyword is repeated throughout the plaintext message as many times as necessary to cover its entirety. Each letter in the keyword correspond to a ceaser cipher with a different shift value. To encrypt each letter in the message, the row corresponding to the plaintext letter and the column corresponding to the keyword is intersected (Mittal et al 2019).

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Figure 2: Vigenere cipher.

Example

Encryption:

Step 1: Select a Message to Encrypt Message-“HELLO”

Step 2: Select a key Key-LEMON

Step 3: Expand the key

"H E L L O L E M O N"

Now, consider plain text in column wise and key in row wise, the row and column corresponding letter is a key letter

H in row,L in column = S E,E =I L,M=X L,O=Z O,N=B

Cipher key : S I X Z B

Decryption:

Cipher key: S I X Z B

Key : L E M O N

Original text: H E L L O

The Vigenere Cipher is susceptible to frequency analysis assaults, in which an attacker decodes the plaintext by examining the frequency of the ciphertext characters (Mittal et al 2019). The cipher is also susceptible to well-known plaintext assaults, in which a perpetrator uses knowledge of a small number of plaintext-ciphertext combinations to figure out the key and decrypt a larger number of ciphertexts.

Despite being more secure than the Vigenere Cipher, the Polybius Square Cipher is still susceptible to numerous attacks. An attacker may, for instance, test all possible keys using a brute-force attack or use known plaintext or chosen plaintext assaults to extract portions of the key.

A combination of the Vigenere and Polybius Square ciphers may offer greater security than any one used alone.

4 METHODOLOGY

Hybrid cryptographic system is a complex and challenging task, and it requires careful consideration of the security properties and vulnerabilities of each individual component as well as how they interact with each other (Taha et al 2017). In this answer, I will describe a possible approach to combining the Vigenere Cipher and Polybius Square Cipher, but please note that this is not a proven or rigorously analyzed system and should not be used for security-critical applications.

The general idea of the hybrid system is to use the Vigenere Cipher to encrypt the resulting ciphertext (Vatshayan et al 2020) by a key that is generated from the plaintext itself Polybius Square Cipher to encrypt the plaintext (Maity 2014), and then use. The Vigenere Cipher and Polybius Square Cipher's inverse operations are then used to reverse-decrypt the generated ciphertext.

Algorithms for encryption and decryption of hybrid Vigenere-Polybius Cipher is as follow:

A. Encryption:

Create a vigenere square by writing the alphabet out multiple times in rows, each time shifting it over by one letter. This creates a 26* 26 grid of letters.

Choose a keyword for the vigenere cipher wite the keyword repeatedly above the plain text message, aligning each letter of the keyword with the letter corresponding to the message.

Using the Vigenere square, locate the letter that crosses both the message letter's column and row.

The output compared with Polybius cipher with 5*5 grid.

The result of Polybius is the encryption output.

B. Decryption:

The output of encryption is compared with Polybius square 5*5 grid.
The resultant of Polybius is computed with cipher text key (Arroyo 2020).
Convert the ciphertext number back to letter using vigenere square cipher
Identify the intersection of the keyword letter's row and column in the cipher text. This letter has been decoded.
Wrap around to the start of the keyword if necessary, and repeat step 4 for each letter of the cipher text and keyword.
The resulting letters are the plaintext.

A. Encryption:

Phase1: **(**Vigenere cipher)
STEP 1: Message-NIPHAVIRUS
STEP 2: KEY-BAT
STEP 3: OUTPUT-OIIIAOJANT

Phase 2: (Polybius Cipher)
STEP 4: TEXT-OIIIAOJANT
STEP 5: Output- 43424242114342113344

B. Decryption:

Phase 1: (Polybius cipher)
STEP 1: MESSAGE-43
STEP 2: OUTPUT-O
Phase 2: (vigenere cipher)
STEP 3: TEXT-O
STEP 4: KEY-BAT

STEP 5: OUTPUT-N

5 CONCLUSION

In conclusion, cryptography is a fundamental aspect of modern-day communication and data security. To ensure confidentiality, integrity, authenticity, and non-repudiation of data which involves the use of mathematical algorithms to encrypt and decrypt message.

The hybrid Vigenere-Polybius Cipher is a combination of two classical ciphers that offers enhanced security for data encryption. The Vigenere Cipher provides a layer of security through its polyalphabetic encryption approach while the Polybius Square Cipher adds another layer of security through its coordinate-based encryption approach (Agarwal & Patankar 2016).

The hybrid strategy combines the capabilities of the Vigenere Cipher and Polybius Square Cipher, making it more challenging for attackers to interpret the message even though both ciphers have their drawbacks when employed alone. It is crucial to remember that even the hybrid cipher has its flaws and is not totally secure. Therefore, it is important to continue to develop and implement stronger encryption algorithms to ensure data security.

REFERENCES

Timothy, D. P., & Santra, A. K. (2017, August). A hybrid cryptography algorithm for cloud computing security. In 2017 international conference on microelectronic devices, circuits and systems (ICMDCS) (pp. 1-5). IEEE.

Qadir, A. M., & Varol, N. (2019, June). A review paper on cryptography. In 2019 7th international symposium on digital forensics and security (ISDFS) (pp. 1-6). IEEE.

Soofi, A. A., Riaz, I., & Rasheed, U. (2016). An enhanced Vigenere cipher for data security. Int. J. Sci. Technol. Res, 5(3), 141-145.

Verma, S., Choubey, R., Soni, R., & Ogi, P. (2012). An efficient developed new symmetric key cryptography algorithm for information security. International Journal of Emerging Technology and Advanced Engineering, 2(7), 18-21.

Mandal, S. K., & Deepti, A. R. (2016). A cryptosystem based on vigenere cipher by using mulitlevel encryption scheme. International Journal of Computer Science and Information Technologies, 7(4), 2096-2099.

Mittal, V.K., & Mukhija, M. (2019). Cryptosystem based on modified Vigenere cipher using encryption technique. International Journal of Trend in Scientific Research and Development (IJTSRD) International Journal of Trend in Scientific Research and Development, 3(5), 1936-1939.

Taha, A. A., AbdElminaam, D. S., & Hosny, K. M. (2017). NHCA: Developing new hybrid cryptography algorithm for cloud computing environment. International Journal of Advanced Computer Science and Applications, 8(11), 479-486.

Vatshayan, S., Haidri, R. A., & Verma, J. K. (2020, July). Design of hybrid cryptography system based on vigenère cipher and polybius cipher. In 2020 international conference on computational performance evaluation (ComPE) (pp. 848-852). IEEE.

Maity, M. (2014). A modified version of polybius cipher using magic square and western music notes. International Journal For Technological Research In Engineering, ISSN, 2347-4718.

Arroyo, J. C. T., Dumdumaya, C. E., & Delima, A. J. P. (2020). Polybius square in cryptography: a brief review of literature. International Journal, 9(3).

Agrawal, A., & Patankar, G. (2016). Design of hybrid cryptography algorithm for secure communication. International Research Journal of Engineering and Technology (IRJET), 3(01), 1323-1326.