Enhanced Bit Enciphering using Gates, Mathematical Operations and Text Key

B. Reddaiah
Assistant Professor
Yogi Vemana University
Kadapa

ABSTRACT
E-commerce is field that is growing all over the world at a greater speed. This is possible with extension of internet services to each and every corner of the world. As the users are moving towards online business and increasing in number day by day towards online services there is every need to have security at various levels in electronic business. Security mechanisms play a vital role in providing security to online business applications and there is need to improve security services periodically to counter the activities of hackers. In this paper concept of gates and different mathematical operations are used in existing RC2 model to extend the security and examine the possibility of inclusion of different operations in existing systems.

General Terms
Cryptography & Network Security

Keywords
Plain text, Cipher text, Key, Encryption, Decryption, Gates, Arithmetic operations.

1. INTRODUCTION
E-commerce is the area in Computer Science that is significantly gaining its importance in each and every corner of the world by better communication. In network there is every possibility to face different kinds of risks [1]. There will be some cases where there is no need for users to hide information for others and in some cases like dealing with e-commerce where business activities are carried-out one requires hiding the sensitive information. In providing security from previous days we were using cryptography which is a scientific approach. Cryptography, the science of encryption and decryption was used way back in around 1900BC when a scribe in Egypt first used a derivation of the standard to communicate [3]. In past Julius Ceaser also created one of the earliest cryptographic systems to send military messages to his generals. Cryptography is the science that hides information from disclosing to unauthorized people. It is defined as a technique of converting ordinary information into meaningless information to keep the message safe [4]. Once this procedure is applied on message it is very difficult to get back the original form of message without using decryption procedure [5].

Converting the original form of information into an unreadable indecipherable message is by using encryption algorithm. When it comes to getting back the original decipherable message from indecipherable message one has to use decryption. With such kind of activities from cryptography the information is not disclosed to others except the sender and receiver. Cryptography is not only to provide security for data, beyond that it provides solutions for problems that generates to integrity, authentication, non-repudiation and access control. Cryptographic algorithms are divided into two categories based on the usage of key. Key plays an important role in cryptography and it is one of the main ingredients. The key determines the processing of text by algorithms in cryptography. The first type is symmetric algorithms also called as secret key algorithms. Here a single key is used for both encryption and decryption.

The second one is asymmetric algorithms also called as public key algorithms in which different keys are used, one for encryption and another for decryption. This work is based on the system of cryptography. The proposed algorithm deals with multiple functions and they operate sequentially. These functions are one after the other which is different from traditional algorithms with its own advantages.

This paper is organized as the second chapter discusses the background of cryptography, the third chapter discuss some of the important standard of cryptography. Fourth chapter discuss the existing method and the fifth discuss the proposed method and followed by conclusion.

2. PRINCIPLES OF CERYPTOGRAPHY
The process of converting plaintext to cipher text is known as enciphering or encryption and the reverse process of converting plain text from cipher text is called deciphering or decryption. The overall process of providing security depending on how text is processed in encryption and decryption algorithms is termed differently.

Enciphering is the process of translating letters or symbols individually. Encoding is the process of translating entire words or phrases into other works or phrases. Decryption is the reverse process of encryption algorithm with reverse operations for operations that are used in encryption algorithm.

Logical channel that is laid inside physical channel is not secure. In the unsecured channel sender and receiver knowingly transmit data from one place to another. While dealing with cryptography we come across different ingredients that are associated in providing security. With respect to text in these ingredients one is original text called as plain text that sender wants to send. The other is unreadable text also called as cipher which is derived from plain text. Then the next type are encryption algorithms for converting plain text to cipher text and then decryption algorithms for converting cipher text to plain text. By using cryptography the plain text which is in human readable from can be converted into unreadable form and this is generally referred as encryption. The security of an algorithm is based on keeping it secret it is referred as restricted cipher [2].

Every proposed algorithm for encryption and decryption constitute mathematical operations that are used to transform the text from plain text to cipher text. Two basic principle of cryptography are commonly used. They are called substitution

and transposition which are usually used in every encryption and decryption algorithms.

Substitution is the process in which each element of plain text like bit or letter or group of bits or letters are mapped into another element(s) of unreadable text that cannot be easy to read by others. Transposition is the process in which each element of plain text bit or letter or group of bits or letters are rearranged in different order than plain text which is also not easy to read by others. These two techniques are applied on the plain text, the fundamental requirement is that no information of the original text is to be lost and all operations are to be reversible.

Among the intergradient's of cryptography key is the most important one. The overall activity of processing the text and strength of the mechanism does not exist on the encryption or decryption algorithms. But it lies in the strength of key. Symmetric cryptographic algorithms use the symmetric or same key for encryption and decryption, while asymmetric cryptographic algorithms use an asymmetric or public \ private key pair [6].

2.1 Private Key Cryptography

Private key cryptography is also called as symmetric key cryptography. In this type of cryptography only one key is used for encrypting the data where we transform plain text to cipher text and for decrypting the data where we transform cipher text to plain text as shown in Fig 2.1. When this private key is used confidentiality to data can be provided to a greater extent. But the main problem with this approach is that how long key can be trusted as hackers are continually striving to break the key. Other than this threat lies in developing key and receiving the key. Even though it has disadvantages private key is very good in providing confidentiality when we periodically change the form of security mechanisms.

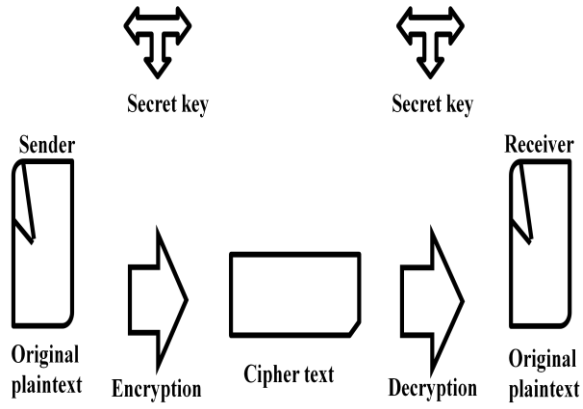

Fig 2.1: Symmetric key Diagram

2.2 Public Key Cryptography

Public key cryptography is also called as asymmetric key cryptography. In this type of cryptography two keys are used one for encrypting the data and other for decrypting the data. Among these two key one key is called private key and other is called as public key as shown in Fig 2.2. Public is sharable to all the users in the network, whereas private key is not sharable. This public key can be accessed by authorized users from key directories which are for that particular purpose. When this public key is used along with confidentiality we can achieve data integrity, authentication. But the main problem with this approach is that key development requires more number of mathematical operations that slowdowns the performance of Operating system.

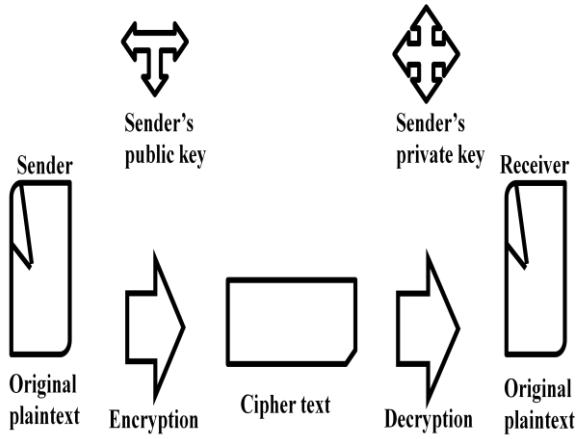

Fig 2.2: Asymmetric key Diagram

3. PROPOSED METHOD

3.1 Model of Encryption

In cryptography, encryption is the process of encoding a message or information in such a way that only authorized parties can access it. This method describes a conventional block encryption algorithm, based on the principles of Rc2, which may be considered as a proposal for a DES replacement. The input and output is a stream of bits. The key size is variable, and it is taken from the text, although the current implementation uses eight bits.

3.1.1 Representation of Encryption

To convert plain text to the cipher text the representation of encryption is as shown in the figure 3.1

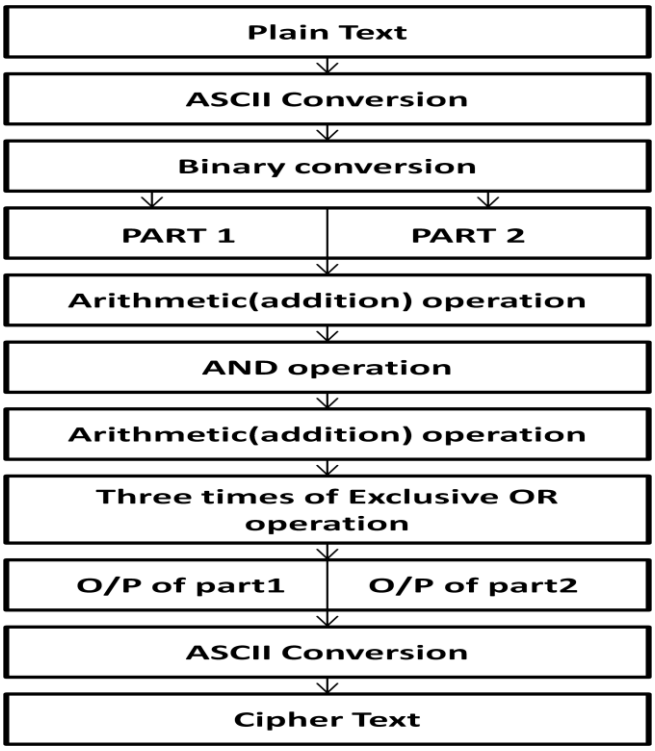

Fig 3.1: Representation of Encryption

3.1.2 Block Diagram of Encryption

The Block Diagram as shown in the figure 3.2 and 3.3 uses logic gates, mathematical operations in the process of substitution and transposition. To show the operations clearly

the block diagram is divided into two parts. The input is considered character by character and it is divided into two parts as the first four bits and another four bits for second part.

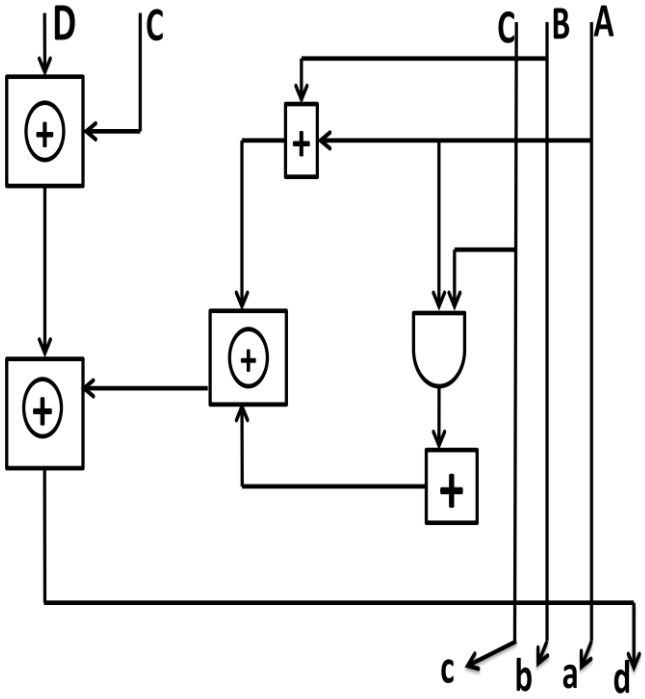

Fig 3.2: Encryption Diagram for first four bits of a byte

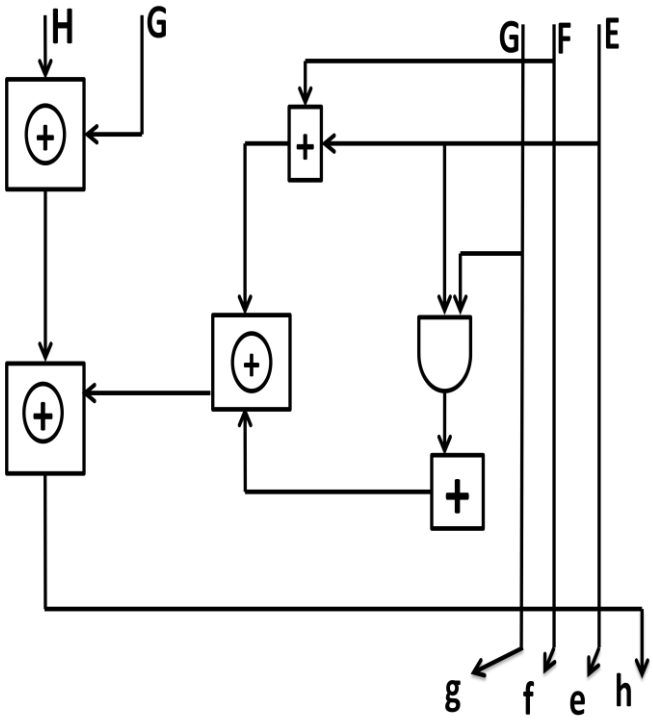

Fig 3.3 Encryption Diagram for next four bits of a byte

3.1.3 Algorithm for Encryption

In this process plain text is converted into cipher text.

STEP1: Start

STEP2: Read the plain text.

STEP3: Generate numeric value for the text.

STEP4: Convert Numeric values to Binary Value.

STEP5: Divide the Binary values in two parts.

STEP6: First part is A, B, C, D and Second part is E, F, G and H.

STEP7: Perform Addition operation to A, B and the output is stored in 'X'.

STEP8: Perform AND operation to C, A.

STEP9: With the output of the AND operation and C Perform Addition operation and store in 'Y'.

STEP10: For X and for Y perform XOR operation and store the result in 'X2'.

STEP11: For D and for C perform XOR operation and store the result in 'X1'.

STEP12: Perform XOR operation on X1 and X2 and store the result in 'X3'.

STEP13: For the 4-Bits is A, B, C, D the output is c, b, a, d.

STEP14: Again A, B, C, D is replaced with the E, F, G, H and perform the same operation.

STEP15: Perform the addition operation on E, F and store the output in 'X'.

STEP16: Perform operation on G, E.

STEP17: With the output of the AND operation and with G performs Addition operation and store the output in 'Y'.

STEP18: For X and Y perform XOR operation and store the output in 'X2'.

STEP19: For H and G perform XOR operation and store it in 'X1'.

STEP20: For X1 and X2 perform XOR operation and store it in 'X3'.

STEP21: For 4-Bits is E, F, G, H output is g, f, e, h.

STEP22: Combine the output of A, B, C, D, E, F, G, H.

STEP23: The output value is converted in to numeric value.

STEP24: The numeric value is converted in to ASCII value.

STEP25: The ASCII value is cipher text.

STEP26: STOP

3.1.4. Results:

After processing Encryption algorithm by using the proposed method on word 'MAN' the following results are shown in the table 3.1 and 3.2s. As the block diagram itself is divided into two parts the results and the table that holds the results are also divided into two parts. In the first table out of eight bits of a character first four bits are shown and in the second table the remaining four bits are shown.

Table 3.1. Results of Encryption

Plain Text	ASCII Value	Conversion to Binary	Two parts of Binary	Part 1 (A, B, C, D)									
				A	B	C	D	X=B+C	A&C	Y=(A&C)+C	X1=D^C	X2=X^Y	X3=X1^X2
M	077	01001101	(0100) (1101)	0	1	0	0	1	0	0	0	1	1
A	065	01000001	(0100) (0001)	0	1	0	0	1	0	0	1	1	1
N	078	01001110	(0100) (1110)	0	1	0	0	1	0	0	0	1	1

Table 3.2. Results of Encryption continued

Part 1 (A, B, C, D)										Part 1 output	Part 2 output	Output of Binary value	ASCII value	Cipher Text
E	F	G	H	X=F+E	E&G	Y=(E&G)+G	X1=H^G	X2=X^Y	X3=X1^X2					
1	1	0	1	1	0	0	1	1	0	(0101)	(0110)	01010110	086	V
0	0	0	1	0	0	0	1	0	1	(0101)	(0001)	01010001	081	Q
1	1	1	0	1	1	1	1	0	1	(0101)	(1111)	01011111	095	_

Cipher Text that is processed in Decryption function is: MAN

Plain Text that is obtained after Decryption is: VQ_

3.2 Model of Decryption

Decryption is the process of transforming cipher text back to unencrypted form

3.2.1 Representation of Decryption

The process of converting cipher text to plain text process is shown in 3.4. The Block Diagram are shown in the figure 3.5 and 3.6

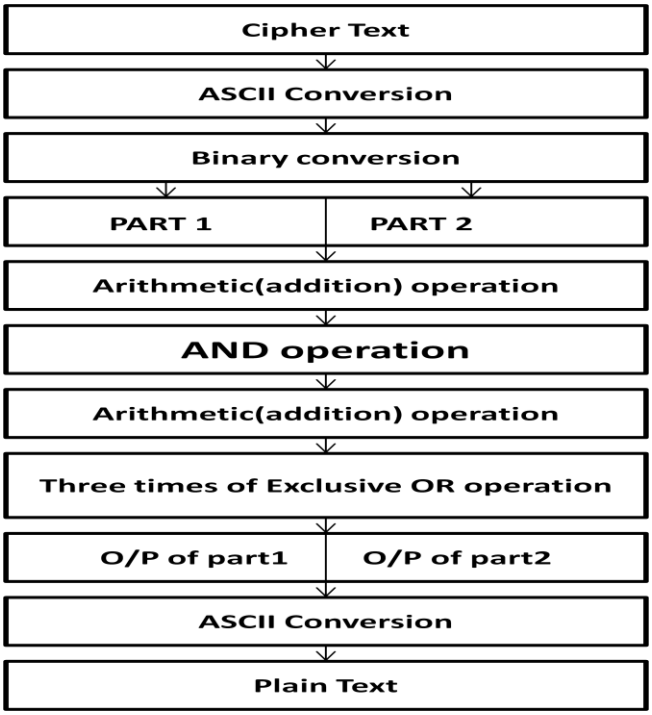

Fig 3.4: Representation of Decryption

3.2.2 Block diagram of Decryption

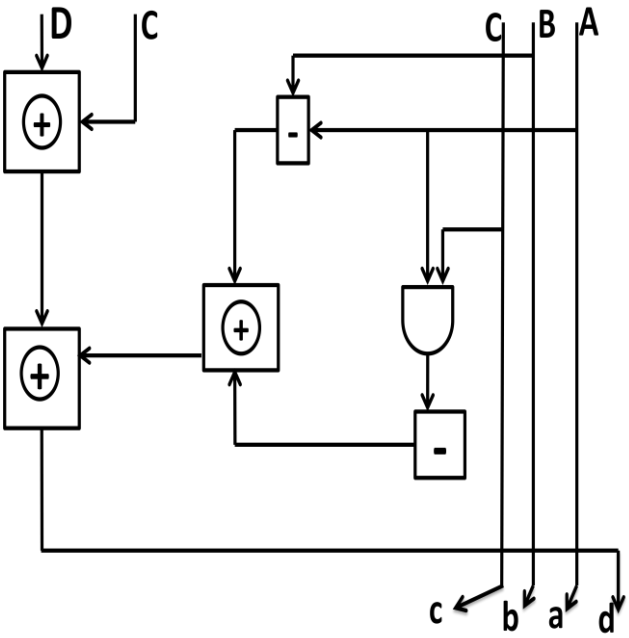

Fig: 3.5 Decryption Diagram for first four bits of a byte

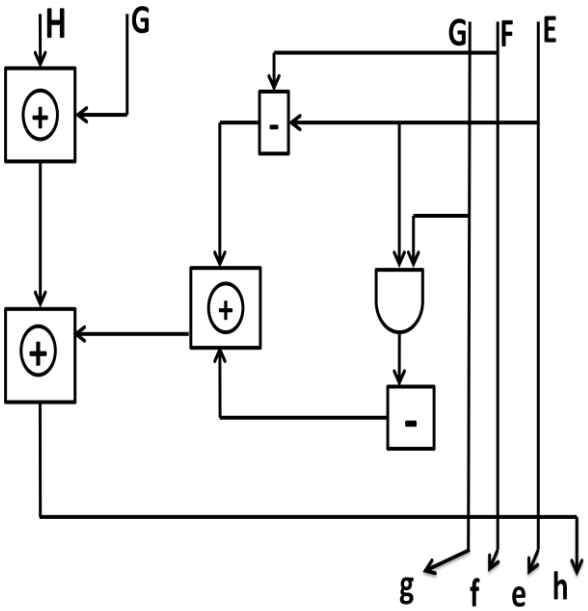

Fig 3.6: Decryption Diagram for next four bits of a byte

3.2.3 Algorithm for Decryption

STEP1: Start

STEP2: Read the cipher text.

STEP3: Generate the Numeric value to cipher text.

STEP4: Convert the numeric value to binary value.

STEP5: Divide the Binary values in two parts.

STEP6: The first is A, B, C, D and second is E, F, G, H.

STEP7: Perform addition to A, B and stored in ‘X’.

STEP8: Perform AND operation between C, A.

STEP9: Perform addition between ‘X’ and C, result in ‘Y’.

STEP10: Perform XOR between X and Y and result in ‘X2’.

STEP11: Perform XOR between D and C and result in ‘X1’.

STEP12: Perform XOR between X1 and X2, result in ‘X3’.

STEP13: For the 4-Bits A, B, C, D output is c, b, a, d.

STEP14: A, B, C, D replace with the E, F, G, H.

STEP15: Perform Addition to E, F and stored in ‘X’.

STEP16: Perform AND operation to G, E.

STEP17: Perform Addition between ‘X’ and G, result in ‘Y’.

STEP18: Perform XOR between X and Y and result in ‘X2’.

STEP19: Perform XOR between H and G and result in ‘X1’.

STEP20: Perform XOR between X1 and X2, result in ‘X3’.

STEP21: For 4-bits E, F, G, H the output is g, f, e, h.

STEP22: After the operation 8-bits value is generated.

STEP23: The output value is converted to numeric value.

STEP24: The numeric value is converted to ASCII value.

STEP26: STOP.

3.2.4. Results:

Table 3.3. Results of Decryption

Cipher Text	ASCII Value	Conversion to Binary	Two parts of Binary	Part 1 (A, B, C, D)									
				A	B	C	D	X=B-A	A&C	Y=(A&C)-C	X1=D^C	X2=X^Y	X3=X1^X2
V	086	01010110	(0101) (0110)	0	1	0	1	1	0	0	1	1	0
Q	081	01010001	(0101) (0001)	0	1	0	1	1	0	0	1	1	0
_	095	01011111	(0101) (1111)	0	1	0	1	1	0	0	1	1	0

Table 3.4. Results of Decryption continued

Part 1 (A, B, C, D)										Part 1 output	Part 2 output	Output of Binary value	ASCII value	Cipher Text
E	F	G	H	X=F-E	E&G	Y=(E&G)-G	X1=H^G	X2=X^Y	X3=X1^X2					
0	1	1	0	1	0	1	0	1	1	(0100)	(1101)	(01001101)	077	M
0	0	0	1	0	0	0	1	0	1	(0100)	(0001)	(01000001)	065	A
1	1	1	1	0	1	1	0	0	0	(0100)	(1110)	(01001110)	078	N

Cipher Text that is processed in Decryption function is: VQ_

Plain Text that is obtained after Decryption is: MAN

4. CONCLUSION

The proposed method in this research work has new algorithms that process the text bit by bit. It is a stream cipher. By the outlook it seems as RC2 model. But this new model is different from RC2 as this model is developed on complex mathematical operations and with Gates. In addition to this one of the inputs for any operation in the form of key is also taken from the text itself. With this feature there is no need for this model to go for sub keys, which is complex in standard RC2 model. This makes the hacker to think in different way to break this algorithm, and it takes more time to do that. This is because the property confusion and diffusion is exactly achieved in this model.

REFERENCES

[1] R. Pradeep Kumar Reddy, B. Reddaiah, C. Nagaraju,December 2014, "A Review on Security Issues Related to Computer Networks",International Journal of Scintific Engineering and Technology Research(IJSETR), Voll.03 Issue 46, 9388-9393.

[2] B. Reddaiah, R. Pradeep Kumar Reddy, S. Hari Krishna, July 2015, "Enciphering Using Bit-Wise Logical Operators and Pairing Function with Text Generated Hidden Key", International Journal of Computer Applications, Vol.121 Issue 8, 30-35.

[3] S. Hebert, "A Brief History of Cryptography", an article available at http://cybercrimes.net/aindex.html.

[4] P. P Charles & P. L. Shari, "Security in Computing: 4th edition", Prentice-Hall, Inc.,2008.

[5] "Basic Cryptography Algorithms", an article available at www.itsc.state.md.us/oldsite/info/InternetSecurity/Crypto/CryptoIntro.html#Algorithms

[6] K. Gary, "An Overview of Cryptography ", an article available at www.garykessler.net/library/crypto.html.