International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2015): 6.391

FPGA Implementation of Cryptographic Algorithm Using ASCII Conversions for Secure Communications

J. Saritha[1], E. Srinivas[2]

[1]M. Tech-student (VLSI system design), CVSR College of Engineering

[2]Assistant Professor, CVSR College of Engineering

Abstract: ***In today's world cryptography has become a necessity for all the organizations. Data security is an essential component of an organization in order to keep the information safe from various competitors. It also helps to ensure the privacy of a user from others. It helps us to securely access bank accounts, electronic transfer of funds and many more daily life applications. In this project it introduces a new algorithm for Cryptography to achieve a higher level of security. In this algorithm it becomes possible to hide the meaning of a message in unprintable characters. If a transmitter sends a message of plain text of 32 characters then according to algorithm it is divided into packets each packet is of 8 characters. Thus four packets are formed. Then in encryption the input is of 256_bit plain text where encrypted using ASCII conversions and cyclic mathematical function. From this 256_bit cipher text is formed. In decryption the input cipher text is of 256_bit where decrypted using ASCII conversions and inverse cyclic mathematical function. From this the original 256_plain text is obtained which can be sent to the receiver.***

Keywords: Cryptography, Encryption and Decryption, ASCII conversions, Level of security, Unprintable encrypted message.

1. Introduction

Message authentication protects two parties who exchange messages from any third party. Several works have been done to develop a new cryptographic algorithm for a higher level of security. The cryptography is the study of mathematical techniques related to aspects of information security such as confidentiality, data integrity, entity authentication and data origin authentication [1]. Also it means hidden writing, and it refers to the practice of using encryption to conceal text [3]. Cryptographic algorithms are used to encrypt and decrypt messages in a cryptographic system. Encryption transforms human readable plaintext into something unreadable, also known as ciphertext. The ciphertext is then decrypted to convert to the original plaintext, making it understandable to the authentic party. Among the available three modern securities offering techniques namely cryptography, stenography and watermarking, cryptography is the base to understand and also to implement ensuring a higher level of security in the real-time security systems. There are many approaches of cryptographic algorithm, most of them classified as symmetric key and asymmetric key cryptography. In symmetric key algorithm same key is used for both encryption of plaintext and decryption of ciphertext. Symmetric key encryption can use either stream ciphers or block ciphers. Asymmetric cryptography is cryptography in which a pair of keys is used to encrypt and decrypt a message. In this paper, we proposed a new cryptographic algorithm which follows a different methodology from the traditional symmetric-key cryptography, asymmetric-key cryptography or hashing function

2. Previous Works

Several works have been done to develop a new cryptographic algorithm for a higher level of security. A new cryptographic algorithm for the real time applications was proposed by A. H. Omari, M.B. Al-Ksasbeh, E.R. Al Qutaish to improve the time for encryption and decryption of data of end-to =-end delay and to provide higher level of security[5]. Some researchers have developed a secure hybrid mode-based crytosystems which provides greater security level than that schemes based on a single hard problem. The enemy or adversary has to solve the two problems simultaneously which is unlikely to happen in order to read any secret message [6]. Some researchers have developed a new cryptosystem using multiple cryptographic assumptions which offers a greater security level than that schemes based on a single cryptographic assumptions [8]. S. Kumar, Addgarla, and Y. Babji made a comparative security study on symmetric key crptosystem based algorithms such as DES, TDES, IDEA, and AES [9]. A basic study on cryptography which is a solution for information security threats has been shown in [10].

3. Proposed Algorithm

Encryption Phase

In the encryption phase of the proposed algorithm, at first the input characters of the text to be encrypted are divided into several packets of N characters taking in order from the beginning character, where the value of N is 8 which may vary only for the last packet as the last packet contains the remaining characters. Its value may range from 1 to 8. For example, if a text consists of 13 characters, the first 8 characters constitute the first packet, the subsequent 5characters constitute the second packet and the remaining 5 characters constitute the last packet. Secondly, a binary matrix P[N,8] is formed for each packet using the 8-bit binary equivalent of the ASCII value of each character. The binary value of each ASCII of a packet is then accommodated row wise in the binary matrix. Thirdly, 8 new ASCII values denoted by NewASCII[i] for each packet

is evaluated using the matrix P[N,8] taking the decimal equivalent of the bits belonging to each column of the matrix. In the example considered above, the NewASCII[1] for the first packet is the decimal equivalent of the bits from P[0,8] to P[0, 0], where P[0,8] is the MSB and P[0,0] is the LSB. The values of the NewASCII[i] range from 0 to 31whosemequivalent characters are unprintable. Now if we take the equivalent character for each NewASCII[i], then all the printable characters in the original data will become unprintable. Thus, this offers a better security making the ciphertext more secured. However, for one step higher security, a cyclic mathematical function has been used to encrypt once again the final ASCII values of the intermediate encrypted data. The mathematical function as shown below is called cyclic because its output is rotated between 0 and 256.

FinalASCII[i] = (NewASCII[i] +M)%32, where, 0<M<32.

Finally the 8 FinalASCII[i] values are converted to their equivalent characters whose are undoubtedly unprintable so that the final ciphertext cannot be shown at all. This encryption process repeats for each packet of N characters for the original data. Then combining all the encrypted packets as a single it is sent to the receiver.

PSEUDOCODE OF ENCRYPTION

The pseudocode of the encryption procedure using the parameters discussed above can be summarized as follows:
1. Input original message.
2. Divide the original message into their equivalent ASCII of the characters.
3. For each packet
a. Convert the characters to their equivalent ASCII
b. Create binary matrix p[N,8] with the binary value from the ASCII of the characters
c. Calculate new ASCII as:
initialize i=0
For (k=1 to 8)
Increment I by 1
New ASCII[i]=0
For (j=0 to N-1)
New ASCII[i]+=(p[N-j, k])*2^{N-j-1}
End inner loop
End outer loop
d. Re_calculate each NewASCII[I] using the cyclic mathematical function
FinalASCII[i]=(NewASCII[i]+ M)%256,where 0<M<32
e. Convert each FinalASCII[i] to its equivalent character
4. End of encryption

DECRYPTION PHASE

In the decryption phase of the algorithm, at first the characters of the received unprintable ciphertext are converted to their equivalent ASCII. After which the inverse cyclic mathematical function is applied to the ASCII as shown below:

DecASCII_1[i] = (ASCII[i] –M+32)%32, (2)where 0<M<32.

Then all the DecASCII_1[i] are divided into the same number of packets of 8 characters in order as done the encryption phase. Secondly, a binary matrix Q[N, 8] is formed using the equivalent binary of the ASCII value in each packet, where the value of N is 5 which may vary only for the last packet. Its value may range from 1 to 5. The binary value of each ASCII of a packet is then accommodated column wise in the binary matrix. Thirdly, the final N ASCII denoted by DecASCII_Final[i] for each packet is evaluated using the binary matrix Q[N,8] taking the decimal equivalent of the of the bits belonging to each row of the matrix. For the example considered in the above encryption phase, the DecASCII_Final[1] for the first packet is the decimal equivalent of the bits from P[0,0] to P[7, 0], where P[0,0] is the MSB and P[7,0] is the LSB. Finally, the N DecASCII_Final[i] values for each packet are converted to their equivalent characters whose are undoubtedly same as in the original message. This decryption process repeats for each packet of 8 characters of the encrypted data.

PSEUDOCODE OF DECRYPTION

The pseudocode of the decryption procedure using the parameters discussed above can be summarized as follows:
1. Input encrypted message.
2. Convert the characters to their equivalent ASCII
3. Calculate DecASCII_1[i] using the inverse cyclic mathematical function
DecASCII_1[I]=(ASCII[i]-M+256)%256,where 0<M<32
4. Divide the DecASCII_1[i] into several packets of 8 characters each
5. For each packet
a. Create binary matrix Q[N,8] with the binary value from the DecASCII
b. Re_calculate new ASCII as:
Initialize i=0
For(j=1 to N)
Increment i by 1
DecASCII_Final[i]+=(Q[j,k])*2^{8-k}
End inner loop
c. Convert each DecASCII_Final[i] to its equivalent character
6. End of decryption.

4. Explanation With Example

As an example, let's consider that the user wants to encrypt,and then conceal the message "**FinalASCII[i] = (NewASCII[i] +M)%cb**". According to the discussion the algorithm divides the input into 2 packets, where all the packets contains 8 as shown below: Figure

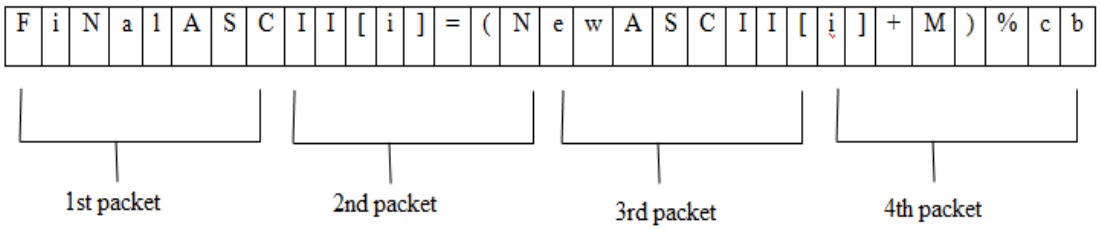


Figure 4.1: Dividing the Original Message into four Packets

Encryption

As the explanation in the encryption phase the characters of each packet are converted to their equivalent ASCII. Then using the 8-bit binary equivalent of the ASCII the first matrix P1[8,8] is formed for the first packet as shown in Fig.4.1 with the subsequent calculations to encrypt the characters of the packet.

First Packet

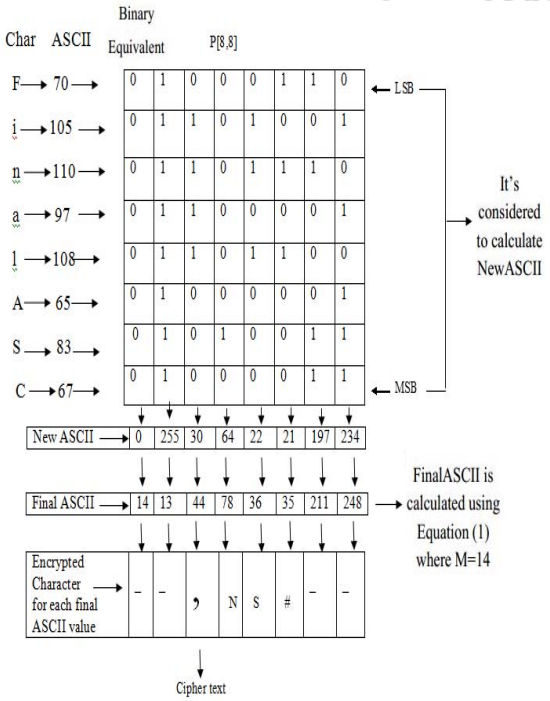


Figure 4.2: Encryption steps for First packet.

Second Packet

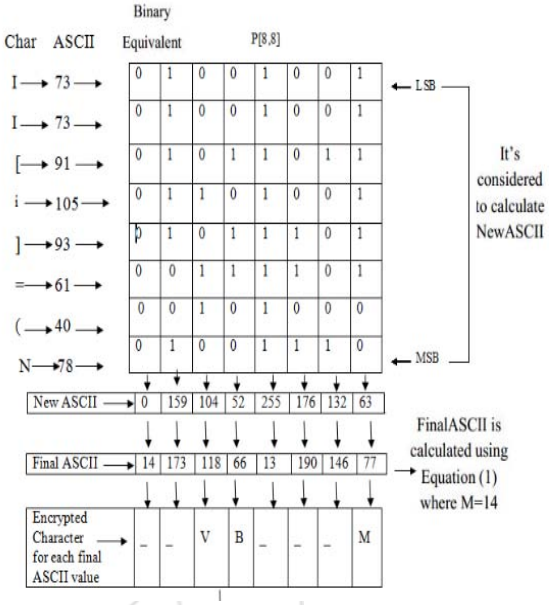


Figure 4.3: Encryption steps for Second packet.

Third Packet

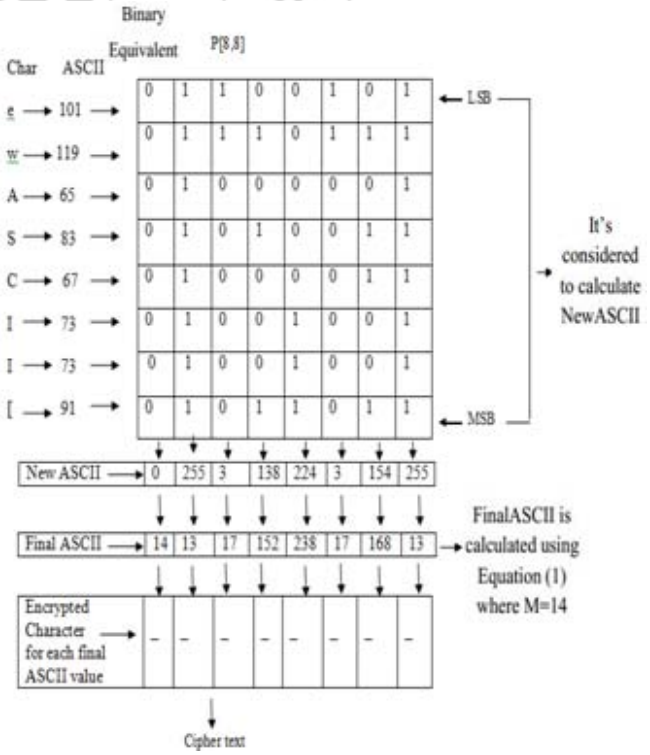


Figure 4.4: Encryption steps for third packet..

Fourth Packet

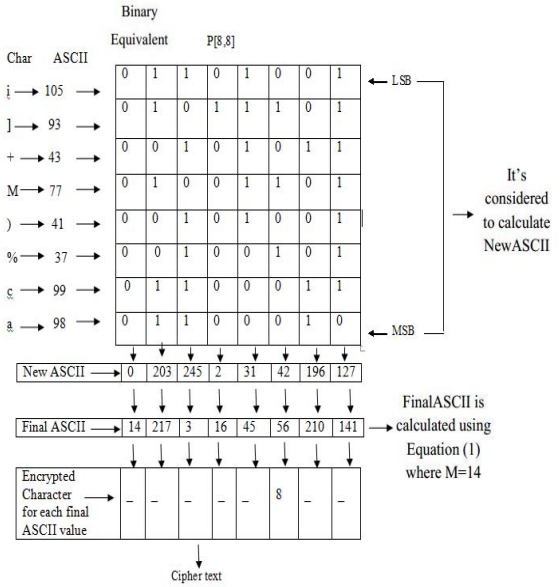


Figure 4.5: Encryption steps for fourth packet.

Finally the 8 FinalASCII[i] values are converted to their equivalent characters whose are undoubtedly unprintable so that the final ciphertext cannot be shown at all. This encryption process repeats for each packet of N characters for the original data. Then combining all the encrypted packets as a single it is sent to the receiver.

Decryption

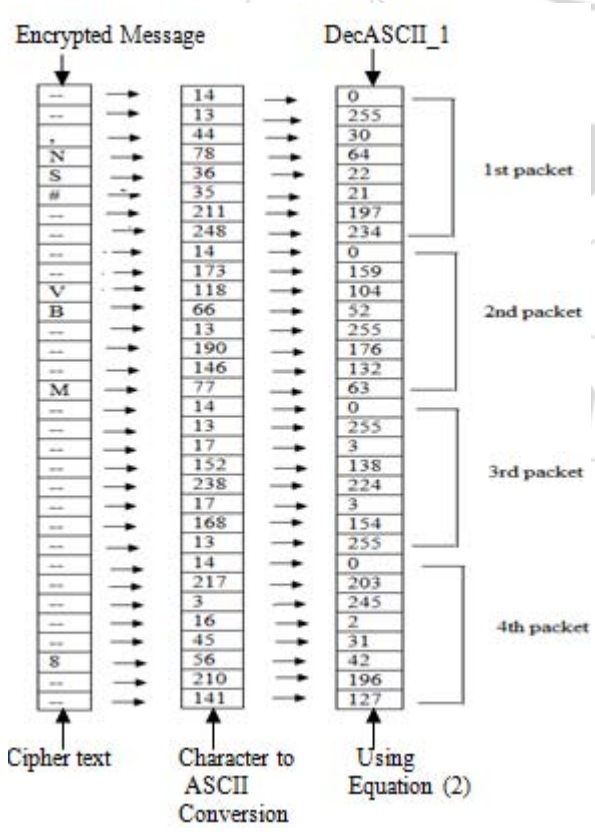


Figure 4.6: Conversion of encryption to DEC_ASCII values.

In the decryption phase of the algorithm, at first the characters of the received unprintable ciphertext are converted to their equivalent ASCII. After which the inverse cyclic mathematical function is applied to the ASCII as shown below:
DecASCII_1[i] = (ASCII[i] –M+32)%256, where 0<M<32.

Then all the DecASCII_1[i] are divided into the same number of packets of 8 characters in order as done the encryption phase. Secondly, a binary matrix Q[N, 8] is formed using the equivalent binary of the ASCII value in each packet, where the value of N is 8 which may vary only for the last packet. Its value may range from 1 to 8. The binary value of each ASCII of a packet is then accommodated column wise in the binary matrix. Thirdly, the final N ASCII denoted by DecASCII_Final[i] for each packet is evaluated using the binary matrix Q[N,8] taking the decimal equivalent of the of the bits belonging to each row of the matrix. For the example considered in the above encryption phase, the DecASCII_Final[1] for the first packet is the decimal equivalent of the bits from P[0,0] to P[7, 0], where P[0,0] is the MSB and P[7,0] is the LSB. Finally, the N DecASCII_Final[i] values for each packet are converted to their equivalent characters whose are undoubtedly same as in the original message. This decryption process repeats for each packet of 8 characters of the encrypted data.

First Packet

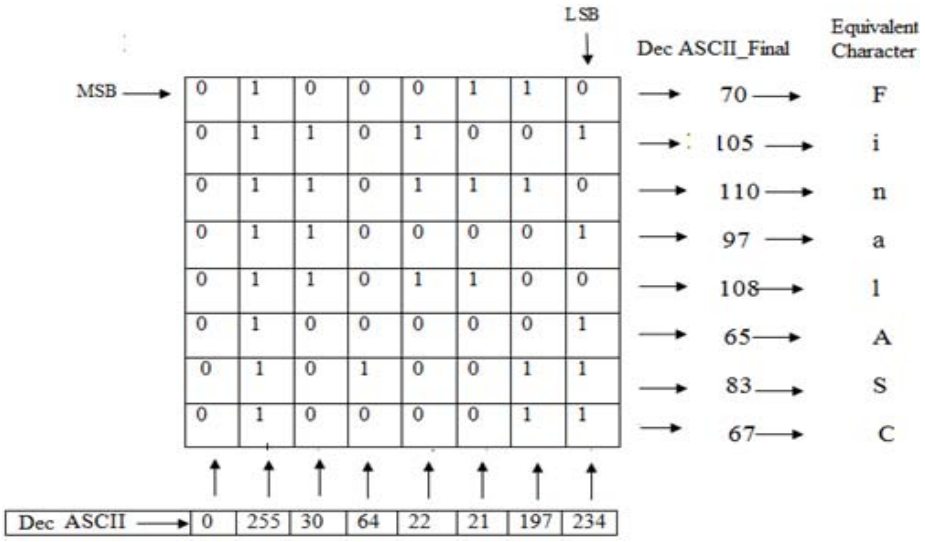


Figure 4.7: Decryption steps for first packet

Second Packet

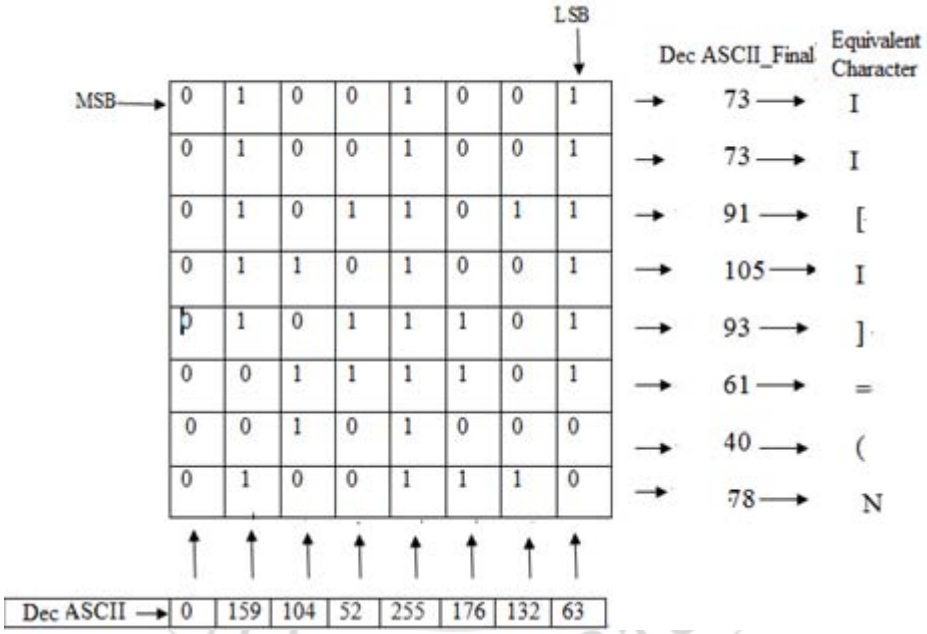


Figure 4.8: Decryption steps for second packet

Third Packet

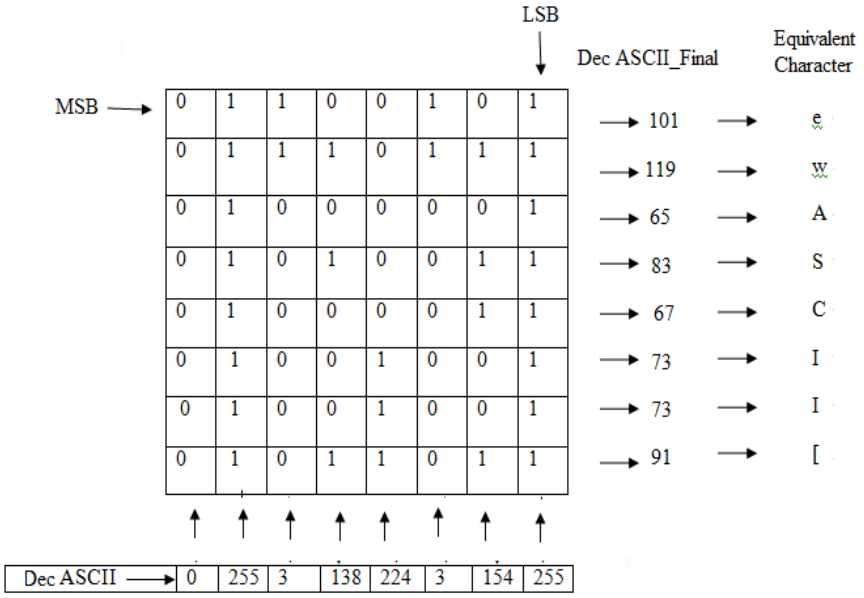


Figure 4.9: Decryption steps for third packet

Fourth Packet

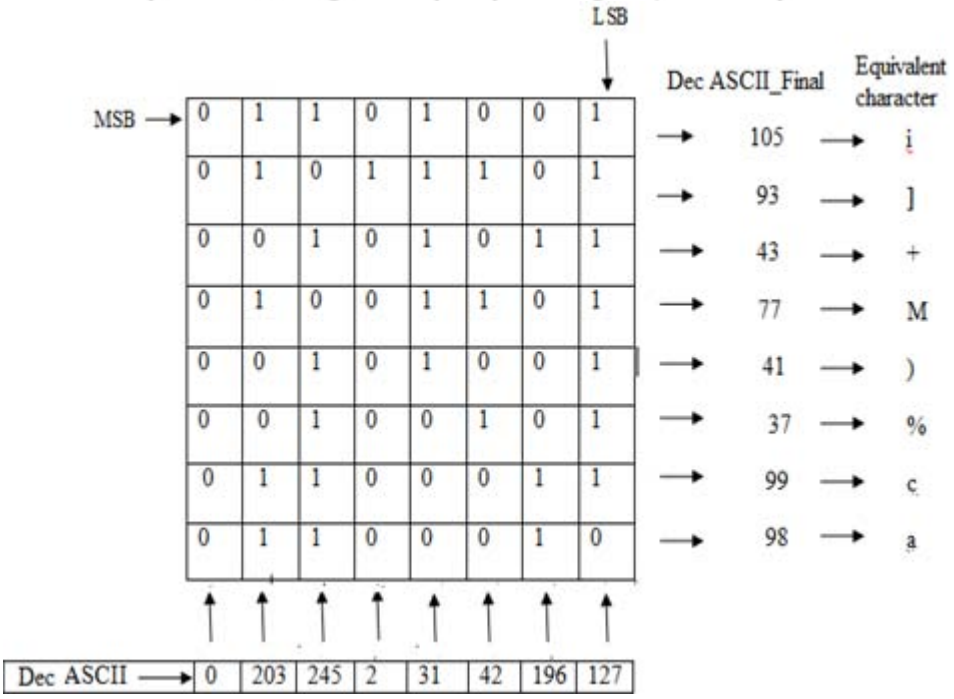
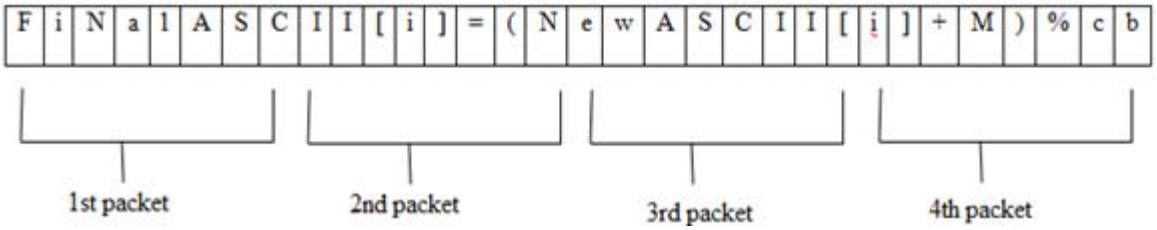


Figure 4.10: Decryption steps for fourth packet

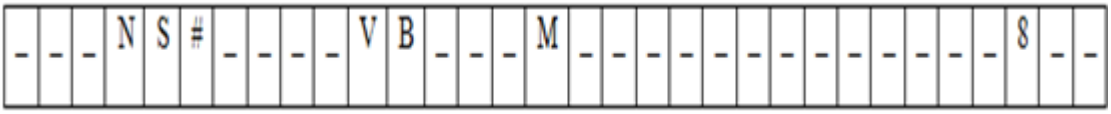
5. Result Analysis

Here 256 bit encryption and decryption are used. The fig.4.1 shows the plaintext to be encrypted though the algorithm. Applying the encryption algorithm the cipher text of characters is shown in Fig.4.2. Thus, the cipher text is a collection of boxes in which the original message is concealed. Again at the receiver, applying the decryption algorithm on the cipher text the original message is shown in Fig.4.3.

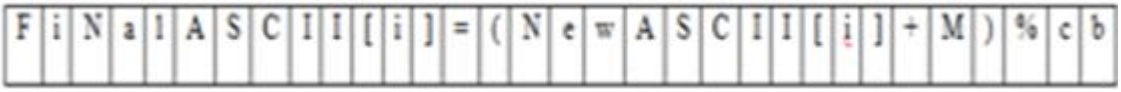
Plain Text



Cipher Text



Original Plain Text



6. Conclusion

As cryptography is a big deal in all type security systems, this developed algorithm will be a great part for the same. We presented the algorithm based on ASCII conversions and a simple cyclic mathematical function. We emphasized mainly on the concealing of the encrypted message ensuring a better security. In future, we will develop another version of the algorithm based on radix conversion with the ASCII and also try to implement some real-time security systems using the algorithm.

References

[1] E. Cole, R. Krutz and J.W. Conley, Netowrk Security Bible, Publishing Inc. 2005.
[2] Sidhpurwalahuzaifa A Brief History of Cryptography. [Online].
[3] A Menezes, V. Oosrschot and A. Vanstone, Handbook on Applied Cryptography, CRC Press Inc., NY, USA, 2000.
[4] D. Stinson, Cryptography Theory and Practice, CRC Press Inc., NY, USA, 1995.
[5] A.H. Omari, B.M. Al-Kasabeh, R. E. A1- Qutaish, and M.I. muhairat, "A New Cryptographic Algorithm for the Real Time Application", Proc. Of the 7th WSEAS. International Conference on INFORMATTION SECURITY and PRIVACY (ISP) , 3338, 2008.
[6] E.S. Ismail and S. Baharudin, "Secure Hybrid Mode-Based Cryptosystem", American Journal of Applied Sciences, vol9, no 3, pp 289-292, 2012.
[7] E.S. Ismail and M.S Jijazi, "New Cryptosystem Based on Factoring and Discrete Logarithm Problems", Journal of Mathematics and Statistics, vol 7, no 3, pp. 165-168, 2011.
[8] E.S. Ismail and M.S. Hijazi "New Cryptosystem using Multiple Cryptographic Assumptions", Journal of Computer Science, vol 7 no 12, pp. 1765-1769, 2011.
[9] S. Kumar, Addagarla, and Y. Babji, "A Comparative Security Study Review on Symmteric Key Cryptosystem Based Algorithms", International Journal of Computer Science and Mobile Computing, vol 2, no 7, pp 146-151, 2013.
[10] M.V. Kumar, "Cryptography- A solution for information security Threats" Golden Research Thoughts,vol.2.No.1,2013.