A Novel Encryption RAAM Algorithm in Different Multimedia Applications

Chirag Sharma, Aman Kumar, Akancha Sinha, Meraj Ahmad

***Abstract:** In this era where everything is becoming digital the most challenging topic in front of us is Data Security in every aspect even in the secured communication channel. These issues can be tackled by using strong Data Encryption and the trusted third party who maintains the database. The fast development in Digital Technology also comes with the rapid crimes and the insecurity of data theft. From time to time engineers came up with many encryption techniques like Caser Ciphers, Vernam Ciphers, Vigenère Cipher which helped us in securing the data but with lots of flaws that later were exploited by the cybercriminals. So, they cannot provide sufficient security. In this research paper, we have proposed a new, more efficient encryption algorithm. This algorithm will use multiple keys during encryption or decryption so it will be very less vulnerable against the attacks like Brute force.*

***Keywords:** Cryptography, Ciphers, Private Key, Public Key.*

I. INTRODUCTION

In the modern world, where technology is advancing every minute. Privacy and security have become a serious concern. With the internet being available to everyone and anyone the chances of security breach have also increased. People have access to almost everything, on the touch of a screen and this makes them vulnerable to fraud and personal information leaks. According to the University of Maryland[1], a cyber-attack occurs every 39 seconds. The cost of one stolen record in a data breach is roughly $146 described by IBM). It costs around $146 for one single stolen record in a data breach as stats given by IBM[2]. In 2019, data breaches cost companies a total of 2 trillion dollars stats to Juniper. With these stats in mind data security is a very huge concern for both companies as well as the general public, as it's their personal information that is at stake. Cybersecurity is a vast platform that is helping us in dealing with these breaches and threats. Cybersecurity is also a developing field, there are a variety of ciphers we can use to prevent mishaps.

Manuscript received on April 26, 2021.
Revised Manuscript received on May 03, 2021.
Manuscript published on May 30, 2021.
* Correspondence Author

Chirag Sharma, Department of Computer Science and Engineering, Lovely Professional University, Jalandhar (Punjab), India. E-mail: chiragsharma1510@gmail.com

Aman Kumar*, Department of Computer Science and Engineering, Lovely Professional University, Jalandhar (Punjab), India. E-mail: asapaman@gmail.com

Akancha Sinha, Department of Computer Science and Engineering, Lovely Professional University, Jalandhar (Punjab), India. E-mail: akanchasinha99@gmail.com

Meraj Ahmad, Department of Computer Science and Engineering, Lovely Professional University, Jalandhar (Punjab), India. E-mail: merajahmad7755@gmail.com

Cipher's literary meaning is to a disguised way of writing. In the term of computer science or cybersecurity, they are algorithm or code that is used for encryption and decryption. These ciphers are vastly used for providing security making networking through the internet safer. Ciphers don't only work on the text there are some specifically designed for multimedia. These ciphers are vastly used for providing security making networking through the internet safer. These ciphers make use of encryption and decryption to secure the data.

II. CRYPTOGRAPHY THEORY

The main idea behind the cryptographic system is to make an encrypted system or data to achieve confidentiality to make it more secure in transferring the data in a way that no other unauthorized person can access the data without the approval of the authorized person. Cryptography has two common use, first one is to transfer the data securely over the unsecured network and the other is to make sure that no unauthorized person can access the data.

In cryptography, the raw data is known as the “plain text” and the process of encoding the data is known as “Encryption” and the data which we get after the encryption is known as “Cipher Text”. All this is done by some sets of rules and instructions called encryption algorithms.

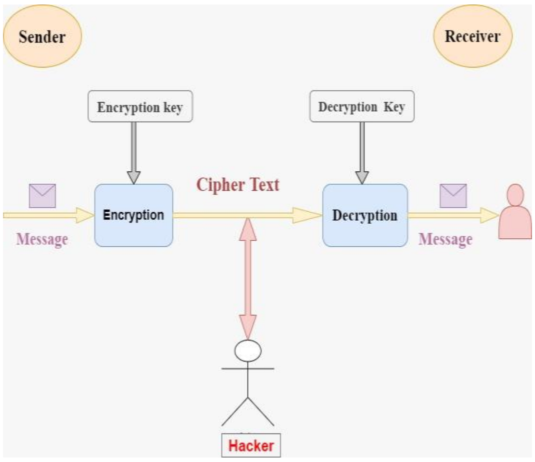

Fig. 1. Cryptography Theory

III. OLD ALGORITHMS

Here we will be seeing some of the oldest encryption algorithms used for encoding the data. We will be using the simplest example so that even non-technical readers could also understand. These algorithms were used in a time when there was no proposal for Public-key cryptography.

Retrieval Number: 100.1/ijsce.F34920510521
DOI: 10.35940/ijsce.F3492.0510521
Journal Website: www.ijsce.org

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication
© Copyright: All rights reserved.

A. Caesar Cipher: Caesar cipher is one of the oldest methods known for cryptography, it was named after Julius Caesar as he used this technique to communicate with his officials and for passing his messages securely. In this cipher, each letter of a plain text is replaced by another letter with the use of a certain key (a fixed number). There we also include spaces and other special characters. The formula used is [3] :

Ex= (x+n) mod 26 (Encryption)

Dx= (x-n) mod 26 (Decryption)

Where n is the number used for shifting.

As easy as this algorithm seems it has its drawbacks. This algorithm is pretty easy and thus makes it more vulnerable, one of the major give away of this cipher is that the repetition of certain alphabets gives away a lot of information.

B. Simple Substitution Cipher: This is the most simple and basic form of encryption where we take the alphabet letters and then place them randomly under the alphabets written correctly as written in Fig. 2.

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

Fig. 2. Simple Substitution Cipher

In this cipher same key is used for both encryption and decryption. In this cipher, each letter gets replaced by the letter beneath it and vice versa for the decryption[4].

C. Playfair Cipher. It is the one which has the most significant history it was used by the British in World War I. It was developed by Charles Wheatstone but was promoted by Lord Playfair. In this cipher, we encrypt using words, not alphabets. For this cipher, we have a key and plain text which are both words. For the first step, we create a matrix of 5×5 which can only hold only 25 letters, so 'J' is usually omitted. The first rows are filled with alphabets that are there in the key and after others, letters are placed in alphabetical order. The plane is split into parts, each part has two alphabets. Then we apply the rules: In case the pair of alphabets are in the same row we take the, we take the alphabets on the right side. If in the same column we take the alphabets that are right below. And in case they are not in the same row or column we use the rectangle method, that is we form a rectangle taking both of alphabets as diagonal vertices. Then we take the horizontal vertex as the replacement alphabet. For decryption, we just do the opposite of the encryption algorithm. As Playfair was widely used in history it is old and has certain drawbacks, the symmetrical cryptography is easy to break. It cannot transform huge amounts of data[5].

IV. NEW ALGORITHMS

A. Advanced Encryption Standard(AES): At present time AES is one of the most widely used symmetric algorithms which is almost 6 times faster than DES. This algorithm was designed to overcome the security flows of DES as the key size of DES was very low which was very much vulnerable against the search key attack. At first Triple DES was developed but it was consuming too much time[6].

AES is an iterative cipher and works on the principle of Substitution permutation network. It uses the bytes during computations instead of the bits. It uses 128 bits of plain text as a block of 16 bytes. These 16 bytes are then redistributed in the 4 rows and 4 columns that form the matrix. We can see the whole encryption method in Fig. 3.

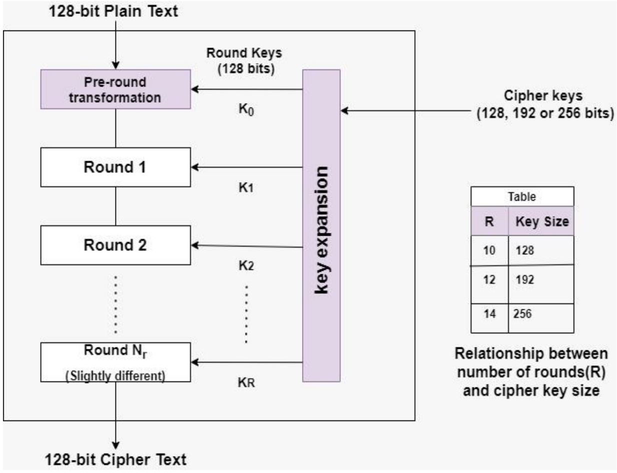

Fig. 3. Advanced Encryption Standard

B. Rivest-Shamir-Adleman (RSA): It is an asymmetric cryptographic algorithm and uses 2 key which is public and private key concept is used here. Public key is known to all the other user while the private key is kept secret. If the public key of the user is used for encryption, then we have to use the private key of the same user for decryption. The RSA scheme is a block cipher in which the plain text and ciphertext are integers between 0 and n-1 for some value n[7]. Encryption and Decryption of RSA can be seen in Fig. 4.

Encryption:

$$\begin{array}{ll} \textit{Plaintext} & M < n \\ \textit{Ciphertext} & C = M^e (mod\ n) \end{array}$$

Decryption:

$$\begin{array}{ll} \textit{Ciphertext} & C \\ \textit{Plaintext} & M = C^d (mod\ n) \end{array}$$

Fig. 4. Rivest-Shamir-Adleman

C. DES (Data Encryption Standard): It is a symmetric key block cipher that uses the same key for both encryption and decryption. It encrypts the data in the block size of 64 bits each in 16 rounds, each round is a fiestal round. It can be understood in four basic steps which are Initial permutation, 16 fiestal rounds, swapping, Inverse Initial Permutation[8]. Its basic structure is shown in Fig. 5.

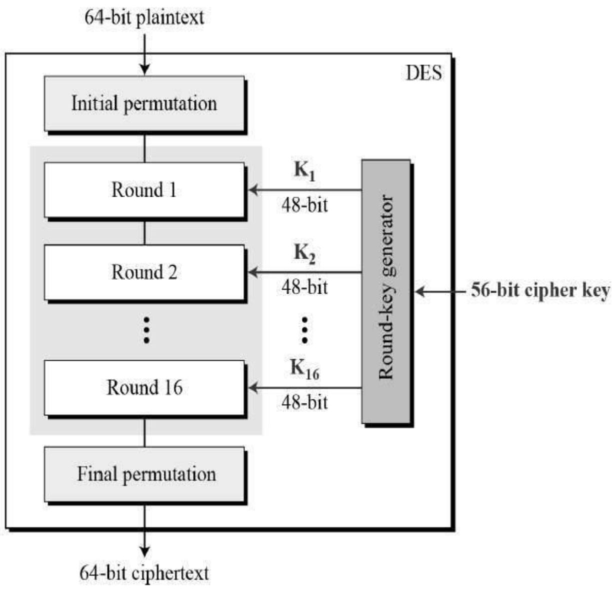

Fig. 5. Data encryption Standard.

DES was used on almost all digital platform, but its dominance came to end in 2002 after the AES was developed which tackled the biggest challenge of DES of key search attack due to its low key size resulting it into a vulnerable algorithm. Its upgrade was developed Triple-DES but it was found to be very slow so it could not be used for a long time.

V. LITERATURE SURVEY

Atish Jain et al. [9] proposed the algorithm that emphasizes the improvement of security of Caesar cipher, as the randomization of text for substitution in combination with double column transposition. This makes breakages impossible using brute force. The person trying to break in would have tried for total key length raised to 256 times. Another way proposed was that we use an asymmetric key instead of a symmetric key.

A.R Deepti et al. [10] Proposed in their work to improve the security of vigenere cipher by the implementation of multilevel encryption. In this fixed length of the key and plain text is used to generate ciphertext using vigenere cipher, now that ciphertext will be used as a key for encryption. This makes the algorithm immune to brute force attacks.

Md. Ahnaf Tahmid Shakil et al. [11] In his paper improved the Playfair Cipher by changing the way to create the matrix, traditional it was left to right and top to bottom but for an improved model we have multiple matrix generation patterns. In this method, the pattern is selected by the user, which increases the security. The additional security is added by making the matrix 7×7 and also reducing the i/j ambiguity, adding more characters.

Dr.Sudesh Kumar et al. [12] In his paper improved the Des algorithm by increasing the number of columnar transposition, to make it difficult to hack using brute force attack. Even if the attacker manages to get the key but the different number of transpositions will be still be required to reach the plain text.

Maulik Kothari et al. [13] Used the scrambler algorithm to increase the security by removing the repetition problem in Vernam Cipher. In this, after a key had been generated it is passed through a function that checks the repetition of words replacing it.

Sharma [14,15] added hyperchaotic encryption to encrypt watermark before embedding to selected frame of video. Hyperchaotic encryption provided good results against different attacks.

VI. PROPOSED METHODOLOGY

We proposed a new algorithm to tackle the Key search and brute force attack named RAAM(Rahul-Akancha-Aman-Meraj) Algorithm. This is a Symmetric-key stream cipher designed by us. DES is an implementation of a Feistel Cipher which uses a 16 round Feistel structure while this algorithm uses 10 rounds which reduces the time complexity. It is having a variable key having a minimum length of 4. It is developed to mitigate the brute force attack which was very much possible on other present ciphers. We will see it in the flowchart in Fig. 6 and the diagram in Fig 7.

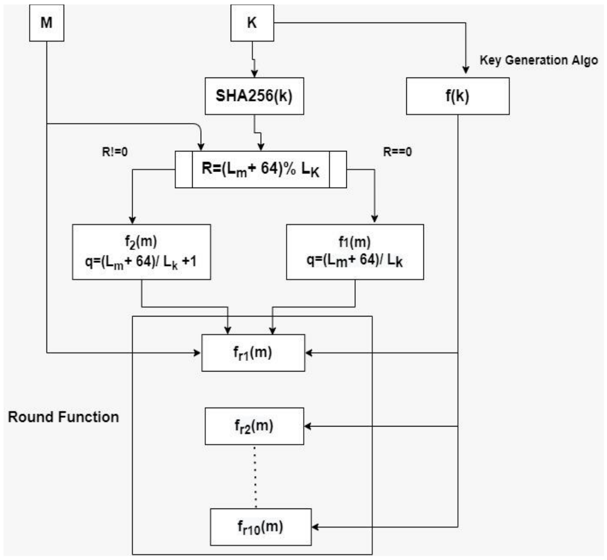

Fig. 6. RAAM Algorithm Flowchart

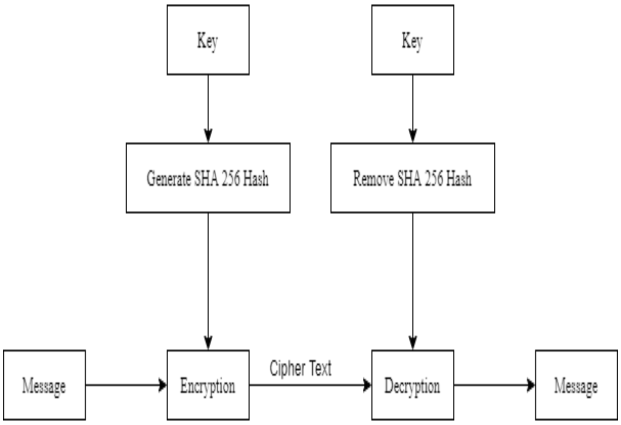

Fig.7 Diagram of RAAM Algorithm

The algorithm breaks down into the following steps:

Encryption:

msg: input message

sh: sha256 of message

Lm: Length of Message

Lk: Length of Key

Nz: Number of 'z' to be appended

Q: Quotient of Lm and Lk

Mx: Formed Matrix of size Lk X Q

i,j,k: loop variable

E: Encrypted text formed

```
Begin:
(1) msg=input_message()
(2) sh=sha256(message)
(3) update: msg <-- sh[0-31] + msg + sh[32-63]
(4) if( Lm%Lk !=0){
(5)         Nz=Lk-(Lm%Lk)
(6)         if(Nz>2)
(7)                 update: msg <-- msg+ 'z'*(Nz-2)+(Nz-2)
(8)         else
(9)                 update: msg <-- msg+ 'z'*Nz
(10)        Q=Lm/Lk
(10) for(i=1; i<=10; i++){
(11)        write: Mx <-- matrix[Lk X Q]
(12)        for( j=1; j<=Q; j++){
(13)                update: Mx[j] <-- Mx[j]+Key  }
(14)        update: msg <-- ""
(15)        for (j=1; j<=Lk; j++) {
(16)                for (k=1; k<=Q; k++) {
(17)                update: msg <-- msg+ Mx[k][i]  } } }
(18)        write: msg --> E
END
```

Decryption:

msg: input message

Lm: Length of Message

Lk: Length of Key

Nz: Number of 'z' to be appended

Q: Quotient of Lm and Lk

Mx: Formed Matrix of size Lk X Q

i,j,k: loop variable

E: Encrypted text formed

```
Begin:
(1) write: Q <--Le/Lk
(2) for(i=1; i<=10; i++){
(3)         write: Mx <-- matrix[Lk X Q]
(4)         for( j=1; j<=Lk; j++){
(5)                 update: Mx[j] <-- Mx[j]-Key  }
(6)         update: msg <-- ""
(7)         for (j=1; j<=Lk; j++) {
(8)                 for (k=1; k<=Q; k++) {
(9)                 update: msg <-- msg+ Mx[k][i]  } } }
(10) write: E --> msg
(11) if(type(msg[-2:])==int){
(12)        Nz=msg[-2:]
(13)        update: msg <-- msg[:Nz+2] }
(14) else {
(15)        while(msg[-1]==z) {
(16)                update: msg <-- msg[:-2] } }
(17) update: msg <-- msg[32:-32]
END
```

VII. COMPARISION ANALYSIS

After studying the different algorithms, we can clearly see that the security of the algorithm depends mostly upon the key management. So we did comparison of multiple algorithms mentioned in Table 1 on various parameters like key length, Number of rounds, attack type and encryption and decryption process.

Table 1: Comparison with existing algorithms

Techniques used	Key Length	No. of Rounds	Attack Type	Encryption and Decryption Process
Caesar Cipher	1	1	Brute force	Symmetric
DES	8	16	Brute force	Symmetric
Hill Cipher	May-56	1	Known Plain Text attack	Symmetric
Vernam cipher	Depends On message	1	Cipher text	Symmetric
Vigenère cipher	4	1	Brute force	Symmetric
RAAM	4+	10		Symmetric

VIII. CONCLUSION

The encryption method for this algorithm has been used in such a way that it mitigates the chances of brute force attack because it uses multiple keys for the encryption. This paper has also discussed the many other ciphers and their present work and how is that important to us in the current digital world. This paper talks about multimedia data encryption and what are the challenges we are facing in these techniques. The paper presented good work and helps in finding the vulnerable part of the present modern-day ciphers. For future work, researchers can use this paper and make the ciphers even more strong for more security in the digital world.

REFERENCES

1. https://eng.umd.edu/news/story/study-hackers-attack-every-39-seconds
2. https://logsentinel.com/blog/2020-data-breach-statistics/
3. Atish Jain, Ronak Dedhia, Abhijit Patil, “Enhancing the Security of Caesar Cipher Substitution Method using a Randomized Approach for more Secure Communication” International Journal of Computer Applications, November 2015.
4. https://www.geeksforgeeks.org/substitution-cipher/
5. R.Deepthi, “A Survey Paper on Playfair Cipher and its Variants”, April 2017.
6. https://searchsecurity.techtarget.com/definition/Advanced-Encryption-Standard
7. Shireen Nisha, Mohammed Farik, “RSA Public Key Cryptography Algorithm – A Review” International Journal of Computer Applications, July 2017.
8. Indumathi Saikumar, “DES- Data Encryption Standard” International Research Journal of Engineering and Technology (IRJET), March 2017
9. Atish Jain, Ronak Dedhia, Abhijit Patil, “Enhancing the Security of Caesar Cipher Substitution Method using a Randomized Approach for more Secure Communication” International Journal of Computer Applications, November 2015.
10. Sanjeev Kumar Mandal, A R Deepti, “A Cryptosystem Based On Vigenere Cipher By Using Multilevel Encryption Scheme”, IJCSIT 2016
11. Md. Ahnaf Tahmid Shakil and Md. Rabiul Islam, “An Efficient Modification to Playfair Cipher ” ULAB JOURNAL OF SCIENCE AND ENGINEERING VOL. 5, NO. 1, NOVEMBER 2014 (ISSN: 2079-4398).
12. Sombir Singh, Sunil K. Maakar, Dr.Sudesh Kumar, “International Journal of Advanced Research in Computer Science and Software Engineering”, June 2013.
13. Maulik Kothari, Manthan Shah, Meet Malde, Ashutosh Wad, “Comcrypt: An Encryption Algorithm based on Vernam Cipher”, International Journal of Computer Science And Technology, December 2012.
14. C. Sharma, A. Bagga, B.Singh, M.Shabaz, “A Novel Optimized Graph Based Transform Watermarking Technique to Address Security Issues in Real Time Application”, Mathematical Problems in Engineering,2021.
15. C. Sharma, A. Bagga , R. Sobti ,T. Lohani, M.Shabaz, “A Secured Frame Selection Based Video Watermarking Technique to Address Quality Loss of Data: Combining Graph Based Transform, Singular Valued Decomposition, and Hyperchaotic Encryption”, Security and Communication Network,2021.

AUTHORS PROFILE

Chirag Sharma, has completed M.TECH 2012 and submitted PHD thesis in 2021 from Lovely Professional University. His research interests include security, image processing, and machine learning.

Aman Kumar, is currently pursuing Computer Science Engineering at Lovely Professional University, Jalandhar. His research interest includes Cyber Security, Artificial Intelligence and IOT.

Akancha Sinha, is currently pursuing Computer Science Engineering at Lovely Professional University, Jalandhar. Her research interest includes Security and Data Science.

Meraj Ahmad, is currently pursuing Computer Science Engineering at Lovely Professional University, Jalandhar. His research interest includes Security and Machine Learning.