Evaluating Facebook's Encryption Mechanisms: Methodologies, Efficiency, and Improvement Strategies

Dr.Mukhtiar Bano

Dept.of Software Engineering

Mukhtiar.bano@fjwu.edu.pk

Laiba Sohail,Neha Amjad,Tanzeela Asghar

Abstract: In the digital age, the security and privacy of user data have become paramount, especially for social media platforms like Facebook that handle vast amounts of personal information. This paper presents an in-depth analysis of the encryption algorithms employed by Facebook to safeguard user data, emphasizing the significance of robust encryption in maintaining data confidentiality and integrity. The study delves into the methodologies of prominent encryption algorithms such as Advanced Encryption Standard (AES), Rivest-Shamir-Adleman (RSA), and Diffie-Hellman key exchange, providing a detailed examination of their operational mechanisms and integration within Facebook's infrastructure. Performance metrics, including speed, scalability, and security efficacy, are scrutinized to assess each algorithm's effectiveness in real-world applications. Furthermore, the paper identifies potential vulnerabilities and drawbacks inherent in these algorithms, such as key management challenges, susceptibility to side-channel attacks, and implementation flaws. To address these issues, the study offers targeted recommendations and innovative strategies for enhancing encryption practices. These suggestions aim to bolster Facebook's data protection capabilities, ensuring stronger defense mechanisms against emerging cyber threats. This comprehensive evaluation not only underscores the critical role of encryption in protecting user data but also contributes to the ongoing discourse on advancing encryption technologies in the ever-evolving landscape of cybersecurity.

1. Introduction

1.1 Background

The proliferation of digital communication and social networking has revolutionized the way people interact and share information. As one of the largest social media platforms, Facebook handles an immense volume of personal data, making the security and privacy of this information a critical concern. The increasing prevalence of cyber threats, data breaches, and unauthorized access incidents underscores the need for robust encryption mechanisms to protect user data. Encryption, the process of converting information into a coded format to prevent unauthorized access, plays a vital role in ensuring the confidentiality and integrity of user communications and data storage on social media platforms.

1.2 Importance of Encryption in Social Media

In the context of social media, encryption is paramount for several reasons. It not only protects sensitive user information from being intercepted by malicious actors but also ensures that user communications remain private and secure. This is particularly important as social media platforms are often targeted by cybercriminals due to the vast amounts of valuable data they contain. Effective encryption helps build trust among users, assuring them that their personal information is secure and their privacy is respected.

1.3 Scope of the Paper

The scope of this paper is to provide a comprehensive analysis of the encryption algorithms used by Facebook to secure user data. By focusing on widely used algorithms such as Advanced Encryption

Standard (AES), Rivest-Shamir-Adleman (RSA), and Diffie-Hellman key exchange, this paper aims to evaluate their implementation within Facebook's infrastructure, assess their performance, identify potential drawbacks, and propose recommendations for improvement. This detailed examination will offer insights into the strengths and weaknesses of these encryption methods and suggest ways to enhance their effectiveness in safeguarding user data.

2. Overview of Facebook's Encryption Algorithms

Encryption algorithms form the backbone of data security for platforms like Facebook, ensuring that sensitive information is protected from unauthorized access and cyber threats. Facebook employs several advanced encryption techniques to maintain the confidentiality and integrity of user data. This section provides an overview of the key encryption algorithms used by Facebook: Advanced Encryption Standard (AES), Rivest-Shamir-Adleman (RSA), and Diffie-Hellman Key Exchange. Each of these algorithms has unique characteristics and serves specific purposes in the realm of data security.

2.1. REVIEW OF RELATED RESEARCH ISSUES

In this section, we present several related research issues, including the practical obstacles of protecting social data privacy, how encryption techniques are used in data protection, and the specific algorithms utilized in Facebook's encryption mechanisms.

A. Social Data Privacy

Numerous studies have highlighted the challenges of maintaining user privacy on social media platforms. Vijay Bhuse's work [1] discusses the significance of end-to-end encryption in social media to safeguard user data from unauthorized access and breaches. Despite the implementation of encryption, user privacy can still be compromised through various means, such as data theft and unauthorized access by attackers. Chen-Da Liu and Simone Santini [5] explore an encryption protocol designed to be resistant to correlation attacks, further emphasizing the need for robust encryption methods to protect user privacy from sophisticated attacks.

In addition to external threats, internal threats also pose significant risks to user privacy. As highlighted by Cho Fai Bartholomew Cheung [2], enhancing user privacy through browser plugins demonstrates the ongoing efforts to protect users from data misuse by the platforms themselves. This is crucial, given the historical precedents of data misuse scandals involving major social media companies.

B. Encryption Techniques for Data Protection

Encryption techniques are fundamental in protecting data on social media platforms. Vandana Guleria and Deep Chandra Mishra [3] introduce a multi-layer RGB image encryption algorithm based on Diffie-Hellman cryptography, which showcases the potential of combining traditional encryption methods with additional cryptographic transformations to enhance security. This approach aligns with the need for more robust encryption techniques capable of securing multimedia content on social media.

Jason Hiney and colleagues [4] illustrate the use of Facebook for image steganography, where hidden messages are embedded within images, showcasing an alternative method of securing communication.

This technique highlights the diverse approaches available for data protection beyond traditional encryption methods.

C. Enhancements and Hybrid Approaches

Recent research has also focused on enhancing existing encryption algorithms and exploring hybrid approaches to improve data security. Omar Salah et al. [8] discuss a hybrid algorithm combining RSA and Diffie-Hellman to enhance data security during network transmission. This hybrid approach aims to leverage the strengths of both asymmetric and symmetric encryption methods, providing a more secure solution for data protection.

M Tharunraj and colleagues [10] describe a private messaging service utilizing AES encryption combined with toxicity detection. This innovative approach not only secures the messages but also ensures the content is appropriate, highlighting the potential of combining encryption with content analysis for comprehensive data protection.

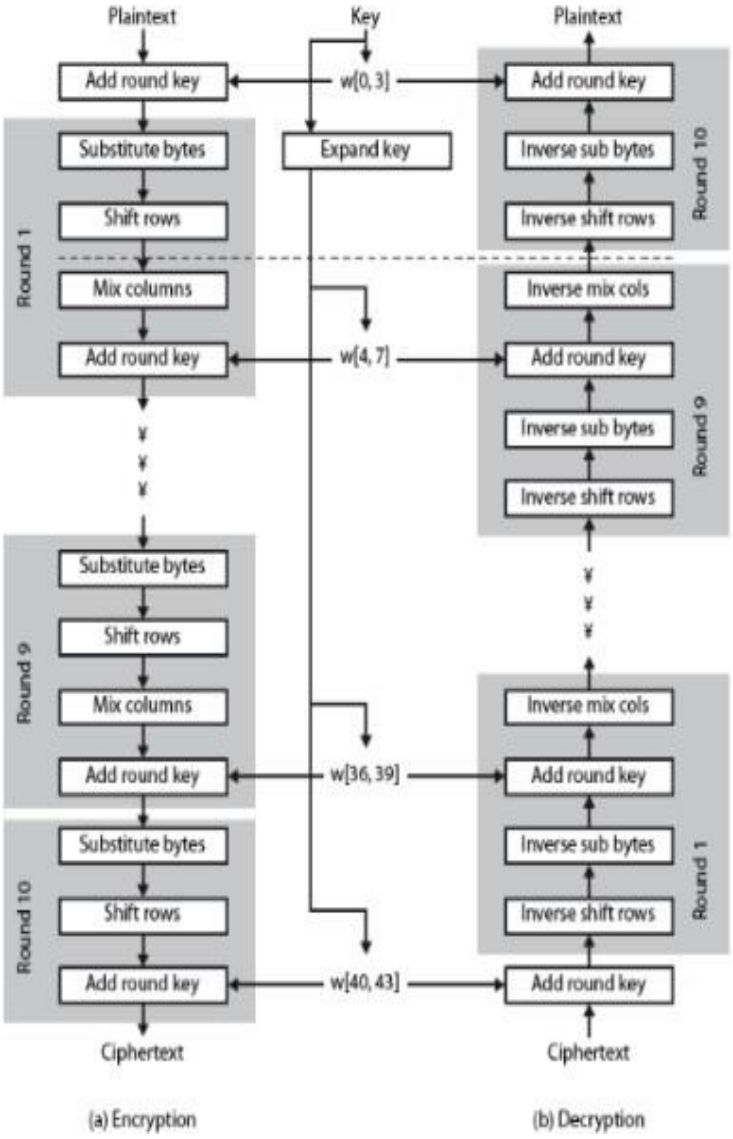
3. Detailed Analysis of Algorithms

3.1 Advanced Encryption Standard (AES)

The Advanced Encryption Standard (AES) is a symmetric encryption algorithm, meaning the same key is used for both encryption and decryption of data. It is widely recognized for its efficiency and security, and is the standard encryption algorithm adopted by the U.S. government.

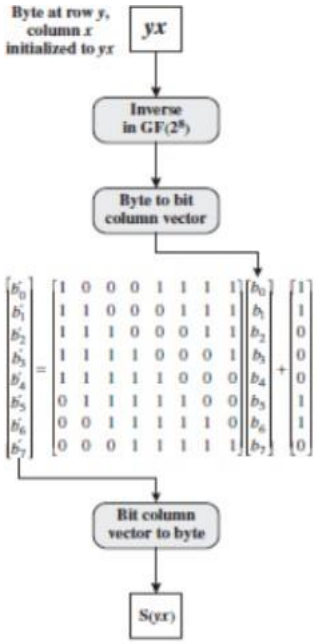
3.1.1 Method and Working

The Advanced Encryption Standard (AES) is a block cipher adopted by the U.S. National Institute of Standards and Technology (NIST) in 2001. It is used worldwide for secure data encryption.

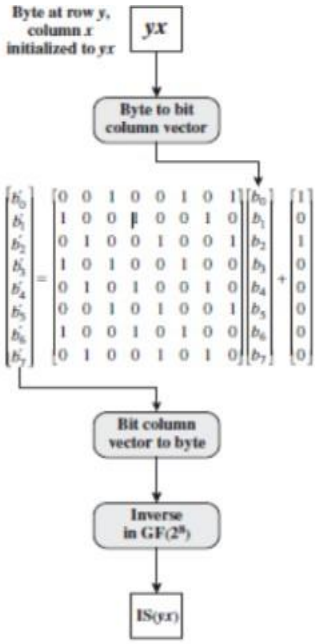


Block Size and Key Sizes: AES operates on fixed block sizes of 128 bits. It supports three different key sizes: 128 bits, 192 bits, and 256 bits.
Rounds: The number of rounds in AES depends on the key size:
AES-128 (3.4×10^{38}): 10 rounds
AES-192 (6.2×10^{57}): 12 rounds
AES-256(1.1×10^{77}):14 rounds

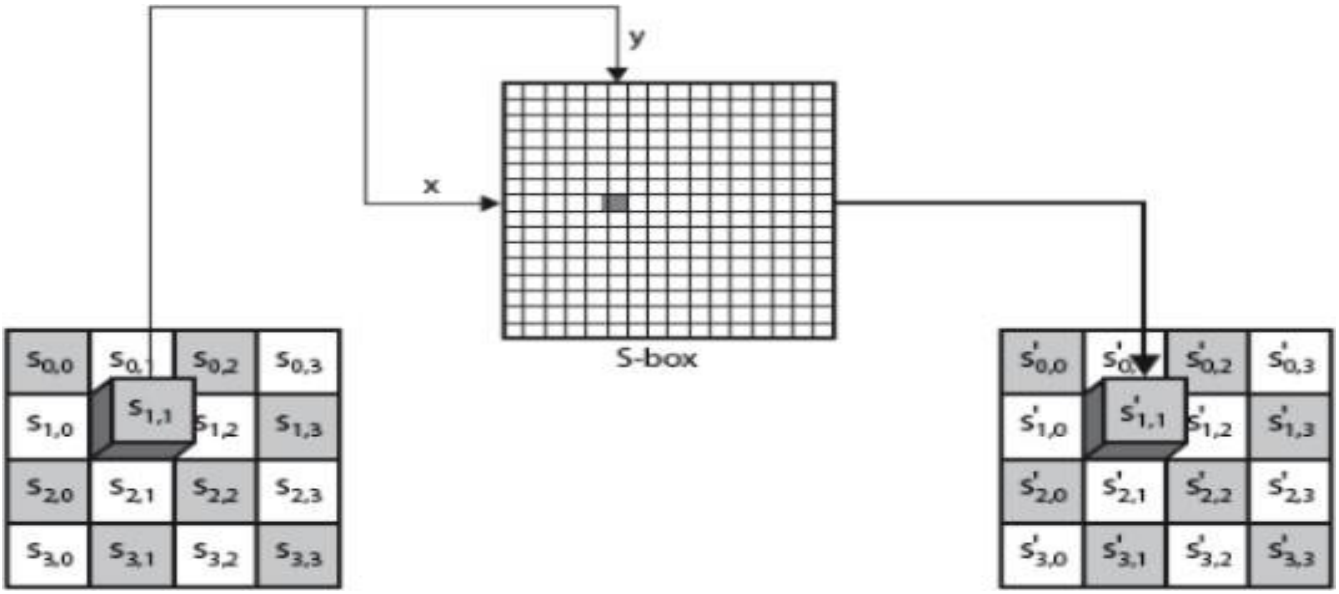
Each round consists of four main transformations (except the final round, which exclude the MixColumns step):
SubBytes: This is a non-linear substitution step where each byte in the 4x4 state matrix is replaced with another byte using a substitution table (S-box). The S-box is designed to provide non-linearity and resistance against linear and differential cryptanalysis.
Mathematically: S[ai,j]=S[ai,j]S[a_{i,j}] = S[a_{i,j}]S[ai,j]=S[ai,j], where SSS is the S-box and ai,ja_{i,j}ai,j is the byte in the state matrix.



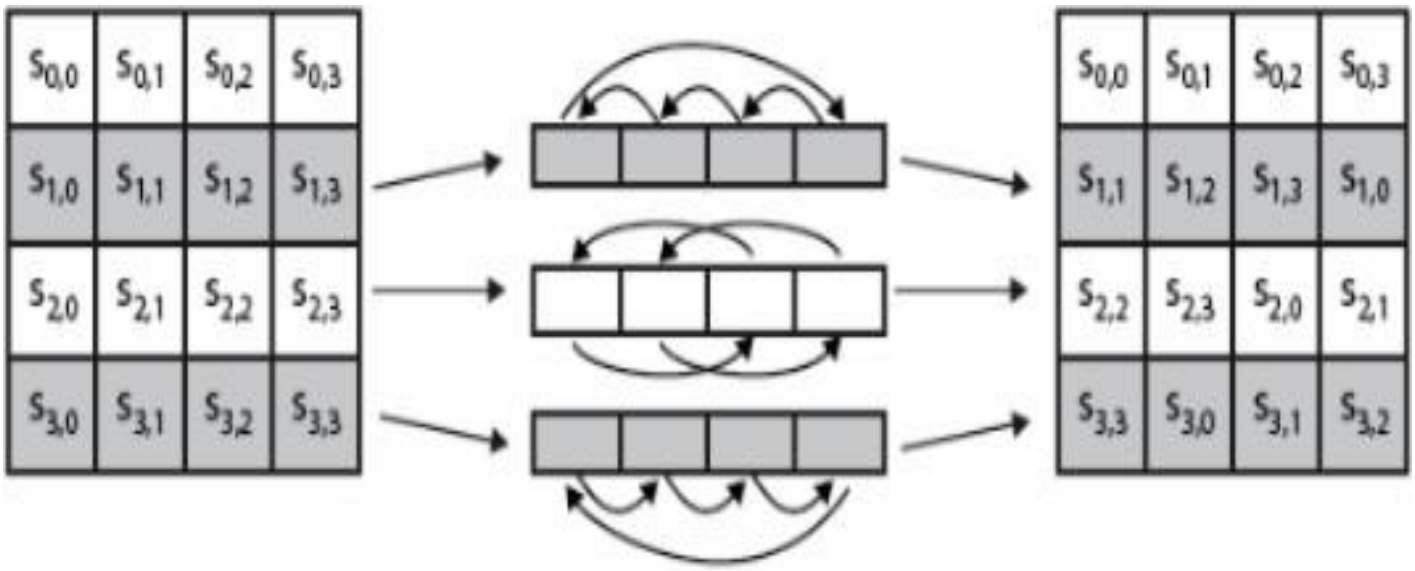
(a) Calculation of byte at row y, column x of S-box



(a) Calculation of byte at row y, column x of IS-box



1. **ShiftRows:** This is a transposition step where the bytes in each row of the state matrix are shifted cyclically to the left by a certain number of positions.
    - First row: no shift.
    - Second row: 1-byte shift.
    - Third row: 2-byte shift.
    - Fourth row: 3-byte shift.

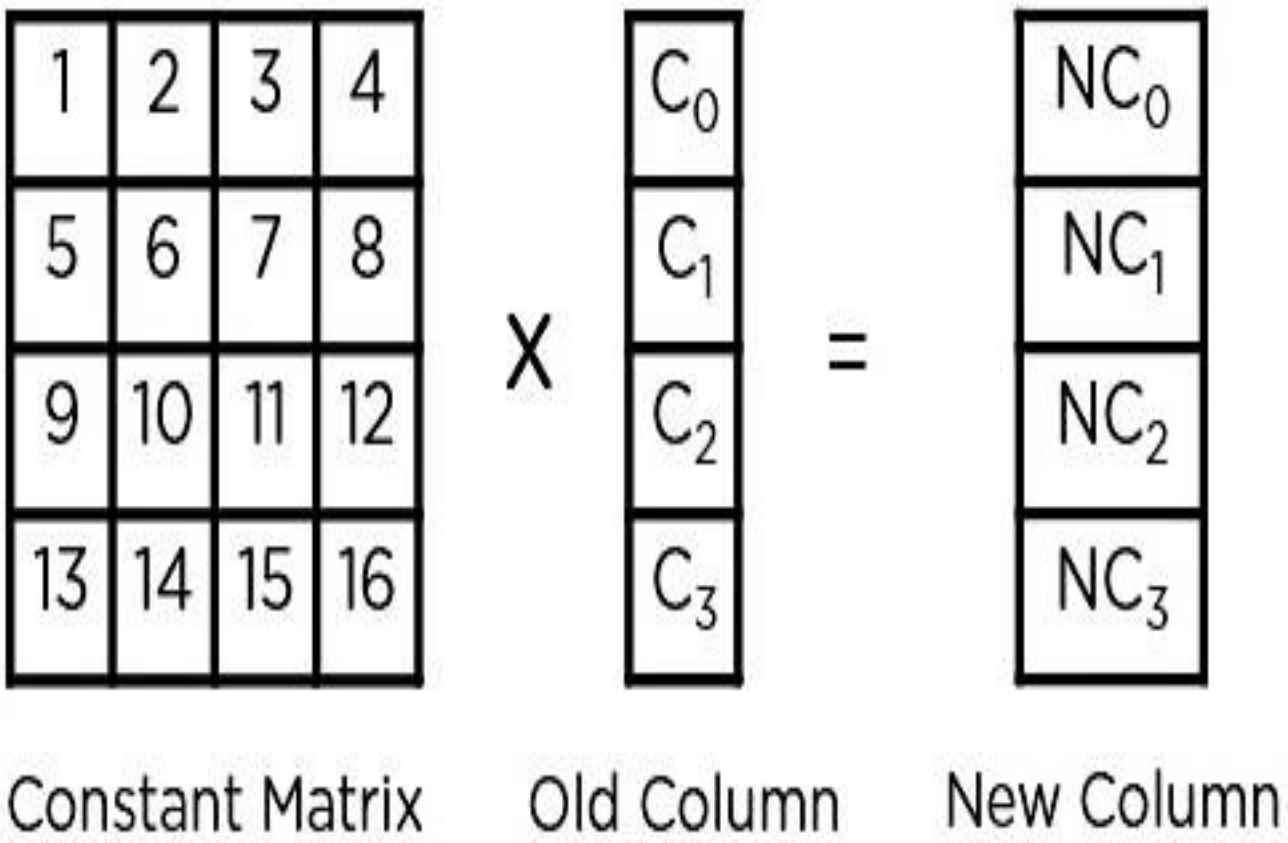


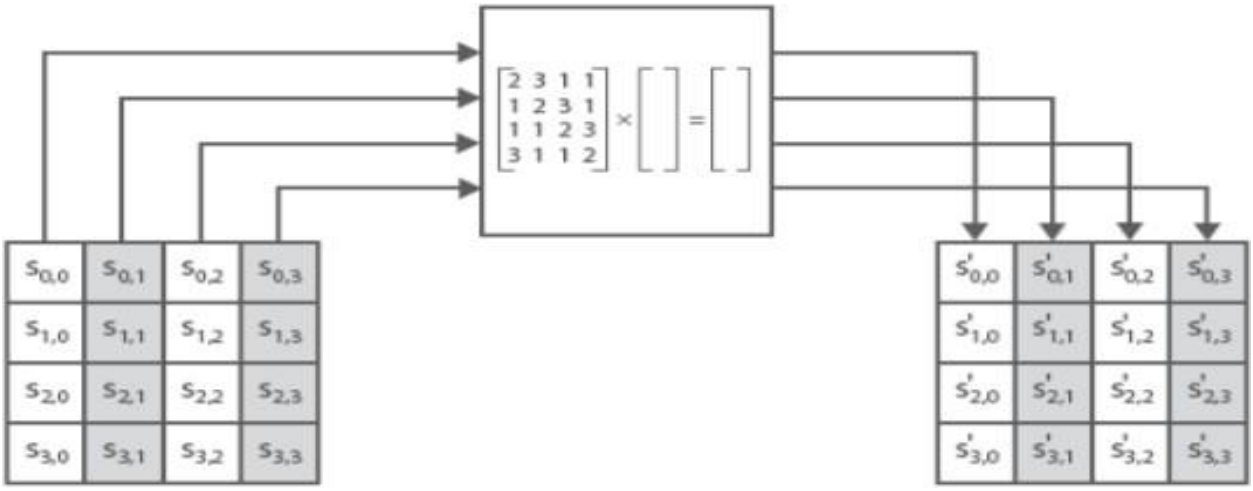
87	F2	4D	97
EC	6E	4C	90
4A	C3	46	E7
8C	D8	95	A6

→

87	F2	4D	97
6E	4C	90	EC
46	E7	4A	C3
A6	8C	D8	95

2. **MixColumns:** This transformation mixes the bytes within each column of the state matrix. Each column is treated as a four-term polynomial and is multiplied by a fixed polynomial c(x)=03x3+01x2+01x+02c(x) = 03x^3 + 01x^2 + 01x + 02c(x)=03x3+01x2+01x+02 modulo x4+1x^4 + 1x4+1.
    - Mathematically: ai,j′=c(x)·ai,ja'_{i,j} = c(x) \cdot a_{i,j}ai,j′=c(x)·ai,j, where ai,j′a'_{i,j}ai,j′ is the new value of the byte after the MixColumns transformation.





3. **AddRoundKey:** In this step, the state matrix is XORed with a round key derived from the main key using the key schedule. The round key for each round is derived from the original key using a key expansion algorithm.

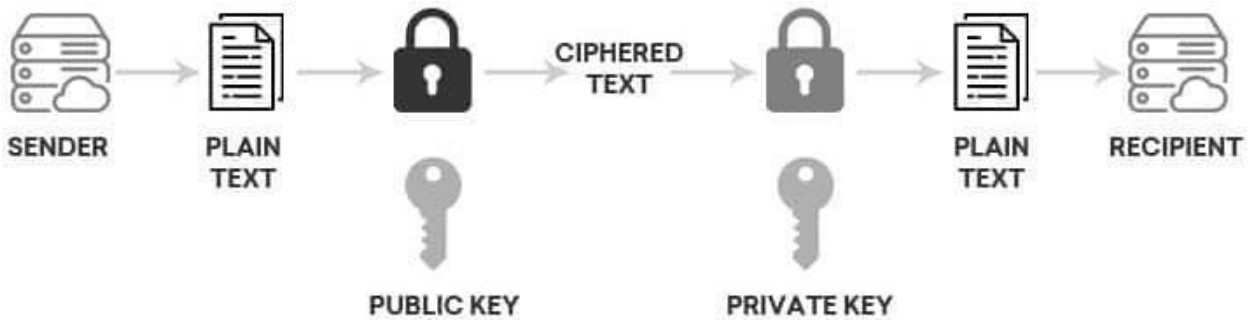
Mathematically: ai,j=ai,j⊕ki,ja_{i,j} = a_{i,j} \oplus k_{i,j}ai,j=ai,j⊕ki,j, where ki,jk_{i,j}ki,j is the corresponding byte of the round key.

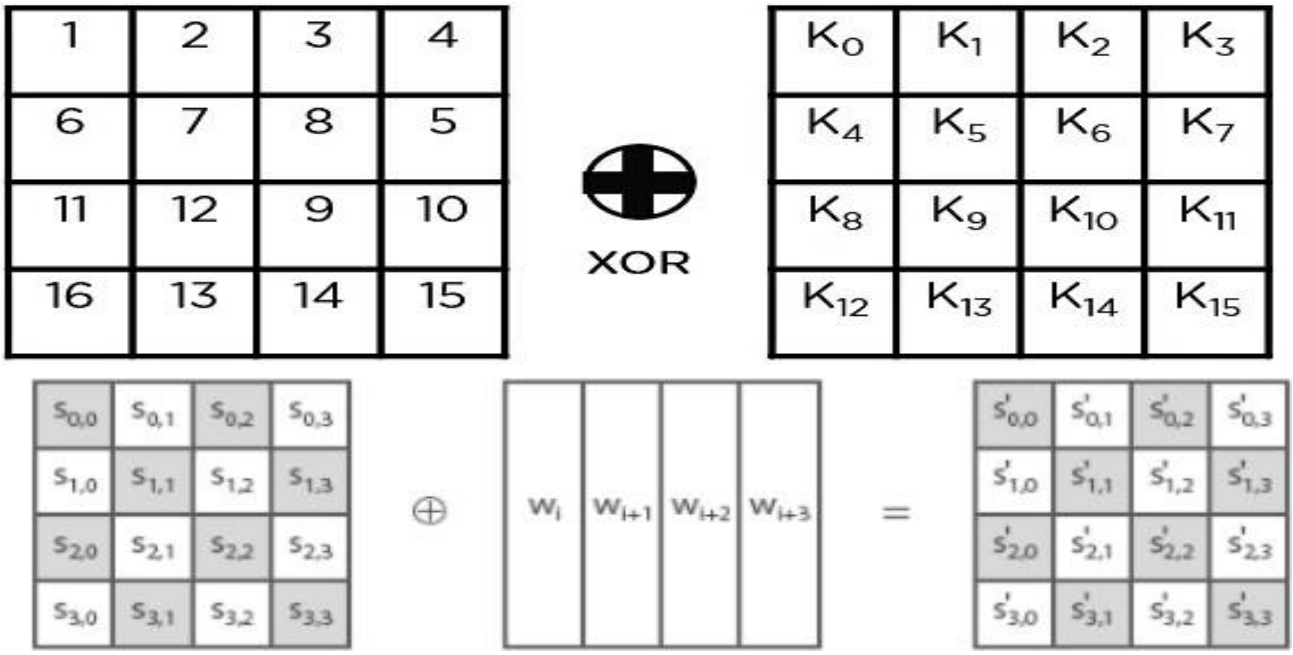
The process begins with an initial AddRoundKey step before the first round and ends with a final AddRoundKey step after the last round.

3.1.2 Performance Analysis

AES is highly efficient and performs well across various platforms, including both hardware and software. Its symmetric nature allows for rapid encryption and decryption processes.

- **Speed:** AES is known for its fast encryption and decryption speeds. The algorithm can be efficiently implemented on both general-purpose CPUs and dedicated hardware accelerators.
- **Throughput:** In hardware, AES can achieve high throughput, making it suitable for applications requiring fast data processing, such as VPNs, secure communication protocols, and disk encryption.
- **Resource Usage:** AES has a relatively low memory footprint and can be implemented in environments with limited computational resources, such as embedded systems and IoT devices.





3.1.3 Drawbacks

- **Key Management:** The security of AES relies heavily on the secure management of encryption keys. If keys are compromised, the encrypted data can be decrypted by unauthorized parties.
- **Side-Channel Attacks:** AES implementations can be vulnerable to side-channel attacks, where attackers exploit information leakage from the physical implementation, such as timing information, power consumption, or electromagnetic emissions.
- **Implementation Flaws:** Weak or incorrect implementations of AES can introduce vulnerabilities. For instance, improper handling of padding schemes or key management protocols can lead to security breaches.

3.1.4 Suggestions for Improvement

- **Advanced Key Management Solutions:** Implementing robust key management frameworks, such as Hardware Security Modules (HSMs) and key vaults, can enhance the security of AES key management.
- **Countermeasures for Side-Channel Attacks:** Employing constant-time algorithms, masking techniques, and other side-channel attack countermeasures can mitigate the risks associated with physical information leakage.
- **Regular Security Audits:** Conducting regular security audits, code reviews, and penetration
- testing can help identify and rectify implementation flaws, ensuring that the AES implementation remains secure.

3.2 Rivest-Shamir-Adleman (RSA)

Rivest-Shamir-Adleman (RSA) is an asymmetric encryption algorithm used for secure data transmission. Unlike symmetric algorithms, RSA uses a pair of keys – a public key for encryption and a private key for decryption.

3.2.1 Method and Working

RSA is an asymmetric encryption algorithm widely used for secure data transmission. It is based on the mathematical properties of large prime numbers and the difficulty of factoring their product.

- **Key Generation:**
  1. **Select Primes:** Choose two distinct large prime numbers ppp and qqq.
  2. **Compute Modulus:** Calculate n=pqn = pqn=pq. The modulus nnn is used in both the public and private keys.
  3. **Compute Totient:** Calculate the totient function ϕ(n)=(p−1)(q−1)\phi(n) = (p-1)(q-1)ϕ(n)=(p−1)(q−1).
  4. **Choose Public Exponent:** Select a public exponent eee such that 1<e<ϕ(n)1 < e < \phi(n)1<e<ϕ(n) and gcd(e,ϕ(n))=1\gcd(e, \phi(n)) = 1gcd(e,ϕ(n))=1.
  5. **Compute Private Exponent:** Compute the private exponent ddd as the modular multiplicative inverse of emod ϕ(n)e \mod \phi(n)emodϕ(n), i.e., ed≡1mod ϕ(n)ed \equiv 1 \mod \phi(n)ed≡1modϕ(n).
  6. **Public Key:** The public key is the pair (e,n)(e, n)(e,n).
  7. **Private Key:** The private key is the pair (d,n)(d, n)(d,n).

Select two prime no's. Suppose **P = 53 and Q = 59.**

Now First part of the Public key : n = P*Q = 3127.

We also need a small exponent say **e :**

But e Must be

An integer.

Not be a factor of Φ(n).

1 < e < Φ(n) [Φ(n) is discussed below],

Let us now consider it to be equal to 3.

Our Public Key is made of n and e

We need to calculate Φ(n) :

Such that **Φ(n) = (P-1)(Q-1)**

so, Φ(n) = 3016

Now calculate Private Key, **d :**

d = (k*Φ(n) + 1) / e for some integer k

For k = 2, value of d is 2011.

- **Encryption:** Convert the plaintext message MMM to an integer mmm such that 0<m<n0 < m < n0<m<n. Compute the ciphertext ccc as c≡memod nc \equiv m^e \mod nc≡memodn.

Convert letters to numbers : H = 8 and I = 9

Thus **Encrypted Data c = $(89^e) \mod n$**

Thus our Encrypted Data comes out to be 1394

Decrypted Data = $(c^d) \mod n$

Thus our Encrypted Data comes out to be 89

8 = H and I = 9 i.e. "HI".

- **Decryption:** Recover the plaintext message mmm from the ciphertext ccc using the private key ddd: m≡cdmod nm \equiv c^d \mod nm≡cdmodn.

3.2.2 Performance Analysis

RSA's performance varies based on the size of the keys used. Larger keys provide greater security but require more computational power.

- **Encryption Speed:** RSA encryption is generally faster than decryption, especially when using a small public exponent eee, such as 65537, which is commonly used.
- **Decryption Speed:** RSA decryption is slower and more computationally intensive due to the large private exponent ddd and the necessity of performing modular exponentiation with large numbers.
- **Key Generation:** The key generation process is also computationally intensive, as it involves selecting large prime numbers and calculating their product.

3.2.3 Drawbacks

- **Performance:** RSA is slower compared to symmetric algorithms like AES, particularly for decryption and key generation.
- **Key Length:** The security of RSA relies on large key sizes (2048 bits or more) to remain secure against modern computational capabilities. This increases computational requirements and affects performance.

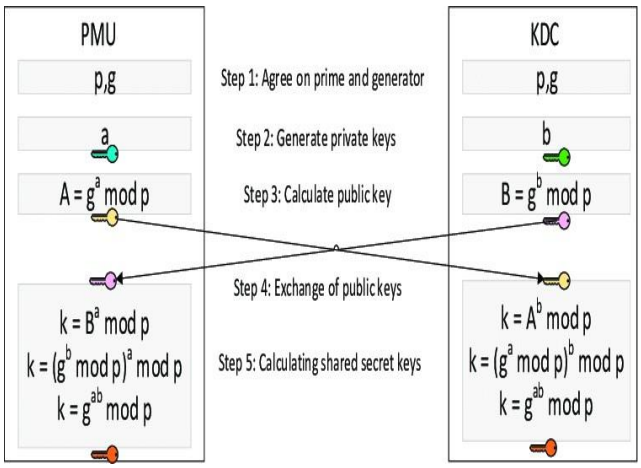
- **Quantum Vulnerability:** RSA is potentially vulnerable to quantum computing attacks, which could efficiently factor large numbers using Shor's algorithm.

3.2.4 Changes in Algorithms.

- **Optimized Implementations:** Using optimized libraries and algorithms, such as the Chinese Remainder Theorem (CRT) for decryption, can significantly improve RSA's performance.
- **Hybrid Encryption:** Combining RSA with symmetric algorithms (e.g., using RSA to securely exchange AES keys) can leverage the strengths of both encryption types, providing fast encryption with robust security.
- **Quantum-Resistant Algorithms:** Researching and transitioning to post-quantum cryptographic algorithms, such as lattice-based cryptography, can address potential future vulnerabilities posed by quantum computers.

3.3 Diffie-Hellman Key Exchange

The Diffie-Hellman Key Exchange is a method used to securely exchange cryptographic keys over a public channel. It enables two parties to establish a shared secret key, which can then be used for encrypted communication.



3.3.1 Method and Working

1. **Compute Shared Secret:** Each party computes the shared secret key using their private key and the other party's public value: s=Bamod ps = B^a \mod ps=Bamodp for Alice and s=Abmod ps = A^b \mod ps=Abmodp for Bob. Both computations result in the same shared secret sss due to the properties of modular arithmetic.

   The Diffie-Hellman Key Exchange (DH) is a cryptographic protocol that allows two parties to securely exchange cryptographic keys over a public channel. It is based on the mathematical problem of computing discrete logarithms in a finite field.

- **Public Parameters:** Two large prime numbers, ggg (a base) and ppp (a prime modulus), are agreed upon and shared publicly.

- **Key Exchange:**
2. **Private Keys:** Each party selects a private key (aaa for Alice and bbb for Bob) which are random integers kept secret.
3. **Public Values:** Each party computes their respective public values: A=gamod pA = g^a \mod pA=gamodp and B=gbmod pB = g^b \mod pB=gbmodp.

Alice	Bob
Public Keys available = P, G	Public Keys available = P, G
Private Key Selected = a	Private Key Selected = b
Key generated = $x = G^a mod P$	Key generated = $y = G^b mod P$

4. **Exchange Public Values:** The public values AAA and BBB are exchanged between the parties.

Algebraically, it can be shown that

$$k_a = k_b$$

3.3.2 Performance Analysis

Diffie-Hellman is efficient and suitable for real-time applications where secure key exchange is necessary.

- **Speed:** The key exchange process is relatively fast, involving only a few modular exponentiations.
- **Resource Usage:** DH does not require significant computational resources, making it suitable for environments with limited processing power.
- **Scalability:** The algorithm scales well with the size of the parameters, providing flexibility in balancing performance and security.

3.3.3 Drawbacks

Aspect	Advanced Encryption Standard (AES)	Rivest-Shamir-Adleman (RSA)	Diffie-Hellman Key Exchange (DH)
Security	High security when key management is proper.	High security with large key sizes (2048 bits or more).	Provides secure key exchange over an insecure channel. Security depends on the size of the prime modulus.
Speed	Very fast encryption and decryption.	Slower compared to AES, especially in decryption. Key generation and encryption/decryption are computationally intensive.	Fast key exchange process. Involves fewer computations compared to RSA.
Scalability	Scales well with larger data sets.	Does not scale well with large data due to slow encryption/decryption. Large key sizes required for security increase computational burden.	Scales well with larger key sizes for security. Performance is efficient even with large parameters.
Practical Implementation in Facebook	Used for encrypting data at rest and in transit. Ideal for securing large volumes of data quickly. Utilized in TLS/SSL for secure communication.	Used for securing key exchange and digital signatures. Ensures the secure transmission of symmetric keys. Often used in conjunction with AES for a hybrid approach.	Used for secure key exchange during initial connection setup. Helps establish a shared secret key for symmetric encryption. Often used in combination with AES and RSA.

- **Post-Quantum Vulnerability:** Like RSA, DH is vulnerable to quantum computing attacks that can solve the discrete logarithm problem efficiently.

3.3.4 Suggestions for Improvement

- **Authenticated Key Exchange:** Combining DH with authentication methods, such as digital signatures or certificates, can mitigate the risk of man-in-the-middle attacks.
- **Elliptic Curve Diffie-Hellman (ECDH):** Using elliptic curve cryptography can provide stronger security with smaller key sizes and improved performance. ECDH offers the same security level with significantly smaller keys compared to traditional DH.
- **Post-Quantum Cryptography:** Exploring and adopting post-quantum key exchange algorithms, such as lattice-based key exchange, can enhance future-proofing against quantum threats.

4. Comparative Analysis of Algorithms.

AES (Advanced Encryption Standard): Symmetric encryption algorithm known for its speed and robust security in encrypting large volumes of data.

RSA (Rivest-Shamir-Adleman): Asymmetric encryption algorithm used for secure key exchange and digital signatures, relying on the mathematical difficulty of factoring large prime numbers.

Diffie-Hellman (DH): Key exchange protocol enabling two parties to establish a shared secret securely over an insecure channel, essential for initializing secure communications without pre-shared keys.

5. Recommendations and Future Directions

It encompasses strategic proposals and forward-thinking initiatives aimed at advancing current encryption algorithms, integrating emerging technologies, and establishing effective policies and governance frameworks. This section typically includes suggestions to enhance the performance, security, and scalability of established encryption methods such as AES, RSA, and Diffie-Hellman. It also explores the adoption of innovative encryption technologies like homomorphic encryption and post-quantum cryptography to mitigate evolving threats. Moreover, it emphasizes the importance of robust policy formulation and compliance measures to ensure secure data management and regulatory adherence in an increasingly digital and interconnected environment.

5.1 Enhancements in Current Algorithms

To enhance current encryption algorithms like AES, RSA, and Diffie-Hellman, several improvements can be considered:

- **AES**: Implementing advanced modes of operation like Galois/Counter Mode (GCM) can provide authenticated encryption with associated data (AEAD), ensuring both confidentiality and integrity

  of data. Additionally, exploring lightweight variants for resource-constrained devices can broaden its applicability in IoT and mobile platforms.
- **RSA**: Researching and implementing optimizations such as the Chinese Remainder Theorem (CRT) for faster decryption and exploring post-quantum cryptography algorithms to mitigate vulnerabilities against quantum computing threats are crucial. Moreover, enhancing key management practices and integrating hardware security modules (HSMs) can strengthen overall security.
- **Diffie-Hellman**: Adopting elliptic curve cryptography (ECC) variants like Elliptic Curve Diffie-Hellman (ECDH) can offer stronger security with smaller key sizes, reducing computational overhead without compromising security. Furthermore, integrating authentication mechanisms during key exchange (e.g., Digital Signatures or Hashed Message Authentication Code, HMAC) can

mitigate risks associated with man-in-the-middle attacks.

5.2 Potential Adoption of Emerging Encryption Technologies

Looking towards emerging encryption technologies can further bolster security:

- **Homomorphic Encryption**: Exploring and integrating homomorphic encryption schemes that enable computation on encrypted data without decryption can revolutionize privacy-preserving data processing, particularly in cloud computing environments.
- **Post-Quantum Cryptography**: Transitioning to and evaluating post-quantum cryptographic algorithms such as lattice-based cryptography, code-based cryptography, or multivariate cryptography can future-proof against the potential advent of quantum computers capable of breaking RSA and DH.
- **Blockchain and Distributed Ledger Technologies (DLT)**: Leveraging cryptographic techniques within blockchain and DLT ecosystems, such as zero-knowledge proofs (ZKPs) and secure multi-party computation (MPC), can enhance data privacy, integrity, and authentication mechanisms.

5.3 Policy and Governance Recommendations

Effective policies and governance frameworks are essential to ensure robust encryption practices and data protection:

- **Data Protection Regulations**: Adhering to and advocating for strong data protection regulations (e.g., GDPR, CCPA) that mandate encryption of sensitive information both at rest and in transit can enhance user privacy and mitigate data breaches.
- **Standardization and Compliance**: Promoting industry-wide adoption of standardized encryption protocols and compliance with international security standards (e.g., NIST, ISO) ensures interoperability, reliability, and trust in encryption solutions.
- **Public Awareness and Education**: Educating stakeholders, including users, developers, and policymakers, about the importance of encryption, its implementation best practices, and potential risks associated with inadequate security measures fosters a culture of cybersecurity awareness and resilience.

1. Conclusion

In this research, a comprehensive analysis of Facebook's encryption strategies centered on AES, RSA, and Diffie-Hellman has been presented. AES, renowned for its efficiency in symmetric encryption, serves as a cornerstone in securing both data at rest and in transit within Facebook's infrastructure. Its rapid processing speeds and robust security mechanisms make it an ideal choice for handling large volumes of user data securely. However, ensuring effective key management practices remains pivotal to mitigating potential vulnerabilities. RSA, employed for asymmetric encryption purposes such as key exchange and digital signatures, provides strong security through complex mathematical operations. Despite its computational intensity, particularly during key generation and decryption processes, RSA plays a critical role in securing sensitive communications on the platform. Diffie-Hellman, a key exchange protocol, facilitates secure initial connections and the establishment of shared secrets over untrusted networks. Its reliance on the discrete logarithm problem ensures secure communication channels, although precautions against potential man-in-the-middle attacks are essential.

Looking ahead, the landscape of encryption and cybersecurity continues to evolve rapidly. Enhancements in AES through advanced modes like Galois/Counter Mode (GCM) can further bolster its capabilities in providing authenticated encryption with associated data (AEAD), ensuring both confidentiality and integrity of transmitted data. Exploring emerging encryption technologies such as homomorphic encryption, which allows computations on encrypted data without decryption, holds promise for enhancing privacy in data processing applications. Additionally, with the advent of quantum computing on the horizon, the adoption of post-quantum cryptography algorithms becomes imperative to maintain robust security standards against future threats. Furthermore, advocating for rigorous policy frameworks and compliance measures will be crucial in aligning encryption practices with

evolving regulatory landscapes, thereby reinforcing user trust and data protection principles. By embracing these advancements and strategic initiatives, Facebook can continue to enhance its encryption strategies, safeguard user information, and uphold its commitment to cybersecurity excellence in a digital age.

2. References.

[1] Vijay Bhuse. Review of end-to-end encryption for social media. In Interna-tional Conference on Cyber Warfare and Security, volume 18, pages 35–37,2023.

[2] Cho Fai Bartholomew Cheung. Improving the privacy of Facebook users through browser plugin. PhD thesis, Dublin, National College of Ireland, 2021.

[3] Vandana Guleria and Deep Chandra Mishra. A new multi-layer rgb im- age encryption algorithm based on diffie-hellman cryptography associated with frdct and arnold transform. Multimedia Tools and Applications, 79(43):33119–33160, 2020.

[4] Jason Hiney, Tejas Dakve, Krzysztof Szczypiorski, and Kris Gaj. Using facebook for image steganography. In 2015 10th international conference on availability, reliability and security, pages 442–447. IEEE, 2015.

[5] Chen-Da Liu and Simone Santini. Hiding from facebook: An encryption protocol resistant to correlation attacks. arXiv preprint arXiv:2404.18817, 2024.

[6] Xiaoqing Liu, Yinyin Peng, Jie Wang, and Zhaoxia Yin. Image en- cryption algorithm based on facebook social network. arXiv preprint t arXiv:1906.03175, 2019.

[7] N Nalini and B Harini. Implementing end to end encryption to communica- tion apps. In 2023 7th International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC), pages 201–209. IEEE, 2023.

[8] Omar Salah, Ahmed El-Sawy, and Mohamed Taha. A hybrid algorithm for enhancement of the data security during network transmission based on rsa and dh. International Journal of Intelligent Engineering & Systems, 16(3), 2023.

[9] Monu Singh and Amit Kumar Singh. A comprehensive survey on encryp- tion techniques for digital images. Multimedia Tools and Applications, 82(8):11155–11187, 2023.

[10] M Tharunraj, Sanjay Kannan, et al. Private messaging service using aes encryption and toxicity detection. In 2022 International Conference on Electronic Systems and Intelligent Computing (ICESIC), pages 173–178. IEEE, 2022