iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 9 **Issue:** XII **Month of publication:** December 2021

DOI: https://doi.org/10.22214/ijraset.2021.39581

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 9 Issue XII Dec 2021- Available at www.ijraset.com

A Comprehensive Review of Cryptographic Algorithms

Kinjal Raut[1], Chaitrali Katkar[2]
[1, 2]*Final Year students, Computer Science and Engineering, PES Modern College of Engineering, Pune*

Abstract: ***The internet has revolutionized advancements, it's conveniences and uses come at the price of new perils. To be safe from being the victim of fraud, theft and other damage security and vigilance is critical. Cryptography plays an important role in securing information and communications using a set of rules, it ensures the integrity of our data. It maintains confidentiality by protecting the privacy of personal information stored in enterprise systems. Hence Encryption is the only way to ensure that your information remains secure while it is stored and being transmitted. Cryptographic Algorithms mathematically maintain the integrity, confidentiality and authenticity of sensitive information by preventing data disclosure, data tampering and repudiation. The three main types of cryptography are Symmetric Key Cryptography, Asymmetric Key Cryptography and Hash Functions. In this Paper, several important algorithms used for encryption and decryption are defined and analysed, the algorithms are DES, AES, ECC, RSA, MD5***

Keywords: Cryptography, Encryption, Decryption, AES, DES, ECC, RSA, Blowfish, MD5

I. INTRODUCTION

Cryptography is a Greek word in which crypt means "hidden" and graphy means "writing". Cryptography is a system used to secure information and communication techniques derived from mathematical foundations and a set of rule-based calculations called algorithms, to transform messages in ways that are hard to decipher. These algorithms are used for cryptographic key generation, digital signing, to protect data privacy, web browsing on the internet and confidential communications such as card transactions and email and protecting from malicious third parties. The basic working of cryptography requires two steps Encryption and Decryption. The original message is called as Plain text (also known as cleartext). The encryption uses a cipher to encrypt plaintext and convert it into ciphertext and decryption on the other hand applies that same cipher to convert ciphertext back into plaintext. The encryption algorithms are only considered secure if the attackers do not determine any of the property of plaintext or the key along with ciphertext. Even if they have many combinations of plaintext or ciphertext they should not be able to determine the secret key and its properties. A real-world example can be considered of Credit Card Information that is used daily on many e-commerce sites. The code in the web browser encrypts the plaintext, card number, into ciphertext, which will not be recognized by malicious party and will look illegible, random text. Once the card number reaches its intended recipient, the online platform, their software would decrypt it back into plaintext so the payment can be completed successfully.

A. *Common terms in Cryptography*

1) *Encryption:* Encryption is the security method in which data is encoded by converting from plaintext to ciphertext, which can be accessed by only authorized parties.
2) *Decryption:* Decryption is the process in which encrypted data is transformed into its original format that is the cipher text is converted into plain text.
3) *Plaintext:* Plaintext is any text that is not formatted text that is in readable form before it is encrypted into Ciphertext.
4) *Cipher text:* Ciphertext is an unreadable text which contains encrypted information transformed from plaintext using an encryption Algorithm.
5) *Key:*Key is a piece of information usually containing a string of characters and numbers stored in a file which encodes or decodes the cryptographic data.

B. *Objectives of Cryptography*

1) *Confidentiality:* Data Confidentiality ensures that the information should be limited and can be understood by only those who are authorized to view it and should not be understood by anyone for whom it was unintended. The one who has the secret key only should be able to access the data.
2) *Integrity:* Integrity is the protection that certain information contained within the message cannot be modified while the data is being stored or transmitted.

©IJRASET: All Rights are Reserved

3) *Non-repudiation:* In non-repudiation the creator or sender of the information cannot deny the validity of the data in future.
4) *Authentication:* Authenticity ensures that the sender and receiver can verify each other's identities and the origin or destination of the information.

C. Types of Cryptography

1) *Symmetric Key Cryptography:* Symmetric Key Cryptography also known as Secret Key Cryptography uses a single key for data encryption and decryption. When the data is to be sent using Symmetric Key Cryptography the Secret Key is decided before sending the information. The sender utilizes the key to encrypt plaintext and send the ciphertext to the receiver. The receiver can access the data with the same secret key and decrypt the data and recover the plaintext. Symmetric Encryption Algorithms include AES, DES, T-DES, E-DES, RC6, TWOFISH, Serpent, Blowfish.

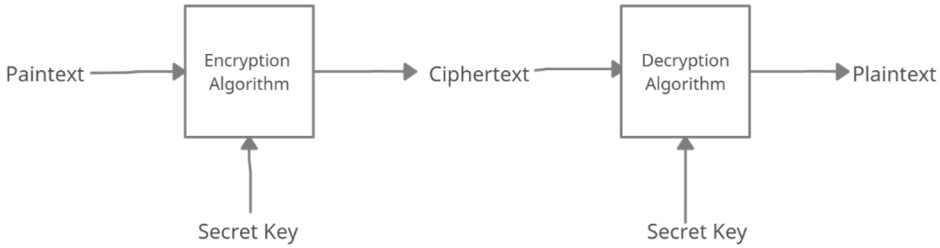


Fig 1. Process of Encryption and Decryption in Symmetric Key Cryptography

2) *Asymmetric Key Cryptography:* Asymmetric Key Cryptography or Public Key Cryptography uses two different keys one private key and other public key. The public key in Asymmetric is used for in encryption and private key is used for decryption. The private key cannot be derived from the public key but the public key can be derived from the private in Asymmetric. The private key should be authorized by only the owner. Asymmetric Encryption Algorithm include ECC, RSA, EES, Digital secure, Diffie Hellman.

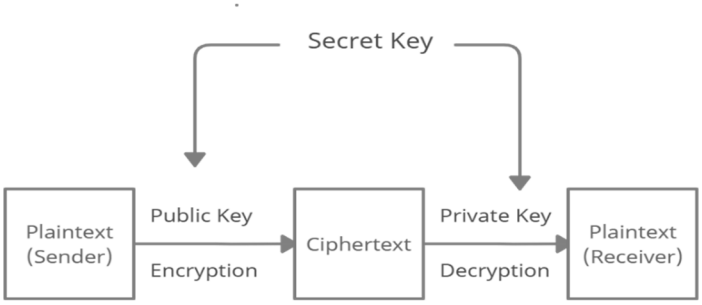


Fig 2. Process of Encryption and Decryption in Asymmetric Key Cryptography

3) *Hash Functions:* Hash functions are one-way functions in which no key is used. Hashing is a method in which plaintext is transformed into fixed-length value and makes it impossible to recover the original information. During the process the same plaintext will always hash to the same output, so to crack a hash try every possible input until the exact same hash is found. Hashing can be used to compare Passwords without even storing them. The various Hash functions include MD5, SHA-1, SHA-2, NTLM, and LANMAN.

II. CRYPTOGRAPHY ALGORITHMS

A. Data Encryption Standard (DES)

DES is a symmetric-key block cipher in which 64-bits encrypted plaintext is taken as input and it produces 64-bits ciphertext using 48-bit Sub Key. In DES same secret key is used for encryption and decryption. DES is an implementation of Feistel Cipher in which 16 round Feistel structure is used. The initial key length is 64 bits, after elimination of 8 keys which are not required the effective key length is 56 bit and further 56 bit is divided into two halves each of 28 bits.

The Steps involved in DES are:

1) Initially 64-bit plain text block is handed to an Initial Permutation (IP) function.
2) The Initial Permutation is performed on the plain text.
3) Then, the initial Permutation creates two halves of the permuted block, namely Left Plain Text(LPT) and Right Plain Text(RPT)
4) Next, each of the LPT and RPT go through 16 rounds of the encryption process.
5) At the end, LPT and RPT are re-joined and a Final Permutation (FP) on the newly combined block.
6) Finally, the output of this process is 64-bit ciphertext is produced.

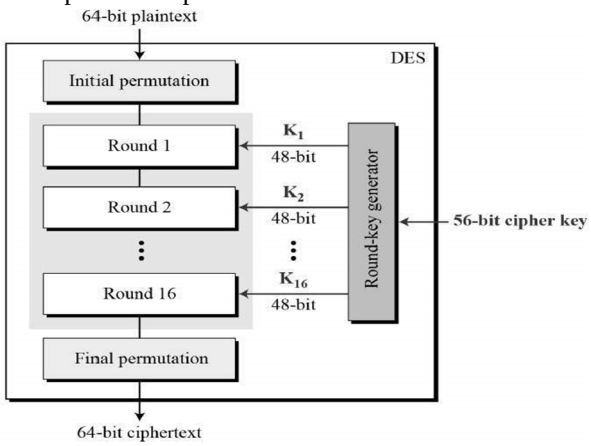


Fig. 3 DES Structure

B. Advanced Encryption Standard (AES)

AES also known as Rijndael algorithm is a symmetric block cipher with a key size of 128/192/256 bits and encrypts data in 128 bits block size data. It works on an SP network structure and is 16 bytes a 4x4 matrix which holds the data in a single block during the first stage which is later expanded to multiple keys used in individual rounds. Given input to the AES is in the form of text message and converts that message in the form of block which further converts that block on the form of state array.

The steps in AES are:

1) *Add round key:* The block data stored in the state array is passed through an XOR function with the first key generated.
2) *Sub-Bytes:* Each byte of the state is converted into hexadecimal and divided into two equal parts as rows and columns mapped with a substitution box(S-Box) to generate new values for the final state array.
3) *Shift Rows:* In this permutation step, the state rows are shifted cyclically. The first row is skipped and then the second row is shifted by one byte to the left, then the third row is shifted by two bytes to the left and it shifts the last row three positions to the left.
4) *Mix Columns:* Mix Columns is a linear process in which a constant matrix is multiplied with each column in the state array to get a new column for subsequent state array. The result is after mixing the columns a new matrix of 16 bytes is formed.
5) *Add round key:* The 16 bytes of the matrix are now considered as 128 bits and are XORed to the respective key. Here the resultant Ciphertext for the specific block is formed or else it passes as the new state array input for the next round.

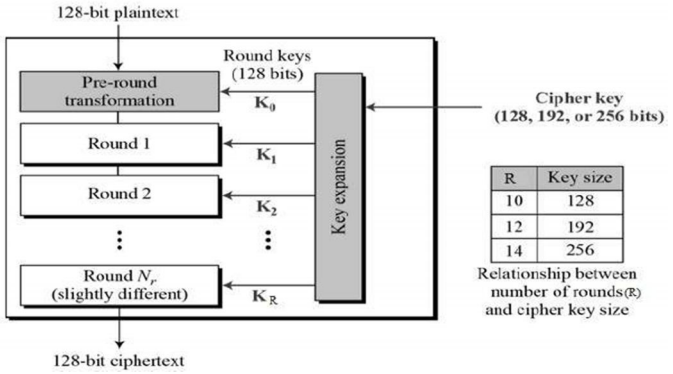


Fig. 4 AES Structure

C. Elliptic Curve Cryptography (ECC)

ECC is a public key cryptography based on elliptic curve theory for encrypting data. ECC uses both public keys and private keys for encryption and decryption. The private key is used to generate digital signatures and the public key is used to verify the generated digital signature. In contrast to RSA, ECC is stronger than RSA because it can attain similar level security as RSA with smaller number of keys whereas RSA requires larger number of keys i.e., an ECC key of 384 bit achieves same level of security as an RSA of 7680 bit.

RSA key length – 1024 2048 3072 7680 15360 in bits

ECC key length – 160 224 256 384 521 in bits

ECC algorithm is based on elliptic curve theory and studies how elliptic curves are structured algebraically over finite fields, hence ECC creates keys that are more difficult mathematically to solve, this is the reason ECC is the next generation implementation of public key cryptography and is more secure than RSA.

ECC is a plane and asymmetrical curve, which traverses a finite filed comprising the points sustaining following ECC equation: y^2 = x^3+ax+b

ECC provides bunch of algorithms based on the math of the elliptic curves over finite fields:

ECC digital signature algorithms like Elliptic Curve Digital Signature Algorithm (ECDSA) using classical curves and Edwards-curve Digital Signature Algorithm (EdDSA) using twisted Edwards curves.

ECC algorithms and hybrid encryption schemes like the Elliptic Curve Integrated Encryption Scheme (ECIES) and EEECC (EC-based EIGamal)

ECC key agreement algorithms like Elliptic-curve Diffie-Hellman (ECDH), Fully Hashed Menezes-Qu-Vanstone (FHMQV), and X22519 is an elliptic curve Diffie-Hellman key exchange using curve22519.

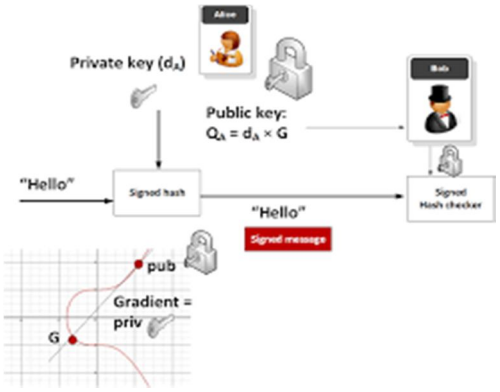


Fig 5. ECC Structure

D. Rivest-Shamir-Adleman (RSA)

RSA algorithm is a public key cryptography using both private key and public key i.e., two different mathematically linked keys for encryption and decryption. In RSA, both public key and private key can encrypt a message. One key is used for encryption and the other is used for decryption irrespective of whether it is a public key or private key. RSA is based is difficult to factorise a large integer. The public key and the private key both consists of two prime numbers, in which the larger number is factorised and the private key is compromised. Thus, the encryption strength depends on the key size and as the key size is increased the encryption increases exponentially. In RSA plaintext and ciphertext are integers between 0 and n-1(for some n). The size of n usually is 1024bits or 309 decimal digits, which means n is less than 2^1024.

Working of RSA involves 3 steps as follows:

1) Key Generation

a) Select two larger prime numbers (x and y)

b) Calculate n=x*y where n is modulus for encryption and decryption

c) Calculate the totient function Phi(n) = (x-1) * (y-1)

d) Choose public key exponent e such that 1<e<Phi(n) e is prime to Phi(n) i.e. GCD(e,Phi(n))=1

e) Calculate private key exponent d such that e*d=1*mod (Phi(n)) Thus, Public key: (n,e) Private key: (n,d)

2) *Encryption:* To encrypt message, plain text sent is sent to the one having public key(n,e) C = P^e mod(n)
3) *Decryption:* The private key(n,d), the plaintext is P = c^d mod(n)

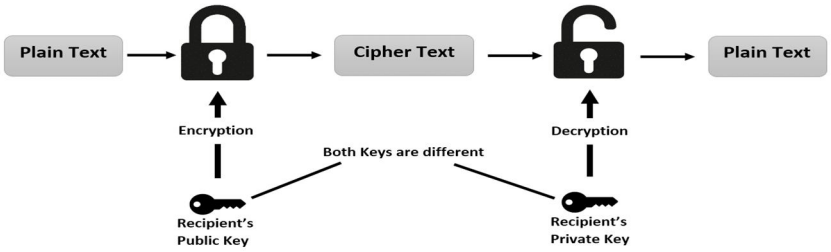


Fig 6. RSA Structure

E. Blowfish

Blowfish is a 64-bit symmetric block cipher used for drop-in replacement of DES or IDEA, it's variable key-length from 32 bits to 448 bits. Blowfish is a 16-round structure used for encryption process and providing security to confidential data. The input for encryption process is 64-bit plaintext and converted into 64-bit ciphertext and uses same secret key for both encryption and decryption.

It follows the Feistel network and the working process of the algorithm is divided into four parts:

1) *Key expansion*: It has a minimum 32-bits and maximum 448-bits. The process converts a key of most 448-bits into several sub key arrays such that total will count to 4168 bytes. Two sub key arrays are kept, the P-array consists of 18 32-bit entries and 4 32-bits S-boxes with 256 entries each.
2) *Data-Encryption*: In data encryption process the process involves iteration of network 16 times. Blowfish is a very fast algorithm which converts plaintext into ciphertext.
3) *Key Generation*: Blowfish generates large number of sub-keys.

P-array consists of 18, 32-bit sub-keys with key size ranging from 32 bits to 448 bits or 14 words.
4 S-boxes consists of 256 entries of 32 bits.
S1,0, S1, 1……S1,255
S2,0, S2, 1……S2,255
S3,0, S3, 1…….S3,255
S4,0, S4, 1...…S4,255

4) *Steps to generate Sub-keys:* First initialize the P-array and then four S-boxes with a fixed string. This string also contains the hexadecimal digits of pi (less than initial 3). After the initialization of P-array XOR P1 with the first 32 bits of the key and XOR P2 is XORed with 320bits of the key. The process is repeated until the entire P-array is XORed with key bits.

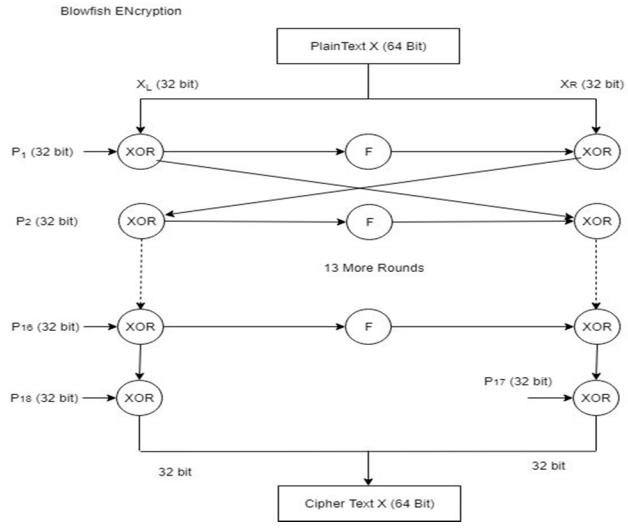


Fig. 7 Blowfish Structure

F. Message Direct Algorithm (MD5)

MD5 is a cryptographic one-way algorithm used to create a 128-bit string value from a string of any length and digests as 32-digit hexadecimal numbers. MD5 is used to ensure the authenticity of the message or any text sent where every message is padded into block of 512 bits each. 16 operations each are performed in 4 rounds which implies that in total 64 operations are performed in each block and output of every block is fed into subsequent block and hence the process is continued till the last block. The output of last block is message direct. It is intended for digital signature applications, where a larger file is compressed in a secure manner before being encrypted with a secret key under a public key cryptosystem. The steps performed in MD5 algorithm are:

1) *Append Padding Bits:* When an input is received the size should be 64bits short of a multiple of 512. While padding 1 is added at the beginning and the rest 0s to round out with extra characters.
2) *Append Length Bits:* Append the 64bits message and add length bits such that the total number of bits in the message becomes multiple of 512.
3) *Initialize MD Buffer:* The entire string is converted into multiple blocks of 512 bits each and 4 buffers of 32 bits each are used. Initialize four buffers as A, B, C, D

A = 0,1,2,3,4,5,6,7
B = 8,9,a,b,c,d,e,f
C = f,e,c,b,a,9,8
D = 7,6,5,4,3,2,1,0

4) *Process Each Block:* Each 512-bit block in which last block is the output message digest which gets broken down further into 16 sub-blocks of 32 bits each and 4 rounds of operations with each utilizing all the sub-blocks, the buffers and a constant array value.

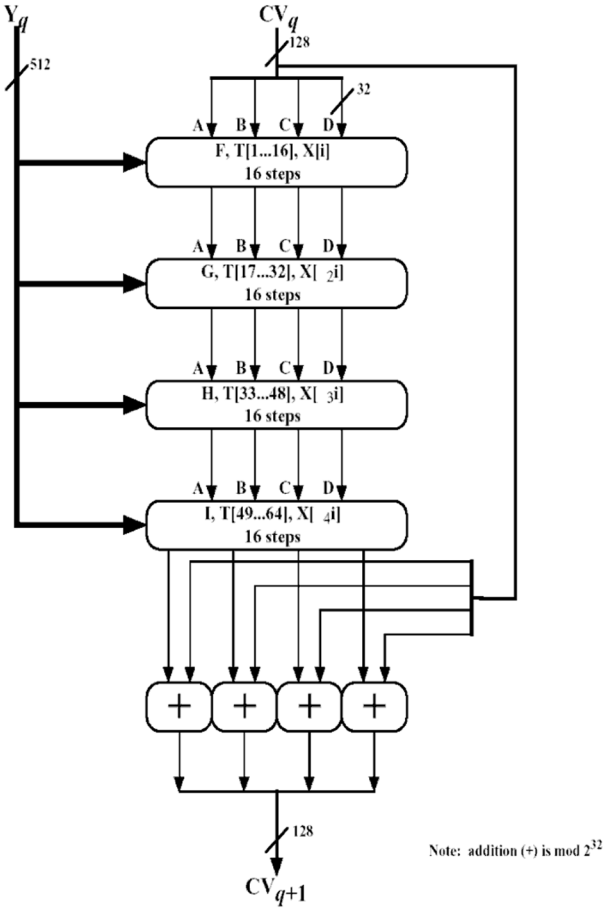


Fig 8. MD5 structure

TABLE I
Comparison Table of all above Algorithms

Algorithm	Structure	Key size	Block Size	Rounds	Flexible	Scalability	Processing Speed	Features
DES	Feistal	64 bits	64 bits	16	No	Scalable	Very low	Not Strong Enough
AES	Substitution Permutation	128, 192, 256 bits	128 bits	10, 12, 14	Yes	Not Scalable	Faster	Security is Excellent, Replacement for DES
ECC	Public Key Algorithm	More than symmetric variable	Variable	1	Yes	Scalable	Very Fast	Highly Secure and Fast Speed
RSA	Public Key Algorithm	1024 to 4096	128 bits	1	No	Not Scalable	Average	Good Security, Low Speed
Blowfish	Feistal	32-448	64 bits	16	Yes	Scalable	Very Fast	Excellent Security
MD5	Merkle-Damgard Construction	Series of MD	512	4	Yes	Scalable	Fast	Excellent Security

III. RESULT AND DISCUSSION

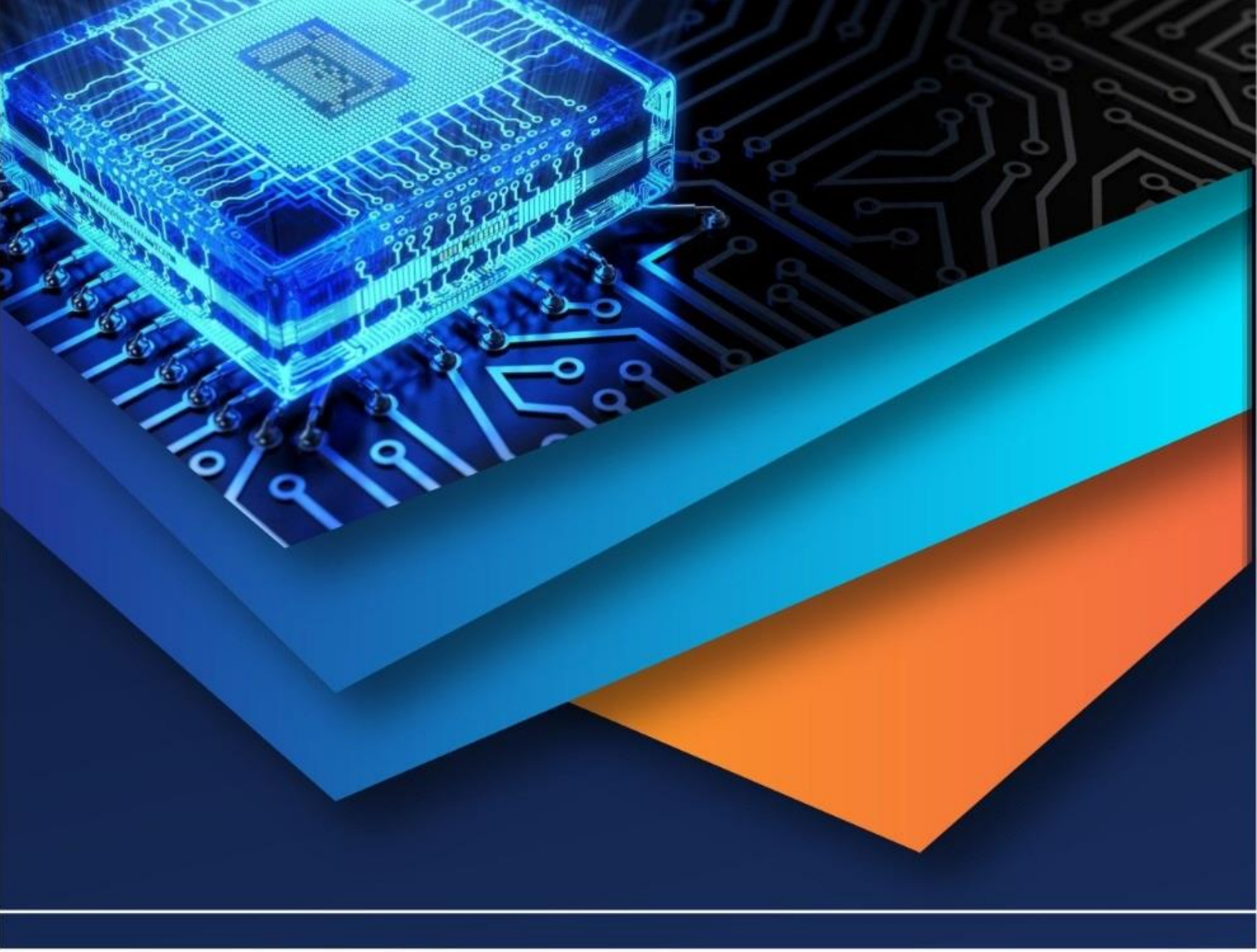
From the above table, the comparisons are based on Structure, Key-Size, Block-Size, Rounds, Flexibilty, Scalability, Processing speed and Features. The result shows that algorithms AES, Blowfish, ECC and MD5 are secure than other algorithms. The result further also shows that AES is the most efficient and best in Processing speed, structure, encryption, decoding and decoding.

IV. CONCLUSION

In this paper a holistic comparative study of different algorithms in Modern Cryptography is performed. All the algorithms have proven their own advantages and disadvantages, between symmetric and asymmetric algorithms Symmetric are faster than Asymmetric. However, the most reliable algorithm is AES based on the factors such as encryption, decryption, length of the key, flexibility and speed.

REFERENCES

[1] Sanjeev Kumar Mandal, A R Deepti 2019. A Review Paper on Encryption Techniques. International Journal of Research and Analytical Reviews (IJRAR).
[2] Mazoon AlRoubiei, Thuraiya AlYarubi, Basant Kumar, 2020. Critical Analysis of Cryptographic Algorithms. IEEE Xplore.
[3] Abdalbasit Mohammed, Nurhayat Varol, 2019. A Review Paper on Cryptography. 978-1-7281-2827-6/19/$31.00 ©2019 IEEE
[4] Anjula Gupta, Navpreet Kaur Walia,2014. Cryptography Algorithms: A Review. International Journal of Engineering Development and Research (www.ijedr.org).
[5] Omar G. Abood, Shawkat Guirguis,2018. A Survey on Cryptography Algorithms. International Journal of Scientific and Research Publications, Volume 8, Issue 7, July 2018 495 ISSN 2250-3153.
[6] Dudhatra Nilesh, Prof. Malti Nagle,2014. The New Cryptography Algorithm with High Throughput. 2014 International Conference on Computer Communication and Informatics (ICCCI -2014), Jan. 03 – 05, 2014, Coimbatore, INDIA.
[7] Yahia Alemami, Mohamad Afendee Mohamed, Saleh Atiewi, 2019. Research on Various Cryptography Techniques. International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-8, Issue-2S3, July 2019.
[8] Ramesh Yegireddi, R Kiran Kumar, 2016. A survey on Conventional Encryption Algorithms of Cryptography. 978-1-5090-5515-9/16/$31.00 ©2016 IEEE



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)