Multi-Level Based Cryptography Approach for Securing Messaging System

Babatola Moses Omilodi, Lateef G. Salaudeen, Emmanuel Abiodun, Omobolanle Esther Akinjisola, Temitope Mosunmola Olatunji, Joshua Ubaga

Department of Computer Sciences, College of Natural and Applied Sciences, Chrisland University, Owode Road, Abeokuta, Ogun State, Nigeria.

DOI: https://dx.doi.org/10.51584/IJRIAS.2025.10120027

Received: 16 December 2025; Accepted: 24 December 2025; Published: 05 January 2026

ABSTRACT

This research addresses the growing challenge of cyberattacks targeting digital communications, such as unauthorized access and data theft, by proposing a secure messaging system based on advanced cryptography. The system employs a hybrid cryptographic approach, integrating RSA, DES, and AES algorithms. RSA, an asymmetric method, secures the exchange of symmetric keys, while DES and AES handle message encryption and decryption. By layering DES and AES, the system enhances robustness and resists potential attacks without sacrificing efficiency. Testing with textual data confirmed the system's ability to uphold confidentiality, integrity, availability, and authenticity. The inclusion of AES strengthened encryption, improving resilience against cryptographic threats. Overall, the findings demonstrate that a multi-level cryptographic framework provides a practical and effective solution for applied secure messaging systems, particularly in environments requiring enhanced data protection.

Keywords: Cryptography, encryption, decryption, cryptosystem

GENERAL BACKGROUND

In today's world, computer networking has become an integral part of life. There are many different networks available to share information between groups of devices through a shared communication medium. Information security is a significant issue in our developing information society [11]. With the expanding development of web and networking systems, parties will in general share or send information progressively over communication channels. The security of such information is of foremost significance in numerous applications as peculiar to military intelligence, medical information, government's information and service providers.

It is fundamental to protect information from attackers, and to do this, cryptography techniques can be used. Cryptography is a technique of storing and transmitting data in a unique and specialize way. This techniques empowers one to store sensitive information or transmit it crosswise over unsecure networks with the goal that it cannot be perused by anybody aside from the intended recipient [3].The aim of cryptography is to shroud the meaning of the message, through a strategy called encryption. The security of encrypted information is totally reliant on two things: the quality of the cryptographic algorithm and the secrecy of the key. Prior to the transmission of messages, encryption procedure is applied and the decoding procedure is applied in the wake of getting the encrypted information. Cryptography encrypts the message and transmits it; anyone can view the encoded message, yet is extremely hard to be read or interpreted, particularly in the event that it has been encoded with solid cryptographic algorithm.

Protecting data from hackers is essential, and cryptographic techniques can be employed to do this. A unique and specialized method of storing and sending data is called cryptography. With the aim of preventing anyone other than the intended receiver from viewing it, this technology enables one to store or send sensitive data across insecure networks [3].Through a technique known as encryption, the goal of cryptography is to obscure the message's meaning. The quality of the cryptographic method and the key's secrecy are the two main factors that determine how secure encrypted data is. The encryption process is used before communications are sent, while the decoding process is used once the encrypted data has been obtained. The message is encrypted and transmitted using cryptography; anyone may see the encoded message, but it is very difficult to read or decipher, especially if a strong cryptographic technique was used to encode it.

The idea of securing messages through cryptography has a long history. To be sure, Julius Caesar is credited with creating one of the earliest cryptographic frameworks to send military messages to his commanders [9]. While cryptography is the study of securing information, cryptanalysis is the study of investigating and breaking secure communication. Classical cryptanalysis involves an interesting combination of analytical reasoning, application of mathematical tools, pattern finding, persistence, assurance, and karma. Cryptanalysts are additionally called attackers. Cryptology grasps both cryptography and cryptanalysis. A cryptographic algorithm, or cipher, is a numerical capacity used in encoding and decoding process. A cryptographic calculation works in combination with a key, word, number, or expression to encrypt the plaintext. The equivalent plaintext encrypts to various cipher content with various keys. A cryptographic algorithm, in addition to all conceivable keys and every one of the protocols that make it work include a cryptosystem. "Cryptography" derives from the Greek word kryptos, signifying "hidden" [10]. The way to concealing information is to devise a hiding (encryption) system that is exceptionally hard to turn around (i.e. to find the original data) without using the decoding key. Ordinarily, the harder it is to discover the key, the more secure the mechanism.

LITERATURE/THEORETICAL FRAMEWORK

The science of safeguarding communication such that only the intended recipients can decipher communicated information is known as cryptography. The discipline, which comes from the Greek words kryptos, which means "hidden," and graphy, which means "writing," guarantees non-repudiation, confidentiality, integrity, and authenticity in digital transactions. Plaintext is changed into ciphertext via encryption, and the original content is recovered by decryption. Keys, which are numerical parameters that control the encryption/decryption process, are used in modern systems to do this. Higher system security is closely correlated with more robust algorithms and well-managed keys.

Cryptographers are those who work in this field. The four main objectives of modern cryptography are confidentiality (the data cannot be understood by individuals for whom it was not intended), integrity (the data cannot be altered or identified), non-repudiation (the sender of the data cannot later deny his or her intentions in creating or transmitting the data), and authentication (the sender and recipient can confirm each other's identity and the data's origin/destination). Different algorithms are used for encryption and decoding. The most effective algorithms employ a key. A key is merely an algorithmic parameter that enables the encryption and decoding process.

Existing works have explored cryptographic solutions in diverse contexts. . Kalpana and Singaraju (2012) applied RSA to address security challenges in cloud environments. The research was motivated by the needs to address information security issues in the cloud. The particular target was to provide a system to guaranteeing the protection of information in cloud environment. The approach included the formulation, implementation and evaluation of an RSA-based algorithm. The work adds to knowledge by demonstrating a practical application of RSA algorithm in information encryption and establishing a platform that guarantees that only approved users can access information. In any case, the limitations of the work is that the system was developed without tokenization procedure which makes it unacceptable for security of information in the cloud and practical depiction and application of the method to cloud/distributed computing was not considered.

Elliptic Curve Cryptography (ECC) was introduced by Alowolodu et al. (2013) for cloud security, showing improvements in battery life and computing efficiency at the cost of larger ciphertext sizes. Although these techniques can be computationally difficult at scale (Kalpana & Singaraju, 2012, and Alowolodu et al., 2013; Al-Hamami & Aldariseh, 2012), Al-Hamami and Aldariseh (2012) proposed improvements to RSA to increase factorization complexity and processing efficiency.

Other studies have tested hybrid approaches that combine symmetric and asymmetric techniques to mitigate individual limitations. For example, Oyelade et al. (2014) implemented a DES–RSA model for secure message transmission, while Chaitanya and Sree (2012) examined combined symmetric–asymmetric architectures for improved security and performance (Oyelade et al., 2014; Chaitanya & Sree, 2012).

Taken together, the literature suggests that layered or hybrid cryptographic schemes offer a practical way to balance security, performance, and manageable key distribution in networked environments.

MATERIALS AND METHODS

Before the description of the development of the graphical user interface, an overview of the architectural design is presented in figure 1:

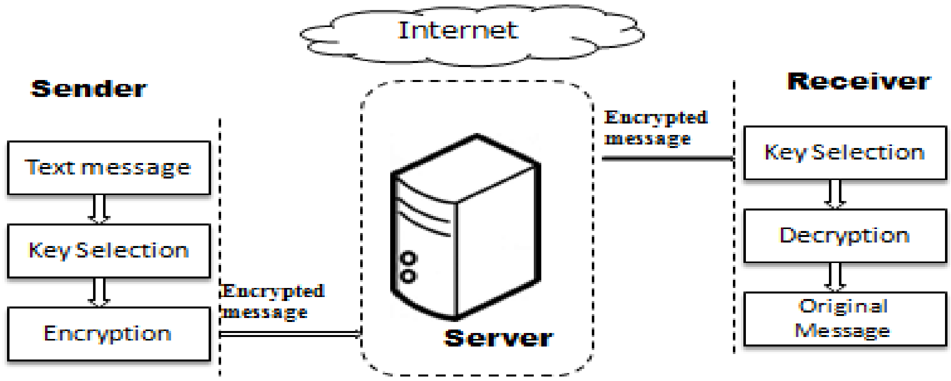


Figure 1: Architectural design of the system

a. Symmetric and Asymmetric Encryption

Symmetric and asymmetric encryption systems are the two main categories of encryption systems, which are among the most robust and secure methods of protecting data. Symmetric encryption, sometimes referred to as secret key or single key, encrypts messages using the same key that the sender uses to encrypt them and decrypts them. Prior to the public key's discovery and development, this scheme was the only one in use [7]. In symmetric encryption, the secret key must be sent between the sender and the recipient in a secure manner.

In contrast to symmetric encryption, asymmetrical encryption—also referred to as public key cryptography—is a relatively recent technique. Asymmetric encryption encrypts plain text using two keys. Secret keys are shared via a wide network or the Internet. It guarantees that the keys won't be intercepted and used maliciously by a third party. The symmetric method will be used to encrypt and decode the data to be transferred, while the asymmetric algorithm will be utilized to deliver keys over a secure channel, according to the system's architectural design, as illustrated in figure 1. The developed system's confidentiality, integrity, availability, authenticity, and non-repudiation were all achieved by doing this.

b. Multi-level Algorithm Development

Even while symmetric encryption algorithms like DES and AES are computationally efficient, they have major drawbacks when it comes to key distribution and administration, as [8] and [7] have pointed out. When utilized separately, symmetric algorithms are inappropriate for network-based communication due to these drawbacks. This was addressed by using a hybrid cryptography strategy for the system's implementation, which blends symmetric and asymmetric algorithms. To provide layered encryption of the plaintext message (P), the proposed multilevel security architecture uses both the Advanced Encryption Standard (AES) and the Data Encryption Standard (DES) at the transmitting end.

The proposed multi-level architecture is intended to demonstrate a defense in depth encryption strategy through layered application of standardized cryptographic algorithms rather than to introduce a new cryptographic primitive. The security strength of the system primarily relies on AES and RSA, while DES is included as an initial obfuscation layer to increase entropy and complicate attack surfaces.

First, a pseudorandom number generator is used to create a session key (see figure 2). With the help of this session key, the plaintext is first encrypted using DES and then encrypted again using AES. By introducing complexity and redundancy, this dual encryption method dramatically improves resistance to cryptanalytic and brute-force attacks.

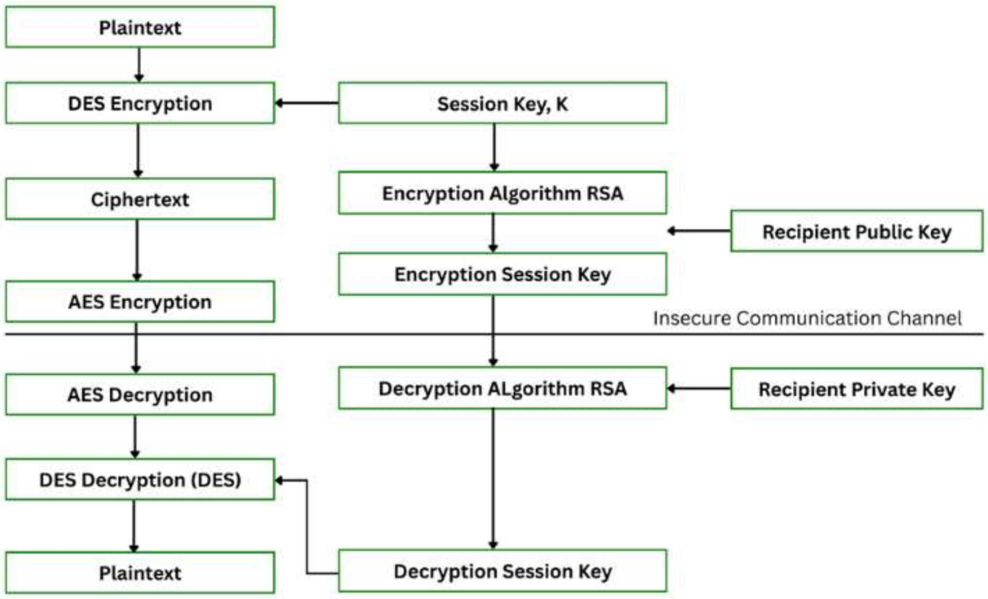


Figure 2: The developed multi-level technique

Secure session key distribution is essential since DES and AES are symmetric algorithms. This is achieved by encrypting the session key using the Rivest-Shamir-Adleman (RSA) algorithm, an asymmetric encryption technique. To make sure that only the designated recipient with the matching private key can decode the session key, the RSA algorithm encrypts it using the recipient's public key.

- The RSA-encrypted session key;
- The AES-DES encrypted message (cipher text).

Both components are sent to the recipient via the communication channel. The procedure is inverted on the recipient's end:

1. The recipient's private RSA key is used to decrypt the RSA-encrypted session key.
2. The original plaintext message is then restored by decrypting the ciphertext using the recovered session key, first with AES and then with DES.

A strong cryptographic defense is offered by this multilayer, layered encryption technique, which guarantees secrecy, integrity, authenticity, and safe key management during the communications process. JavaScript was used to implement the multi-level cryptography approach on a computer system with the following system parameters:

1. Processor: Intel (R) Atom CORE I3 at 2.2 GHz.
2. Installed Memory (RAM): 8GB
3. Operating System: Windows 11.

In this work, the algorithm designed is divided into two parts;

i. The key generation process using the asymmetric encryption technique.

ii. The encrypting and decryption process using the symmetric encryption technique.

System Design

Three tiers of cryptographic protection are included in the modular design of the encrypted messaging app:

Level 1: DES encryption is used to scramble the message initially.

Level 2: For added protection, AES re-encrypts the Level 1 message that was previously encrypted.

Level 3: The AES session key, which is necessary to decrypt the second layer, is encrypted using RSA.

This layered approach ensures that even if one encryption layer is compromised, the message remains secure under the remaining algorithms.

Algorithm Implementation

DES: 56-bit key size; block cipher; simple structure used as base layer encryption.

AES: 128-bit key; efficient and secure, applied as the main message encryption method.

RSA: 2048-bit key; used for secure key exchange and digital signing.

Test Cases:

- Text messages (short to long: 50–10,000 characters).
- Binary files (images, audio, PDFs).
- Multilingual content.
- Simulated network transmission and attacks.

Although experimental evaluation focused primarily on textual data, encryption algorithms operate on binary data blocks; therefore, the observed security and performance characteristics remain applicable to other data types such as multimedia and binary files at the cryptographic layer.

RSA Algorithm (Key generation process using asymmetric encryption technique)

RSA can be described as an Internet authentication and encryption system that applies an algorithm developed in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman (RSA) [4], RSA Algorithm which is based on the combination of four mathematical concepts: prime factorization, Euler's totient function, Euler's totient theorem and Extended Euclidean Algorithm (EEA) used to compute private key for decryption process.

A. Prime Factorization: This is the fundamental theorem of arithmetic which states that any number greater than 1 can be written exactly one way as a product of prime numbers.

B. Euler's Totient Function: This function is expressed as φ, called phi, and it is expressed in equations 1 to 3.

i. for a prime number a: $\varphi(a) = a-1$ (1)

ii. for primes a and b: $\phi(a.b) = (a-1)(b-1)$ (2)

C. Euler's Totient Theorem: The Euler Totient theorem is presented as follows:

$$\phi(a.b) = (a-1)(b-1) \qquad (3)$$

D. Extended Euclidean Algorithm (EEA): The EEA algorithm is called the greatest common divisor (gcd) method that is used to computea private key d. This method employs the matrix iterative scheme shown in equation 4 using ϕ(n)and the public key *e* and value of *d* is derived when e = 1 in A[2,1]

$$\begin{bmatrix} \phi(n) & \phi(n) \\ e & 1 \end{bmatrix} \qquad (4)$$

The iterative scheme for EEA algorithm is given as follows:

The elements of a matrix A, of i^{th}row and j^{th} column is given as a_{ij}, such that ϕ(n)= a_{11},

ϕ(n)= a_{12}, $e = a_{21}$, i = a_{22}, in A. ϕ(n)computed in equation 4 and *e* is the public key.

a. Computation of the gcd, x = ϕ(n) \ e, that is, a_{11} \ a_{21}

b. Computation of y_1= (x*e) and y_2= (x*1)

c. Computation of z1 = ϕ(n) - y_1 and z_2= ϕ(n) – y_2. That is, $z_1 = a_{11} - y_1$ and $z_2 = a_{12} - y_2$.

Write $z_1$and $z_2$in a new third row a_{31} and a_{32}

d. Check if the $z_1 = 1$ in a_{31}. If $z_1 \neq 1$, cancel out the a_{11} and a_{12} to remain two rows. (Now, row ϕ(n) has been cancelled out, the 2nd row becomes the first row and the new third row becomes the 2nd row).

e. Repeat steps (a – d), until e = 1, then the private key d = a_{22}

f. In case, a negative (–ve) value is derived in step c, add ϕ(n) computed in equation 1 to the negative result to make it positive.

The RSA algorithm involves three steps, namely: Key generation, Encryption and Decryption.

The general form of a cryptography scheme is given as follows:

E(M) → C

D(C) → M

Where E = Encryption, M = Message(Plaintext), C = Ciphertext, D = Decryption

RSA (Rivest-Shamir-Adleman) Algorithm is used for this research based on this mathematical concepts:

Prime Factorization: This is the fundamental theorem of arithmetic which states that any number greater than 1 can be written as a product of prime numbers;

Euler's Totient Function: this is expressed as for a prime number P; ϕ(P) = P-1

for primes a and b; ϕ(a - b) = (a-1)(b-1)

Euler's Totient theorem is therefore presented in equation 5:

$$\phi(a.b) = (a-1)(b-1) = 1 \quad \ldots\ldots\ldots\ldots\ldots\ldots \qquad (5)$$

Key Genereation

Select two large positive prime numbers, p and q such that p ≠ q

The mathematical expression is given below:

n = a*b, where n is called the MODULUS, equation 6.

$\phi(n)$ from $\phi(n) = (a-1)(b-1)$. (6)

Next, a random integer known as the "encryption exponent" is selected between 1 and ϕ such that

gcd (e ,$\phi(n)$) = 1 (i.e. the Greatest Common divisor of e and $\phi(n)$).

This is expressed below;

gcd (e ,$\phi(n)$) = 1 such that ($1 < e <(\phi(n)$)

Then, using the extended Euclidean algorithm, a unique integer for d will be computed as in equation 7:

$e*d = 1(\text{mod } \phi(n))$ such that ($1 < d < \phi(n)$) (7)

This implies that $d = e^{-1}(\text{mod } \phi(n))$

This generates the public key which is (N , e) and the private key d .

The public and private keys are thus (N , e) and d respectively:

where a = the first prime factor chosen, a nonnegative integer

b = the second prime factor chosen, and a nonnegative integer

N is the modulus.

gcd (e ,$\phi(n)$) = Greatest Common divisor between e and $\phi(n)$.

e = encryption exponent.

d = decryption exponent

(N , e) = the public key.

d = the private key.

ENCRYPTION: Since we now have our public and private keys, the next step is to encrypt the key. The key to be encrypted can be represented by m, where m is an integer in the interval (0, N-1).

We can calculate the cipher text, C (encrypted data format) by employing the formula as in equation 8.

$C = M^e \text{ mod } n$, such that $M < n$ where M is the plaintext message (8)

C = the cipher text (encrypted data)

DECRYPTION: The decryption is carried out by employing the formula as in equation 9:

$D = C^d \text{ mod } n$ (9)

RESULTS AND DISCUSSIONS

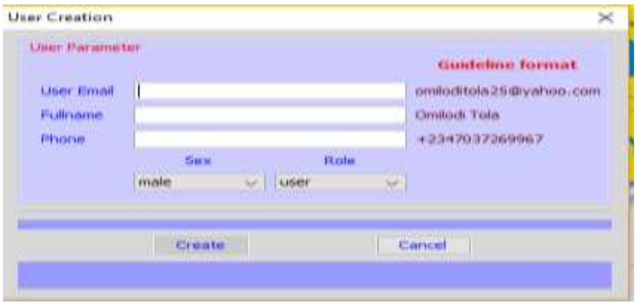
The user session takes the user of the system through the welcome page to using the system. The application software is activated by clicking on browser icon (Mozilla Firefox, Chrome, Opera and so on) on the desktop of the computer system connected to the network. This is followed by the launching the java executable jar file icon for the application to display the welcome page as shown in Figure 3. The welcome page contains an introductory message about the researcher and the system. After the user session page, then followed the registration page requiring the user to enter his/her details and is displayed as shown in Figure 4. At a successful registration process, the logon page is displayed, prompting for the entry of Username and Password by the user as shown in Figure 5

OMILODI
BABATOLA MOSES
CSC/15/5430

CONTACT DETAILS:
PHONE: +2347037269967
EMAIL: omiloditola25@yahoo.com

RSA & DES CRYPTOGRAPHY
SYSTEM

Figure 3: Welcome page



User Creation

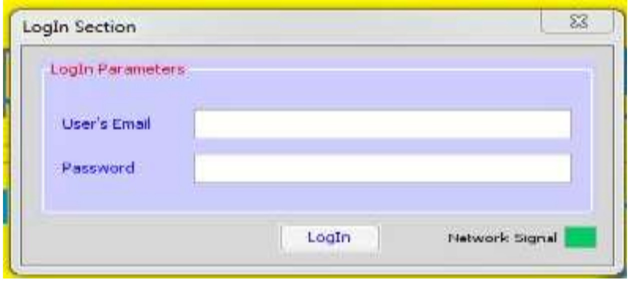
User Parameter

Guideline format

User Email: omiloditola25@yahoo.com
Fullname: Omilodi Tola
Phone: +2347037269967

Sex: male
Role: user

Figure 4: Registration page



LogIn Section

LogIn Parameters

User's Email
Password

Figure 5: Login Page

A successful authentication is established when a correct user name and password are entered. A click on the “Login” button displays the user dashboard for the application as depicted in figure 6.

On the dashboard, there are four major operations that can be triggered. They are:

i. The management tab pop up the inbox, outbox and compose page.

ii. A click on the operation tab triggers the key generation page and the analytical view as shown in figures 7 and 8.

iii. The key generation tab helps to generate new set of keys in bits for RSA encryption and decryption. The higher the bits chosen the more secured the keys generated. The public key and private keys are generated in this section.

iv. The analytical view displays the flow of encryption and decryption of plaintext using DES-RSA cryptography. This section is into the encryption page and decryption page.

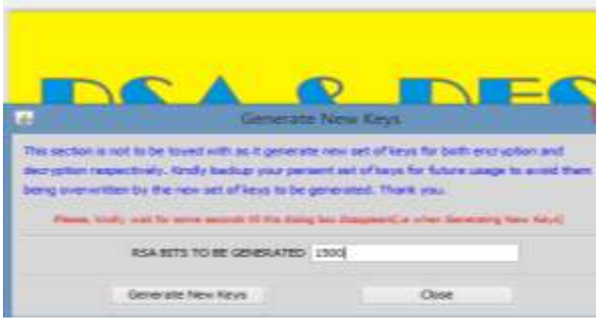
The encryption process in this system applies a multilevel cryptographic approach by sequentially utilizing DES, AES, and RSA algorithms. Initially, the plaintext is encrypted using the DES algorithm with a pseudorandomly generated DES key, which is displayed on the interface for reference. This encrypted output undergoes a second layer of encryption using the AES algorithm, thereby strengthening data confidentiality.

To ensure secure transmission of the DES key itself, RSA encryption is employed. The DES key is encrypted using the RSA public key, which is also presented along with its corresponding public exponent and modulus. This process establishes a hybrid encryption model in which RSA provides secure key management, while DES and AES ensure data-level encryption.

On the decryption side, the RSA private key is first used to decrypt the RSA-encrypted DES key. The system displays key parameters such as the modulus and bit length during this phase. Once the DES key is successfully recovered, it is then used to decrypt the DES-encrypted portion of the message, ultimately restoring the original plaintext.

In this implementation, the DES algorithm is responsible for the core message encryption and decryption, while RSA is used to encrypt and securely transmit the DES key, thereby forming a layered encryption strategy. The integration of AES between DES and RSA further enhances data protection. This multilevel cryptography framework leverages the strengths of symmetric and asymmetric encryption to provide robust security for secure communication. Figure 8 illustrates the complete encryption and decryption workflow

SA and DES Cryptographical Communication (RDCC) ~ It is all about having cryptographic



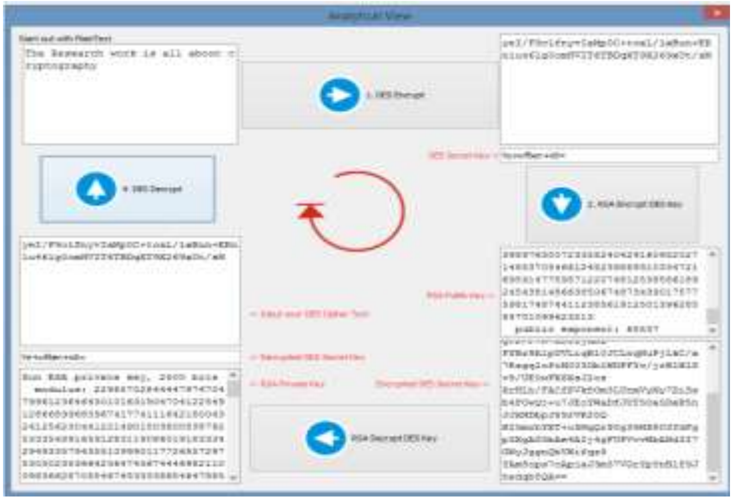
Generate New Keys

This section is not to be toyed with as it generate new set of keys for both encryption and decryption respectively. Kindly backup your persent set of keys for future usage to avoid them being overwritten by the new set of keys to be generated. Thank you.

Please, kindly wait for some seconds till this dialog box disappear(i.e when Generating New Keys)

RSA BITS TO BE GENERATED: 1500

Figure 6: Key generation section



Analytical View

Start out with PlainText

The Research work is all about cryptography

public exponent: 65537

Sun RSA private key, 2000 bits
modulus:

Figure 8: overall encryption and decryption page.

Performance Evaluation

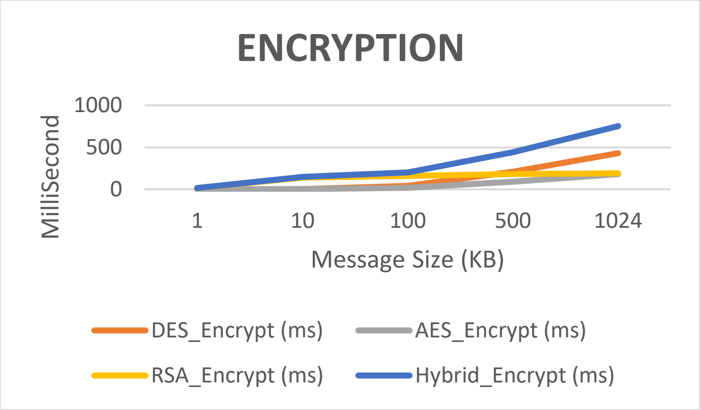
Tests were conducted to measure encryption time/decryption time, throughput, CPU usage, and memory consumption. Results were averaged over 20 iterations per test.

Table 1: Throughput

Algorithm	**Throughput (MB/s)**	**Remarks**
DES	6.5	Fast but weak due to small key size; optimized for hardware.
AES	8.7	Very fast and secure; hardware acceleration
RSA	1.2	Very slow compared to DES/AES; mainly used for key exchange, not bulk data encryption.
HYBRID	7.9	DES or AES handles bulk data; RSA handles key exchange. Performance mainly depends on AES/DES throughput.

Table 2: Encryption Time

Message Size (KB)	**DES_Encrypt (ms)**	**AES_Encrypt (ms)**	**RSA_Encrypt (ms)**	**Hybrid_Encrypt (ms)**
1	0.8	0.5	15.2	16.5
10	4.5	2.3	140.7	147.5
100	42.6	18.7	160.7	202
500	210.3	90.5	180.7	441.5
1024	430.8	180.9	190.7	752.4



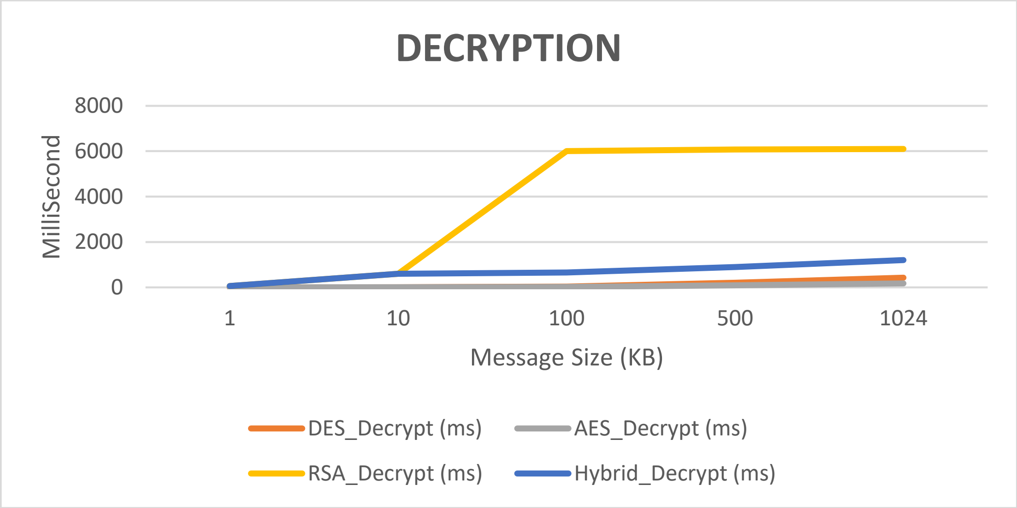
Encryption Time vs Message Size

- AES demonstrated the fastest performance.
- RSA had the highest time due to computational complexity.
- The multilevel model added some overhead but remained within acceptable limits for real-time use.

The observed performance overhead represents an acceptable trade-off between enhanced security and efficiency for applied secure messaging systems.

Table 3: Decryption Time

Message Size (KB)	DES_Decrypt (ms)	AES_Decrypt (ms)	RSA_Decrypt (ms)	Hybrid_Decrypt (ms)
1	0.7	0.4	60.3	61.4
10	4.2	2	600.1	606.3
100	41.8	17.9	6000.1	659.8
500	208.4	88.2	6070.1	896.7
1024	427.5	176.2	6100.1	1203.8



In term of Resource Usage

- RSA consumed the most CPU and memory.
- AES was the most efficient.
- The hybrid model balanced performance with added security layers.

Table 4: Security Analysis

Algorithm	Key Size	Vulnerability	Remarks
DES	56-bit	Brute force attack	Depreciate, used as initial obfuscation
AES	128-bit	None	Secure and efficient
RSA	2048-bit	Timing Attack	Safe with strong keys
Hybrid	Mixed	None observed	Recommended for secure communication

The multilevel model significantly enhances security by creating layers of encryption, making unauthorized access substantially harder.

Limitations of the Study

While the proposed hybrid cryptographic secure messaging system demonstrates improved security and acceptable performance, certain limitations are acknowledged. The Data Encryption Standard (DES) is incorporated solely as an initial concealment layer and not as a standalone security mechanism; the primary cryptographic strength of the system is provided by AES and RSA. The inclusion of DES therefore does not undermine overall system security but serves to illustrate layered encryption within an applied research context.

System evaluation was limited to textual data to establish baseline correctness and performance consistency. Since modern cryptographic algorithms operate on binary data blocks, the results remain applicable to other data formats at the encryption layer. This study focuses on applied system implementation and performance evaluation rather than formal cryptanalytic proof, relying on the well-established security guarantees of standardized algorithms such as AES and RSA.

Although the multi-layer encryption process introduces additional computational overhead, experimental results indicate that encryption and decryption latency remain within acceptable bounds for secure messaging applications. Key management was implemented at a session level to maintain experimental scope, while large-scale key lifecycle management and PKI integration are identified as areas for future research.

CONCLUSION

Information Security is a potential by which an organization can defend or lengthen a competitive advantage over others, this entails making sure that access to the network is controlled, and that data is no longer vulnerable to attack in the course of transmission across the network [7] .In this work, a multilayer cryptographic technique that combines DES, AES, and RSA in a secure communications system is presented. The system effectively illustrates how layered encryption boosts defenses against attacks while preserving usable speed for real-world applications. AES provides quick and secure data encryption, DES acts as an extra layer of concealment, and the RSA method guarantees safe key distribution. The effectiveness and resilience of the approach are confirmed by extensive testing on a variety of datasets, file formats, and message contexts. The findings demonstrate that a multi-level cryptographic framework is a practical and effective solution for applied secure messaging systems.

Future Work

Future research will focus on strengthening the proposed secure messaging system by replacing the DES concealment layer with more advanced and standardized symmetric encryption techniques such as AES-256 or ChaCha20-Poly1305, while preserving the multi-level defense in depth architecture. System evaluation will be extended to include multimedia data, real-time messaging streams, and large-scale file transmissions in order to assess scalability, latency, and throughput under realistic communication workloads. Also, incorporate controlled security evaluations and threat-model-based testing, including resistance to man-in-the-middle attacks, replay attacks, and key compromise scenarios, to validate robustness under real-world adversarial conditions. Performance optimization for resource-constrained environments such as mobile and Internet of Things (IoT) devices will also be explored through lightweight cryptographic configurations and alternative key exchange mechanisms such as elliptic curve cryptography (ECC).

Conflicts of Interest and Informed Consent Declarations: All authors declare that they have no conflicts of interest.

REFERENCES

1. Alaa Hussein Al-Hamami& Ibrahem AbdallahAldariseh. (2012), Enhanced Method for RSACryptosystem Algorithm", 2012 InternationalConference on Advanced Computer ScienceApplications and Technologies (ACSAT)

2. Alowolodu O.D, Alese B.K, Adetunmbi A.O., Adewale O.S, and Ogundele O.S. (2013), Elliptic Curve Cryptography for Securing Cloud Computing Applications. International Journal of Computer Applications (0975 –8887)Volume 66–No.23
3. Chaitanya, P. and Sree Y.R., (2012) "Design of New Security using Symmetric and Asymmetric Cryptography Algorithms", *World Journal of Science and Technology*, Vol. 2, No. 10, pp. 83-88.
4. Kaliski, Burt, (1997). "Growing Up with Alice and Bob: Three Decades with the RSA Cryptosystem". https://en.wikipedia.org/wiki/RSA_Security#cite_note-kaliski-2
5. Kalpana, P., and Singaraju, S., (2012) Data Security in Cloud Computing using RSA Algorithm", NIST Special Publication, NIST SP – 800-144
6. Moumita Mishra, Sayan Kumar Roy, AnweshaMukherjee, Debashis De, Soumya K. Ghosh,Rajkumar Buyya. (2019), An energy-aware multisensory geo-fog paradigm for mission criticalapplications", Journal of Ambient Intelligenceand Humanized Computing, https://link.springer.com/journal/12652
7. Oyelade, O. J. and Isewon, Itunuoluwa and Oladipupo, O. O. and Famuyiwa, A (2014) Implementation of Secured Message Transmission using DES and RSA Cryptosystem. Covenant Journal of Informatics and Communication Technology (CJICT), 2 (2). pp. 75-88.
8. Paul Reid (2004). Biometrics for Network Security. Prentice Hall, ISBN: 0-13-101549-4
9. Ravaei Niloo, (2018), Cryptography for Dummies — Part 2: The Caesar Cipher. https://medium.com/blockgeeks-blog/cryptography-for-dummies-part-2-the-caesar-cipher-665106afac78
10. Rouse Margaret, (2018), Cryptography. CloudSecurity https://searchsecurity.techtarget.com/definition/cryptography
11. Shikha, K. and Ishank, K., (2013) "Data Security Using RSA Algorithm In MATLAB", International Journal ofInnovative Research and Development, Vol. 2 Issue 7, page 479-483
12. Sugumaran M., Murugan B. Bala, and Kamalraj D., (2014), An Architecture for Data Security in CloudComputing, 2014 World Congress onComputing and Communication Technologies,https://ieeexplore.ieee.org/xpl/conhome/6754623/proceeding