IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

# A SIMPLEST AND STRONGEST CRYPTOSYSTEM FOR CIPHERS USING BITS CIRCLE SWAPPING TECHNIQUES

[1]Dr. Ummadi. Thirupalu, [2]Dr. S. V. Padmavathi Devi,
[3]Mavalluru. Swathi, [4]Kondisetty Kavitha

[1]Asssociate Professor, [2]Professor, [3, 4] Assistant Professor
[1,2,3,4] Department of Computer Science and Engineering
[1,2,3,4] Audisankara College of Engineering & Technology, Gudur, Andhra Pradesh, India.

***Abstract*:** Cryptography is the practice and study of techniques for securing communication and data in the presence of adversaries. It involves creating written or generated codes that allow information to be kept secret. Cryptography transforms readable data (plaintext) into an unreadable format (ciphertext) through encryption, and converts it back into readable format through decryption. In this paper, we swap internal bits of both the plaintext and the key using different techniques usually a bit circle swapping, and then perform an XOR operation on both to generate the Ciphertext.

***Index Terms* – Cryptography, Plaintext, Circle Swap, XOR, Key Generation, Cipher text**.

## I. INTRODUCTION

Cryptography has a rich history that dates back to ancient civilizations. The earliest forms of cryptography were used by the Egyptians, Greeks, and Romans. For example, the Caesar cipher, used by Julius Caesar, is a well-known ancient encryption technique.

Modern cryptography[1] is far more complex and is essential for securing digital communications and transactions. It encompasses various methods and algorithms, including:

1. Symmetric Key Cryptography [2][3]: Both the sender and receiver share the same key for encryption and decryption. Examples include the Advanced Encryption Standard (AES) and Data Encryption Standard (DES).

2. Asymmetric Key Cryptography: Uses a pair of keys—a public key and a private key. The public key encrypts the data, while the private key decrypts it. This method is widely used in secure communications, such as in the SSL/TLS protocols for internet security. Examples include RSA and ECC (Elliptic Curve Cryptography).

3. Hash Functions: These produce a fixed-size string of characters (a hash) from input data of any size. Hashes are typically used for ensuring data integrity. Examples include SHA-256 and MD5.

4. Digital Signatures: These are used to verify the authenticity and integrity of a message, software, or digital document. They are created using a private key and verified with a corresponding public key.

## II. PROPOSED WORK

In this proposed work, we introduced a simplest and strongest cryptosystem for ciphers using bits circle swapping technique.

### 2.1. BIT SWAPPING

Bit swapping is a technique [4] in digital computing and data processing where individual bits within a binary number are exchanged or swapped. This operation is often used in various algorithms and applications, such as data encryption[5][6], error detection and correction, and optimization routines.

Bit swapping refers to the process of exchanging specific bits within a binary number. The operation can be performed on individual bits or groups of bits, and it usually involves the following steps:

1. Identify the Positions: Determine the positions of the bits to be swapped.

2. Extract the Bits: Retrieve the values of the bits at the specified positions.

3. Swap the Values: Exchange the values of the identified bits.

4. Update the Binary Number: Place the swapped bits back into their new positions within the binary number.

**Example of Bit Swapping**

Consider a simple example where we swap the first and last bits of an 8-bit binary number:

Original binary number: `10101001`

1. Identify the positions: Bit positions 0 and 7 (indexing starts from 0).

2. Extract the bits: Bit at position 0 is `1`, bit at position 7 is `1`.

3. Swap the values: Since both bits are `1`, the values remain the same.

4. Update the binary number: The binary number remains `10101001`.

For a more noticeable change, consider swapping the second and second-last bits of the same binary number:

Original binary number: `10101001`

1. Identify the positions: Bit positions 1 and 6.

2. Extract the bits: Bit at position 1 is `0`, bit at position 6 is `0`.

3. Swap the values: Since both bits are `0`, the values remain the same.

4. Update the binary number: The binary number remains `10101001`.

If we choose positions where bits differ:

Original binary number: `10101001`

1. Identify the positions: Bit positions 0 and 3.

2. Extract the bits: Bit at position 0 is `1`, bit at position 3 is `0`.

3. Swap the values: Bit at position 0 becomes `0`, and bit at position 3 becomes `1`.

4. Update the binary number: The new binary number is `00111001`.

In our paper, for the first byte of data bits of the plaintext is swapped every two bit positions. For example $7^{th}$ bit position with $6^{th}$ bit position, $5^{th}$ bit potion with $4^{th}$ bit position and so on. Whereas in key bytes $7^{th}$ bit position is swapped with $0^{th}$ bit position, $6^{th}$ bit position with $1^{st}$ bit position and so on. Then finally perform XOR operation on two bytes (both key and plaintext bytes) to generate cipher text. The following figure shown the process of circle swapping on key bits.

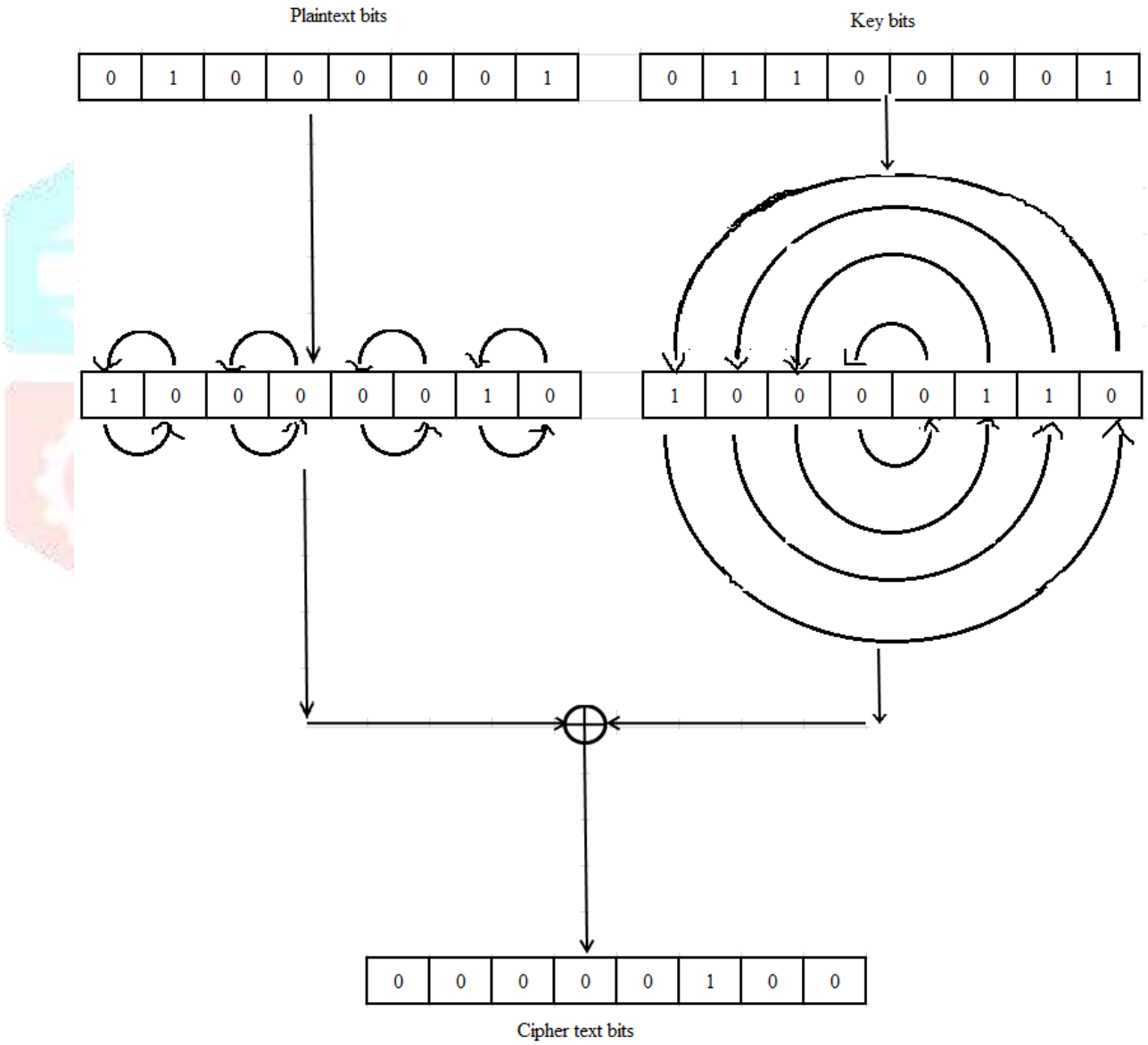


Fig. 1: Key side circle swapping

For next byte of data bits of the plaintext swapping technique is as the same above but the key swapping text is implements to plaintext and the plaintext techniques are implements to the key. It means for plaintext bytes $7^{th}$ bit position is swapped with $0^{th}$ bit position, $6^{th}$ bit position with $1^{st}$ bit position and so on. For the key bytes $7^{th}$

bit position with 6th bit position, 5th bit potion with 4th bit position and so on. The following figure shown the process of circle swapping on plaintext bits.

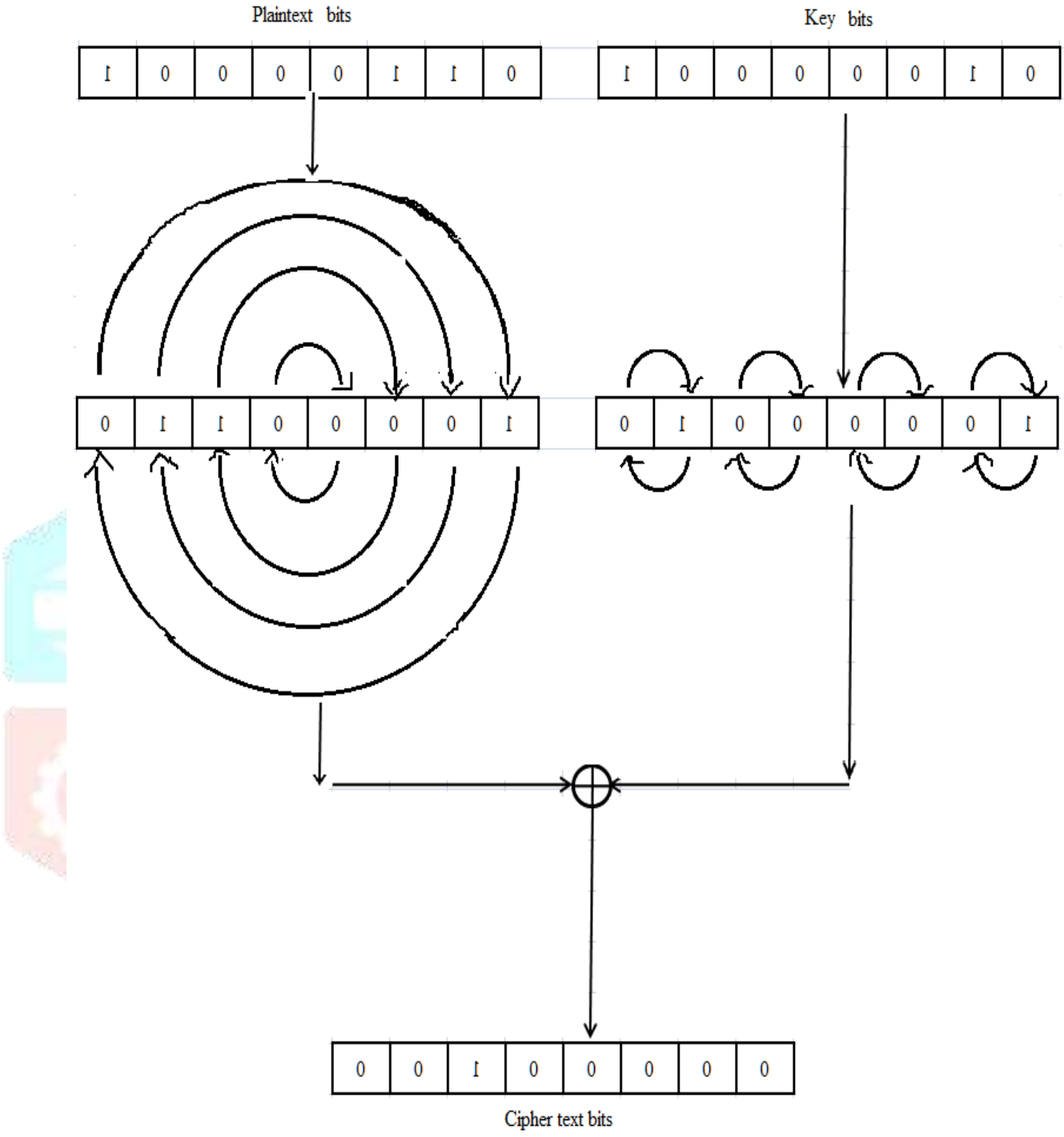


Fig. 2: Text side circle swapping

Like the above, a set of cipher text is generated for a set of plaintext with the set of key elements. This technique may be implemented for a block of text or a stream of text. If we apply this technique to a block, we divide the stream of plaintext into convenient blocks as desired. Alternatively, you may directly implement this technique on a stream of bytes to generate a stream of ciphertext.

For generating a stream of ciphertext, we have developed and introduced the bit circle swapping technique in the following way.

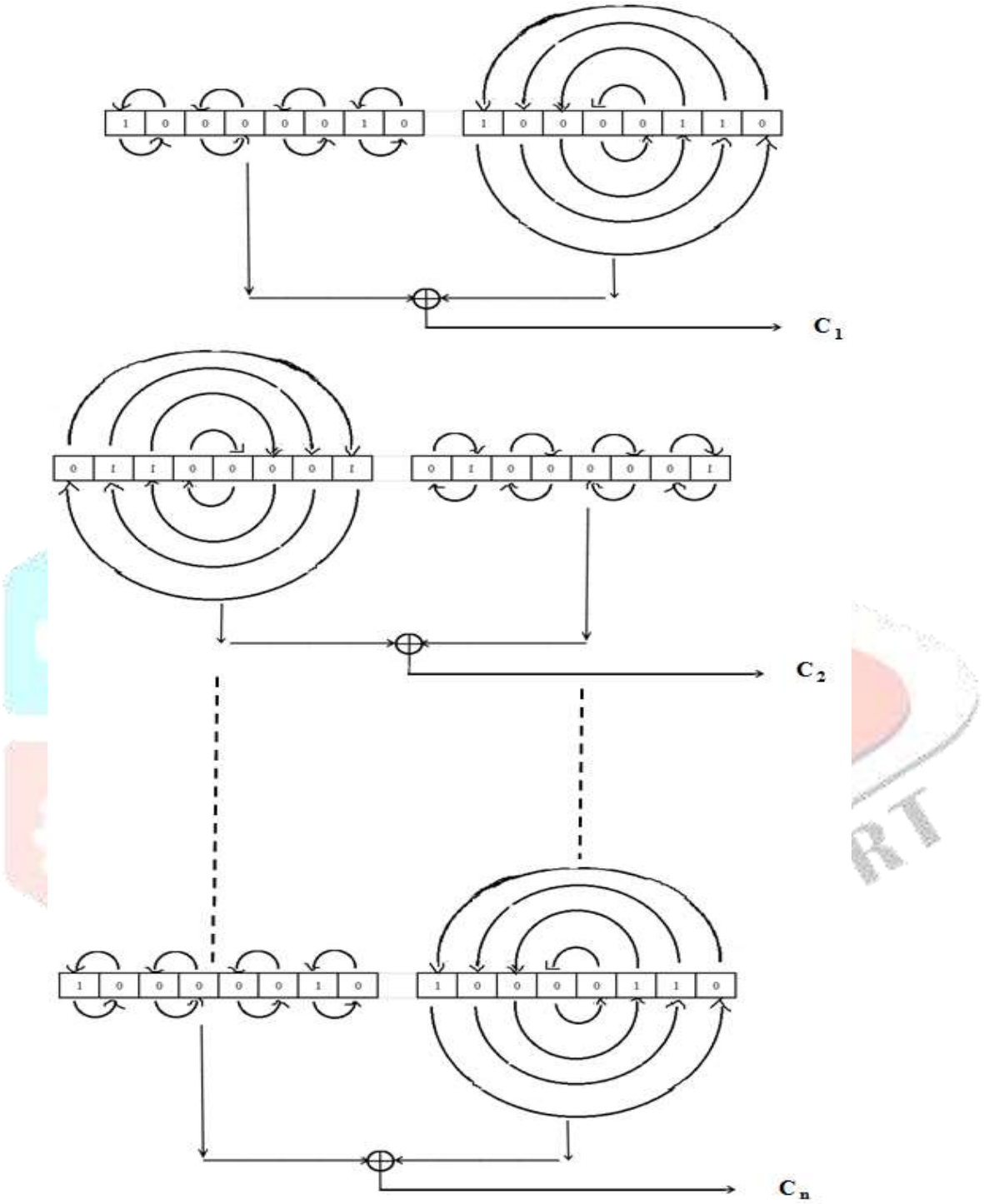


Fig. 3: A block or stream of cipher text generation

This kind of complex process is more challenging for cryptanalysts to break. Therefore, we have introduced one of the strongest and most advanced cryptosystems for the intended users or protocols.

**III. CONCLUSION**:

Cryptography is fundamental to cybersecurity, enabling secure online banking, confidential communications, secure data storage, and more. Its applications are vast, ranging from securing personal information to protecting

national security. As technology evolves, cryptography continues to advance, addressing new security challenges in an increasingly digital world.

Bit swapping is a fundamental operation in many algorithms and is especially prevalent in low-level programming and digital circuit design. It is often used to improve performance, enhance security, or optimize certain computational tasks.

**REFERENCES**:

[1] Rebeiro, Chester, Debdeep Mukhopadhyay, and Sarani Bhattacharya. "Modern cryptography." Timing Channels in Cryptography. Springer International Publishing, 2015. 13-35.

[2] Qahtan M. Shallal and Mohammad Ubaidullah Bokhari, "A Review on Symmetric Key Encryption Techniques in Cryptography", International Journal of Computer Applications (0975 – 8887) Volume 147 – No.10, August 2016.

[3] Raychev, Nikolay. "Classical cryptography in quantum context."Proceedings of the IEEE 10 (2012): 2015.

[4] Krasimir Yordzhev, "The Bitwise Operations in Relation to the Concept of Set", *Asian Journal of Research in Computer Science, 1(4): 1-8, 2018; Article no.AJRCOS.44314.*

[5] Kahate, Atul. Cryptography and network security. Tata McGraw-Hill Education, 2013.

[6] Stallings, William. Network security essentials: applications and standards. Pearson Education India, 2007.

[7] Schneier, Bruce. Applied cryptography: protocols, algorithms, and source code in C. john wiley & sons, 2007.