IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 13, Issue 7, July 2024

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.423

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 7, July 2024

|DOI: 10.15680/IJIRSET.2024.1307112|

A Secure and Fast Approach for Encryption and Decryption of Data

Nimisha S[1], Mahalakshmi G[2], Mr. Raghu Prasad K[3], Mr. Hemanth Kumar G[4]

P.G. Student, Department of Master of Computer Applications, RNS Institute of Technology, Channasandra, Bangalore, India[1 2]

Assistant Professor, Department of Master of Computer Applications, RNS Institute of Technology, Channasandra, Bangalore, India[3 4]

ABSTRACT: Cryptography might be the most crucial thing of the conversation is protection and becoming a primary constructing block for computer security. One method is encryption for protecting information this is shared via internet.The procedure for using encryption is what encoding(coding into a few unreadable form of records) the information to hide its message contents.Encrypted facts may be recovered handiest use the secret key in the Decryption procedure present day cryptography utilizes several cozy The procedures of encryption and decryption use algorithms. The proposed crypto device for Data encryption and decryption is Elliptic Curve Cryptography.

KEYWORDS: Encryption, Decryption, RSA, AES, DES, ECC, Key

I. INTRODUCTION

The need for safety in the modern world has become greater essential than ever because of the fact there are extra variety of those who want To be able to maximize statistics and use it for their personal advantage had been growing every day.Cryptography is the procedure for safe communique within the presence of adversaries. It includes some algorithms to change plaintext into ciphertext, ensuring honesty, integrity, and secrecy of information. In ultra-modern world, where statistics is stored and transmitted electronically, statistics security has become an important situation. Cryptography performs an essential function in making sure statistics protection using supplying strategies for secure conversation, facts encryption, digital signatures, and authentication.In this research paper, we are able to dig into the numerous aspects of cryptography and its utility in information security. We are able to explore exceptional Cartographic strategies, including Symmetric and Asymmetric key cryptography, hash functions, and virtual signatures.Moreover, we will discuss the numerous Cartographic requirements including AES, RSA, SHA, and ECC and their implementation in cryptography.Normal, this research paper goals in order to offer a overview of cryptography and its role in ensuring data protection in safeguarding sensitive facts in latest interconnected international.

II. RELATED WORK

1) **Symmetric Key Cryptographic algorithm:** There are numerous styles of cryptography, Both Asymmetric and Symmetric Keys Cryptography. Symmetric key algorithm quickest and they may be normally used shape of encryption. Few well-known Symmetric key algorithm rau encryption and decryption are DES, RC2, RC4, concept and so on.

2) **Efficient,sophisticated symmetric key encryption technique for data protection:** They proposed a few new encryption set of policies and used block cipher generating mechanism.They proposed evaluation, effects with the useful resource of using calculation with unique plaintexts with in the identical key mode. using the effects they show that, below the identical key duration and for the equal duration of the data, proposed set of policies painting faster than present set of policies.

3) **A observe of Encryption Algorithms AES, DES and RSA for protection:** They carried out three methods of encryption such as the RSA, DES, and AES algorithms and their standard performance of various encryption strategies are primarily based mostly on time in order to encrypt and decrypt.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 7, July 2024

|DOI: 10.15680/IJIRSET.2024.1307112|

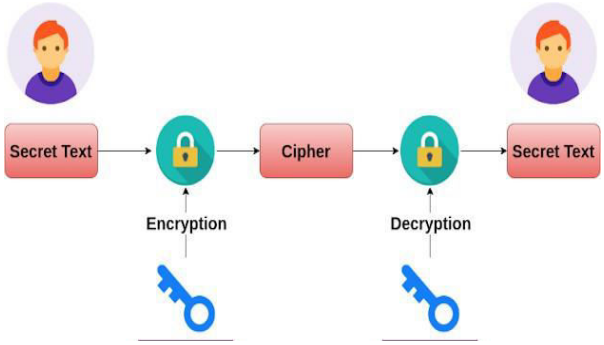
4) **Efficient Encryption strategies in Cryptography and higher safety Enhancement:** They proposed Encryption techniques and cited with their barriers and method. For encryption they used Huffman coding and B2G, G2B. additionally they moreover referred to transpositional techniques like Route cipher, Easy row, Simple columnar, Transposition.

III. CRYPTOGRAPHY

Cryptography is the method of shielding information via apply rules only to those in the known is intended can read and process it.The technique of coverting simple text to cipher text with using key's referred to as Encryption.The technique of changing cipher text to standard text using identical key or different key is recognized as Decryption.

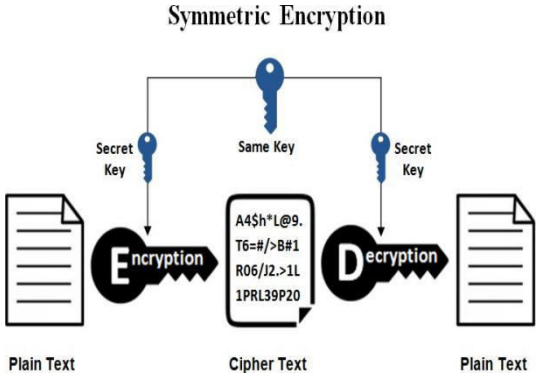
ENCRYPTION:Encryption is the way of scrambling information in order that only authorized events can recognize the facts. In technical phrases, it is the procedure of changing human-readable plaintext to incomprehensible textual content, also known to as ciphertext. In easier terms, encryption takes readable records and alters it so that it appears random. Encryption calls for the application of a cryptographic key: A set of mathematical values that the sender and the recipient, respectively of an encrypted message agree on.

DECRYPTION:This algorithm kind is employed for encrypting informationto both encrypt and decode numerous components of the message, consisting of the body content and the signature. Data decryption algorithms specify the algorithm uniform resource identifier (URI)of the encrypted data



IV. TYPES OF CRYPTOGRAPHY

SYMMETRIC KEY CRYPTOGRAPHY:
Information can be both encryptd and decrypted using symmetri c key encryption. This implies that the encryption The key used to encrypt and decode the data must be the same. The keys stand for a shared secret That could be utilised to maintain a link for private information between two or more people. The reality that each party possesses access to the main thing, fundamental disadvantages of symmetric key encryption.



International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

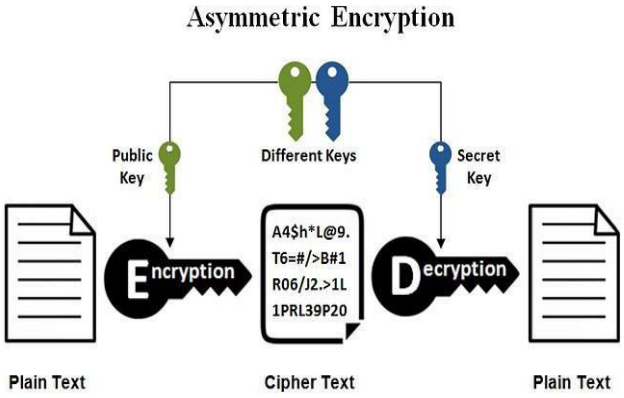
Impact Factor 8.423

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 7, July 2024

|DOI: 10.15680/IJIRSET.2024.1307112|

ASYMMETRIC KEY CRYPTOGRAPHY :
Asymmetric key encryption are the general Public Key Infrastructure (PKI), a cryptographic scheme requiring two unique keys, one to lock or encrypt the plaintext, and one to unlock or decrypt the cyphertext. Neither key will do each features. One key's published (public key) and the other is stored private (private key). If the lock/encryption key's the one published, the machine allows private communique from the general public to the unlocking key's owner. If the unlock/decryption key's the only published, then the system serves as a signature verifier of documents locked by utilizing the proprietor of the non-public key. This machine also is known to as asymmetric key cryptography.



V. ALGORITHMS

There are several kinds of methods for encrypting data and decryption: AES, 3-DES, RSA

AES Algorithm:
NIST created the Advanced Encryption Standard (AES) as a specification for the encryption of electronic data in 2001. AES is widely used today despite being more difficult to implement than DES and 3 DES since it is far more powerful.

Remember that :
a) AES is a block cypher.
b) The key size can range from 128 to 256 bits.
c) Information is encrypted in blocks of 12 8 bits apiece

The answer is 128 bits of encrypted cipher text, which are output after 128 bits of input. Based on substitution-permutation network theory, AES has so far was successful in using a series of connected operations that entail replacing and rearranging the input data.

3-DES Algorithm:
The 3-DES algorithm employs three separate instances of the DES algorithm To encrypt a single piece of plain text. It uses 3 different key selection techniques: one where all the used keys are unique, another where all the keys Are the same but one is different, and a third where all the keys are the same.Since Triple DES uses a 2112 total security level instead of a 168 bit key, it is susceptible to a meet-in-the-middle attack. Short block sizes and using the identical key to encrypt large amounts of text allow the block collision attack to be performed as well. Also, a sweet32 attack could happen.

RSA Algorithm:
An asymmetric cryptography algorithm is the RSA algorithm. In actuality, asymmetric refers due to the reality that it operates on the both public private keys, two distinct keys. As implied by the name, the private key is kept secret while the public key is distributed to everybody.With the ECC algorithm, There is a quick and secure method for encrypting and decoding data (Elliptive curve cryptography).

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

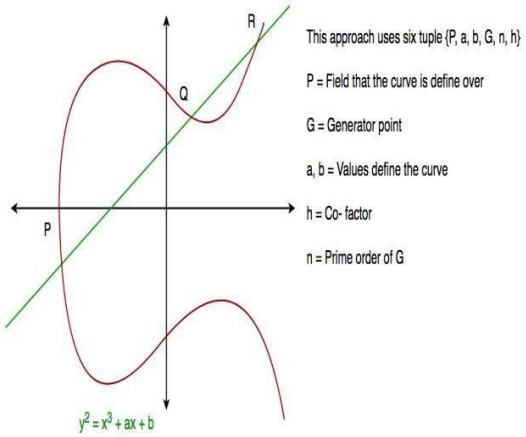
|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 7, July 2024

|DOI: 10.15680/IJIRSET.2024.1307112|

VI. ECC ALGORITHM

The asymmetric encryption technique ECC makes use of algebraic models of finite field elliptic curves.as its name suggests. Cryptography using Elliptic Curves (ECC) what is encrypted method that supports public-key encryption and is analogous to RSA.Whereas RSA's security is reliant on enormous prime numbers, ECC uses the elliptic curves mathematical theory to accomplish the identical degree of protection with much smaller keys.



Like other public-key cryptosystems, the security of elliptic curve cryptosystems is dependent on challenging mathematical problems. Provided are two points on an elliptic curve, G and Y, where Y = kG.The ellipse is the source of the word "elliptic curve." After the 17th century, elliptic curves were identified in the Diophantine equation for c. In addition, while computing the surface of the ellipse is straightforward, doing so is challenging. It is possible to reduce the equation to an integral.

Elliptic curve cryptography's components include:
1) ECC keys:Private key: Private key generation in ECC is extremely quick and as easy as safely generating integer in the given field. A valid ECC private key is represented by each number in the field.
2) Generator Point:For elliptic curves of finite field, the ECC coding system provides a special predefined EC point, called generating point G (base point), which can generate the subgroup of the elliptic curve by the following method. Any
Another task: To multiply an integer in the range [0...r] by G. There are many number generating points, but cryptographers pick one of them to create a complete (group Or subgroup) is crucial to optimizing performance. This is how generator "G" looks like.

Algorithms of ECC :
Schemes for Digital Signatures:
Among the digital signature techniques is the Elliptic Curve Digital Signature Algorithm (ECDSA). Algorithm for Elliptic Curve Digital SIGNATURE (ECDSA)
is a complex general digital signature encryption technology. Public key cryptography, known as elliptic curve cryptogr aphy, is based on the algebraic structure of finite field elliptic curves. ECC is often used to createdigital signatures, pse udorandom numbers, and other information.

Encryption Algorithms:
Elliptic Curve Integrated Encryption Scheme (ECIES): ECIES uses KDF (Key Derivative Function) to generate symme tric encryption keys and media access independent of the ECDH key. It is an encryption system that is verified by a pub lic key. Since the ECIES algorithm uses a password, it can access any number of files. In fact, ECIES is used in standar ds such as intelligent transportation. ElGamal is an asymmetric encryption technology for sending messages securely o ver long distances. Unfortunately, if the encrypted message is short enough, it's easy for this techniqueto come together in the midst.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 7, July 2024

|DOI: 10.15680/IJIRSET.2024.1307112|

Algorithm for Key Agreement:
Elliptic Curve Elliptic Curve Diffie-Hellman (ECDH) Diffie-Hellman (ECDH) is an important communication The contract allows both parties establish a common security channel. This secret expression can be utilized to generate additional keys or can be used directly as the key.Subsequent communications can then be encrypted using the key or the received key using key ciphers. The entire process is summarized in Menezes-Qu-Vanstone. MQV, like other Diffie-Hellman proofs, provides direct protection against adversaries. Any finite group can use this

VII. CONCLUSION

Encryption tiab decryption siv elliptical nkhaus cryptography (ECC) provides a secure and effective way to protect data.This approach is particularly useful because it provides a High level of security with a relatively small key compared to other algorithms such as RSA. ECC's small size speeds up operations and reduces resources, making it ideal for today's encryption needs.ECC's mathematical foundation, based on finite field elliptic curves, ensures stable security, which is important in today's connected world, where data crimes and cyber threats are very common. The performance of ECC allows it Can be used in many cryptographic applications including digital signatures, key switches, and secure communications.It is used in hardware and software systems to enhance the total protection security framework without compromising performance. Its adoption in various security protocols marks a major advancement in cryptographic technology to provide some protection of sensitive information. Continuous investigation and creation of ECC may lead to more secure and optimized encryption technology in the future.

REFERENCES

[1] “A secure and fast approach for encryption and decryption of message communication” – Ekta Agarwal, Parashu Ram Pal.
[2] “End-to-End Encryption Techniques” – Karthik giri, Namit Saxena, Yash Srivastava, Pranshu Saxena.
[3] “A Review Paper on Cryptography” – Abdalbasit Mohammed Qadir.
[4] Implementation of Encryption and decryption Methodologies - Lohit H1, Dr. Umarani C2.
[5] A NEW APPROACH FOR COMPLEX ENCRYPTING AND DECRYPTING DATA - Obaida Mohammad, Awad Al-Hazaimeh
[6] Menezes, A., Vanstone, S., & Van Oorschot, P. (1997). Handbook of Applied Cryptography. CRC Press. This book provides comprehensive coverage of cryptographic algorithms, including detailed information on elliptic curve cryptography.
[7] Koblitz, N. (1987). Elliptic curve cryptosystems. Mathematics of Computation, 48(177), 203-209. This paper introduces the concept of elliptic curve cryptography and its application in secure communications.
[8] Miller, V. (1986). Use of elliptic curves in cryptography. In Advances in Cryptology—CRYPTO'85 Proceedings (pp. 417-426). Springer, Berlin, Heidelberg. A foundational paper that discusses the application of elliptic curves in cryptographic systems.
[9] Certicom Research (2004). Standards for Efficient Cryptography SEC 1: Elliptic Curve Cryptography. This technical report provides standards and guidelines for implementing ECC in various cryptographic protocols.
[10] National Institute of Standards and Technology (NIST). FIPS PUB 186-4: Digital Signature Standard (DSS). This publication includes standards for digital signatures using elliptic curve algorithms, providing a basis for secure digital communications.
[11] Hankerson, D., Vanstone, S., & Menezes, A. (2004). Guide to Elliptic Curve Cryptography. Springer-Verlag. This book serves as a practical guide for implementing ECC, covering both theoretical and practical aspects.
[12] Blake-Wilson, S., Johnson, D., & Menezes, A. (1996). Key agreement protocols and their security analysis. In Proceedings of the Sixth IMA International Conference on Cryptography and Coding (pp. 30-45). Springer, Berlin, Heidelberg. This paper discusses the security of key agreement protocols, including those based on ECC.
[13] Gallant, R. P., Lambert, R. J., & Vanstone, S. A. (2001). Improving the parallelized Pollard lambda search on binary anomalous curves. Mathematics of Computation, 69(232), 1699-1705. This paper presents improvements in the computational techniques used in ECC.
[14] http://haliustasi.com/wp-content/themes/busify/tl6wqb/cipher-algorithm.html

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details