A New Technique for Ciphers for Generating Ciphertext using Reverse Key Diagonal XOR Operation

Dr. Ummadi. Thrirupalu[1]

Mr. N.Anil Kumar Chowdari[2]

Mr. Addala Hemantha Kumar[3]

[1,2,3] Department of Computer Science and Engineering

[1,3] Audisankara College of Engineering & Technology, Gudur, Andhra Pradesh, India.

[2]N.B.K.R Institute of Science and Technology, Vidyanagar, Andhra Pradesh, India.

[1]ummadi70@gmail.com

Abstract – Cryptography is the practice and study of techniques for securing communication and data from adversaries. It involves creating and analyzing protocols that prevent third parties or the public from reading private messages. It is also an art that incorporates various mathematical techniques for generating Ciphertext. In this paper, we introduce a new technique called the Reverse Key Diagonal XOR Operation. Using this concept, we generate a notorious cipher that is more challenging for cryptanalysis.

Keywords – Plaintext, Encryption, Diagonal XOR, Decryption, Ciphertext.

1. INTRODUCTION

Cryptography [1] is a fundamental aspect of information security, encompassing the tools and techniques used to protect information from unauthorized access, alteration, or destruction. It includes methods for secure communication, data integrity, and authentication. In this aspect, various kinds of cryptosystems [2] have come into existence to secure data and information. The most Cryptosystems can be broadly categorized based on their underlying principles and applications. Here are some of the existing cryptosystems:

1. 1. Symmetric Key Cryptosystems [3][4][5]:

- AES (Advanced Encryption Standard) : Widely used for secure data encryption.
- DES (Data Encryption Standard) and 3DES (Triple DES): Older standards still in use in some legacy systems.
- Blowfish and Twofish: Fast and flexible block ciphers used in various applications.

1. 2. Asymmetric Key Cryptosystems [6]:

- RSA (Rivest-Shamir-Adleman): Commonly used for secure data transmission and digital signatures.
- ECC (Elliptic Curve Cryptography): Provides strong security with smaller key sizes, used in mobile devices and SSL/TLS.
- Diffie-Hellman Key Exchange: Allows secure exchange of cryptographic keys over a public channel.

1. 3. Hash Functions [7]:

- SHA (Secure Hash Algorithms): Includes SHA-1, SHA-256, SHA-3, etc., used for data integrity and digital signatures.
- MD5 (Message Digest Algorithm 5): Used for checksums and data integrity (though now considered insecure for cryptographic purposes).

1. 4. Digital Signatures [8]:

- DSA (Digital Signature Algorithm): Used for digital signatures.
- ECDSA (Elliptic Curve Digital Signature Algorithm): Combines ECC with DSA for efficient and secure digital signatures.

1. 5. Post-Quantum Cryptography [9]:

- Lattice-based Cryptography: Potential future standard to withstand quantum attacks.
- Hash-based Cryptography: Uses hash functions to create secure signatures resistant to quantum attacks.
- Code-based Cryptography: Utilizes error-correcting codes for encryption and signatures.

1. 6. Hybrid Cryptosystems [10][11]:

- Combine symmetric and asymmetric cryptography to leverage the strengths of both. For example, SSL/TLS protocols use RSA (asymmetric) for key exchange and AES (symmetric) for data encryption.

These cryptosystems serve various purposes in securing data, ensuring privacy, and maintaining the integrity and authenticity of information across different applications and industries.

2. PROPOSED SYSTEM

In recent years, many innovations have emerged to protect data and information, whether stored on a device or transmitted over the internet. These advancements include:

2.1. Advanced Encryption Techniques:

- AES-256: A more secure version of the Advanced Encryption Standard, widely adopted for encrypting sensitive data.
- Quantum-resistant cryptography: Developing algorithms that can withstand potential quantum computer attacks, such as lattice-based and hash-based cryptography.

2.2. Secure Communication Protocols:

- TLS 1.3 (Transport Layer Security): The latest version of TLS, offering enhanced security and performance for secure web communications.
- HTTPS Everywhere: Increased adoption of HTTPS to ensure encrypted connections between browsers and websites.

2.3. Authentication and Access Control:

- Multi-factor Authentication (MFA): Combines multiple methods of verifying identity, such as passwords, biometrics, and security tokens.
- Zero Trust Security Models: Assumes no implicit trust and requires continuous verification for access to resources, minimizing the risk of breaches.

2.4. Blockchain Technology:

- Decentralized Security: Blockchain provides a secure, transparent, and tamper-proof way to store and verify data, widely used in cryptocurrencies and supply chain management.
- Smart Contracts: Automatically enforce and execute agreements without intermediaries, enhancing security and reducing fraud.

2.5. Data Masking and Tokenization:

- Data Masking: Obscures sensitive information by replacing it with fictitious data, used in development and testing environments.
- Tokenization: Replaces sensitive data with unique identification symbols (tokens) that retain essential information without compromising security.

2.6. Secure Storage Solutions:

- Encrypted File Systems: Automatically encrypt data stored on disks, ensuring protection even if the physical device is compromised.
- Cloud Security Enhancements: Providers implement advanced encryption, secure access controls, and continuous monitoring to protect data in the cloud.

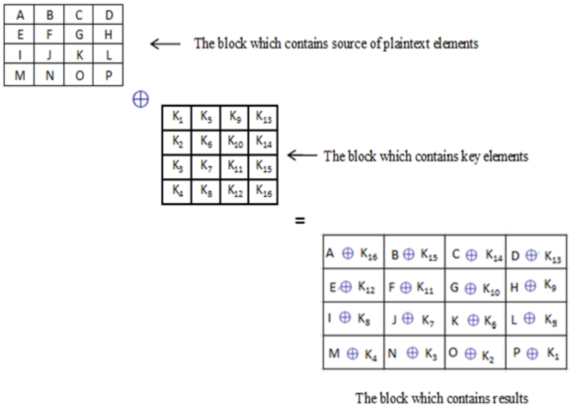
2.7. AI and Machine Learning in Cybersecurity:

- Threat Detection: AI algorithms analyze patterns and behaviors to detect and respond to threats in real-time.
- Anomaly Detection: Machine learning models identify unusual activities that may indicate a security breach.

2.8. Privacy-preserving Technologies:

- Homomorphic Encryption: Allows computation on encrypted data without decrypting it, preserving privacy while enabling data processing.
- Differential Privacy: Ensures individual data privacy when performing data analysis and sharing aggregate information.

Most of the existing techniques mentioned above perform an XOR operation on data, usually row by row or column by column. In this paper, we introduce a new technique called “Reverse Key Diagonal XOR Operation.” In this diagonal XOR operation, the contents of the plaintext diagonal elements are XORed with the reverse diagonal elements of the key. The pictorial representation of the new technique we introduced is depicted as follows.



A	B	C	D
E	F	G	H
I	J	K	L
M	N	O	P

The block which contains source of plaintext elements
⊕

K_1	K_5	K_9	K_{13}
K_2	K_6	K_{10}	K_{14}
K_3	K_7	K_{11}	K_{15}
K_4	K_8	K_{12}	K_{16}

The block which contains key elements
=

$A \oplus K_{16}$	$B \oplus K_{15}$	$C \oplus K_{14}$	$D \oplus K_{13}$
$E \oplus K_{12}$	$F \oplus K_{11}$	$G \oplus K_{10}$	$H \oplus K_9$
$I \oplus K_8$	$J \oplus K_7$	$K \oplus K_6$	$L \oplus K_5$
$M \oplus K_4$	$N \oplus K_3$	$O \oplus K_2$	$P \oplus K_1$

The block which contains results

Figure 1: Overview of Reverse Key Diagonal XOR Operation

In the above pictorial representation, plaintext element ‘A’ is XORed with key element ‘K_{16}’. Next, element ‘F’ is XORed with key element ‘K_{11}’, and so on. In this manner, all elements of the plaintext block are XORed with the corresponding elements of the key block, generating a result as a block of code. This resulting block acts as the ciphertext. The key aspect of this new technique is the handling of key block elements. Although the elements of the key block are shown in sequence, during the actual operation, the elements of the key block are XORed in reverse order with the plaintext block. This reversal is a critical factor in the effectiveness of this new technique.

To decrypt the data for getting the actual plaintext, perform the reverse operation on result block. After performing the decryption operation the on the ciphertext block, the result usually called as plaintext.

3. CONCLUSION:

In this paper, we introduce a new technique called Reverse Key Diagonal XOR operations. For crypto-designers, this feature can be embraced in various existing techniques to strengthen the security of systems.

By using this new technology, we can protect data and information more securely from attackers.

REFERENCE:

1. Tushar et. al. “Cryptographic Algorithm For Enhancing Data Security: A Theoretical Approach”, International Journal of Engineering Research & Technology (IJERT), Vol. 10 Issue 03, March-2021.
2. Mr. Kumar K and Dr. K. Sasikala, “Comparative Study of Cryptographic Algorithms”, International Journal of Engineering Research & Technology (IJERT), Vol. 9 Issue 11, November-2020.
3. Dr.P. Manikandaprabhu, Ms. M. Samreetha, “A Review of Encryption and Decryption of Text Using the AES Algorithm”, International Journal of Scientific Research & Engineering Trends, Volume 10, Issue 2, Mar-Apr-2024, ISSN (Online): 2395-566X
4. Gowtham Tumati et. al. “A New Encryption Algorithm Using Symmetric Key Cryptography”, *International Journal of Engineering & Technology, 7 (2.32) (2018) 436-438.*
5. Mohammed N. Alenezi et. al. “Symmetric Encryption Algorithms: Review and Evaluation study”, International Journal of Communication Networks and Information Security (IJCNIS) Vol. 12, No. 2, August 2020.
6. Mohammed Nazeh Abdul Wahid et. al. "A Comparison of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish for Guessing Attacks Prevention",Journal of Computer Science Applications and Information Technology,Received: June 22, 2018; Accepted: July 12, 2018; Published: August 10, 2018.
7. Suparnesh Bhattacharyya, “Hash Function on Cryptography”, International Journal of Humanities Social Science and Management (IJHSSM) Volume 3, Issue 4, Jul.-Aug., 2023, pp: 385-389.
8. J. Chandrashekhara et. al. “A Comprehensive Study on Digital Signature”, International Journal of Innovative Research in Computer Science & Technology (IJIRCST) ISSN: 2347-5552, Volume-9, Issue-3, May 2021.
9. Dr. N. Suba Rani, Dr. A. Noble Mary Juliet, K. Renuka Devi, "An Image Encryption & Decryption And Comparison With Text - AES Algorithm", INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH VOLUME 8, ISSUE 07, JULY 2019 ISSN 2277-8616.
10. Pooja Patil and Dr. Rajesh Bansode, “Performance Evaluation of Hybrid Cryptography Algorithm for Secure Sharing of Text & Images”, International Research Journal of Engineering and Technology (IRJET), Volume: 07 Issue: 09 | Sep 2020.

11. Saja Mohammed Suhael et. al. “Proposed Hybrid Cryptosystems Based on Modifications of Playfair Cipher and RSA Cryptosystem”Baghdad Science Journal Open Access, P-ISSN: 2078-8665, Published OnlineFirst: May, 2023.