A Hybrid Cryptographic Encryption System Using Affine Cipher and RSA for Secure Text Communication

***Abstract*—The paper represents the hybrid cryptographic encoder and decoder that combines the classical Affine cipher with modern RSA encryption to enhance message security.Intially the Affine cipher gives us a non-understanble text of the plaintext,while RSA encryption ensures strong asymmetric protection and by combining two encryption methods, this approach fixes the weaknesses of each one, making the overall system much stronger and more secure for the communication.The system is built using Python, and its performance is measured based on how long it takes to encrypt, decrypt, and generate keys .**

***Index Terms*—Cryptography, Affine Cipher, RSA, Hybrid Encryption, Python, Modular Arithmetic, Cybersecurity**

I. Introduction

In today's modern and digital world,secure communication is more important than anything ever.Traditional ciphers like the Affine cipher are easy to implement but it can be decode which has lack of strong security.On the other side RSA provides powerful encryption but computationally heavy.By combining the both methods,we can balnce the speed and security for the pratical use.This project introduces the hybrid encryption system that holds the strengths of both Affine and RSA to protect messages effectively.

II. Background

A. Affine Cipher

Affine cipher is basically monoalphabetic subsitution which is using the encryption function $E(x) = (ax + b) \mod 26$, and decryption function $D(x) = a^{-1}(x - b) \mod 26$. Here, a must be coprime to 26 to ensure the invertibility.

B. RSA Algorithm

RSA is based on number theory and public-key cryptography. It usually generates keys using two large prime numbers. The public key (e, n), is used for encryption, while the private key, (d, n), is used for decryption. This system ensures both confidentiality and proves that someone cannot deny their actions.

C. Cryptographic Principles

The hybrid system uses modular arithmetic, GCD , modular inverses, and prime number generation to ensure that the keys and operations are in the secure way

III. Methodology

The hybrid cryptographic system integrates the **Affine Cipher** and the **RSA** algorithm to offer a dual-layered encryption process. And this section will provides the step-by-step of the both encryption and decryption using these algorithm

A. Affine Cipher Encryption

1) User's Input: The user provides:

- A plaintext message
- A multiplicative key a (must and should be coprime to 26)
- An additive key b

2) Mathematical Basis: The Affine Cipher is based on modular arithmetic and over the 26 letters in the English alphabets. Each letter is converted to its corresponding numerical position starting from 0 to 25 ,x (A = 0, B = 1, ..., Z = 25) and the encryption is performed by using the formula:

$$E(x) = (a \cdot x + b) \mod 26$$

3) Key Constraints:

- a must be co-prime with 26 to ensure that the existence of a modular inverse.
- b is any integer used for additive key

4) Encryption Output: The final numbers are converted back into letters to get the encrypted message using the Affine Cipher.

B. RSA Encryption

The output of the Affine Cipher is input to the RSA algorithm.

1) Key Generation:

- Choose two large prime numbers p and q
- Compute:
$$n = p \cdot q$$
- Compute the Euler's totient function:
$$\phi(n) = (p - 1)(q - 1)$$
- Choose an encryption exponent e such that:
$$1 < e < \phi(n), \quad \text{and} \quad \gcd(e, \phi(n)) = 1$$
- Compute the modular inverse d (decryption exponent), satisfying:
$$e \cdot d \equiv 1 \mod \phi(n)$$

2) Public and Private Keys:

- Public Key: (e, n) — used for encryption process
- Private Key: (d, n) — used for decryption process

3) Encryption Process RSA:

- Convert each character of the Affine-encrypted text to its ASCII value P
- Apply the RSA encryption:

$$C = P^e \mod n$$

C. RSA Decryption

1) Decryption Process:

- Decrypt each encrypted value C using:

$$P = C^d \mod n$$

- Convert the numeric value of P back to a character using ASCII.

2) Affine Cipher Decryption: After RSA decryption, the original message is retrieved using the inverse Affine Cipher formula which is affine cipher decrption formula:

$$D(y) = a^{-1} \cdot (y - b) \mod 26$$

Where:

- a^{-1} is the modular inverse of a modulo 26
- y is the position of encrypted character's

D. Security Features

The proposed hybrid encryption system offers several built-in security advantages:

- The proposed hybrid encryption system offers the built-in security advantages:
- The system applies two layers of encryption—Affine Cipher and RSA—making it much take harder for the decoders and also for attackers.
- The Affine Cipher provides the fast and simple encrpytion like puzzlement of the message.
- RSA adds a strong layer of protection through secure key-based encryption.
- Modular arithmetic ensures operations are performed within a secure and consistent range.
- GCD (Greatest Common Divisor) checks validate that the chosen keys are they mathematically safe and also usable.
- Modular inverse computations make sure that every step of encryption is properly incomplete, so the decryption process which becomes reliable and also consistent.
- Prime number generation introduces randomness and also it increases the unpredictability of both RSA keys.
- Usage of public and private key pairs keeps that the data safe by making sure that authorized users can decrypt the data.
- The dual encryption design ensures that if one is been attacked, the other still protects the data.
- Together, from these techniques we create a system that's strong, secure, and resistant to tampering—perfect for safely transmitting sensitive information.

E. Chi-square

Chi-square test is a mathematical derivation that's utilized in main statistics and different comparison techniques which differentiate between expected data values and observed values [**?**]. It's used to determine how closely actual data fit with expected data. The value of chi-square will help us to obtain the solution to the question on the importance of the difference in expected and observed data statistically. A small chi-square value indicates that any differences in actual and expected data are due to usual chance.

$$\chi^2 = \sum \frac{(\text{Observed value} - \text{Expected value})^2}{\text{Expected value}} \quad (1)$$

Best Chi-Square test values show the non-homogeneity of the plain text files and respective cipher text files. We apply Chi-Square tests to our Proposed Algorithm, RSA, hybrid cryptosystems, and Algorithm . Our proposed algorithm has the best chi-square test values which prove the non-homogeneity of our proposed approaches is greater than all other techniques that we have analyzed.

TABLE I
CHI-SQUARE VALUES FOR RSA AND HYBRID ALGORITHMS

Samples	RSA	Hybrid
Sample_1	90.98	108.222
Sample_2	140.059	182.132
Sample_3	98.518	105.481
Sample_4	114.379	142.448

IV. PERFORMANCE METRICS AND RESULTS

Performance is evaluated on three metrics: encryption time, decryption time, and key generation time.

TABLE II
PERFORMANCE METRICS OF HYBRID CRYPTOGRAPHIC SYSTEM

Metric	Affine Cipher	RSA	Hybrid (Affine + RSA)
Key Generation Time	N/A	28.5 ms	28.5 ms
Encryption Time	1.2 ms	13.9 ms	12.4 ms
Decryption Time	1.1 ms	12.6 ms	12.3 ms
Security Level	Low	High	Very High
Brute-Force Resistance	Low	High	Very High
Frequency Attack Resistance	Low	Medium	High
Implementation Complexity	Low	Medium	Medium
Performance on Short Text	High	High	High
Layered Protection	No	No	Yes
Overall Effectiveness	Moderate	Strong	Excellent

The hybrid system slightly increases encryption/decryption time but drastically enhances security. Testing shows accurate recovery of original text and stability under different inputs.

V. DISCUSSION

This system offers a better improvement compared to traditional encryption methods by combining simplicity with the strength.Although RSA adds some extra computation time ,it greatly enhances the overall security of the system.And also it helps to protect messages that would otherwise that would

be easy to break with basic ciphers.Creating the project in python makes easy to understand,modifying and run on any platform.This balance between the security and accessibility makes the system in both practical and educational.

VI. Future Scope

In the future, this hybrid encryption system can be expanded to secure not just messages or text, but also files, images, and real-time data. A user-friendly GUI and support for IoT devices could make it more practical and accessible. We can also improve its speed and strength by using better key generation methods and parallel processing. This model holds promise for educational tools and lightweight secure communication platforms.

VII. Conclusion

The project successfully combines the both Affine Cipher and RSA algorithm to create a more secure message encryption system.By layering the two methods,it should overcomes the individual weakness and enhances the overall security.The usage of python makes the system efficient and easy to implement far away.And the key validation through the modular arithematic and prime checks and ensures reliability.Overall this approach gives us a simple yet powerful solution for secure communication.

References

1) A New Approach of Cryptography for Data Encryption and Decryption, 2022.
2) Chaotic Encoder-Decoder on FPGA for Crypto System, 2022.
3) Secure Data Communication and Cryptography Based on DNA-Based Message Encoding, 2021.
4) Designing of AES Algorithm Using Verilog, 2020.