International Journal of Information Technology and Knowledge Management
January-June 2011, Volume 4, No. 1, pp. 77-80

NORMALIZER BASED ENCRYPTION TECHNIQUE [NBET] USING THE PROPOSED CONCEPT OF RUBICRYPTION

Rajdeep Chowdhury[1] & Saikat Ghosh[2]

Until recent advent, Cryptography exclusively referred to encryption, which is coined as the process of converting ordinary information (Plain Text) into unintelligible gibberish (Cipher Text). Decryption has been coined as the reverse process of moving from the unintelligible Cipher Text back to the original Plain Text. But, with modernization and globalization of notions, the podium has posed for alternative coinage. In colloquial use, the term Code is often used to mean any method of encryption or concealment of meaning. However, in Cryptography, Code has a more specific meaning, with a significant role too. Code means the replacement of Plain Text with a Code word. Increased literacy and adequate exposure was required by actual Cryptography. The classical cipher types can be significantly classified into transposition cipher and substitution cipher. Simple versions of either offered little confidentiality from enterprising opponents, and still continues to do so. The modern study of symmetric-key ciphers relates mainly to the study of block ciphers and stream ciphers and their allied applications in various genres at each and every stage of Cryptanalysis. One or more Cryptographic primitives are often used to develop a more complex algorithm, called a Cryptosystem. Cryptosystems use the properties of the underlying Cryptographic primitives to support the system's security properties. In many cases, the Cryptosystem's structure involves back and forth communication among two or more parties in space or across time. Cryptosystems of this type are sometimes referred as Cryptographic Protocols.

Keeping all these nuances and facets under consideration, the data encryption technique using the proposed concept of Rubix Cryptography ensures a whole new dimension to Cryptology with optimum security solutions, privacy maintenance and proper decryption mechanism using generated Normalizer.

The paper establishes via implementation the study of data encryption as well as data decryption, based on the proposed innovative concept of Rubicryption using the freshly devised algorithm coined Normalizer Based Encryption Technique [NBET].

Keywords: Rubicryption, Plain Text, Cipher Text, Normalizer, Rubix, Default Rubix, Normalized Rubix, X-Normal Form, Y-Normal Form

1. Introduction

Data encryption techniques that have been used over the years and are still being used are fragmented below, namely: Symmetric Key Cryptography, Public Key Cryptography, Cramer-Shoup Cryptography, Hybrid Cryptosystems, etc.

But, owing to their individual limitations, the proposed concept of Rubicryption by the authors turn out to be a new methodology of data encryption / decryption and promises on the onset to serve in a much better way, as and when required in various genres that require data encryption and decryption for privacy issues.

Rubicryption uses a device devised by the authors termed as the Rubix on the line of the most sold toy on the planet till date is the Rubik's Cube. It uses the concept of shifting colored rows or columns to form a mixture of the four basic colors, namely; Blue, Green, Yellow and Red. The trick is to tactfully rearrange all rows and columns to get mono-colored four sides.

[1,2]Department of Computer Application, JIS College of Engineering, Block 'A', Phase III, Kalyani, Nadia-741235, West Bengal, India

Email: [1]dujon18@yahoo.co.in, [2]saikat0903@yahoo.com

Inspired from the above and amalgamating with it the concept of matrix we can arrive to a Structured Alphabet Matrix Set that uses the former concept to encrypt data by rearranging the 'Rubix' according to the 'Normalizer.'

The algorithm has been devised keeping in mind the three facets, namely; Normalizer, Default Rubix and Normalized Rubix, thereby ensuring the righteous implementation of the Rubicryption and its allied characteristics.

Rubicryption aligns its mechanism with the dual Rubix, keeping in mind all the nuances of the freshly conceived concept, that is, the use of the Default Rubix and the Normalized Rubix, along with the implementation of the Normalizer.

2. Conceptual Literature Review

Rubix: A Rubix is a conceptual design inspired from the Mathematical Matrix, which has been transformed into a character-only design that is amalgamated with the sole purpose of data encryption and data decryption techniques.

A	B	C	D
E	F	G	H
I	J	K	L
M	N	O	P
Q	R	S	T
U	V	W	X
Y	Z	@	#

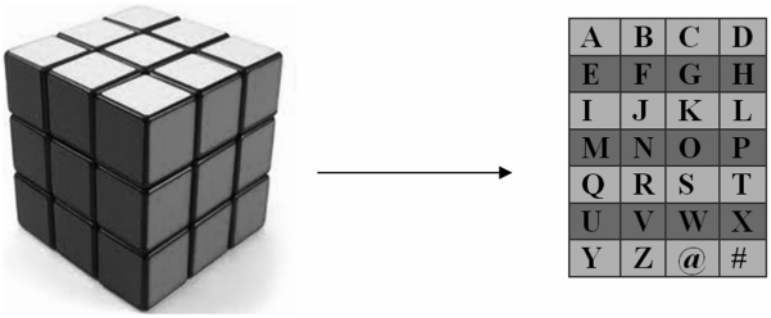
Fig. : Rubix

Plain Text: A Plain Text is a normal text that is initiated for data encryption by the Cryptologist.

Normalizer: A Normalizer is either the co-ordinate for retrieving the X-Normal Form of the Default Rubix or the Y-Normal Form of the Default Rubix.

X-Normal Form: X-Normal Form is that form of the Rubix in which the X-axis is normalized effectively.

Y-Normal Form: Y-Normal Form is that form of the Rubix in which the Y-axis is normalized effectively.



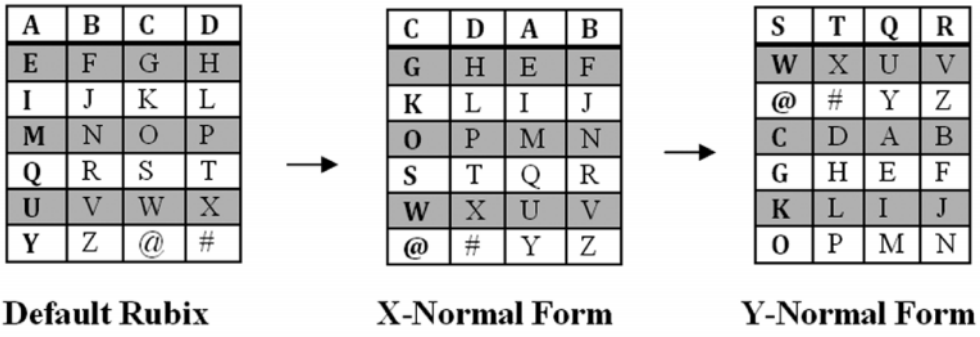
3D to 2D Transformation

3. IMPLEMENTATION VIA CASE STUDY

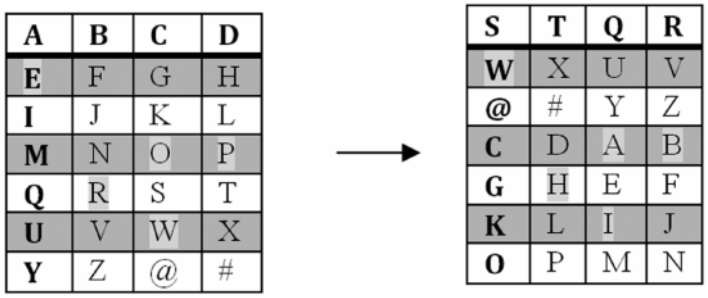
Plain Text: Power words

Normalizer: (2, 4)

Encryption:



Step 1: For the word "Power", the Encrypted Text is "Baiwh"



Step 2: For the word "words", the Encrypted Text is "iahre"

A	B	C	D
E	F	G	H
I	J	K	L
M	N	O	P
Q	R	S	T
U	V	W	X
Y	Z	@	#

→

S	T	Q	R
W	X	U	V
@	#	Y	Z
C	D	A	B
G	H	E	F
K	L	I	J
O	P	M	N

Final Encrypted Text → Baiwh iahre

Encrypted Text: Baiwh iahre

Normalizer: (2, 4)

Decryption:

A	B	C	D
E	F	G	H
I	J	K	L
M	N	O	P
Q	R	S	T
U	V	W	X
Y	Z	@	#

Default Rubix

→

C	D	A	B
G	H	E	F
K	L	I	J
O	P	M	N
S	T	Q	R
W	X	U	V
@	#	Y	Z

X-Normal Form

→

S	T	Q	R
W	X	U	V
@	#	Y	Z
C	D	A	B
G	H	E	F
K	L	I	J
O	P	M	N

Y-Normal Form

Step 1: For the word "Baiwh", the Decrypted Text is "Power"

S	T	Q	R
W	X	U	V
@	#	Y	Z
C	D	A	B
G	H	E	F
K	L	I	J
O	P	M	N

→

A	B	C	D
E	F	G	H
I	J	K	L
M	N	O	P
Q	R	S	T
U	V	W	X
Y	Z	@	#

Step 2: For the word "iahre", the Decrypted Text is "words"

S	T	Q	R
W	X	U	V
@	#	Y	Z
C	D	A	B
G	H	E	F
K	L	I	J
O	P	M	N

→

A	B	C	D
E	F	G	H
I	J	K	L
M	N	O	P
Q	R	S	T
U	V	W	X
Y	Z	@	#

Final Decrypted Text → Power words

4. ALGORITHM

(A) Encryption

Step-1: Using the innovatively devised Normalizer, the Default Rubix is first normalized to obtain the X-Normal Form.

Step-2: Using the innovatively devised Normalizer, the X-Normal Form of the Rubix is used to obtain the final Y-Normal Form.

Step-3: The Default Rubix and the Normalized Rubix is kept side by side and the Plain Text words are individually chosen to be encrypted. Each character of the word is individually marked on the Default Rubix. The Normalized Rubix is now compared and contrasted with the Default Rubix and all the marked cells are marked on the former. The marked characters of the Normalized Rubix are written in sequence as that of the Default Rubix. This generates the encrypted text.

Step-4: Step3 is repeated for all the words in the given sentence.

Step-5: All encrypted texts are sequentially arranged to obtain the final encrypted text.

(B) Decryption

Step-1: Using the innovatively devised Normalizer, the Default Rubix is first normalized to obtain the X-Normal Form.

Step-2: Using the innovatively devised Normalizer, the X-Normal Form of the Rubix is used to obtain the final Y-Normal Form.

Step-3: The Normalized Rubix and the Default Rubix is kept side by side and the Cipher Text words are individually chosen to be decrypted. Each character of the word is individually marked on the Normalized Rubix. The Default Rubix is now compared and contrasted with the Normalized Rubix and all the marked cells are marked on the former. The marked characters of the Default Rubix are written in sequence as that of the Normalized Rubix. This generates the decrypted text.

Step-4: Step3 is repeated for all the words in the given sentence.

Step-5: All encrypted texts are sequentially arranged to obtain the final encrypted text.

5. CONCLUSION

The Implementation via Case Study clearly shows that any given Plain Text by the end user can be encrypted using the devised Rubix and the proposed NBET Algorithm constituted. Furthermore, the Encrypted Text can also be decrypted back to its original form instantaneously. Rigorous testing of the proposed technique with different form of Plain Texts has shown comprehensive success rate in its methodology and implementation.

The concept mainly focuses on the innovative technique devised named Rubicryption with its two allied Rubix, namely; Default Rubix & Normalized Rubix, depending on the defined Normalizer and its correlation with both the Rubix.

The paper "Normalizer Based Encryption Technique Using the Proposed Concept of Rubicryption" ensures the culmination of an innovative mechanism devised by the authors to furnish an alternative podium for the end users to implement in diurnal struggle for futile existence in this modern era where security is a major concern for one and all. The perseverance with the innovative concept has laid down the implementation on the whole, conjuring up the very nuances of innovating with a paper like this. The paper's main aim is to implement a prevalent idea into its practical implementation via thorough case study.

REFERENCES

[1] T. Bhattacharya, M. Paul, A. Dasgupta, "A Novel Session-based Text Encryption & Hiding Technique Using Bit-level Cross Fold Transposition & Genetic Algorithm" International Journal of Information Technology & Knowledge Management, 2, No.2, 2009, pp 419-423.

[2] T. Bhattacharya, T. K. Bhattacharya, S. R. B. Chaudhuri, "A General Bit Level Data Encryption Technique using Helical & Session Based Columnar Transpositions" in Proceedings of IEEE International Advance Computing Conference (IACC'09), 2009, pp 364-368.

[3] T. Bhattacharya, S. Bhowmik, S. R. B. Chaudhuri, "A Steganographic Approach by Using Session Based Stego Key, Genetic Algorithm and Variable Bit Replacement Technique" in Proceedings of International Conference on Computer and Electrical Engineering, 2008, [ICCEE 2008], pp 51-55.

[4] S. Contini, Y. L. Yin, "On Differential Properties of Data Dependent Rotations and their use in MARS and RC6" In Proceedings of Second AEF Conference, 2008.

[5] Z. Shi, R. B. Lee, "Implementation Complexity of Bit Permutation Instructions" in Proceedings of the Asilomar Conference on Signals, Systems and Computers, 2003.

[6] Z. Shi, X. Yang, R. B. Lee, "Arbitrary Bit Permutations in One or Two Cycles" in Proceedings of the 14th International Conference on Application-Specific Systems, Architectures and Processors, 2003, pp 237–247.

[7] R. B. Lee, Z. Shi, X. Yang, "Efficient Permutation Instructions for Fast Software Cryptography" in IEEE Micro, 21(6), 2001, pp 56–69.

[8] Z. Shi, R. B. Lee, "Bit Permutation Instructions for Accelerating Software Cryptography" in Proceedings of the 11 International Conference on Application-Specific Systems, Architectures and Processors, 2000, pp 138–148.