iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 12 **Issue:** XII **Month of publication:** December 2024

DOI: https://doi.org/10.22214/ijraset.2024.65962

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 XII Dec 2024- Available at www.ijraset.com

Innovative Security Framework for Enhancing Data Protection in Mobile Cloud Environments

Asst. Prof. Mr. Suresh P[1], Kritika Taank[2], Madaka Akshay Kumar[3], Muskan Patel[4]
Dept. Of Computer Science And Engineering Sri Venkateshwara College Of Engineering, Bengaluru – 562157.

Abstract: ***There is especially a challenging problem for secure communications in the last few years among the resource-poor environments like IoT devices and embedded systems which had driven the research to lightweight cryptography algorithms, performing wonderfully on the constraints of computations, memory, as well as also energy resources. It involves the implementation along with performance analysis of probably the most impressive lightweight block ciphers, such as SIMON, SPECK, and HIGHT. It also encompasses ECC as a safe alternative substitute to the traditional ones that contain AES. SIMON and SPECK are new-generation lightweight block ciphers developed by NSA for hardware efficiency so that performance is maximized at low speeds with very high levels of security. Also included are the performance characteristics of HIGHT, which is a specially designed block cipher for environments with very low resources. ECC is presented as the asymmetric encryption algorithm that provides at least some level of security yet its key sizes are dramatically smaller than the counterparts making it well applicable within these environments. In addition, an overall comparison in the aspect of the computational cost, usage of the memory, and the security level among the algorithms is made.***

Keywords: Lightweight cryptography, SIMON algorithm, SPECK algorithm, HIGHT algorithm, Elliptic Curve Cryptography (ECC), block ciphers, resource-constrained environments, embedded systems, IoT security, cryptographic performance analysis, computational efficiency, memory usage, key size optimization, encryption algorithms, security trade-offs, asymmetric encryption, cryptographic solutions, hardware efficiency, security level, energy-efficient cryptography.

I. INTRODUCTION

Mobile cloud computing has been developed drastically with the rapid Internet of Things. The nature of mobiles and IoT devices are resource-constrained where processing power and memory are unavailable. It also consumes lesser energy as well. So such limitations increase threats and decrease the usage of traditional cryptography. Since this is the age of getting smarter devices, where all information goes and passes through them, hence this further makes it vital for smooth yet safe data-encryption mechanisms.

Of those cryptos used, one finds that ECC is still amongst the ones having minimum keys with equivalent levels of safety. These algorithms, compared with others, such as RSA, require much fewer computations to execute the same security, and this is what makes ECC so popular in situations where a device can afford average computational resources. Still, even in this light, ECC becomes unbearably expensive for environments ultra-constrained in every dimension-memory byte and milliseconds of computation.

Such a demand for secure yet efficient cryptographic solutions in such environments has elicited the development of lightweight cryptographic algorithms. Concurrently, SIMON, SPECK, PRESENT, HIGHT can be optimized and are optimized with low power usage, in use of memory, high speed processing. All these have been found to be in effect use for various applications ranging from embedded systems, to RFID devices, wireless sensor networks, mobile cloud platforms and so many more. The study will hence compare their performance and highlight the trade-offs along with how suitable such algorithms may or may not be for respective applications.

A. Elliptic Curve Cryptography (ECC)

This means the system is a public-key cryptosystem based upon certain properties of the mathematical underpinning for elliptic curves over finite fields. Essentially, the computational intractability of the Elliptic Curve Discrete Logarithm Problem allows for virtually unparalleled strengths; that is, with ECC, the same strength at multiple orders-of-magnitude smaller keys, compared with algorithms previously known, namely the traditional RSA or DSA.

Elliptic Curve Equation:

An elliptic curve is defined as:

$$y2 \equiv x3 + ax + b \bmod p$$

Where:

- a and b are curve parameters.
- p is a large prime number defining the field.

1) Key Exchange (ECDH):

Given a private key d and a public point P, the public key is:

$$Q = d * P$$

To compute the shared secret between two parties A and B:

$$S = dA * QB = dB * QA$$

Encryption (ElGamal ECC):

For plaintext M and random k:

$$C1 = k * P, C2 = M + k * Q$$

Decryption recovers M as:

$$M = C2 - d * C1$$

2) Key Features:

- Much stronger security at shorter key lengths as one 256-bit ECC key is comparable to the strength of one 3072-bit RSA key
- Lower level overhead makes it suitable for use in battery powered devices
- It is very extensively used in secure communications, in fact for use with TLS/SSL.

3) Working:

- The private key used is a random number.
- The elliptic curve point is a public key
- Shared secret computation with the receiver's public and sender's private key in encrypting mode.
- Shared secret as a base for symmetric encryption of the original data.

B. SIMON

SIMON is the lightweight block cipher from the United States National Security Agency. The design is simple, efficient, and secure so extremely suitable for use on Internet of Things devices as well as other embedded systems.

1) Encryption Equation:

Let L and R denote the left and right halves of the plaintext block:

$$Ri+1 = Li + f(Ri) + Ki$$
$$Li+1 = Ri$$

Where:

- $f(x) = (x \ll 1) \wedge (x \ll 8) + (x \ll 2)$
- Ki is the round key.

Decryption Equation:

The decryption follows the reverse process, applying the same function and round keys in reverse order.

2) Key Features:

- It follows a Feistel structure oriented towards operations sliced into bits: AND, XOR, and cyclic shifts
- Block and key : 32/64-128/256 bits.
- Low in memory and computational

3) Working:

- The plaintext is divided into two halves
- Rounds are performed using bitwise operation together with the round keys on both halves.
- The resulting output will be the ciphertext for the input plaintext.

4) Advantages:

- Optimized highly for hardware
- Good against differential and linear cryptanalysis.

C. SPECK

SPECK is a lightweight cipher companion designed by NSA, to SIMON. While SIMON is optimized to hardware, SPECK is optimized for software efficiency.

Encryption Equation:

Let L and R denote the left and right halves of the plaintext block:

$$\mathbf{Li+1 = ((Li \gg \alpha) + Ri + Ki) \bmod 2n}$$

$$\mathbf{Ri+1 = (Ri \ll \beta) + Li+1}$$

Where:

- $\gg$ and $\ll$ denote bitwise rotation.
- α and β are rotation constants.
- Ki is the round key.
- n is the word size.

1) Decryption Equation:

Similar to encryption but the operations are reversed, and keys are applied in reverse order.

2) Key Features:

- ARX structure of Addition, Rotation, and XOR to enable high-speed encryption of the software platforms.
- Block size configurations are flexible and vary between 32 to 128 bits while key sizes vary flexibly from 64 to 256 bits.

3) Working:

- Data is divided into two halves.
- The ARX operations and round keys are performed to encrypt the data.
- It is extremely light on computations, hence this is a process to produce ciphertext

4) Advantages:

- It is an extremely fast operation on both microcontrollers as well as low power devices
- Extremely easy to implement

D. PRESENT

PRESENT is lightweight block cipher targeting resource-constrained devices. In other words, those used by IoT as well as for RFID applications. In fact, it is built from SPN structure. For that reason, at a glance of the first aspect, PRESENT manages simultaneously the conditions of easiness and of safety.

1) Encryption Process:

The PRESENT algorithm encrypts a 64-bit plaintext block using an 80-bit or 128-bit key through 31 rounds of substitution and permutation.

Round Function: The encryption process can be expressed as:

$$\mathbf{C = P31(S31(...P1(S1(P + K1)) ...))}$$

Where:

- C: Ciphertext
- P: Plaintext
- Ki: Round keys
- Si: Substitution layer
- Pi: Permutation layer

2) Decryption Process:

The decryption process in PRESENT involves reversing the encryption steps using the same round keys in reverse order.

3) Key Features:
- has a fixed size 64 bits block-size 80/128.
- it derives advantage from 31 round of encrypting process towards good confusion and diffusion.
- hardware footprint is small with low memory

4) Working:
- Data is divided into blocks.
- Substitution layer: The data bits are replaced by values of a predefined S-box.
- Permutation layer: The bits are reordered for better diffusion.
- Repeat the process for 31 rounds to produce the ciphertext.

5) Advantages:
- High security-to-resource ratio.
- Resistant to a wide variety of cryptanalytic attacks

E. HIGHT

HIGHT is a block cipher efficiently designed for IoT and embedded systems requiring robust security.

1) Encryption Equation:

Let P[i] denote the i-th byte of the plaintext block and KKK the round keys:

$$C[i] = (P[i]+K[i]) + F(P[i-1], K[i])$$

Where F(x,y) is a nonlinear function involving rotation and addition:

$$F(x,y) = (x \ll \delta) + y \bmod 2 \wedge n$$

δ is a rotation constant.

2) Decryption Equation**:**

Reverse the process with inverse operations.

3) Key Features:
- 64-bit block size, and it uses 128-bit key
- It utilizes 32 rounds of encryption that incorporates modular addition, XOR, and left rotation.
- It is very lightweight, as the utilization of both power and memory is pretty low.

4) Working:
- It breaks up the input data into blocks.
- This employs round keys used iteratively in a series of simple arithmetic and logical operations.
- Atlast, it produces ciphertext output after the completion of 32 rounds.

5) Benefits:
- It is optimized for low resource environments.
- Known security against wide-ranging cryptanalysis attacks.

II. LITRATURE REVIEW

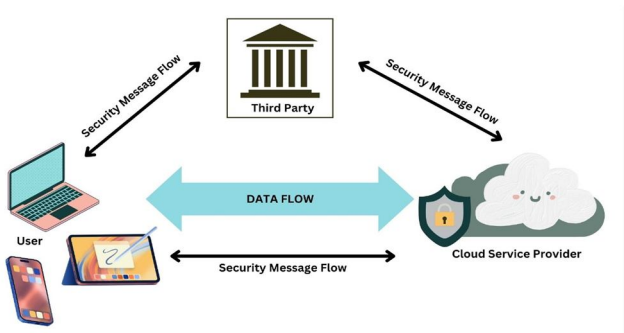
Of all of the known secure communication systems, it is those ECCs which are widely understood and especially implemented for IoT and mobile devices that make use of the intractability of ECDLP for any reasonable time. Hence such a system means that the level of security is highly extremely small key size. Thus it turns to be rather an ECC, quite efficiently using bandwidth and storage. ECC scalar multiplication is quite computationally intensive by design. So it is much more energy greedy for constraintive devices. Such ultra-constrained environments motivated lightweight cryptographic algorithms that accompany the ECC.

SIMON and SPECK are block ciphers designed by the NSA using simple operations such as XOR, rotation, and bitwise AND to optimize hardware as well as software performance. Although SIMON has been optimized for better hardware-friendly operation, SPECK has been optimized for better software performance. That is why they came into light for lightweight security.

Other two lightweight algorithms are PRESENT and HIGHT which are specifically designed for extreme environments with extreme resource constraint. PRESENT is one type of SPN cipher working on block size 64-bit while it can take the keys to be either 80 bit or 128 bit long. Compact design and efficient implementation put it firmly in the running for Internet of Things applications. Similarly, HIGHT has Feistel like structure with modular addition that is considered for low power encryption targeted for embedded systems and RFID technologies.

Comparative studies suggest that while ECC cannot be compared to the strength of cryptography, lightweight algorithms like SIMON, SPECK, PRESENT, and HIGHT are much faster than ECC concerning the processing speed, memory usage, and energy efficiency. Solutions shall therefore be application-dependent.

FLOWCHART



III. METHODOLOGY

This paper analyses ECC and lightweight cryptography algorithms such as SIMON, SPECK, PRESENT, and HIGHT using a multi-stage holistic approach within a resource-constrained environment, which can be similar to mobile cloud platforms and IoT ecosystems. At every stage of supplementation, it is guaranteed that the results obtained are absolutely reliable and relevant for practice. Supplementing is used at all points to make sure that the final result is fully reliable and relevant for practice.

A. Algorithm Selection and Study

Considering the applications of these algorithms in a resource-constrained environment, yet keeping in mind their capability to counter modern security challenges, the cryptographic algorithms selected for this study are ECC, SIMON, SPECK, PRESENT, and HIGHT. The analysis of each algorithm to understand its working mechanism, computational requirement, and encryption mechanism is given as follows:

1) ECC: Has high security with small key size giving superb resistance against brute force and side-channel attacks.
2) Lightweight Algorithms (SIMON, SPECK, PRESENT, HIGHT): designation is for minimum power overhead along with memory and computation such algorithms suitable for IoT and its related embedded systems.

This design used here is the same as that in SPN of PRESENT and in Feistel structures of HIGHT for which the security and computationally efficient march side-by-side are well clarified and understood.

B. Simulated Implementation Platforms

The algorithms have a controlled simulated mobile cloud and IoT environment. This simulates in real-world constraints of;

1) Low CPU processing and their memory
2) Energy constraint and battery-driven
3) Highly demanding real-time encryption that is required at speeds of high rates.

This is achieved by forming the simulations based on actual IoT usage cases such as the below examples: sending sensor readings, mobile apps communication edge computing in the processing, etc. Coupling together the simulation acquired above combined with lightweight algorithms integrated with ECC for benchmarking whether both may perform equally and as effectively against each other under equivalent conditions.

C. Performance Metrics

1) This is reflected in the running of algorithms in terms of
2) This includes the time the encryption and decryption processes, but which are more vital when it comes to the operation of real-time applications
3) Concerns the memory requirement needed for the running of the algorithms, especially in high-memory device such as a mobile gadget and IoT sensor Determine how much energy is utilized given per operation, but highly crucial in battery-dependent apparatus.
4) Key Generation Time: In protocols such as ECC, which mainly comprise the establishment of the first secure communications, this is an important performance metric.

All the above measurements are taken in an organized manner so that the performance of algorithms can be compared directly.

D. Security Analysis

1) Every algorithm needs to be tested for vulnerabilities to various types of cryptographic attacks:
2) ECC: It is proved due to the resistance against brute-force attacks and relies on the hardness of the elliptic curve discrete logarithm problem (ECDLP).
3) Lightweight Algorithms : Testing resistance against well known cryptanalysis techniques in both differential and linear attacks,
4) Security trade-offs comprise checks whether simplicity of lightweight algorithms brings riskiness in high-risk applications.

E. Hybrid Approach of Cryptography

Hybrid implementations are the ones with pros and cons based on a related consideration about ECC and light algorithms. In hybrid designs, ECC is useful while key exchanges are primarily offered to a better high-grade of security in view of proper PKI. Lightweight algorithms could support better data encryption and decryption procedure in performance while providing lesser resource usage.

This hybrid model enables ECC security features to be combined with lightweight algorithms so that the balanced solution for resource-constrained environments is retained.

F. Use Cases Practical Evaluation

These algorithms can be applied to the real-time cases. For which some are depicted as follows:

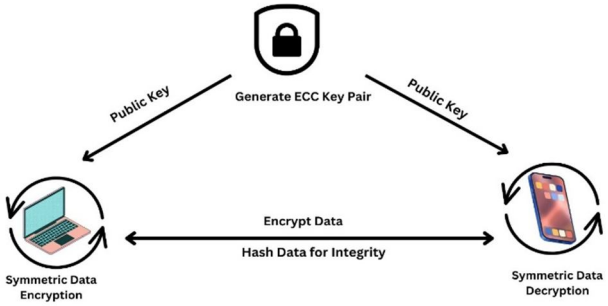
1) IoT Networks: It deals with information that has been secured from smart devices-as such health monitors, smart home sensors etc. in real time.
2) Mobile Cloud Storage: Involves encryption of private information uploaded to his cloud servers by a user.
3) Authentication in Embedded Systems : Deals with inter-device authentication and control in such systems.
4) Each use case has been evaluated based on the performance and resource utilization as well as the security strength of an algorithm or hybrid technique.

G. Comparison

Comparison is finally done to represent the results:

1) Performance Comparison- It presents the strengths and weaknesses of each algorithm in respect of speed, memory usage, and energy consumption.
2) Security Comparison- Analyzes the strength of each algorithm in terms of attack resistance and data protection
3) Suitability Analysis: It reveals algorithms for the application and is reliant on determining the performance trade-off against security.

Hence, the simulation methodologies, security analysis, and testing on real-world applications may well bring insight into the application of ECC along with lightweight cryptographic algorithms towards the solution of modern problems of data security in the Cloud and IoT environments.



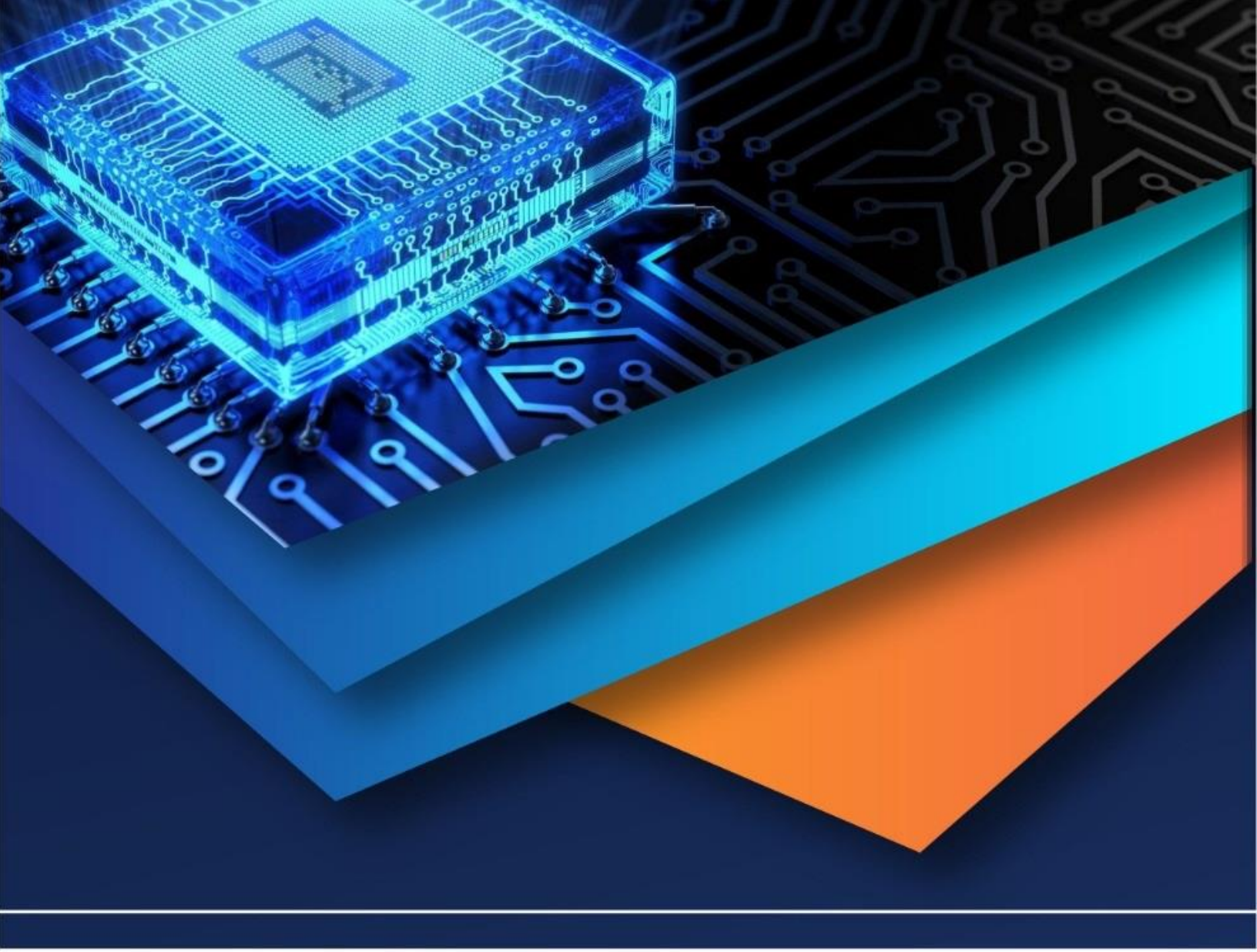
IV. CONCLUSION

It turns out to be one of the more robust crypto solutions having its best security profile with somewhat reduced sizes keys. Computational overhead makes systems used in resource-restricted devices from IoT and mobile cloud use that quite becomes a challenge. In the said scenario, lightweight encryption algorithms such as SIMON, SPECK, PRESENT, and HIGHT are helpful for easy deciphering and encryption with minimized resources.

This research study will therefore focus on the merits and demerits of ECC as well as lightweight algorithms but will do so under the need for tailored cryptographic solutions. As much as ECC stands practically destined to be the answer from high-security applications in areas of efficiency and resource-saving requirement, lightweight algorithms can themselves become very practical in their application as an alternative. Then, the hybrid approach would be quite efficient in most applications by taking the virtues of ECC along with the efficiencies of lightweight algorithms.

REFERENCRES

[1] R. Beaulieu et al., "The SIMON and SPECK lightweight block ciphers," in Proceedings of the Design Automation Conference (DAC), San Francisco, CA, USA, June 2015, pp. 1–6.
[2] A. Bogdanov et al., "PRESENT: An ultra-lightweight block cipher," in Proceedings of the 9th International Workshop on Cryptographic Hardware and Embedded Systems (CHES), Vienna, Austria, September 2007, pp. 450–466.
[3] D. Hong et al., "HIGHT: A new block cipher suitable for low-resource device," in Proceedings of the 8th International Workshop on Cryptographic Hardware and Embedded Systems (CHES), Yokohama, Japan, October 2006, pp. 46–59.
[4] N. Koblitz, "Elliptic curve cryptosystems," Mathematics of Computation, vol. 48, no. 177, pp. 203–209, Jan. 1987.
[5] V. S. Miller, "Use of elliptic curves in cryptography," in Advances in Cryptology – CRYPTO '85 Proceedings, Springer, 1985, pp. 417–426.
[6] C. Paar, J. Pelzl, and B. Preneel, Understanding Cryptography: A Textbook for Students and Practitioners. Berlin, Germany: Springer-Verlag, 2010.Data Encryption Standard (DES), Federal Information Processing Standards Publication 46-3, Oct. 1999.
[7] W. Stallings, Cryptography and Network Security: Principles and Practices.
[8] T. Wang and K. R. Babu, "Design of a Hybrid Cryptographic Algorithm," International Journal of Computer Science and Communication Networks (IJCSCN), vol. 2, no. 2, pp. 277–283.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY