iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 12 **Issue:** III **Month of publication:** March 2024

DOI: https://doi.org/10.22214/ijraset.2024.59538

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 12 Issue III Mar 2024- Available at www.ijraset.com

Review on Symmetric and Asymmetric Cryptography

Bhanu Sankhyan, Anupam Baliyan, Abhishek Kumar
Computer Science and Engineering Chandigarh University, Punjab, India

Abstract: ***As the technology is progressing, internet is growing day by day and it has became more vulnerable than ever. To prevent data from being tampered or viewed by third parties, cryptography is used. Cryptography has it's roots from ancient egypt, where secret writings are developed to transfer messages. Now, modern cryptography is used to secure data over the network, which are classified into symmetric and asymmetric cryptography. Both cryptographic methods has it's own limitations and advantages, which are further used to develop algorithms for better security. More and more efficient algorithms are developed which are discussed in this paper.***

Index Terms: Cryptography, Symmetric Cryptography, Asym- metric Cryptography, Security

I. INTRODUCTION

Cryptography is defined as the study and practice of tech- niques used to hide information. It dates all the way back to ancient Egypt but still in use to prevent information from undetected alteration or being read by unauthorized person. The term cryptography is derived from Greek words "krypto´s" and "gra´phein" which can be interpreted as "hidden writing". In a broad sense cryptography is a process to secure commu- nications and information in transit. As shown in the diagram below message is encrypted using a key and an encryption algorithm, then transferred over an unsecure network to the receiver and is decrypted using the same algorithm and de- cryption key to obtain the original message. [1]

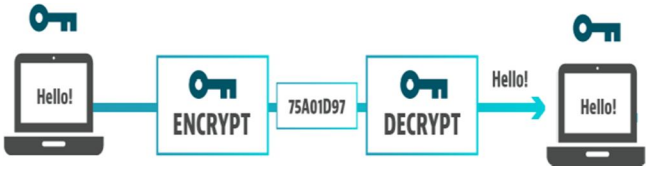


Fig. 1. Encryption of message [2]

For the process of encryption and decryption an algorithm is used described as cryptographic algorithm. An algorithm is comprised of mathematical functions used to transform plain-text into cipher-text. Cryptographic algorithms are being evolved as the time progress and with the advancement in the technology.

Some of the earlier ciphers that are Caeser cipher, Vignere cipher which were compromised due to technological advance- ments. During the time of world war Enigma cipher was adopted by Germans to secure their communications, which was eventually broken by British intelligence, compromising the geographical coordinates for attacks. In the modern era various algorithms were developed such as Advanced En- cryption Algorithm, Data Encryption Standard, Blowfish, RC4 which are based on advanced transposition and substitution techniques. A new approach for encryption and decryption of methods is developed which involves use of complex mathematical functions, which is considered as the most secure form of cryptographic algorithms till date. Some of them are Rivest Shamir Adleman, Diffie Hellman, Elliptical Curve Cryptography. [3] Cryptographic algorithms are defined on the basis of four basic principles which can be described as follows:

A. Confidentiality

This is the primary aspect of cryptogra- phy, used to keep information in secure and private manner. Suppose sender A sends the message to receiver B, but it is intercepted in the channel confidentiality makes sure that data is not compromised. This is extremely important in financial, government sectors. As there are million of transactions happening on day-to-day basis and classified documents are being shared over the network. Data confidentiality ensures that information stays hidden to the third party.

B. Data Integrity

Integrity of data ensures that data trans- ferred over the network has not been tampered or altered by an eavesdropper. There is no way of knowing that data has been modified or completely changed on the network. A common example is transfer of emails over the network. They doesn't offer any security and which makes it very easy to alter or completely change the message that is being transmitted. To avoid such type of intrusions hash digest are used, these are used to generate message digests which are sent along with the original message and both are compared at the receiver's end to ensure integrity of data.

C. Authentication

It makes sure that information is received by the only person to whom it belongs. Suppose sender A sends the message to user B, and the message is read by the B by performing the operations that can only be performed by user B, ensures that message is authenticated.

D. Non Repudiation

It ensures that sender of the message is the one who say it is. An example would be if sender A sends the message to user B and denies sending it, to prevent it from happening digital signatures, message authentication codes are used. [4]

Cryptography is classified into two categories symmetric cryptography and asymmetric cryptography which is further discussed in the following sections.

II. SYMMETRIC KEY CRYPTOGRAPHY

Symmetric cryptography is used for encryption of the message, in which sender and receiver shares the similar key to maintain the confidentiality of the message. Symmetric key ciphers are divided into two types, stream cipher and block cipher. Stream cipher takes input as the individual characters whereas block cipher converts whole block of text. To better understand symmetric cryptography lets take an example where M is the plain-text, C is the cipher-text, K is the Key and (E, D) refers to the pair of encryption and decryption.

- $E : X \times K \rightarrow C$; plain-text along with the key is used to produce the cipher-text.
- $D : C \times K \rightarrow M$; cipher-text along with the key is used to produce plain-text.

Symmetric ciphers are evolved according to the needs and advancement in technology, which can be furthur discussed below:

A. Caeser Cipher

Caeser cipher is one of the oldest way to transfer messages securely, which was used in ancient times. This cipher is based on the shifting of alphabets a certain number of times. A caeser cipher with an offset of 2 will shift the original letter with letter placed after two places. An example would be message 'A' would be converted to 'D'. This cipher was used in ancient times and was named after King Julius Caeser. It's major drawback lies in it's security, it can be easily broken by brute force attack. [4]

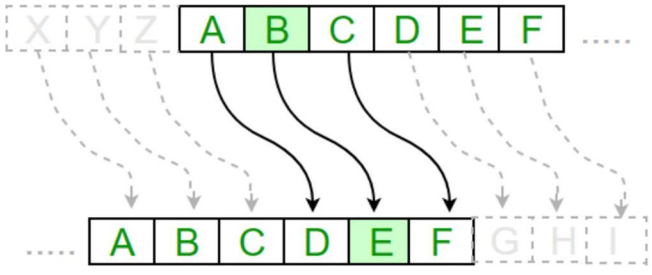


Fig. 2. Caeser Cipher [14]

B. Playfair Cipher

Playfair cipher was first practical substitution cipher. En- cryption and decryption of the message depends on the matrix created from the key. Original playfair cipher used was of 5x5 matrix, after then further advancements were made and larger matrices are being used for encryption and decryption process. [5] It's major drawbacks lies in known plaintext attack. [7]

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

Fig. 3. Playfair cipher [13]

C. *Vignere Cipher*

Vigenere cipher is a substitution cipher which uses a matrix for encryption and decryption 26x26 matrix based on caeser shifts. Encryption of the plaintext is done on the basis of key and corresponding text using square matrix. A letter from both plaintext and key is taken and is looked up in the matrix, to convert it into ciphertext. [6] The major drawback of vignere cipher Kasiski examination and frequency analysis attack. [7]

Fig. 4. Vignere Cipher [15]

D. *Blowfish*

Blowfish is considered a modern cipher, which is used for encryption of the messages block by block. Blowfish has a block size of 64-bit. Blowfish accepts a key size of 32-448 bits. It's encryption process is divided into two parts key expansion and data encryption. In the key expansion key is expanded to 4168 bytes. These are divided into 18 sub parts called as subkeys. Four substitution boxes are needed in the encryption and decryption process. Encryption process follows two step process, initial rounds where in each round plaintext from previous round and corresponding key is taken as input.

First step consist of 16 rounds. In second step post processing of the output is done to obtain the coiphertext. [8] Blowfish major drawback lies in weak key and second order differential attack. [7]

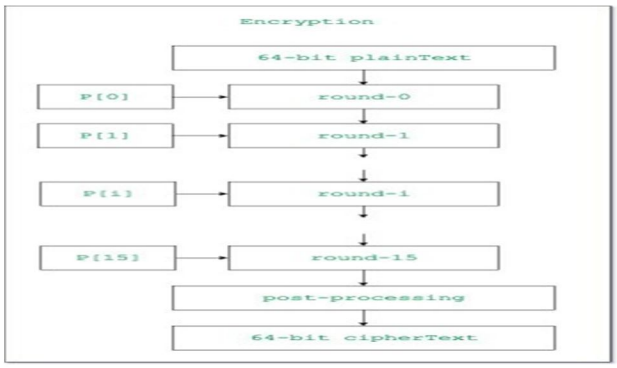


Fig. 5. Blowfish Cipher [16]

E. Twofish

Twofish is a block cipher, which consists block size of 128 bits and key size upto 256 bits. Twofish consist of 16 rounds for the encryption and decryption process, 128-bit of plaintext is divided into four parts of 32-bit each, each is XORed with four keys and then Pseudo Hadamard transform(PHT). Twofish requires 14000 gates to be implement. Twofish is considered more secure than DES and tripple DES algorithms. [9] The main disadvantage of the twofish algorihtm is truncated dif- ferential attack. [7]

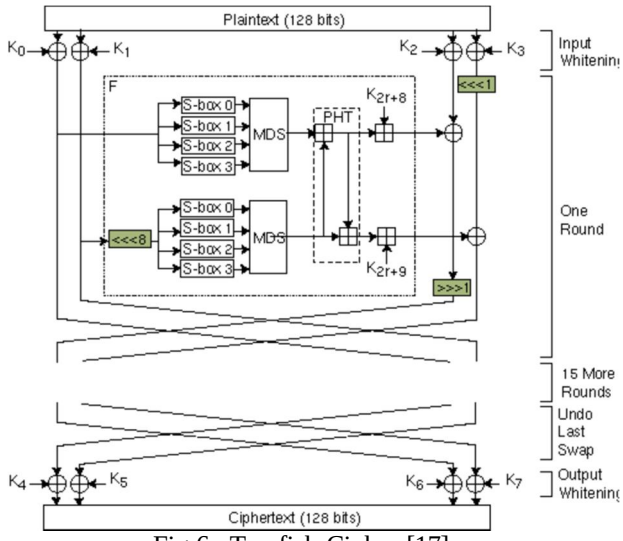


Fig.6. Twofish Cipher [17]

F. Data Encryption Standard

DES is block cipher which converts plaintext into ciphertext in the block of 64-bits. Key used in DES is of length 56 bits. In the DES intial permutation is performed on the plaintext, obtained text is divided into two parts Left Plain Text and Right Plain Text. Each of which goes through further encryp- tion process of 16 rounds having different subkey. Similarly, tripple DES is developed to provide better security, it simply DES performed three times. [10] DES is vulneranble to brute force attack, linear and differential cryptanalysis. [7]

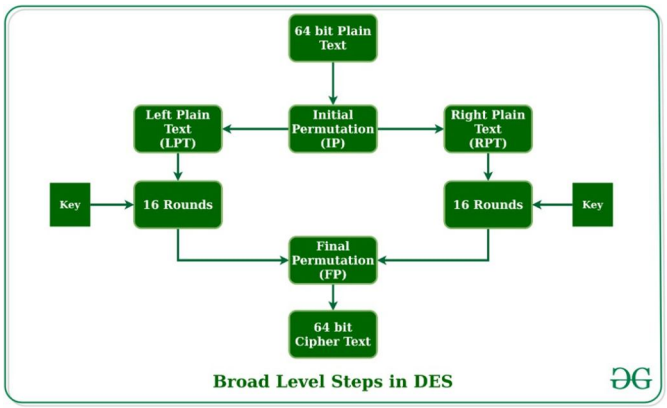


Fig. 7. Twofish Cipher [18]

G. RC-6

RC-6 is a block cipher takes input as 128-bit block and key size of 128, 192 and 256 bit. RC-6 consist of two algorithms key expansion and encryption algorithm. In the key expansion algorithm, keys are generated for each round to be performed in encryption process. In the encryption process ecvery round consist of four steps substitution, permutation, mixing and key addition. The output from previous round is given as input to the next round. RC-6 consist of 20 rounds. [11] The major drawback of RC-6 is chosen ciphertext, known plaintext attack. [7]

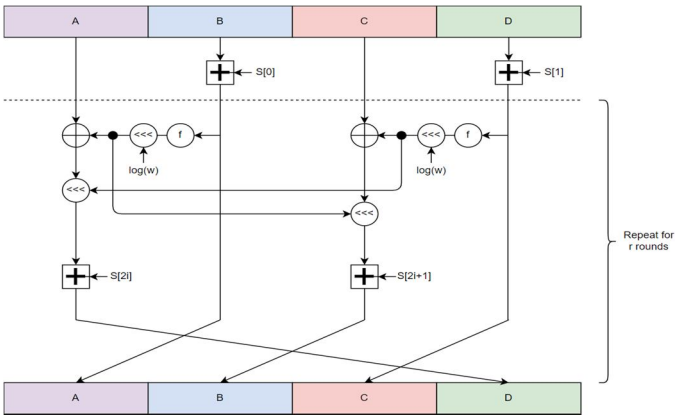


Fig. 8. Twofish Cipher [19]

H. Advanced Encryption Standard

AES is standardized by National Institute of Standards and Technology and is widely adopted algorith for secure transfer of confidential information. AES is a symmetric block cipher. It converts block of 128-bit at a time. AES consist of key size of 128 bit, 192 bit and 256 bit. Encryption process in AES is performed in number of rounds depending on the key size 10,12 and 14 rounds respectively. In each and every round four functions are performed Add round key, Byte Sub, Shift Row and Mix Column. [12] The major drawback of AES lies in side channel attack and know plaintext attack. [7]

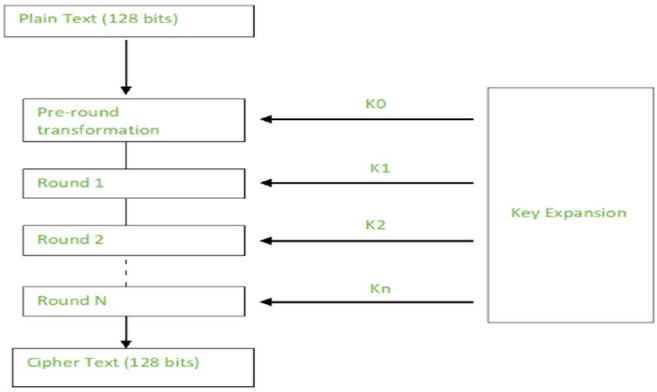


Fig. 9. Twofish Cipher [20]

III. ASYMMETRIC KEY CRYPTOGRAPHY

Asymmetric cryptography is considered relatively modern way to secure messages. It is also termed as public key cryptography as it requires both private and public key for conversion of plaintext into ciphertext and plaintext into ci- phertext. Private key is held by the owner and public keys are distributed over the network to ensure the security of the communication. The asymmetric key encryption is shown in the figure below.

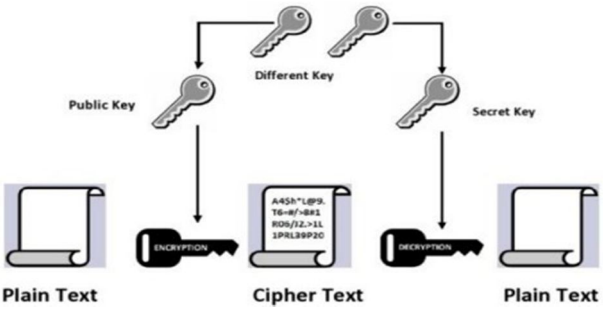


Fig. 10. Asymmetric Encryption and Decryption [20]

These algorithms are considered complex as it involves heavy mathematical computations. Design of asymmetric al- gorithms rely on mathematical equations, which are hard to reverse and considered one way. These are also called as trapdoor functions. Therefore, are slower as compared to symmetric algorithms. Messages encrypted using one key can only be decrypted using another key. Both keys can be used for encryption or decryption of the message. Asymmetric key algorithms are also used to generate digital signatures. Digital signature are generated using private key and can only be verified(signed) using public keys. These signatures are used to confirm the authenticity of the message. [21]

A. Rivest Shamir Adleman

RSA is a asymmetric key algorithm which relies on prime factorization method. It involves heavy mathematical computa- tions,, which leads to slow encryption and decryption time. Se- curity of RSA algorihtm depends on trapdoor functions which are hard to reverse. RSA uses modular arithematic, which are hard to reverse for for sufficiently large mathematical values. Therefore, RSA is not likely to be used for transfer of larger data. [22]

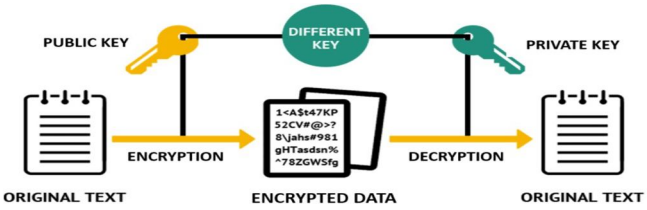


Fig. 11. RSA [23]

B. Diffie Hellman Key Exchange

Diffie Hellman Key Exchange is a method in cryptogra- phy used to securly exchange keys over the network. Diffie Hellman is based on exponential problems and is considered efficient than RSA algorithm. This methods provide a secure way to exchange keys over an insecure channel using trapdoor functions. A smaller key size than RSA provides much better security for Diffie Hellman Algorithm. Similar concept as of Diffie Hellman is used in Elliptical Curve Diffie Hellman to exchange keys generate using elliptical curves. [24]

C. Elliptical Curve Cryptography

Elliptical Curves are used to generate much more efficient keys. It provides a key pair of public and private key. A key size of 256-bit provides similiar security as of 3072-bit key for RSA, which are further shared using Diffie Hellman for Elliptical Curves. ECC generates keys using point multiplica- tion performed on the select curve satisfying the curve, which can be shown in the diagram below.

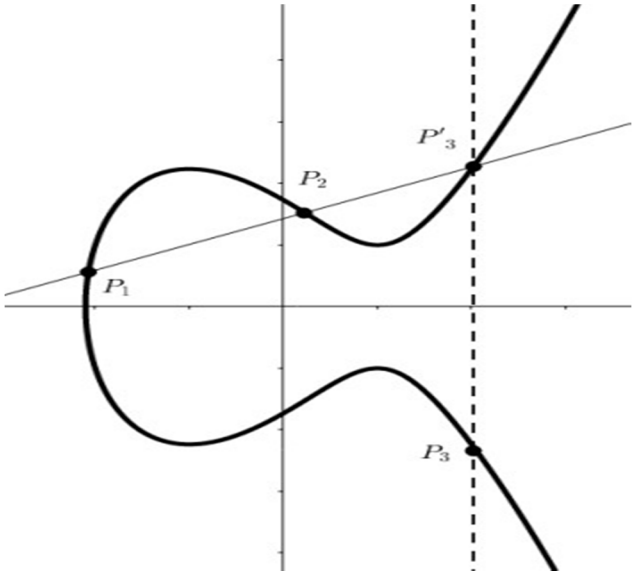


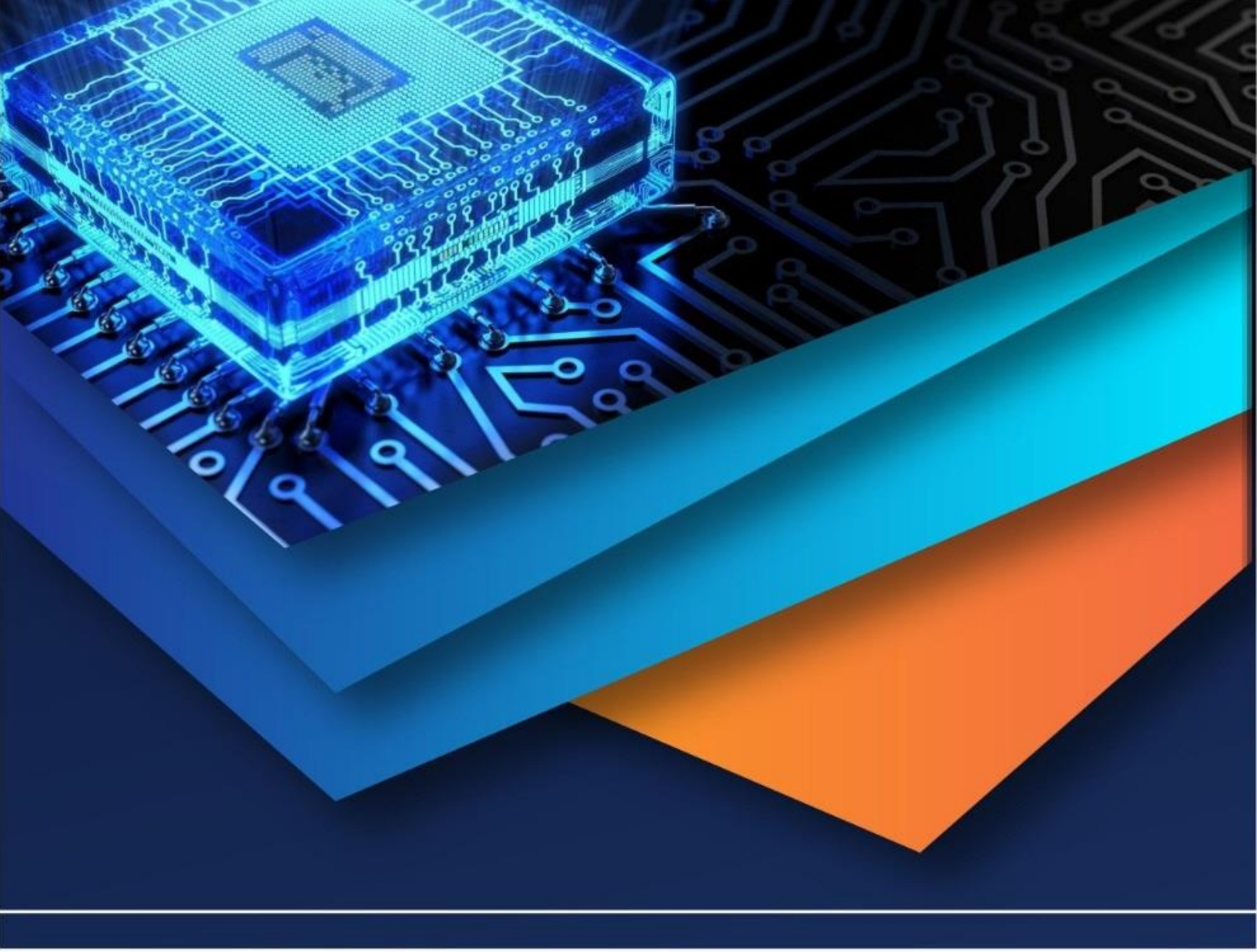
Fig. 12. Elliptical Curve Cryptography [23]

IV. CONCLUSION

In this paper a brief discussion of different symmetric and asymmetric key algorithms is provided. Symmetric key algo- rithms are based on combination of substitution and permuta- tion methods, which makes them very efficient as compared to asymmetric key algorithms. Symmetric key algorithms are less secure as they don't use complex and unsolvable methods to perform encryption and decryption. Asymmetric key algorithms uses more complex mathematical functions and they require heavy calculations makes them less efficient but more secure. In the modern times a blend of both algorithms are used to develop secure protocols making them both secure and efficient at the same time.

REFERENCES

[1] R. Oppliger, "Cryptography 101: From Theory to Practice", Artech House Publishers, 30 June 2021.
[2] A. M. Qadir and N. Narol, "A Review Paper on Cryptography", 7th International Symposium on Digital Forencics and Security, 2019.
[3] W. A. Kotas, "A Brief History of Cryptography", Springer, 2000.
[4] R.Singh and N.Kumar, "A Review Paper on Cryptography of Modified Caesar Cipher", 2018.
[5] S. Khan, "Design and Analysis of Playfair Ciphers with Different Matrix Sizes", International Journal of Computing and Network Systems, 2015.
[6] A.A. Mohammed and A. Olaniyan, "Vigenere Cipher: Trends, Review and Possible Modifications", International Journal of Computer Appli- cations 2016.
[7] Q. Shallal and M. Bokhari, "A Review on Symmetric Key Encryption Techniques in Cryptography", International Journal of Computer Appli- cations, 2016.
[8] V. Parihar and Kulshrestha, "BLOWFISH ALGORITHM: A DETAILED STUDY", International Journal of Biomaterials Research and Engineer- ing, 2016.
[9] H. Harahsheh and M. Qatawneh, "Performance Evaluation of Twofish Algorithm on IMAN1 Supercomputer", International Journal of Com- puter Application, 2018.
[10] N. Kaur, S. Sodhi Data Encryption Standard Algorithm (DES) for Secure Data Transmission, "International Journal of Computer Applications", International Conference on Advances in Emerging Technology, 2016.
[11] R.E. Paje, A. Sison and R. Medina, "Multidimensional key RC6 algo- rithm", 2019.
[12] A. Karki, "A Review on Advanced Encryption Standard – (AES)", International Journal of Computer Sciences and Engineering, 2018.
[13] A. Bhatt, "Playfair Cipher with Examples", in https://www.geeksforgeeks.org/playfair-cipher-with-examples/, 2024.
[14] A. Kumar, "Caesar Cipher in Cryptography", https://www.geeksforgeeks.org/caesar-cipher-in-cryptography/, 2023.
[15] "The Vigenere Cipher – A Polyalphabetic Cipher", https://www.it.uu.se/edu/course/homepage/security/vt09-/labs/vigenere.html.
[16] A. Bhatt,'Blowfish Algorithm with Examples', https://www.geeksforgeeks.org/blowfish-algorithm-with-examples/, 2024.
[17] B. Schneier, The Twofish Encryption Algo- rithm', 'https://www.schneier.com/academic/arc- hives/1998/12/the twofish encrypti.html', 1998.
[18] Shubham, Data encryption standard (DES)—Set 1, 'https://www.geeksforgeeks.org/data-encryption-standard-des-set-1/', 2023.
[19] I. Zahoor,'How RC6 encryption algorithm works', https://www.educative.io/answers/how-rc6-encryption-algorithm-works.
[20] "Advanced Encryption Standard (AES)", https://www.geeksforgeeks.org/advanced-encryption-standard-aes/, 2023.
[21] A. Krishna and L. C. Manikandan, "A Study on Cryptographic Tech- niques," International Journal of Scientific Research in Computer Sci- ence, Engineering and Information Technology, vol. 6, no. 4, pp. 321- 327, 2020.
[22] S. Nisha and M. Farik, RSA Public Key "Cryptography Algorithm – A Review", International Journal of Scientific and Technology Research. 6. 187-191, 2017.
[23] "What Is RSA Algorithm and How Does It Work in Cryptogra- phy?", https://www.simplilearn.com/tutorials/cryptography-tutorial/rsa- algorithm, 2023.
[24] M. Mishra and J. Kar, "A study on diffie-hellman key exchange protocols", International Journal of Pure and Apllied Mathematics, 2017.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY