iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** XII **Month of publication:** December 2022

DOI: https://doi.org/10.22214/ijraset.2022.47982

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 10 Issue XII Dec 2022- Available at www.ijraset.com

Symmetric Cryptographic Approaches

Anoushka Malhotra[1], Ashwin Arora[2], Dr. Manjot Kaur Bhatia[3]
[1, 2, 3]*Jagan Institute of Management Studies, Sector - 5, Rohini, Delhi – 110085*

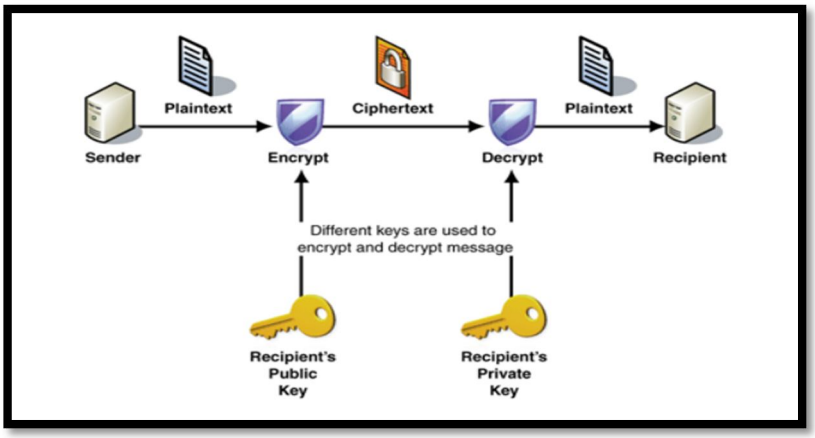
Abstract: ***In recent decades, information security has become a major concern. They have recently been intensively investigated and developed because they need more encryption and decryption and are tough to breach. These constraints need the use of encryption. In recent years, several academics have developed numerous encryption algorithms, such as AES, DES, 3DES, RC4 Algorithm, Blowfish Algorithm, and others. Data encryption techniques have advanced from relatively easy routes to quite hard mathematical calculations to guarantee excellent communication security. This study compares and contrasts symmetric encryption techniques, as well as attack vulnerabilities.***
Keywords: Cryptography, Encryption, Decryption, AES, DES, 3DES, RC4, Blowfish

I. INTRODUCTION

Data security has risen to the top of the priority list in today's data transfer. How can the data be guaranteed during transmission? We employ a technology called cryptography for data security, in which the data is encrypted from beginning to end and the receiver must know how to decrypt the data to know what it is. The technique of transforming plain text data into seemingly random and incomprehensible text (cipher text) is known as encryption. The process of turning encrypted text back to plain text is known as decryption. Specific chunks of the cipher text should be decrypted using encrypted data. Cryptography is a technique for preventing data theft and unauthorized access. A symmetric cryptosystem is one in which the sender and receiver both have the same key. This means that for encryption and decryption, both the sender and the receiver utilize the same key. In an asymmetric cryptosystem, several keys are used. The sender encrypts the communication with the public key, and the receiver decrypts the encrypted data with the private key. Cryptography approaches from the past. The transmitter and recipient agreed on a set of pre-shared encryption/decryption keys in the old cryptosystem. Each following message is encrypted and decrypted using these keys. Disposable pad is a type of encryption that uses a pre-shared key that can't be used more than once. Encryption and decryption must be done with the same key. When the previously shared keys are depleted, the sender and receiver can meet in a safe location to securely exchange a fresh set of keys and store them for future message exchanges. A new cryptographic algorithm has been developed. The main principle of new cryptosystem's is that now we trust the confidentiality of the key rather than the algorithm's confidentiality.

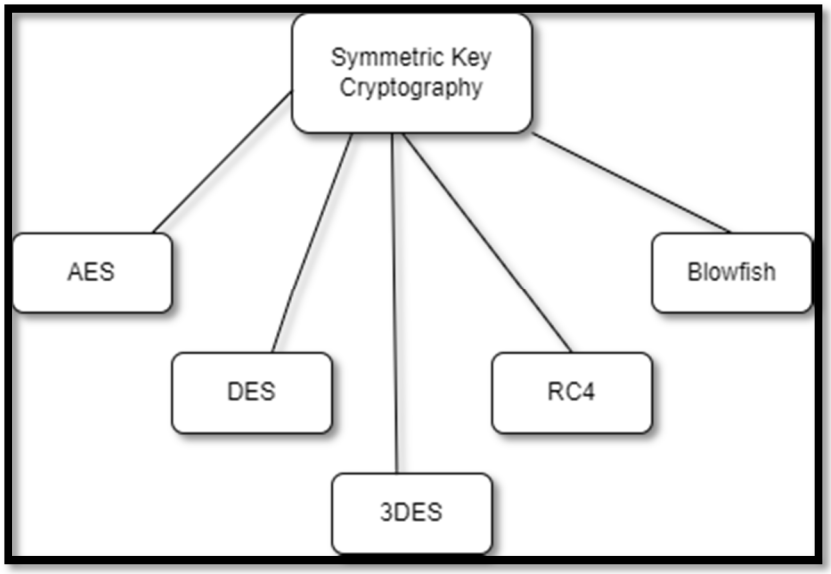
The three basic purposes of modern encryption systems are as follows:

1) *Confidentiality:* Never give out information to someone you don't know. Before sending information, make sure the sender and receiver are both identified and authorized.
2) *Integrity:* Information should not be changed while it is being stored or sent.
3) *Undeniable:* A message's creation/transmission cannot be denied. This ensures transaction legality and "digital" traceability.



GENERAL ALGORITHM FOR SYMMETRIC CRYPTOGRAPHY

AES, DES, 3DES, RC4, Blowfish, and other algorithms are examples of symmetric key cryptography. These fundamental symmetric key algorithms are covered in this section.



A. Advanced Encryption Standard (AES)

NIST (National Institute of Standards and Technology) launched AES in January 1997. For both encryption and decryption, it has a minimum block size of 128 bits and is more reliable than the DES method. Bytes are first substituted, then rows are shifted, then columns are mixed, and lastly the round key is added. Both delicate and unclassified goods can be secured using it.

B. Data Encryption Standard (DES)

This algorithm, which uses a block size of 64 bits, was created by IBM in 1997. Eight S-Boxes make up each of the 16 phases that make up the encryption process. The bits are first shuffled, followed by non-linear substitutions, and lastly the XOR operation is used to obtain the result. The result is merged with the sub key of a specific round using the XOR function. Sub-keys are used in reverse order throughout the decryption process.

C. Triple Data Encryption Standard (3DES)

It is a developed version of the DES algorithm. It has an overall key length of 192 bits [76] and is very dependable. The key is initially divided into three separate sub-keys, each of 64 bits. The subsequent steps are the same as for the DES algorithm, with the exception that they are carried out three times. Data is encrypted using the first key, and then decrypted using the second key. The decrypted data is encrypted again using the third key. There is limited possibility to keep the data safe for a longer time, though.

D. RC4 Algorithm

Ronald Rivest created this algorithm. Continually exchanging state entries based on key sequence is necessary. The key length varies and might be anything between 1 and 256 bytes. It creates a stream using pseudo-random bytes, which is then XOR to change plain text into encrypted text. Compared to the DES algorithm, the encryption method is ten times faster.

E. Blowfish Algorithm

It is the most effective encryption algorithm currently in use. The key length varies and can be anything between 32 and 448 bits. The block size of it is 64 bits. There are only two fundamental steps to the process. Key expansion is carried out initially. There are 18 sub-keys of 32 bits each in the P-array. Four 32-bit S-boxes with 256 entries each are present. Then, XOR techniques are used to encrypt the data. It has many uses for which the key is not regularly altered. Blowfish was created in 1993 by Bruce Schneier as an alternative to traditional encryption methods.

II. LITERATURE SURVEY

In the area of cryptographic algorithms, numerous academics have made significant contributions to data security Researchers.

Wang and Yu [1] have contributed to some of this work by proposing a block cypher technique based on dynamic chains produced by several chaotic systems that circumvents the cyclic degradation of random chains caused by precision. The unique aspect of its encryption method is that it uses a key stream produced by a number of one-dimensional chaotic maps to encrypt plain text. The encryption technique has, however, developed several flaws as a result of this functionality.

To shield data from outside influences, Ankit Fadia and Jaya Bhattacharjee [2] explain how to encrypt it. Explain what encryption and decryption are, what they are used for, and how encryption satisfies the growing demand for protecting people's privacy in communications and transactions.

Performance analysis was done on the implementation of cryptographic software created for pervasive computing by S. Rinne, T. Eisenbarth, and C. Paar [3]. The topic focuses on the unique characteristics of embedded devices that must be taken into account, including cost (which is dictated by memory use) and power needs. DESL, HIGHT, SEA, and TEA/XTEA are some of the cyphers that are covered. The 8-bit AVR microcontroller platform cipher's assembler implementation is examined and contrasted with the byte-oriented AES implementation. TEA / XTEA and SEA at least use a lot less memory than AES, even though none of the cyphers on the 8-bit hardware in issue are superior to it.

A new strong, compact, and effective block cypher called DESL has been proposed by A. Poschmann, G. Leander, and K. Schramm [4] (DES Lightweight Extension). DESL is especially well suited for RFID (Radio Frequency Identification) devices because of the modest chip size limits. The Data Encryption Standard (DES) concept is the foundation for the proposed DESL, although unlike DES, it employs a single Sbox repeatedly eight times. The required chip size can be greatly decreased with this technique. Sbox is highly optimized for DESL to fend off typical attacks like the Davies Murphy attack and linear and differential crypt analysis. As a result, DESL implements many applications with the proper level of security.

Identity-based cryptography, which includes digital signature and encryption technology for identity verification, was studied by Darpan Anand [5]. They looked at the applications for identity-based encryption that are now being used in several types of wireless networks, including ad hoc networks and mobile networks. They also talked about the conditions in which identity-based cryptography should be used, as well as its benefits and drawbacks. The primary restriction is that the methods are only capable of producing fixed output blocks, which is a sign of the cracker.

The power consumption of the RC4 and EAS algorithms in wireless local area networks was proposed by Pra Sithsangaree [6] and examined. Performance metrics include key size fluctuations, CPU workload, power consumption, and encryption performance. AES is more efficient than RC4 at encrypting small data packets, according to experiments, whereas RC4 is quick and energy-efficient at encrypting large data packets. The findings suggest that we can conserve energy by providing encryption for all packet sizes using a combination of RC4 and AES.

III. FUTURE SCOPE OF SYMMETRIC CRYPTOGRAPHY ANALYSIS

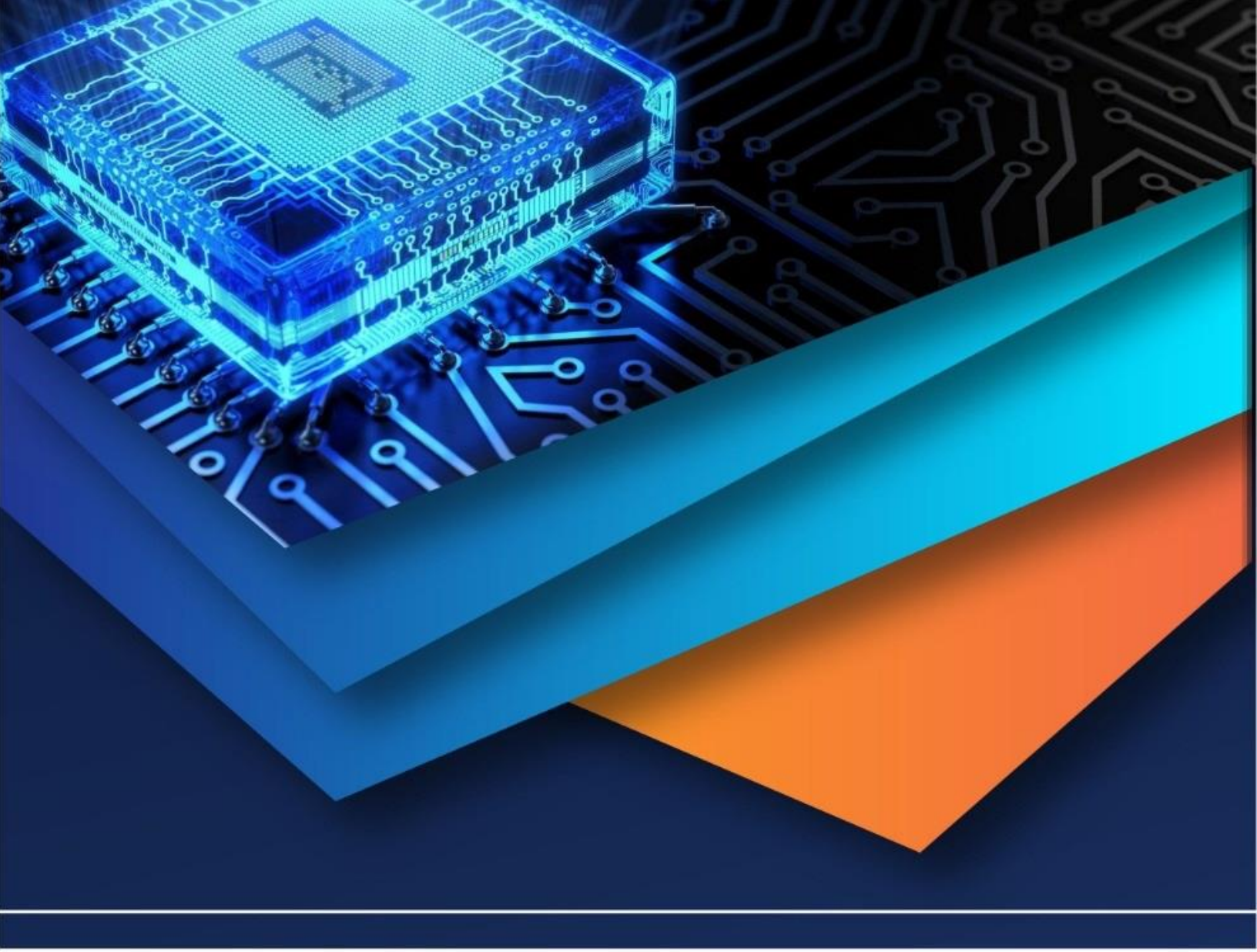
On the basis of symmetric key cryptography, numerous procedures had previously been suggested. They guarantee top-notch data security. However, several topics were left unresolved. Oblivious Attribute Certificates require the development of robust revocation procedures. Data recovery for peer-to-peer security must be quick and able to manage numerous computers. High data transfer rates are suitable for Service Oriented Architecture Systems (SOA). Data security is improved by self-certification of the public key, but this demands a lot of storage. Therefore, techniques can be created to cut both the storage and processing requirements at once. The many parameters of digital watermarking include resilience, transparency, security, capacity, complexity, etc. But we can't accomplish them all at once. An appropriate algorithm can be created based on this circumstance. How a huge message can be embedded while maintaining its robustness can be examined. Better cryptography techniques increase system performance and function effectively in various situations.

IV. CONCLUSION

Through a number of factors, including authentication, confidentiality, non-repudiation, data integrity, etc., cryptography is essential in guaranteeing data security. Various symmetric cryptographic techniques that have been created thus far have been examined in this study. The kind of data and communication channel must be considered while using these encryption and decryption techniques. Based on the fundamental characteristics, benefits, and applications of the suggested mechanisms, we have created a comparison study of them. The public key certification and revocations as well as the digital watermarking technique are proven to be among the most effective. The information is immediately embedded into the media data as part of the watermarking process, which is based on Steganographic technologies. For data privacy, the public key validation is ensured by the public key certification and revocation mechanisms. Both of them provide efficiency, adaptability, security, imperceptibility, transparency, and robustness.

REFERENCES

[1] https://www.hindawi.com/journals/mpe/2010/590590/
[2] Ankid Fadia, Jaya Bhattacharjee, “Encryption, Protecting Your Data”, Vikash Publishing House Pvt Ltd,2007, ISBN: 812592251-2
[3] https://aece.ro/abstractplus.php?year=2013&number=2&article=4
[4] https://en.m.wikipedia.org/wiki/Advanced_Encryption_Standard
[5] https://medium.com/spidernitt/introduction-to-timing-attacks-4e1e8c84b32b
[6] https://en.m.wikipedia.org/wiki/Neal_Koblitz#:~:text=He%20co%2Dinvented%20Elliptic%2Dcurve,women%20scientists%20in%20developing%20countries.
[7] https://www.semanticscholar.org/paper/Identity-Based-Cryptography-Techniques-and-(A-Anand-Khemchandani/93bd06c605d3af191d41323ba6b7ff650a204694
[8] https://en.m.wikipedia.org/wiki/Stream_cipher



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY