ISSN No:-2456-2165

Advanced Encryption Standard (AES) and Hill Cipher: A Comparative Study

Sreeja P,[1,a)] and Mohit Kumar Sharma [2]
[1]PG scholar ,Department of CSE ,Glocal College of Engineering and Technology, Mirzapur Pole,Saharanpur,UP,India
[2] Head Of the Department of CSE ,Glocal College of Engineering and Technology,Mirzapur Pole, Saharanpur, UP,India
[a)]Corresponding Author

Abstract:- From ancient time onwards encryption techniques are used to alter plain text in to cryptic text, to protect privacy of the message and also to ensure the security of the message. Various algorithms are used for encryption and its sole purpose is to ensure the privacy of the message. The objective of this research article is to decipher and compare the traditional encryption technique Hill Cipher and modern encryption method, the AES. Hill Cipher and AES are part of the symmetric encryption meaning that encryption and decryption process uses the same key and in both Hill Cipher and AES Algorithms, there is only one key for encryption and decryption. Encryption methods using symmetric key are of two types block ciphers and stream ciphers with Hill Cipher and AES Algorithms being examples of the block cipher encryption. This paper encompasses the comparison of the advanced encryption standard (AES) along with Hill Cipher encryption.

Keywords:- *Hill Cipher, Encryption, AES, Decryption.*

I. INTRODUCTION

The way of securing data so that only approved parties can recognize the information is called as encryption. In procedural terms, it is the procedure of altering human-comprehensible plain text to cryptic text. The readable data is taken and modified by encryption, so that it seems arbitrary to unauthorised parties. Multiple encryption techniques are existing which are mostly used in information security, which can be further divided into Symmetric and Asymmetric keys. Only one key is used in symmetric keys encryption or secret key encryption to encode and decode data. Two keys are used one private and one public keys[1] are used in asymmetric keys, where public key is used for coding and private key is used for decoding (e.g. RSA). Public key encoding is created on mathematical functions and computationally intense. Multiple examples of robust and feeble keys of cryptography algorithms like AES and DES. One 64-bits key is used by DES while multiple 128-bit, 192-bit or 256-bit keys with 256-bit key being the most encrypted one[2] are used by AES.

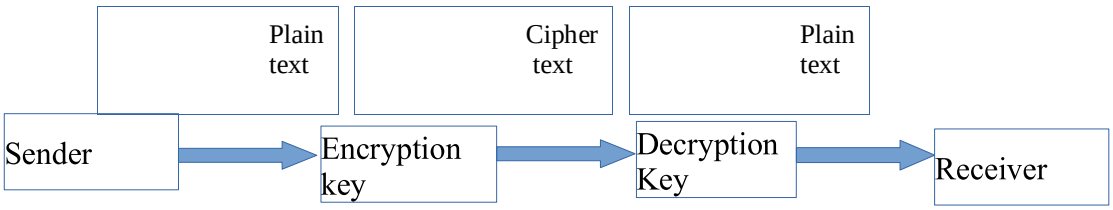

Fig 1.Encryption [3]

Although encoded message appears arbitrary, encoding ensues in a logical and foreseeable way, permitting a party that obtains the encoded data and owns the right key to decode the data, returning it back into normal readable text. Highly complex keys are used by the extremely secure encryption so that an outside party is mostly unlikely to decode or break the coded text. Throughout history, cryptographic codes and encoding methods have been used by multiple civilization in some way or the other to avert un-authorized parties from gaining access to the information which in time have grown in superiority significantly along the times and are used commonly till date.

II. METHODOLOGY

A. *Advanced Encryption Standard (AES)*

Data Encryption Standard (DES), one of the symmetric key encodings is having key length of 56 bits and because of the small key length, it is very easily to be hacked and to overcome this disadvantage The National Institute of Standards and Technology (NIST) developed a novel algorithm called Advanced Encryption Standard (AES) in 1977. The Advanced Encryption Standard (AES) encryption algorithm being the most prevalent symmetric block cipher algorithm has a certain format to encode and decode confidential data which makes it really hard to crack using three diverse key sizes - 128, 192 and 256 bit.

➢ *Working of AES:*

AES prefer bytes to perform operations rather than bits so if the block length is 128 bits, then the cipher calculates 16byts (or 128 bits) at a time. Key length and number of rounds as follows;

- 10 rounds – 128 bit key
- 12 rounds - 192 bit key
- 14 rounds – 256 bit key

ISSN No:-2456-2165

All the round-keys from the key are found out using the key scheduling algorithm. In the corresponding round of the encryption, different round keys will be used which is created by the initial key. Every round has 4 steps that are,

- Sub-Bytes
- Shift-Rows
- Mix-Columns
- Add Round-Key

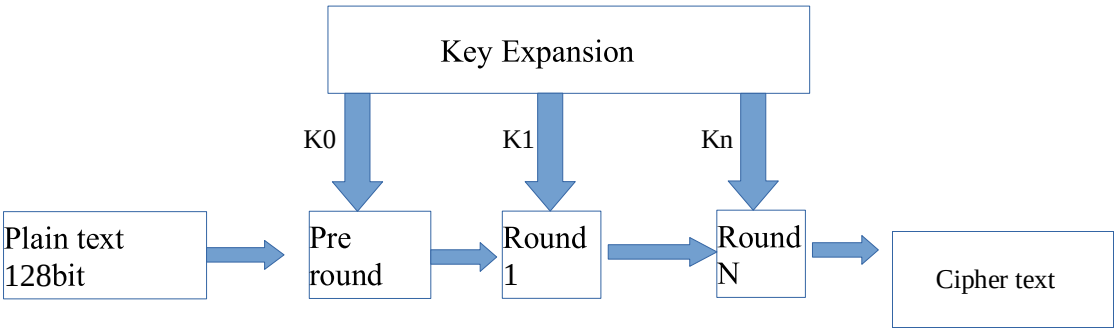

Fig 2. AES Encryption

Numerous transformations are defined by AES encryption algorithm that are to be performed on information stored in an array. The information handed over to the array is the first step of the cipher, followed by multiple encryption rounds which repeats the cipher transformations. The substitution table is used in the initial transformation of the AES encryption cipher for substitution of data. The data rows are shifted in the second transformation followed by mixing of columns in the third one. The final transformation is performed on individual column using a different part of the encryption key. More rounds are needed by Longer keys to complete the iteration.

B. HILL Cipher

Hill Cipher is an example of block cipher using the form of matrix in cryptography. Square matrix is used as a key for encoding and decoding in this encryption method. In 1929, Lester S. Hill created The Hill cipher with the intention of creating a cipher (code) that should be unbreakable by using frequency analysis methods. This encryption technique do not alter every similar alphabet in the plain text with other letter in the same cipher text because it employs matrix multiplication for encoding and decoding. Hill Cipher is a multi-alphabetic cipher that could be defined as a block cipher as the data to be encrypted be partitioned into blocks of a fixed limit. Individual alphabet in each block will affect the next one in the encoding and decoding process, there for the similar alphabets are not mapped into the similar characters. Hill Cipher is one of the typical cryptographic algorithms that is hard for cryptanalysts to crack and is only accomplished by percieving the cryptic text. The drawback of this technique is that it can be solved very easily if the cryptanalysts have both plain text and cipher text. This cryptanalysis method is known as plain text attack.

Encryption technique in the Hill Cipher is calculated by the extent of the block and the key matrix size is same as the size of the block. Before doing the calculation, first divide the plain text to rows of blocks and the alphabet is initially converted in to a number that A is given the value 0, B is given the value 1, up to Y = 24 and Z = 25.

A is equal to 0	B is equal to 1	C is equal to 2	D is equal to 3	E is equal to 4	F is equal to 5
G is equal to 6	H is equal to 7	I is equal to 8	J is equal to 9	K is equal to 10	L is equal to 11
M is equal to 12	N is equal to 13	O is equal to 14	P is equal to 15	Q is equal to 16	R is equal to 17
S is equal to 18	T is equal to 19	U is equal to 20	V is equal to 21	W is equal to 22	X is equal to 23
Y is equal to 24	Z is equal to 25				

Table 1 Hill Cipher

Mathematical formula of the Hill Cipher:
Cyp = Pl.Ke mod26.
Cyp = Cryptic text
Ke = Key
Pl = Plain text

For this Example, plain text:
Pl = ATTACK
As per the procedure, plain text is changed to:
Pl = 0 19 19 0 2 10
A 2 × 2 matrix will be used as a key for plain text encryption in Hill cipher.

$$K=\begin{bmatrix}2 & 3\\ 3 & 6\end{bmatrix}$$

The key matrix Ke is 2*2 so the simple text is split into blocks, each block is having 2 alphabets.

As the the Pl is ATTACK, the first block of plain text P becomes:

$$Pl1=\begin{bmatrix}0\\ 19\end{bmatrix}$$

Now calculate the value using the equation.
That is,
Cyp=Pl Ke mod26

Using the equation, do the calculations, after the calculations will generate a result, as follows:
Pl = ATTACK

Cyp = FKMFIO

After that for decryption,
Cyp = ke^{-1} Cyp mod26

So if we apply the equation and doing the calculation according to the equation, we will get a result like,
Cyp=FKMFIO
Pl=ATTACK

Factors	AES	Hill Cipher
Developed	1977	1929
Key size	128,192,256 bits	Square matrix of integers usually up to 0 to n-1
Algorithm	Symmetric	Symmetric
Inherent vulnerabilities	Brute force attack	Plain text attack.
Encryption	Faster	Faster
Decryption	Faster	Faster
Security	Excellent	Medium
Ciphering and Deciphering algorithm	Same	Same
Scalability	Not scalable	Not scalable

Table 2 Comparison

III. CONCLUSION

This paper analyses the Hill Cipher and AES which uses the encryption techniques of symmetric algorithm also having two types, that are block ciphers and stream ciphers. Hill Cipher and Advanced Encryption Standard (AES) Algorithms are example of the block cipher method that breaks or creates blocks for encryption and decryption for obtaining cipher text. In AES, a 3-block cipher is used and every cipher encodes and decodes data in 128 bit blocks using 128, 192 and 256 bit cryptographic keys respectively whereas the data to be encoded is split into multiple blocks and individual block is encoded in Hill Cipher.

REFERENCES

[1]. Mahajan, D. P., & Sachdeva, A. (n.d.). View of a study of encryption algorithms AES, DES and RSA for security. Retrieved July 29, 2022, from https://computerresearch.org/index.php/computer/article/view/272/272
[2]. Abdul.Mina, D.S, Kader, H.M. Abdual & Hadhoud, M.M. “Performance Analysis of Symmetric Cryptography”. pp. 1. wikiHow. (2020, September 30). *How to create an encryption algorithm: 6 steps (with pictures)*. wikiHow. Retrieved
[3]. July 29, 2022, from https://www.wikihow.com/Create-an-Encryption-Algorithm [online]
[4]. Agarwal, A. K., & Srivastava, D. K. (2014). Ancient kaṭapayādi system Sanskrit encryption technique unified. *2014 International Conference on Signal Propagation and Computer Technology (ICSPCT 2014)*. https://doi.org/10.1109/icspct.2014.6884947
[5]. SHARMA, S. R. E. E. R. A. M. U. L. A. R. A. J. E. S. W. A. R. A. (n.d.). KATAPAYADI NOTATION ON A SANSKRIT ASTROLOBE.
[6]. Raman, A. V. (1997). The katapayadi formula and the modern hashing technique. *IEEE Annals of the History of Computing*, *19*(4), 49–52. https://doi.org/10.1109/85.627900
[7]. *File:Melakarta.katapayadi.sankhya.72.png - Wikimedia Commons*. (n.d.). Retrieved July 29, 2022, from https://commons.wikimedia.org/wiki/File:Melakarta.katapayadi.sankhya.72.png
[8]. Bernstein, C., & Cobb, M. (2021, September 24). *What is the Advanced Encryption Standard (AES)? definition from searchsecurity*. SearchSecurity. Retrieved July 29, 2022, from https://www.techtarget.com/searchsecurity/definition/Advanced-Encryption-Standard
[9]. Lu, B. (2017). A review of modern cryptography: From the World War II era to the big-data era. *International Series in Operations Research & Management Science*, 101–120. https://doi.org/10.1007/978-3-319-53518-0_710.Koshy, J. M. (2020). Introduction advanced encryption standard (AES). https://doi.org/10.14293/s21991006.1.sor-.ppbwb9z.v1