IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

6th National Conference on Science, Technology and Communication Skills – NCSTCS 2K23

Narula Institute of Technology, Agarpara, Kolkata, India

Vol. 10, Special Issue 3, September 2023

Unlocking the Secrets: The Crucial Role of Encoding and Decoding in Cryptography

Payel Mondal[1], Debopriya Dey[2], Shounak Sinha[3] and Krittika Chakraborty[4]

Faculty, Department of Basic Science and Humanities, Narula Institute of Technology, Kolkata, India[1,2]

Student, Department of Computer Science and Engineering, Narula Institute of Technology, Kolkata, India[3,4]

Abstract: We live in an information and knowledge economy; learning is not the things you are "done" only in your youth; it must become the digital lifestyle and develop it as a healthy daily habit. When we access bank account online or perform any financial transaction, we need to secure the communication between our computer and the bank's servers. This ensures that our personal and financial information remains confidential and protected from unauthorized access. Moreover, when we send an email, cryptography is used to encrypt the contents of our message so that it can only be read by the intended recipient. This protects the message from being intercepted and read by unauthorized parties. Here cryptology comes into the role to protect sensitive communications and share information privately. This is mainly, the objective of Cryptography, the study of techniques to keep communications private by means of data encryption and its subsequent decryption. Encryption is used to transform an original information (plain form) into some incomprehensible form (coded form).

One commonly used encoding technique is the Advanced Encryption Standard (AES). AES is a symmetric encryption algorithm that uses a single key to both encrypt and decrypt messages. AES is widely used in a variety of applications, including secure file transfers, secure email, and virtual private networks (VPNs). In this paper we are offering an algorithm on encryption and decryption to convert a plain text into a ciphertext and conversely. We used a non-singular matrix as one process of generation of a key to encrypt a message. In this process, the recipient can decode (decrypt) the message by using the inverse of the matrix to get back the original message. But this process is not so effective. For resolving the drawback of this process, we introduced encryption techniques of circular bit rotation algorithm using generating key of random integers of the size number less than 512 bits i.e. at least 154 digits or 77 pairs of unsigned integers. So, the proposed algorithm in this paper encrypts plain text into cipher text that is unrecognizable and which makes the cipher text unidentifiable when compared to plain text.

Keywords: Cryptography, Encryption, Decryption, Plain Text, Cipher Text, ASCII Code, Bit Rotation

I. INTRODUCTION

Encoding and decoding is a crucial part of cryptography. Encoding is the process to transform plain text like letter, words, numbers in a specialized format (ciphertext) using some techniques for effective and safe transformation of data. Decoding is the method of turning back that specialized format again into normal text to receive using some techniques. In this workwe will discuss about two kinds of techniques to encode and decode normal message using linear algebra (matrix) and binary operations. We will create "secret" using these techniques and again "unlock that secret".

II. ENCODING AND DECODING TECHNIQUES

Encoding: Plain text has ASCII codes. Arrange all ASCII codes in a form of (2×2) matrix B. Multiply with a generating Matrix or encoding matrix (key) A Plain text again (encoded text).
Decoding: Make the inverse Matrix of encoding matrix Multiply the matrix A^{-1} and C. Get the decoded matrix B. B is the actual matrix. Transform those ASCII codes into plain text again.
Illustration:
PLAIN TEXT: **Unlock Secrets**
ASCII CODES OF EACH CHARACTER: 85 110 108 111 99 107 32 83 101 99 114 101 99 116 115 46 [ASCII of space=32 and full stop=46]
ENCODING/GENERATING MATRIX(KEY): Let $A = [1\ 1\ 0\ 1\ ]$, and matrix $B =$
[85 108 99 32 101 114 99 115 110 111 107 83 99 101 116 46]
Then $C = A * B$

$$C = [1\ 1\ 0\ 1\ ] * [85\ 108\ 99\ 32\ 101\ 114\ 99\ 115\ 110\ 111\ 107\ 83\ 99\ 101\ 116\ 46\ ]$$
$$= [195\ 119\ 206\ 115\ 200\ 215\ 215\ 161\ 110\ 111\ 107\ 83\ 99\ 101\ 116\ 46\ ]$$

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

6th National Conference on Science, Technology and Communication Skills – NCSTCS 2K23

Narula Institute of Technology, Agarpara, Kolkata, India

Vol. 10, Special Issue 3, September 2023

Encoded message = 195 110 119 111 206 107 115 83 200 99 215 101 215 116 161 46
ENCODED PLAIN TEXT [CIPHER TEXT]= ĂnwoîksSËc × e × tí
DECODING*: Take* $B = A^{-1} * C$

$$A^{-1} = [1 \ -1 \ 0 \ 1]$$

$$B = [1 \ -1 \ 0 \ 1] * [195\ 119\ 206\ 115\ 200\ 215\ 215\ 161\ 110\ 111\ 107\ 83\ 99\ 101\ 116\ 46]$$
$$= [85\ 108\ 99\ 32\ 101\ 114\ 99\ 115\ 110\ 111\ 107\ 83\ 99\ 101\ 116\ 46]$$

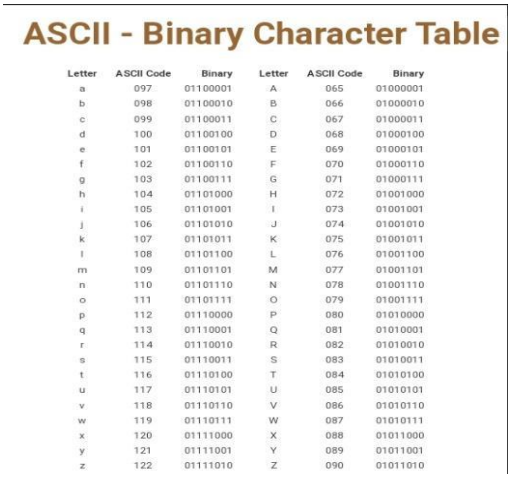
Decoded message*:* = 85 110 108 111 99 107 32 83 101 99 114 101 99 116 115 46
ENCODED PLAIN TEXT = Unlock Secrets

III. ENCRYPTION AND DECRYPTION TECHNIQUE USING CIRCULAR BIT SHIFT IN BINARY FIELD

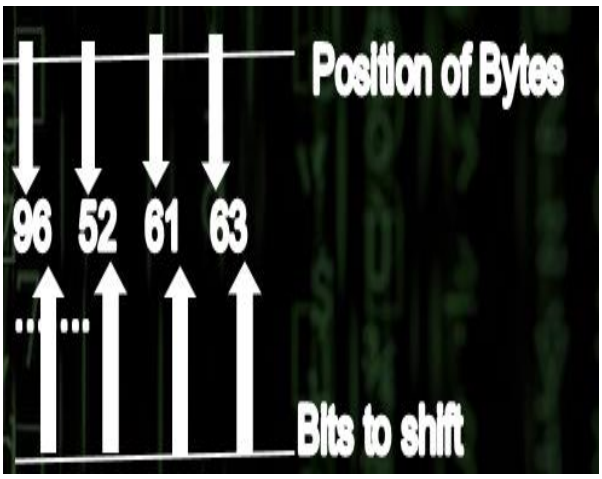
Encryption*:* Divide plain text into blocks with 10 characters but if there's character number less than 10 in a block use paddling instead [1-5].

Generating *key*:

- ❑ Random number generators of size no less than 512 bits i.e. at least 154 digits or 77 pairs of unsigned integers
- ❑ Separated into array of pairs and each pair is generated separately
- ❑ First digit of each pair is the location of the character and second digit is number of bits to shift as shown in figure



Letter	ASCII Code	Binary	Letter	ASCII Code	Binary
a	097	01100001	A	065	01000001
b	098	01100010	B	066	01000010
c	099	01100011	C	067	01000011
d	100	01100100	D	068	01000100
e	101	01100101	E	069	01000101
f	102	01100110	F	070	01000110
g	103	01100111	G	071	01000111
h	104	01101000	H	072	01001000
i	105	01101001	I	073	01001001
j	106	01101010	J	074	01001010
k	107	01101011	K	075	01001011
l	108	01101100	L	076	01001100
m	109	01101101	M	077	01001101
n	110	01101110	N	078	01001110
o	111	01101111	O	079	01001111
p	112	01110000	P	080	01010000
q	113	01110001	Q	081	01010001
r	114	01110010	R	082	01010010
s	115	01110011	S	083	01010011
t	116	01110100	T	084	01010100
u	117	01110101	U	085	01010101
v	118	01110110	V	086	01010110
w	119	01110111	W	087	01010111
x	120	01111000	X	088	01011000
y	121	01111001	Y	089	01011001
z	122	01111010	Z	090	01011010



Decryption:

Encoded message in binary ⇒ circular bit shift operation using the same key but in reverse ⇒ decoded message ⇒ decoded plain TEXT BY CONCATENATING

Circular bit shift:

- ❖ Circular right shift rotation:

In the encryption technique the bits are shifted towards the right and from the end the bits are shifted to the byte from where the bits were shifted.

- ❖ Circular left shift rotation:

In the decryption technique the bits are shifted towards the left and from the beginning the extra bits are shifted to the byte at the end [6-8]. The position of bytes ranges from 0 to 9 and bits are shifted range from 1 to 8 only,0 and 9 will invert the bits instead of shifting [9-10].

IARJSET

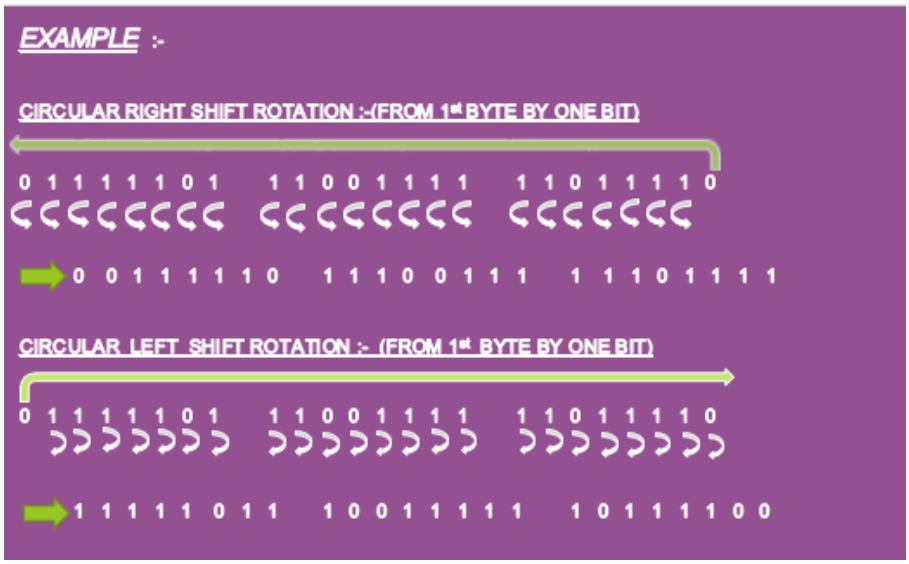
ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

6th National Conference on Science, Technology and Communication Skills – NCSTCS 2K23

Narula Institute of Technology, Agarpara, Kolkata, India

Vol. 10, Special Issue 3, September 2023



IV. EXAMPLE

PLAIN TEXT :- Go and Grow
BLOCK 1: - Go_and_Gro
BLOCK 2:- w_ _ _ _ _ _ _ _ _
For demonstration only 4 pairs of keys are used
KEY :- [24,19,01,00]

i. ENCRYPTION :-

BLOCK 1 :- 01000111 01101111 01011111 01100001 01101110 01100100 01011111 01000111
01110010 01101111
BLOCK 2:- 01110111 01011111 01011111 01011111 01011111 01011111 01011111 01011111
01011111 01011111

ROTATION 1: -
Performing a right shift circular rotation on 3rd byte by 4 bits and KEY=24
BLOCK 1:- 01000111 01101111 11110101 11110110 00010110 11100110 01000101
11110100 01110111 00100110
BLOCK 2:-_0110111 01011111 11110101 11110101 11110101 11110101 11110101
11110101 11110101 11110101

ROTATION 2:-
Here the number of bits to shift is 9, so instead of shifting bits will be inverted instead of shifting from 2nd byte.
KEY = 19
BLOCK 1 :-01000111 10010000 00001010 00001001 11101001 00011001 10111010
00001011 10001000 11011001
BLOCK 2 :-0110111 10100000 00001010 00001010 00001010 00001010 00001010
00001010 00001010 00001010

ROTATION 3 :- Performing a right circular shift rotation on 1st byte by 1 bit

KEY = 01
BLOCK 1: – 10100011 11001000 00000101 00000100 11110100 10001100 11011101
00000101 11000100 01101100
BLOCK 2 :- 00111011 11010000 00000101 00000101 00000101 00000101 00000101
00000101 00000101 00000101

ROTATION 4 :-
Here the number of bits to shift is 0 ,so bits will be inverted from 1st to end byte
KEY = 00
BLOCK 1 :- 01011100 00110111 11111010 11111011 00001011 01110011 00100010
11111010 00111011 10010011

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

6th National Conference on Science, Technology and Communication Skills – NCSTCS 2K23

Narula Institute of Technology, Agarpara, Kolkata, India

Vol. 10, Special Issue 3, September 2023

BLOCK 2 :- 11000100 00101111 11111010 11111010 11111010 11111010 11111010
11111010 11111010 11111010

BLOCK 1:- \7úûvTsú";"

BLOCK 2 :- Ä/úúúúúúúú

BY CONCATENATING

CIPHER TEXT: -\7úû vTsú";"Ä/úúúúúúúú

ii. DECRYPTION: -

For this purpose, only 4 pairs of keys are used.

KEY: -[24,19,01,00]

BLOCK 1 :-01011100 00110111 11111010 11111011 00001011 01110011
00100010 11111010 00111011 10010011

BLOCK 2 :-11000100 00101111 11111010 11111010 11111010 11111010 11111010
11111010 11111010 11111010

ROTATION 1 :-

Here the number of bits to shift are 0 ,so bits will be inverted from 1st byte to end end byte

KEY :- 00

BLOCK 1:- 10100011 11001000 00000101 00000100 11110100 10001100 11011101
00000101 11000100 01101100

BLOCK 2:- 00111011 11010000 00000101 00000101 00000101 00000101
00000101 00000101 00000101 00000101

ROTATION 2 :-

Performing a left circular shift rotation on 1st byte by 1 bit

KEY:- 01

BLOCK 1 ;- 01000111 10010000 00001010 00001001 11101001 00011001 10111010
00001011 10001000 11011001

BLOCK 2:- 01110111 10100000 00001010 00001010 00001010 00001010 00001010
00001010 00001010 00001010

ROTATION 3 :-

Here the number of bits to shift is 9, so, instead of shifting bits will be inverted instead of shifting from 2nd byte.

KEY = 19

BLOCK 1 :- 01000111 01101111 11110101 11110110 00010110 11100110 01000101
11110100 01110111 00100110

BLOCK 2 :- 01110111 01011111 11110101 11110101 11110101 11110101 11110101
11110101 11110101 11110101

ROTATION 4 :-

Performing a right shift circular rotation on 3rd byte by 4 bits

KEY: 24

BLOCK 1:- 01000111 01101111 01011111 01100001 01101110 01100100 01011111
01000111 01110010 01101111

BLOCK 2:- 01110111 01011111 01011111 01011111 01011111 01011111 01011111
01011111 01011111 01011111

DECODED MESSAGE:-

BLOCK 1 :- GoandGro

BLOCK 2 :-w_ _ _ _ _ _ _ _

BY CONCATENATING: -*Go and Grow*

V. CONCLUSION

Cryptography helps us to secure our data privacy and it's not unknown how data is important in our daily life and for organizations. These two techniques are many of those to ensure data security and mathematics is playing a huge role in it. But these algorithms have drawbacks also. So, there are further scopes to enhance the algorithms by increasing efficiency and reducing time complexity. Again, there can be error during message transmission for a lot of reason. We have to enhance our algorithm always to detect and correct errors more easily and efficiently.

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

6th National Conference on Science, Technology and Communication Skills – NCSTCS 2K23

Narula Institute of Technology, Agarpara, Kolkata, India

Vol. 10, Special Issue 3, September 2023

REFERENCES

[1]. Bhardwaj A. and Som S. (2016). Study of different cryptographic technique and challenges in future. 2016 International Conference on Innovation and Challenges in Cyber Security (ICICCS-INBUSH), Noida, 208-212.
[2]. Kunwar V., Agarwal N., Rana A. and Pandey J. P. (2018). Load balancing in cloud—a systematic review. Advances in Intelligent Systems and Computing, 654, 583-593.
[3]. Chauhan B. D., Rana A. and Sharma N. (2017). Testing sufficiency test (TST) - Evolving a new model for estimating software test cases. International Journal of Applied Engineering Research, 12-21.
[4]. Dubey G., Rana A. and Ranjan J. (2017). Fine-grained opinion mining of product review using sentiment and semantic orientation. International Journal of Business Information Systems, 25 (1), 1-17.
[5]. Ghosh S., Rana A. and Kansal V. (2017). Predicting defect of software system. Advances in Intelligent Systems and Computing, 516, 55- 67.
[6]. Nath S. and Som S. (2017, January). Security and Privacy Challenges: Internet of Things. Indian Journal of Science and Technology, 10(3), DOI: 10.17485/ijst/2017/v10i3/110642.
[7]. Goldwasser S. and Micali S. (1984, April). Probabilistic encryption. J. Comput. Syst. Sci. 28(2), 270-299.
[8]. Rivest R. L., Shamir A. and Adleman L. M. (1983): A method for obtaining digital signatures and public-key cryptosystems (reprint). Commun. ACM 26(1).
[9]. El Gamal T. (1985). A public key cryptosystem and a signature scheme based on discrete logarithms. In: Blakely, G.R., Chaum, D. (eds.) CRYPTO 1984. LNCS, 196, 10-18.
[10]. Uludag U., Pankanti S., Prabhakar S. and Jain A. K. (2004, June). Biometric cryptosystems: Issues and challenges. Proc. IEEE (Special Issue Multimedia Security for Digital Rights Management), 92 (6), 948 -960.