iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** IV **Month of publication:** April 2023

DOI: https://doi.org/10.22214/ijraset.2023.50101

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue IV Apr 2023- Available at www.ijraset.com

A Review Paper on Data Encryption and Decryption

Bharti Kaushik[1], Vikas Malik[2], Vinod Saroha[3]
[1, 2, 3]*Department of Computer Science & Engineering, Bhagat Phool Singh Mahila Vishwavidyalaya*

Abstract: ***Cryptography is the technique for hiding data and information from unauthorized users. It is the art of achieving security by encoding messages to make them non-readable. When we send simple message from one location to another then this message called plain text is visible to anybody. If we want to codify the message called cipher text so that no one can easily understand the meaning of message then we use cryptography techniques. There are numerous applications where this technology is used such as ATM pin, Password, Credit Card number or any other secret communication. Cryptography can be divided into following three categories depending upon the types of key used: secret key (symmetric) cryptography, public key (asymmetric) cryptography and hash functions. In this paper we provide review of various types of cryptography techniques.***
Keywords: Cryptography, plain text, cipher text, cryptanalyst

I. INTRODUCTION

Cryptography, then, not only protects data from theft or alteration, but can also be used for user authentication. Cryptography can be divided into following three categories depending upon the types of key used: secret key (symmetric) cryptography, public key (asymmetric) cryptography and hash functions. The rapid continuous increase in exchange of multimedia data over protected and unprotected networks such as the worldwide available internet and local networks such as shared networks and local area networks etc has encouraged activities such as unauthorized access, illegal usage, disruption, alteration of transmitted and stored data. This widely spread use of digital media over the internet such as on social media, on cloud storage systems etc and over other communication medium such as satellite communication systems have increased as applications and need for systems to meet current and future demands evolved over the years. Security concerns with regards to such data transmission and storage has been a major concern of both the transmitters and receivers and hence the security of critical cyber and physical infrastructures as well as their underlying computing and communication architectures and systems becomes a very crucial priority of every institution.

Cryptography is the fundamental platform in which modern information security, which involves the use of advanced mathematical approaches in solving hard cryptographic issues, has gained its grounds in the digital world. This has evolved from classical symmetric, in which shifting keys are normally used as well as substitution methods, ciphers to modern public key exchange cryptosystems, which aims to make cryptanalysis a difficult approach to deciphering ciphers.

In cryptography there are some important terms and are given below (figure 1):

1) *Plaintext:* It is the original text which has to be encrypted.
2) *Cipher Text:* It is the encrypted text. The text obtain after encoding the data with the help of a key is known as cipher text.
3) *Key:* It is a word or value that is used to encrypt the plain text or decrypt the cipher text.
4) *Encryption:* The method of converting the data into coded form with the help of key is called encryption [4].
5) *Decryption:* The method of converting the encoded data to the original form is called decryption.
6) *Crypto Analyst:* A crypto analyst is a person who is an expert in analyzing and breaking codes [3].

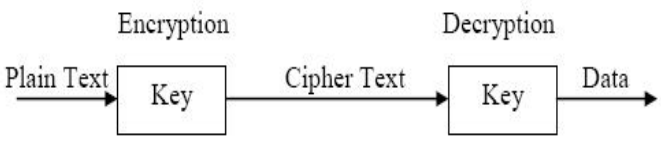


Figure 1: Cryptographic Model [2]

When we send simple message from one location to another then this message called plain text is visible to anybody. If we want to codify the message called cipher text so that no one can easily understand the meaning of message then we use cryptography techniques. The work presented in this paper is to study the existing encryption algorithm used for data security.

II. LITERATURE SURVEY

There are huge amount of work done by the various researchers in the field of cryptographic algorithm for data security. Some of these work done by the researchers are explain in this chapter.

Neal Koblitz*et al*. [4] proposed an elliptic curve cryptosystems for protecting the communication in unsecure network. Elliptic curves over finite fields of public key cryptosystems use the multiplicative group of a finite field. These elliptic curve cryptosystems were more secured because the analog of the discrete logarithm problem on elliptic curves harder than the classical discrete logarithm problem. Limitation of this scheme it was mainly based on the structure either of the multiplicative group or the multiplicative group of a finite field.

Hugo Krawczyk *et al.* [5] worked on the order of encryption and authentication scheme for protecting the communications. They composed a symmetric encryption and authentication scheme for building secured channels for the protection of communications over insecure networks. They also proved that the other method of composing encryption and authentication which includes the authentication encryption method was not so much secured against random attackers. Limitation of this was only forty bit key size can use in this scheme.

Laurent Eschenauer *et al*. [6] proposed a key based scheme for distributed sensor networks. Key management scheme designed to satisfy both operational and security requirements of distributed sensor networks. This scheme requires cryptographic protection of communications, sensor capture detection, key revocation and sensor disabling. So they present a key management scheme designed to satisfy both operational and security requirements of distributed sensor networks.

Jung.Wen Lo *et al.* [7] proposed an efficient key management scheme in a large leaf class hierarchy for access control. In which users were divided this into different security classes. They also proposed a new key assignment scheme for controlling the access right in a large partially ordered set hierarchy and reduce the required computation for key generation. Information retrieval and the number of leaf classes which were substantially larger than the number of non leaf classes.

Bharat B. Madan *et al*. [8] worked on various methods used for modelling and quantifying the security attributes of intrusion tolerant systems**.** Various issues related to quantifying the security attributes of an intrusion tolerant system were also addressed. Response of a security intrusion tolerant system to an attack was modelled as a random process. They facilitate the use of stochastic modelling techniques to predict the attacker behaviour.

Tariq Jamil *et al*. [9] worked upon Rijndael method/algorithm for protecting sensitive unclassified government information. This algorithm was the new advanced encryption standard algorithms recommended by the US national institute of standards and technology. The performance of Rijndael algorithm based on speed of encryption, decryption process and keyset up time.

Ho Won Kim *et al*. [10] worked on Design and Implementation of a private and public key crypto processor and its application for security system. They present the design and implementation of a crypto processor. This special purpose microprocessor optimized for the execution of cryptography algorithms. This crypto processor can be used for various security applications such as storage devices, embedded systems, network routers, security.

Prosanta Gope*et al*. [11] proposed a new block cipher cryptographic symmetric key algorithm named TACIT encryption technique for secure routing. It used an independent approach with suitable mathematical which was assumed to be computationally secured. Key distribution system was being applied on a secure policy based routing. It was limited to conversion of text file.

Ismail .I.A *et al.* [12] worked on how to repair the hill cipher. This technique adjusts the encryption key to form a different key for each block encryption. This algorithm provides a method for adjusting the encryption key, thereby significantly increasing its resistance to various attacks such as a known plaintext attack and statistical attack. The proposed algorithm called HillMRIV cipher.

Yogesh Karandikar *et al*. [13] proposed on effective key management approach for differential access control in dynamic environment. In group communication each user accesses multiple resources and multiple users can access each resource. Each resource encryption key needs to be distributed to all subscribers of the resource and each subscriber must get the entire key. So they developed a new approach of keys management to enforce differential access control in highly dynamic environments for secure group communication framework.

Yanchao Zhang *et al*. [14] worked on Location-Based Compromise-Tolerant Security Mechanisms for Wireless Sensor Networks. They worked on the notion of location-based keys by binding private keys of individual nodes to both their IDs and geographic locations. They developed LBK-based neighbourhood authentication scheme to localize the impact of compromised nodes to their vicinity.

N. R. Potlapally *et al.* [15] worked on energy consumption characteristics of cryptographic algorithms and security protocols. They present a comprehensive analysis of the energy requirements of a wide range of cryptographic algorithms that form the building

blocks of security mechanisms such as security protocols. They also discuss various opportunities for realizing energy efficient implementations of security protocols.

Darpan Anand *et al.* [16] explored identity based cryptography techniques and applications. They reviewed the identity based encryption applications in the field of various networks as ad-hoc networks. The scheme also used in mobile networks and other wireless networks. They also discussed that under what parameters identity based cryptography was used with its benefits and limitations. The main limitation was that the available methods were restricted to fixed output block, which was a trace for crackers.

Pavan. N *et al.* [17] proposed an image steganography scheme based on hill cipher for key hiding. They implement hill cipher algorithm for hiding a text behind the cover image and decrypt the cover image to get original text. The highlight of this paper was that the key was encrypted and scrambled within the cover image scheme eliminates the use of key distribution system and making the system highly secure for various network applications.

Kundan Kumar Rameshwar Saraf et. al. [18] wrote a paper "Text and Image Encryption Decryption Using Advanced Encryption Standard. In this paper they described that images have large data size and also has real time constrain problem hence similar method cannot be used to protect images as well as text from unauthorized access. However with few variations in method AES can be used to protect image as well as text. They had implemented encryption and decryption for text and image using AES."

Smita Desai et. al. [19] wrote a paper "Image Encryption and Decryption using Blowfish Algorithm. This paper was about encryption and decryption of images using a secret-key block cipher called 64-bits Blowfish designed to increase security and to improve performance. This algorithm would be used as a variable key size up to 448 bits. It employs Feistel network which iterates simple function 16 times. The blowfish algorithm was safe against unauthorized attack and runs faster than the popular existing algorithms".

B. Persis [20] in his paper described that "most of the web based applications requires a security for the data, number of symmetric and Asymmetric algorithms approaches with maximum protection for the data to be transferred. This paper describes about the design and implementation of simplified algorithm based on Data Encryption Standard (DES) algorithm which resembles it's almost looks similar to it, but functions in a different way. The data to be encrypted is manipulated with the private key that is created".

D.Maheswari et. al [21] described that "in the recent years the need of security has increased many folds. Cryptography is used widely for the purpose of secure communication and password management. It comprises of two mechanisms namely encryption and decryption. Mathematical principles can be employed to encrypt and decrypt our message and to transmit them securely. In this paper we are using principles of hill cipher for developing an encryption and decryption algorithm to make transmission of messages secure from eavesdropping".

Ali Mohammed et. al [22] described that "Nowadays security is very important to protect our sensitive information in computer or over the internet such as in online banking, online shopping, stock market and bill payments etc. Without security our information exchanged over internet are not safe. Encryption Algorithms provides the security to the information which is exchanged over the internet. In this work we are proposing a new cryptographic algorithm AEDS (Advanced Encryption and Decryption Standard) which is developed by combining properties of DES and AES algorithms. Then we compared all these three algorithms and we found that AEDS is more secure and robust for data security".

Borislav Stoyanov et. al [23] described that "an improved encryption algorithm based on numerical methods and rotation–translation equation is proposed. We develop the new encryption-decryption algorithm by using the concept of symmetric key instead of public key. Symmetric key algorithms use the same key for both encryption and decryption. Most symmetric key encryption algorithms use either block ciphers or stream ciphers. Our goal in this work is to improve an existing encryption algorithm by using a faster convergent iterative method, providing secure convergence of the corresponding numerical scheme, and improved security by a using rotation–translation formula".

Subhi et. al [24] described that "Nowadays there is a lot of importance given to data security on the internet. The DES is one of the most preferred block cipher encryption/decryption procedures used at present. This paper presents a high throughput reconfigurable hardware implementation of DES Encryption algorithm. This achieved by using a new proposed implementation of the DES algorithm using pipelined concept. The implementation of the proposed design is presented by using Spartan-3E (XC3S500E) family FPGAs and is one of the fastest hardware implementations with much greater security. At a clock frequency of 167.448MHz for encryption and 167.870MHz for decryption, it can encrypt or decrypt data blocks at a rate of 10688Mbps".

Pronika et. Al [25] described that "In this tumultuous 21st century, we are surrounding by lots of applications such as social media websites all over the internet or this era can also define as digital era in which everything is accessible over the internet. There are billions of internet users all over the world and they share their information over the same and because of this lots of people intentionally trying to steal the confidential data of other people, so it is always advisable to share and store data in encrypted form.

In this paper, we discuss different encryption and decryption algorithms and compare them with respect to time take by these algorithms for encrypting and decrypting different sizes of files".

Guanxiu Liu [26] described that "With the development of computer network and the popularization of information system, the security of databases, as platforms for centralized storage and sharing of information system data, has increasingly become a serious problem in the field of information security, so data encryption technology has come into people's sight. However, the current data encryption technology still has certain shortcomings, such as the inconsistency of the code text of the encryption and decryption technology, and the low efficiency of decoding and encryption. The purpose of this paper is to study the application of data encryption technology in computer network communication to provide better suggestions and explore better methods for improving network communication security system. This article, through the analysis of the database threat model and database application system structure, puts forward a design scheme of database encryption system model. A complete database encryption system can be divided into five logic modules: a key storage module, key engine module, key information module, key management module, and data storage module, and provides an in-depth analysis of the various parts and implementation details related to these modules. Finally, the designed encryption system model is programmed to be implemented; with the help of online examination system, the function and performance of the encryption system were tested; and the transmission efficiency of data encryption is maintained at more than 95%, which proves the effectiveness of the system".

III. CLASSICAL CRYPTOGRAPHY TECHNIQUES

The technique enables us to illustrate the basic approaches to conventional encryption today. The two basic components of classical ciphers are substitution and transposition [3]. Then other systems described that combines both substitution and transposition.

A. Substitution Techniques

In this technique letters of plaintext are replaced by or by numbers and symbols. If plaintext is viewed as a sequence of bits, then substitution involves replacing plaintext bit patterns with cipher text bit patterns.

1) Caesar Cipher

Caesar Cipher replaces each letter of the message by a fixed letter a fixed distance away e.g. uses the third letter on and repeatedly used by Julius Caesar.

For example:

Plaintext: I CAME I SAW I CONQUERED

Cipher text: L FDPH L VDZ L FRQTXHUHG

Mapping is:

ABCDEFGHIJKLMNOPQRSTUVWXYZ

DEFGHIJKLMNOPQRSTUVWXYZABC

Can describe the Cipher as:

Encryption: C = E (P) = (P + 3) mod 26

Decryption: P = D(C) = (C - 3) mod 26

2) Mono Alphabetic Ciphers

With only 25 possible keys, the Caesar cipher is far from secure. A dramatic increase in the key space can be achieved by allowing an arbitrary substitution. Recall the assignment for the Caesar cipher:

plain: 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

cipher: 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

If, instead, the "cipher" line can be any permutation of the 26 alphabetic characters, then there are 26! possible keys. This is 10 orders of magnitude greater than the key space for DES and would seem to eliminate brute-force techniques for cryptanalysis. Such an approach is referred to as a mono alphabetic substitution cipher, because a single cipher alphabet (mapping from plain alphabet to cipher alphabet) is used per message.

3) Playfair Cipher

The Playfair is a substitution cipher bearing the name of the man who popularized but not created it. The method was invented by Sir Charles Wheatstone, in around 1854; however he named it after his friend Baron Playfair. The Playfair Cipher was developed for telegraph secrecy and it was the first literal digraph substitution cipher.

The best-known multiple-letter encryption cipher is the Playfair, which treats digrams in the plaintext as single units and translates these units into ciphertext digrams. The Playfair algorithm is based on the use of a 5 * 5 matrix of letters constructed using a keyword.

Here is an example:

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

In this case, the keyword is *monarchy*. The matrix is constructed by filling in the letters of the keyword (minus duplicates) from left to right and from top to bottom, and then filling in the remainder of the matrix with the remaining letters in alphabetic order. The letters I and J count as one letter.

Plaintext is encrypted two letters at a time, according to the following rules:

1) Repeating plaintext letters that would fall in the same pair are separated with a filler letter, such as x, so that balloon would be enciphered as ba lx lo on.
2) Plaintext letters that fall in the same row of the matrix are each replaced by the letter to the right, with the first element of the row circularly following the last. For example, ar is encrypted as RM.
3) Plaintext letters that fall in the same column are each replaced by the letter beneath, with the top element of the row circularly following the last. For example, mu is encrypted as CM.
4) Otherwise, each plaintext letter is replaced by the letter that lies in its own row and the column occupied by the other plaintext letter. Thus, hs becomes BP and ea becomes IM (or JM, as the encipherer wishes).

The Playfair cipher is a great advance over simple monoalphabetic ciphers. For one thing, whereas there are only 26 letters, there are 26 * 26 = 676 diagrams, so that identification of individual diagrams is more difficult. Furthermore, the relative frequencies of individual letters exhibit a much greater range than that of diagrams, making frequency analysis much more difficult.

Despite this level of confidence in its security, the Playfair cipher is relatively easy to break because it still leaves much of the structure of the plaintext language intact. A few hundred letters of ciphertext are generally sufficient.

B. Transposition Techniques

All the techniques examined so far involve the substitution of a ciphertext symbol for a plaintext symbol. A very different kind of mapping is achieved by performing some sort of permutation on the plaintext letters. This technique is referred to as a transposition cipher.

The simplest such cipher is the rail fence technique, in which the plaintext is written down as a sequence of diagonals and then read off as a sequence of rows. For example, to encipher the message "meet me after the toga party" with a rail fence of depth 2, we write the following:

m e m a t r h t g p r y
e t e f e t e o a a t

The encrypted message is:
MEMATRHTGPRYETEFETEOAAT

This sort of thing would be trivial to crypt analyze. A more complex scheme is to write the message in a rectangle, row by row, and read the message off, column by column, but permute the order of the columns. The order of the columns then becomes the key to the algorithm. For example:

```
Key:          3 4 2 1 5 6 7
Plaintext:    a t t a c k p
              o s t p o n e
              d u n t i l t
              w o a m x y z

Ciphertext:   TTNAAPTMTSUOAODWCOIXKNLYPETZ
```

A pure transposition cipher is easily recognized because it has the same letter frequencies as the original plaintext. For the type of columnar transposition just shown, cryptanalysis is fairly straightforward and involves laying out the ciphertext in a matrix and playing around with column positions. Digram and trigram frequency tables can be useful.

The transposition cipher can be made significantly more secure by performing more than one stage of transposition. The result is a more complex permutation that is not easily reconstructed. Thus, if the foregoing message is re-encrypted using the same algorithm:

```
Key:          3 4 2 1 5 6 7
Input:        t t n a a p t
              m t s u o a o
              d w c o i x k
              n l y p e t z

Output:       NSCYAUOPTTWLTMDNAOIEPAXTTOKZ
```

To visualize the result of this double transposition, designate the letters in the original plaintext message by the numbers designating their position. Thus, with 28 letters in the message, the original sequence of letters is:
01 02 03 04 05 06 07 08 09 10 11 12 13 14
15 16 17 18 19 20 21 22 23 24 25 26 27 28

After the first transposition we have:
03 10 17 24 04 11 18 25 02 09 16 23 01 08
15 22 05 12 19 26 06 13 20 27 07 14 21 28

which has a somewhat regular structure. But after the second transposition, we have:
17 09 05 27 24 16 12 07 10 02 22 20 03 25
15 13 04 23 19 14 11 01 26 21 18 08 06 28

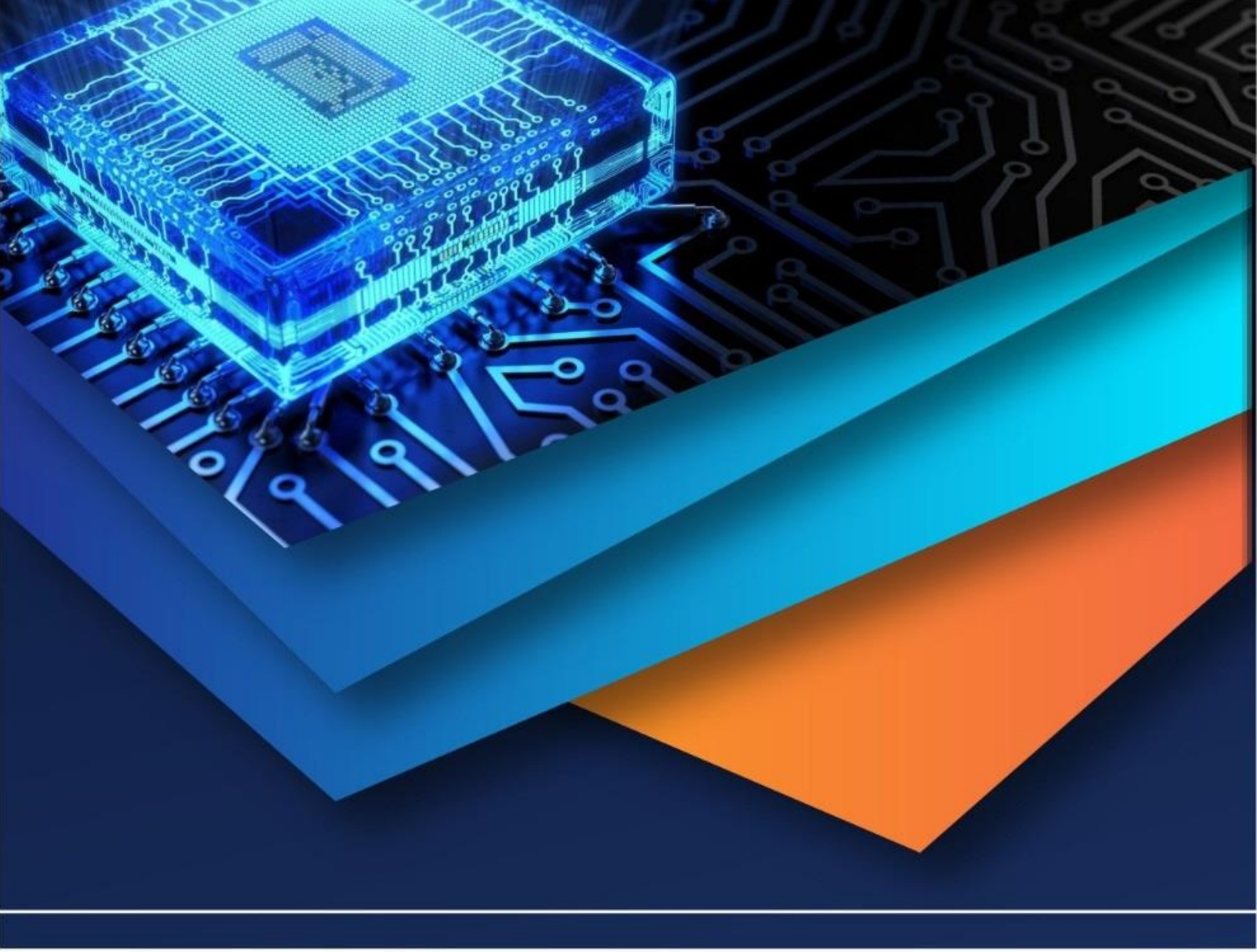
This is a much less structured permutation and is much more difficult to crypt analyze.

IV. CONCLUSION

Data security is an essential component of an organization in order to keep the information safe from various competitors. It helps to ensure the privacy of a user's personal information from others. Secured and timely transmission of data is always an important aspect for an organization. Strong encryption algorithms and optimized key management techniques always help in achieving confidentiality, authentication and integrity of data and reduce the overheads of the system. Cryptography is a technique used to avoid unauthorized access of data. It has two main components; a) Encryption algorithm, and b) Key. Sometime, multiple keys can also be used for encryption. In this paper we studied the existing encryption algorithm used for data security.

REFERENCES

[1] W. Stallings; "Cryptography and Network Security" 2nd Edition, Prentice Hall,1999
[2] Bruce Schneir: Applied Cryptography, 2nd edition, John Wiley & Sons, 1996
[3] A. Kakkar and P. K. Bansal, "Reliable Encryption Algorithm used for Communication", M. E. Thesis, Thapar University, 2004.
[4] N. Koblitz, "Elliptic Curve Cryptosystems", Journal of Mathematics of Computation. Published by American Mathematical Society, Vol. 48, No. 177, pp. 203-209, 1987.
[5] H. Krawczyk, "The Order of Encryption and Authentication for Protecting Communications, http://eprint.iacr.org/2001.
[6] L. Eschenauer, V. D. Gligor, "A Key Management Scheme for Distributed Sensor Networks", ACM conference on Computer Security, Vol.2, pp. 41-47, 2002.
[7] Jung. W. Lo, M. S. Hwang, C. H. Liu, "An efficient key assignment scheme for access control in a large leaf class hierarchy", Journal of Information Sciences Elsevier Science, Vol. 4, pp. 917-925, 2003.
[8] B. B. Madan, K. G. Popstojanova, K. Vaidyanathan and K.S. Trivedi, "A Method for Modeling and Quantifying the Security Attributes of Intrusion Tolerant Systems", Journal of Performance Evaluation, Elsevier Science Publishers, Vol. 56, No. 1, pp. 167-186, 2004.
[9] T. Jamil, "The Rijndael Algorithm", IEEE Potential, Vol.1, pp. 1-4, 2004.
[10] H.W. Kim, S. Lee, "Design and Implementation of a Private and Public Key Crypto Processor and Its Application to a Security System", IEEE Transactions on Consumer Electronics, Vol. 50, No. 1, pp. 214-224, 2004.
[11] P. Gope, A. Singh, A Sharma, N. Pahwa, "An Efficient Cryptographic Approach for Secure Policy Based Routing", IEEE Journal on Selected Areas in Communications, Vol. 1, pp. 359-363, 2013.
[12] I. I. A, A. Mohammed, D. Hossam, "How to repair the Hill cipher", Journal of Zhejiang University Science, Vol. 1, pp. 2022-2030, 2006.
[13] Y. Karandikar, X. Zou, Y. Dai, "An Effective Key Management Approach to Differential Access Control in Dynamic Environments", Journal of Computer Science, Vol. 1, pp. 542-549, 2006.
[14] Y. Zhang, W. Liu, W. Lou, Y. Fang, "Location Based Compromise Tolerant Security Mechanisms for Wireless Sensor Networks", IEEE Transactions Selected Areas in Communications, Vol. 24, No. 2, pp. 1-14, 2006.
[15] N. R. Potlapally, S, Ravi, A. Raghunathan, N. K. Jha, "A Study of the Energy Consumption Characteristics of Cryptographic Algorithms and Security Protocols", IEEE Transaction on Mobile Computing, Vol. 5, No. 2, pp. 128-143, 2006.
[16] D. Anand, V. Khemchandani, R. K. Sharma, "Identity Based Cryptography Techniques and Applications", International Conference on Computational Intelligence and Communication Networks, Vol. 1, pp. 343-348, 2013.
[17] Pavan. N, Nagarjun G. A, Nihaar N, G. S Gaonkar and P. Sharma, "Image Steganography Based On Hill Cipher with Key Hiding Technique", IOSR Journal of Computer Engineering, Vol. 11, pp. 47-50, 2013.
[18] K. R. Saraf, V. P. Jagtap, A. K. Mishra, "Text and Image Encryption Decryption Using Advanced Encryption Standard", International Journal of Emerging Trends & Technology in Computer Science (IJETTCS) Volume 3, Issue 3, May – June 2014
[19] S. Desai, C. A. Mudholkar, R. Khade, P. Chilwant, "Image Encryption and Decryption using Blowfish Algorithm", International Journal of Electrical and Electronics Engineers IJEEE, Volume 07, Issue 01, June 2015.
[20] B. Persis Urbana Ivy, "A Simple and Efficient Counting Algorithm for Data Encryption and Decryption", Taga Journal Vol. 14, 2017.
[21] D. Maheswari, A. Kaushika, A. Jenifer, " A Study on Data Encryption and Decryption Using Hill Cipher Algorithm", International Journal of Technical Innovation in Modern Engineering & Science (IJTIMES) e-ISSN: 2455-2585 Volume 4, Issue 03, March-2018.
[22] Ali Mohammed Ali Argabi, Md Imran Alam, "A new Cryptographic Algorithm AEDS (Advanced Encryption and Decryption Standard) for data security", International Advanced Research Journal in Science, Engineering and Technology Vol. 6, Issue 10, October 2019.
[23] Borislav Stoyanov, Gyurhan Nedzhibov, "Symmetric Key Encryption Based on Rotation-Translation Equation", Symmetry 2020, 12, 73; doi:10.3390/sym12010073
[24] Subhi R. M. Zeebaree, "DES encryption and decryption algorithm implementation based on FPGA", Indonesian Journal of Electrical Engineering and Computer Science Vol. 18, No. 2, May 2020, pp. 774~781.
[25] Pronika, S. S. Tyagi, "Performance analysis of encryption and decryption algorithm", Indonesian Journal of Electrical Engineering and Computer Science Vol. 23, No. 2, August 2021.
[26] Guanxiu Liu, "The Application of Data Encryption Technology in Computer Network Communication Security", Hindawi Mobile Information Systems, Volume 2022.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY