Journal of the Nigerian Association of Mathematical Physics
Volume 57(**June – July** *2020 Issue*), **pp127 – 134**

AN ANALYSIS OF CRYPTOGRAPHY WITH EMPHASIS ON CLASSICAL CRYPTOGRAPHY

S.S. Daodu[1] and E. Akinola[2]

[1]Department of Computer Science, University of Benin, Edo State, Nigeria
[2]Department of Computer Science, The Federal University of Technology Akure, Ondo State

Abstract

In this Paper, we gave an analysis of Cryptography with emphasis on Classical Cryptography. Cryptography is the coding of messages so as to render them unintelligible to other than authorized recipients. Classical Cipher is a type of Cipher that was used historically but now has fallen for the part into disuse. In section 2.0 we presented literature review of cryptography while in section 3.0 we gave the objectives of classical cipher and showed of the classical information channel. In section 4.0 we presented an example of a specific application of a classical cipher which involves the use of the Hill Cipher, multiletter or polyalphabetic cipher. Section 5.0 is the conclusion where we stated that some classical ciphers have fallen for the part, into disuse (which is also true of some modern ciphers), Polyalphabetic substation cipher can be used to strengthen modern ciphers.

***Keywords*:** Cryptography, Classical Cipher, Polyalhabetic, Substitution Cipher.

1.0 Background of Study

According to [3], cryptography is the coding of messages so as to render them unintelligible to other than authorized recipients. The message that is to be encrypted (processed by the sender in order to render it unintelligible to other than authorized recipients) is known as plaintext. In [5], it is stated that the algorithm to encrypt the plaintext is parameterized by a key and the plaintext message that has been encrypted by the function and key is known as ciphentext. Encryption which involves a mathematical manipulation of the data is generally referred to as message authentication code (MAC).

In cryptography, a classical cipher is a type of cipher that was used historically but now has fallen, for the most part, into disuse. In contrast to modern cryptographic algorithms, most classical ciphers can be practically computed and solved by hand. However, they are also usually very simple to break with modern technology. The term includes the simple systems used since Greek and Roman times, the elaborate renaissance ciphers, world war II cryptography such as the Enigma machine and beyond.

Historically, there are two categories of encryption methods: Substitution and Transposition ciphers.

In a substitution cipher, letters (or groups of letters are systematically replaced throughout the message for other letters or group of letters).

In a transposition cipher, the letters themselves are kept unchanged, but their order within the message is scrambled according to some well-defined schema. Many transposition ciphers are done according to a geometric design. More complex algorithms can be formed by mixing substitution and transposition in a product cipher.

On encryption, [5], stated that Public Key encryption is probably one of the most heavily used methods to prevent unauthorized individual from reading information that is not intended for them. This scheme notes just a secret key for both the sender and the receiver, and this can be easily compromised. The author however stated that in public key cryptography, there are two pairs of key involved – a public key and a private key. The encryption/decryption scheme is designed so that one key cannot be derived from the other. This type of double-key encryption/decryption make it very difficult for an unauthorized party to decrypt the message. The public/private key sets that are used by the sender and receiver are specific and cannot be used on another message from a different system. Using two keys where one is private and other part of the set is public is safe because the encrypt and decrypt functions have a one-way property. Either key can be used to encrypt or decrypt a message, but either key by itself cannot perform both functions on the same message. A very critical element in public key cryptography is how the keys are delivered to the proper systems. To facilitate the proper exchange of keys and to generate the keys. In [5], it is further stated that a Certificate Authority (CA) or Key Distributed Centre (KDC) is involved. The CA is either an internal or an external entity that is responsible for verifying who the sender and receiver are,

Corresponding Author**:** Daodu S.S., Email: segedaodu@gmail.com, Tel: +2348130762937

generating the public private key sets for the two entities, delivering the public key to both parties, and delivering the private keys to their respective owners. To authenticate the message's sender, a digital signature can be used, i.e. the message can be digitally signed. A common authentication protocol used in digital signature implementation in Kerberos.

According to [5], a limitation in the use of encryption technology is that although, it help to provide secure transmission of private information over a public network, but it does provide any means to keep our unwanted traffic from the network.

cryptography plays an important role in security. The purpose of cryptography is to take a message or file, called plaintext and encrypt it into ciphertext in such a way that only authorized people know how to convert it back to plaintext. "The secrecy depends on parameters to the algorithms called keys. If P is the plaintext file, KE is the encryption key, C is the ciphertext, and E is the encryption algorithm, then $C = E(P, K_E)$ defines encryption. The idea that algorithm should all be public and the secrecy should reside exclusively in the keys is called Kerckhoffs' Principle. Similarly, $P = (DCC, K_D)$ where D is the decryption algorithm and K_D is the decryption key",[23].

2.0 Literature Review

In [12] a work titled "Classical Encryption Techniques" was presented. The objective of this research was to propose a technique which combines the features of modern cryptography with classical cryptography to get a more secured technique for data encryption. The motivation of this research was to get a safe means where data can be channeled for effective communication without the integrity of the data being compromised, thereby ensuring security. The methodology used in the work fuses positive features of both classical and modern encryption techniques. It uses the advantage of the usage a key in modern cryptography and combines it with scrambling of bit in classical cryptography algorithm. It is a simple, direct, mapping algorithm that uses matrix and arrays. The poly alphabetic cipher text generation makes this technique strong while the combination of poly alphabetic substitution, translation and transportation makes the decryption extremely difficult in absence of a secret key.

The authors also noted that data encryption is the most effective way to ensure information security in an open networked system. Two classes of encryption techniques were discussed in their work namely: (i) Symmetric-key encryption which involves the use of private keys only and (ii) Asymmetric-key encryption which involves the use of public and private keys. Symmetric-key Cryptography is faster than the Asymmetric-key Cryptography, and these two techniques are extensively used to solve the traditional problem of communication over an insecure channel. There are different classical encryption techniques that are used to protect confidential both image data and text data from unauthorized users.

These include:

a) **Block Cipher**: This technique involves substitution and transposition techniques where substitution means replacing an element of the plaintext with an element of the cipher text. Transposition or permutation here means rearranging the order of appearance of the elements of the plaintext.

b) **Symmetric Cipher Model:** This technique has 5 components which are:

(i) **Plaintext:** This is the original intelligible data that is fed as input into the algorithm.

(ii) **Encryption Algorithm:** This is the algorithm that performs different substitutions and transformations on the plaintext.

(iii) **Secret Key:** This key is a value that is independent of the plaintext and also independent of the algorithm in use. The algorithm will produce a different output depending on the specific key being used at the time.

(iv) **Cipher Text:** This is the message that is scrambled and produced as output. It depends largely on the plaintext and secret key.

(v) **Decryption Algorithm:** This is when the encryption algorithm is run in reverse. It takes the cipher text and the secret key and uses them to produce the original plaintext.

Some substitution techniques discussed in this work are:

Cipher text: DUH BRX UHDGB

A general version of this cipher that allows for any degree shift would be expressed as $C = E(k,p) = (p+k) \bmod 26$ and the formular for decryption will be:

$P = D(k,C) = (C-k) \bmod 26$

In these formula, 'k' would be the secret key while the symbols 'E' and 'D' represent encryption and decryption.

a. Mono-alphahetic Ciphers: In this cipher, the substitution characters are a random permutation of the 26 letters of the alphabet:

Plaintext letters: a b c d e f .....

Substitution letters: t h I j a b .....

The key here is the actual random permutation of alphabets used which is the sequence of substitution letters. If the nature of the plaintext is known, any substitution cipher irrespective of the size of the key space can be broken easily with a statistical attack of a number larger than $4 \times 10\text{^}26$ since there are 26! Permutation of the alphabet. The Caesar Cipher which is an example of a mono-alphabetic cipher is given below

b. Caeser Cipher: In this method, each character of a message is replaced by a character three position down in the alphabet. An example is given below:

Plaintext: are you ready?

c. Multi Character Encryption to Mask Plain Text Structure: This Cipher is also known as Playfair Cipher. This cipher involves the construction of a 5×5 matrix whereby an encryption key is first chosen after which letters of the key is entered in a left to right manner

starting with the first cell at the top-left corner. Two plaintext letters that fall in the same row are replaced by letters to the right of each row while two plaintext letters that fall in the same column are replaced by the letters just below them in the column. And for each plaintext letters in a pair, replace it with the letter that is in the same row but in the column of the other letter.

d. Dealing with Duplicate Letters in a Key and Repeating Letters in Plaintext: Duplicates in a key must be dropped. Before applying substitution rules, a chosen letter must be inserted between any repeating letters in the plaintext such that a plaintext word such as "hurray" now becomes "hurxray".

e. Play Fair: The cryptanalysis of the playfair cipher is also aided by the fact that a diagram and its reverse will encrypt in a similar fashion. That is if AB encrypts to XY, then BA will encrypt to XY. This cipher is very easy to break in that by looking for the words that begin and end in reversed diagrams, one can compare them with plaintext words that are similar.

f. One Time Pad: The key is used to encrypt and decrypt a single message and then it is discarded which means that the key can be used once. Each new message requires a new key of the same length as the new message and this makes it unbreakable. This algorithm provides complete security but faces two practical issues which are (i) The problem of making large quantities of random keys and (ii) The problem of key distribution and protection because for every message to be sent, a key of equal length is needed by both sender and receiver.

The authors also discussed some techniques in modern cryptography. These techniques include:

a) S-DES: This process has key generation instead of using key as it is for encryption and the key generation process of S-DES generates 2 sub keys after processing the initial 10 bit input, it has 8 bit plaintext input the two sub keys are generated at both transmission and receiving ends. This algorithm gave some structure and formation to encryption techniques with step to step procedures for both encryption and decryption.

b) DES: This process enhances the structure of S-DES by increasing the key size from 10 bits to 64-bits out of which its effective length is 56-bits. Sixteen keys are generated and each of the 48-bits strengthens the security of this algorithm, and in terms of processing DES is 3 times faster than S-DES.

The limitation of this work was that in the absence of a secret key, if poly alphabetic substitution, translation and transposition are combined, decryption becomes extremely difficult. However, Poly- alphabetic substitution are easily breakable by an attacker.

In [9], a work titled "Security Analysis and Modification of Classical Encryption Scheme" was presented. Classical encryption schemes such as Caesar Cipher, Shift Cipher, Vigenere Cipher, Affine Cipher and Hill Cipher are considered in this work.

The objective of this work is to develop a classical encryption algorithm in the class of mono-alphabetic substitution cipher and polyalphabetic substitution ciphers that can withstand the frequency and the Kasiski test Algorithm. The motivation of this research is to study classical cryptography schemes and to identify their vulnerabilities. The authors defined cryptanalysis as the art of breaking the keys of various cryptographic algorithms in order to identify the weakness that exists in them. The characters in the plain text were mapped to the integer values where a single key plays the role of a generator key. This key is used for generating as many numbers of keys as equal to the total size (interims of length) of the plain text. In order to ensure enhanced security in this algorithm, the key length is chosen proportionally to the message length and the key is selected either by selecting two communicating entities and also securely transferring it to the other entity by means of public key cryptosystem like RSA or Diffie Hellman.

The authors noted that based on information needed by the cryptanalyst, attacks can be classified into seven (7) categories:

i. Ciphertext Only Attack: In this kind of attack, the known information is the encrypted text only. This is considered the weakest way of doing cryptanalysis because of lack of information about the original data known. Modern Ciphers are strong against these type of attacks.

ii. Known Plaintext Attack: In this kind of attack only prior knowledge about the ciphertext is known and a pair of corresponding plaintext is known. The key used for encryption is publicly available and this allows the cryptanalyst to generate the ciphertext for any given plaintext.

iii. Chosen Plaintext Attack: In this attack, the cryptanalyst is having the right to select a number of plaintext which needs to be encrypted and also able to access the ciphertext. This provides the cryptanalyst to explore over the plaintext to identify the vulnerabilities and non- random behavior which found only with specified plaintext.

iv. Chosen Ciphertext Attack: In this class of attack the cryptanalysis is having the right to select a number of ciphertexts which need to be encrypted and also able access to the corresponding plaintext.

v. Brute Force Attack or Exhaustive Key Search: In this category of attack, the attacker tries with all possible keys until the retrieval of the original key. All Ciphers existing are susceptible to this attack excluding the one-time pad. Security depends both on the cipher as well as the length of the key.

vi. The Weird Equivalent Privacy: This is a kind of private protocol that is used to protect Wi-Fi internet devices and it is vulnerable to key search attacks.

vii. Side Channel Attack: This attack does not happen by doing any cryptanalysis with the encrypted data and it does not depend on the strength of the key or the encryption algorithm. It uses mainly other meta data about the encryption or decryption by which acquire some information about the message.

The limitations encountered in this work is that it involves the use of multiple keys for encryption and decryption and also other types of attacks were not discussed in this work.

In [2], a work titled: "A Review on Classical and Modern Encryption Techniques" was presented. The objective of their work was to develop an algorithm for encryption and the motivation was to carry out a detailed comparison between various classical and modern encryption techniques in order to achieve a secured cryptography technique in an electronic society. According to the authors, signature is a fundamental tool required for information security and it is a building block for many other services such as non- repudiation, data

origin authentication and identification. The methodology used in this work is the encryption technique which is a hybrid of Playfair and Vigenere. This combined with modern encryption technique structure of DES and S-DES. This technique begins by producing two sub keys from Playfair and Vigenere to induce more disguise. Black box is introduced in this technique in which 64-bit block size is fed into the box which is divided into 8 octets and these 8 octets take 8-bits each and these 8-bits are divided into two parts R.H and L.H. This technique provides more efficiency of complexity when all the 4 bits of R.H are combined together into forming 32-bits block. The L.H is XORED by R.H and completes the first cycle. The technique used proposes N= 3 cycles of repetitions. The authors stated that cryptography can be divided into two categories: namely Conventional and Public Key Cryptography. Conventional Cryptography uses a Single key for both encryption and decryption process while in Public Key Cryptography, separate keys are used for encryption and decryption processes. In Public key Cryptography excessive communication and processing resources are usually required. Conventional Cryptography in this work is divided into two techniques, namely Classical and Modern techniques. Classical Cryptography techniques discussed in this work are Caesar, Vigenere and Playfair.

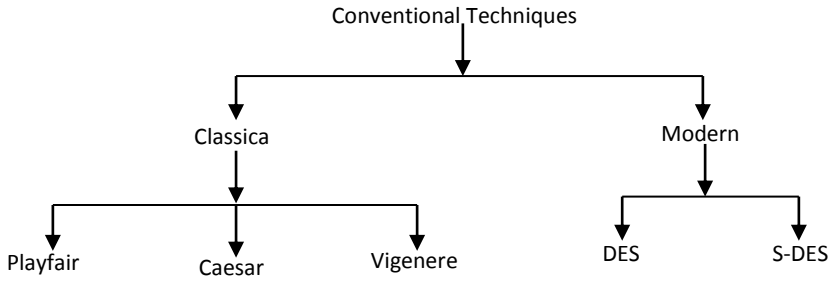

Figure 1: Conventional Cryptography

Caesar Cipher: This is a classical substitution cipher and it is also regarded as one of the simple method of substitution. This algorithm works by replacing the letter of alphabet with a letter that is 3 places ahead of it. An example is "ZULU" will be converted to "CXOX" This Cipher algorithm can easily be broken as there are only 25 possible options of key available.

Vigenere Cipher: This Cipher algorithm is more secured than that of Caesar cipher because in this cipher algorithm there is an introduction of a keyword and this keyword is repeated to cover the length of the plaintext that is to be encrypted. An example is shown below

KEY: f a u z a n f a u z a n
P.T: c r y p t o g r a p h y
Cipher: H R S O T B L R U O H L

From the example above, "fauzan" is the keyword and the plain text is "cryptography" which was encrypted to be "HRSOTBLRUOHL" and this was done using the Vigenere table which contains alphabet in form of rows and columns.

Playfair Cipher: This is another type of Classical Cryptography that has a square of 5 × 5 alphabets letter arranged in an appropriate manner. When a key is selected, it is placed in the matrix and the remaining letters of English are then placed in the matrix of Playfair Cipher. If the pair of letters in same column of matrix then each letter is replaced by the letter in their row that resides at the intersection of paired letters.

Modern Techniques

Modern techniques discussed in this work are S-DES and DES variants.

S-DES: This is referred to as Simplified DES process and has a process of key generation instead of using the same key for encryption and decryption. The generation process of S-DES generates 2 sub keys after processing the initial 10 bit input. It has 8 bit plaintext input and the two sub keys generated are for transmission and receiving.

DES: This enhances the structure of S-DES by increasing the key size from 10 bits to 64 bits out of which its affective length is 56 bits. 16 rounds are introduced with each round containing XOR, substitution and permutation for 16 rounds containing XOR, sixteen keys are generated each of 48-bits which strengthens the security of this algorithm. DES is 3 times faster than 3-DES. DES takes plaintext in 64-bits of block these 64-bits are divided into 32-bits each the right half of 32-bits goes through the expansion block which increases the bit count from 32 to 48 bits by reusing some bits after expansion block comes.

Avalanche Effects

This is the effect in the output cipher text if a single or few bits are changed in the plaintext. Avalanche effect of the proposed technique is given below.

KEY: FAUZANCE
0100011001000001010101101000001010100110101010100010
0010101010010
PLAINTEXT: DISASTER
0100010001001001010011010000010101001101010100010
0010101010010

CIPHER

00010000 0100 000101010111 0100 0111
11100111011 001110001101 11101010

Now there is a change in character of the plaintext will become"DISCSTER"
KEY : FAUZANCE
PLAINTEXT : DISCSTER
CIPHER
11000111 1111 0110 11011100 1111 1100
00101101 0000 1101 00001011 01011111
AVALANCHE EFFECT
Original plaintext's (DISASTER) cipher output
00010000 0100 000101010111 0100 0111
111100111011 001110001101 11101010
Change in one character
11000111 1111 0110 11011100 1111 1100
00101101 0000 1101 00001011 01011111
From the above, it can be seen that there is a 42-bit difference in the cipher of DISASTE and DISCSTER. This means that 65.5% bits were changed when a single character of the Plaintext was changed.
The authors noted that the proposed method in this work is time consuming.
In [14], a work titled "Application of Classical Encryption Techniques for Securing Data - A Treaded Approach" was presented. The objective of the work is to propose a method where encryption and decryption of data will be done in a parallel way using threads. The motivation for the work is to study different classical encryption algorithm to get the best method of crypto operation in a time efficient and secure manner using available hardware technology. The methodology of the proposed method in the work is known as sub division. In this method, the data is divided into a number of small units called chunks of which each chunk is of the same size. Each chunk is moved to the threads and each thread takes a chunk of data as input and encrypts the data which it then gives as the output.
The equation below are used for encryption processes.
$C_p = \text{Plain text} + K_c(\text{Key}) \ldots (1)$ (For encryption process)
$\text{Plaintext} = C_p + K_c(\text{Key})$ (For decryption process)
According to [23], many cryptography systems, like the secret key cryptography have the property that given the encryption key it is easy to find the decryption key and vice versa. Such systems are called secret-key cryptography or symmetric-key cryptography. The author noted that the secret-key systems are efficient because the amount of computation required to encrypt or decrypt a message is manageable, but have a big drawback in that the sender and receiver must both be in possession of the shared secret key. To overcome this problem, public-key cryptography is used. This system has the property that different keys are used for encryption and decryption and that given a well-chosen encryption key, it is virtually impossible to discover the corresponding decryption key.
In some cases, it is possible to have a function, say f, which has the property that given f and its parameter v, to compute y = f(x) will be easy, but given only f(x), to find x will be computationally infeasible. Such a function is called cryptographic hash function; and typically mangles the bits in complex ways.
According to [23], it was further noted that, frequently, it is necessary to sign documents digitally by means of digital signatures, in such that the documents cannot be rejected by the sender. The document is first run through a one-way cryptographic hashing algorithm that is very hard to invent. The hashing function typically produces a fixed length result independent of the original document size. The most popular hashing functions used are MD5 (Message Digest 5) which produces a 16-byte result and SHA-1 (Secure Hash Algorithm) which produces a 20-byte result (NIST, 1995). SHA-256 and SHA-512 are newer versions SHA-1, and produce 32-byte and 64-byte respectively but they are less widely used, [23].
The process of computing a signature block and the result are shown in figure 2.

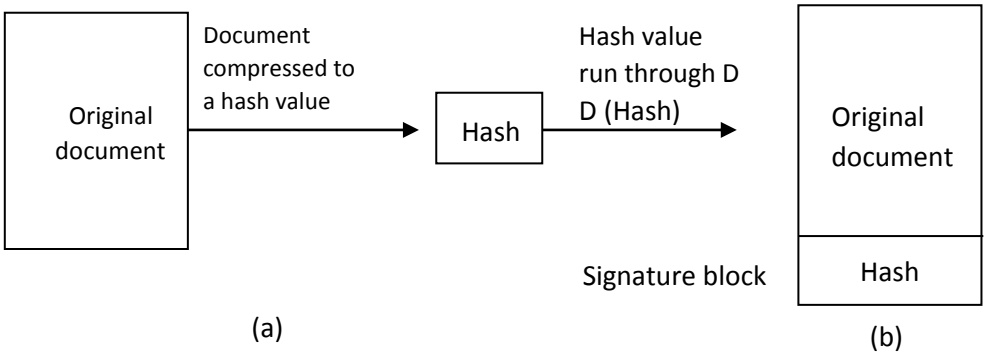

Figure 2: (a) Computing a signature block (b) what the receiver gets

The application of D to the hash is sometimes referred to as decrypting the hash, but it is not really a decryption because the hash has not been encrypted. It is just a mathematical transformation on the hash.

"All cryptography requires keys. If the keys are compromised, all the security based on them are also compromised. Storing the keys securely is thus essential. In order to avoid storing the keys on a system that is not secure, the operating system industry has come up with a chip called the TPM (Trusted Platform Modules), which is a cryptoprocessor with some nonvolatile storage modules inside it. The TPM can perform cryptographic operations such as encrypting blocks of plaintext or decrypting blocks of ciphertext in main memory. It can also verify digital signatures. By doing all these operations in a specialized hardware, they become much faster and are likely to be used more widely" [23]

3.0 Areas of Application

Before Modern era, Classical cryptography was focused on message from a comprehensive form into an incomprehensible one and back again at the other end, rendering it unreadable by interception or eavesdroppers without secret knowledge (namely the key needed for decryption). Also classical cryptography provided secrecy for information sent over channels where eavesdropping and message interception was possible. The sender selected a cipher and an encryption key and either gave it directly to the receiver or sent it indirectly over a slow but secured channel (typically a trusted courier). Messages and replies were transmitted over the unsecured channel in cipher text as shown in figure 3

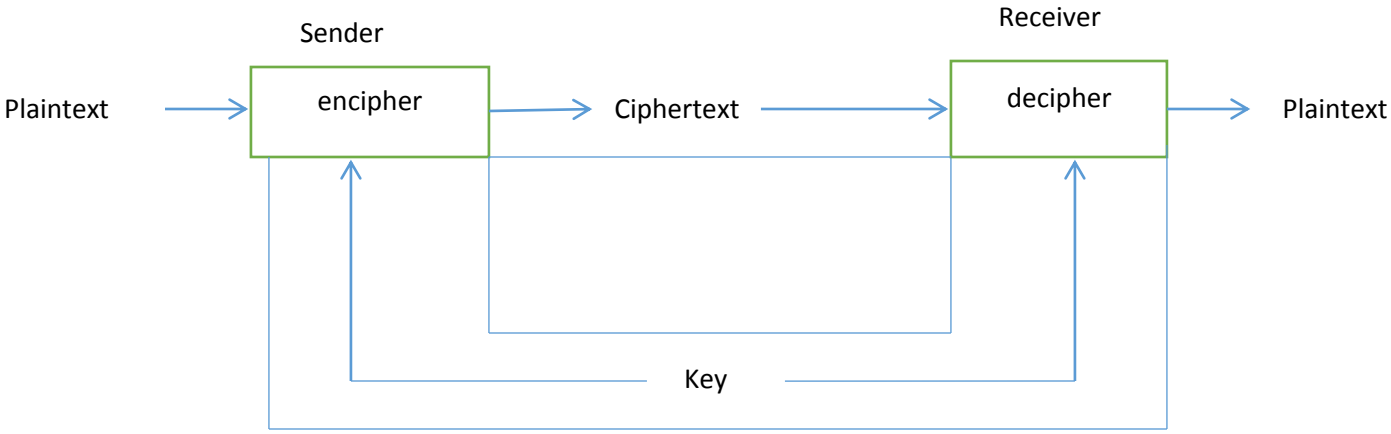

Figure 3: Classical information channel
Source: [4]

4.0 Specific Area of Application

In [10] a work was presented on the Hill Cipher, which according to the author is another interesting multi-letter cipher. The Hill Cipher was developed by the mathematician Lester Hill in 1929. The encryption algorithm takes in successive plaintext letters and substitutes for them in ciphertext letters. The substitution is determined by a linear equations in which each character is assigned a numerical value($a = 0, b = 1 \dots \dots \dots z = 25$). For $m = 3$, the system can be described as follows.

$$\left.\begin{aligned} c_1 &= (k_{11}p_1 + k_{12}p_2 + k_{13}p_3) mod\ 26 \\ c_2 &= (k_{21}p_1 + k_{22}p_2 + k_{23}p_3) mod\ 26 \\ c_3 &= (k_{31}p_1 + k_{32}p_2 + k_{33}p_3) mod\ 26 \end{aligned}\right\} \quad (4.1)$$

This can be expressed in terms of column vectors and matrices:

$$\begin{pmatrix} c_1 \\ c_2 \\ c_3 \end{pmatrix} = \begin{pmatrix} k_{11} & k_{12} & k_{13} \\ k_{21} & k_{22} & k_{23} \\ k_{31} & k_{32} & k_{33} \end{pmatrix} \begin{pmatrix} p_1 \\ p_2 \\ p_3 \end{pmatrix} \text{ mod } 26 \quad (4.2)$$

Or

$c = kpmod\ 26,$

where $c\ and\ p$ are column vectors of length 3, representing the plaintext and ciphertext, and k is a 3×3 matrix, representing the encryption key. Operations are performed mod 26. If we consider the plaintext "paymoremoney" and use the encryption key.

$$k = \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix} \quad (4.3)$$

The first three letters of the plaintext are represented by the vector $(15\ \ 0\ 24), k\ (15\ 0\ 24) = (375\ 819\ 486) mod\ 26 = (11\ 13\ 18) = LNS$.

Continuing in this fashion, the ciphertext for the entire plaintext is LNSHDLEWMTRW.

Decryption requires using the inverse of the matrix k. Recall that the inverse k^{-1} of $kk^{-1} = I$, where I is the identity matrix, i.e the matrix that is all zeroes except for ones along the main diagonal from upper left to lower right.

$I = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ is an example of an Identity of a 3×3 matrix.

Note that the inverse of a matrix exists only if the determinant of a matrix is non zero.

In the case of the matrix in equation (4.3), the inverse is

$k^{-1} = \begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix}$,

i.e $\begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix} \begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix} = \begin{pmatrix} 443 & 442 & 442 \\ 858 & 495 & 780 \\ 494 & 52 & 365 \end{pmatrix} \text{mod}26 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$

If the matrix k^{-1} is applied to the ciphertext, then the plaintext is recovered (Source: Nicholas,).

5.0 Conclusion

We have given an analysis of cryptography with emphasis on classical cryptography. According to [19], [11] and[6], Ciphertexts produced by a classical cipher (and some modern ciphers) will reveal statistical information about the plaintext and that information about the plaintext and that information can often be used to break the cipher. After the discovery of frequency analysis, by Al-Kindi in the 9th century, nearly all such ciphers could be broken by an informed attaity today, though mostly as puzzles. According to [23], although monoalphabetic substitution ciphers are of no longer of interest for serious application, however, some techniques from classical ciphers such as polyalphabetic substitution cipher, examples of which are the the Vinegere Square, the Great Cipher where numbers were used to represent syllables, the Zodiac alphabet, the pigpen cipher and many others can be used to strengthen modern ciphers. Also According to [8], the Mixcolumns step in AES is a Hill Cipher. The Hill Cipher also is of the Polyalphabetic cipher.

REFERENCES

[1] Amador, J. J., & Green, R. W. (2005). Symmetric-key block cipher for image and text cryptography. *International Journal of Imaging Systems and Technology*, *15*(3), 178-188.

[2] Asif, A. M. A. M., & Hannan, S. (2014). A review on classical and modern encryption techniques. *International Journal of Engineering Trends and Technology*, *12*(4), 199-203.

[3] Daintith, J. (2004), cryptography: Oxford Dictionary of Computing, Oxford University Press, Oxford.

[4] Elizabeth D. and Danning R.(1982), Cryptography , Addison, Wesley Publishing Company

[5] Gisin, N., Ribordy, G., Tittel, W., & Zbinden, H. (2002). Quantum cryptography. *Reviews of modern physics*, *74*(1), 145.

[6]. I.M.N Al- Jubouri (2018), " History of Islamic Philosophy: With view of Greek Philosophy and Early History of Islam". Authors on Line Ltd, Retrieved 19 March via Google Books

[7] Karthikeyan, S., Sairam, N., Manikandan, G., & Sivaguru, J. (2012). A parallel approach for improving data security. *Journal of Theoretical and Applied Information Technology*, *39*(2), 2005-2012.

[8] K.C Xintong (2016), Understanding AES Mix-Columns Transformation Calulation, (PDF), Retrieved 26-10-2016

[9] Mohan, M., Devi, M. K., & Prakash, V. J. (2015). Security analysis and modification of classical encryption scheme. *Indian Journal of Science and Technology*, *8*(8), 542-548

[10] Nicholas, R. (1996), Classical Cryptography Course, Laguna Hills, CA: Aegean Park Press

[11] O.Learnan (2015), The Biographical Encyclopedia of Islamic Philosophy, Bloomsbury Publishing. Retrieved 19 March 2018 via Google Books.

[12] Ojha, V., Sharma, A., Lenka, S. K., & Biradar, S. R. (2012). Advantages of Classical Cryptography Over the Quantum Cryptography. *World Appl. Program*, *2*(5), 257-262.

[13] Pfleeger, C. P., & Pfleeger, S. L. (2002). *Security in computing*. Prentice Hall Professional Technical Reference.

[14] Raghu, M. E., & Ravishankar, K. C. (2015). Application of Classical Encryption Techniques for Securing Data-A Threaded Approach. *International Journal on Cybernetics and Informatics (IJCI)*, *4*, 125-132.

[15] Saeed, F., & Rashid, M. (2010). Integrating Classical Encryption with Modern Technique. *IJCSNS International Journal of Computer*, *280*, 280-285.

[16] Saeed, F., Qadir, A. B. A., Mughal, Y. M., & Rashid, M. (2011). A Novel Key Generation for FMET. *IJCSNS*, *11*(6), 197.

[17] Sastry, V. U., Shankar, N. R., & Bhavani, S. D. (2009). A modified playfair cipher involving interweaving and iteration. *International journal of Computer theory and Engineering*, *1*(5), 597.

[18] Sastry, V. U., Shankar, N. R., & Bhavani, S. D. (2010). A Modified Hill Cipher Involving Interweaving and Iteration. *IJ Network Security*, *10*(3), 210-215.

[19] S.Singh (2000), The Code Book,New York: Anchor Books, pp 14-20
[20] Stallings, W. (2017). *Cryptography and network security: principles and practice* (pp. 92-95). Upper Saddle River: Pearson.
[21] Stallings, W. (2003). *Network Security Essentials: Applications and Standards, 4/e*. Pearson Education India.
[22] Stallings, W. (2006). *Cryptography and Network Security, 4/E*. Pearson Education India.
[23] Tanenbaum, A.S. (2009), Basics of Cryptography, Modern Operating Systems. PHI Learning, Private Limited, New Delhi.
[24] Tahghighi, M., Turaev, S., Mahmod, R., Jafaar, A., & Said, M. M. (2011, September). The cryptanalysis and extension of the generalized golden cryptography. In *2011 IEEE Conference on Open Systems* (pp. 65-68). IEEE.