Data Analytics and Artificial Intelligence
Vol: 2(5), 2022
REST Publisher; ISBN: 978-81-948459-4-2
Website: http://restpublisher.com/book-series/data-analytics-and-artificial-intelligence/

DRDP and Matrix Operations in a Cryptographic Algorithm

V P Pavithra
Adhiyamaan College of Agriculture & Research, Athimugam, Hosur, Tamilnadu, India
*Corresponding author Email: poovaragavanvpp@gmail.com

Abstract. The internet serves as a rich platform of exploration for the intruders. The aspect of security has been brought to spot light. The importance of security in data communications and networking cannot be denied. To reduce the severity of destruction many algorithms where proposed. This research work aims to propose an algorithm to serve the aspect of security. The research work entitled "Cryptographic Algorithm Using DRDP and Matrix Operations" is developed with the objective of encrypting and decrypting using 3D matrices and to provide security for information in an efficient manner with less computation power and memory resources. The proposed work uses three keys namely Shared Secret Key, Session Key, and Intermediate Key. The work calculates variable number of keys according to the length of the Plain Text and a technique called Double Reflecting Data Perturbation (DRDP) is used. The work also employs 3D matrices to store the keys during encryption and decryption. The security analysis of the work shows that the proposed work is much secured than the existing work.
Keywords; Cryptography; DRDP; Matrix Operations; Encryption; Decryption

1. Introduction

This section deals with details about the various methods used in the proposed work. Cryptography aids in providing a secure platform to send data through channels that are prone to attack. Cryptography transforms the data in such a way that the data remains secure and prevents unauthorized data modification. It also allows the receiver to retrieve the original data without any aid from the sender. Therefore this technique plays a critical role and is widely used in secure data transmission. The below described concepts are used in the proposed work.

The Double Reflecting Data Perturbation Method: The Double Reflecting Data Perturbation Method denoted by DRDP is a mechanism to preserve privacy in field of data mining. The sum of maximum and minimum value is computed and subtracted from each value. This acts as an apt perturbation method on ASCII values of data.[5]For example let the text be, "abcd". The ASCII values are 97, 98, 99, and 100. The maximum value is 100 and minimum value is 97. The sum of maximum and minimum value is 197.

TABLE 1. Examples for DRDP

Data Before DRDP	Data After DRDP
97	|197-97|=100
98	|197-98|=99
99	|197-99|=98
100	|197-100|=97

Table 1. depicts the ASCII value of the text before and after applying DRDP.

Message Digest: Message Digest deploys a hash function. A hash function is a one-way function, (i.e.) the original message cannot be got back from the digest [7]. This digest is used to provide integrity; it is done by, appending a digest on sender side which is calculated from the message. The receiver on receiving the message, extracts the digest, calculates the hash of the received message, if both the digest matches then message is accepted. Else the message is discarded. The message digest calculated in this algorithm also serves the purpose of authentication. The Shared Secret Key (SSK) is concatenated to the Cipher Text and the digest is calculated. This enables only the sender and receiver to compute the correct digest, which provides authentication and prevents rainbow table attacks, where hash values of texts are computed and stored, and compared against the hash value of received text. Another advantage is that only the message in which the sender digest and receiver digest match decryption is performed. This eliminates the fruitless decryption.

FIGURE 1. Hash computation in proposed work

The hash computation in proposed workis shown in fig 1.

Extracting 3x3 Matrix From 4x4 Matrix: The typical 4x4 matrix exhibit four different possible 3x3 matrices. In order to compute determinant value, extract a 3x3 matrix from 4x4 matrix.

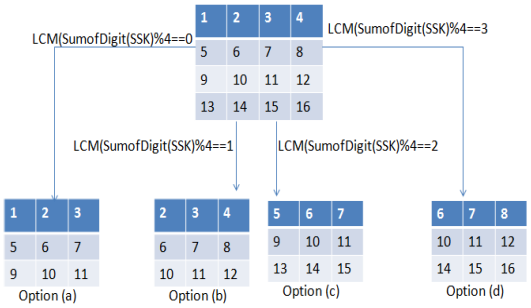

FIGURE 2. Selection Of 3x3 Matrixes

The choice of selecting a 3x3 matrix from a 4x4 matrix is based on the SSK. If LCM(Sumofdigit(SSK))%4==0 use option (a) else if LCM(Sumofdigit(SSK))%4==1 use option (b) else if LCM(Sumofdigit(SSK))%4==2 use option (c) else use option (d) as shown in fig 2.

Cycling: The cycling operation moves each element of the matrix in clock wise direction to the next positional index. If the end of row is reached and if the current row is not the last row, the row below is used, else the prior column of the same row is used. If the start of the row is reached, the column next to the current column is used as shown in fig 3.

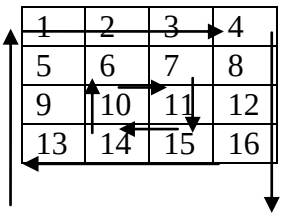

FIGURE 3. Cycling Operation

The arrows shown in fig 1.3, mark the direction of traversal, the result of cycling operation is shown if fig 3.

5	1	2	3
9	10	6	4
13	11	7	8
14	15	16	12

Row Switching: Row switching rotates the elements of the matrix either towards right or towards left. The first remains as such and the further rows are rotated row number-1 times.

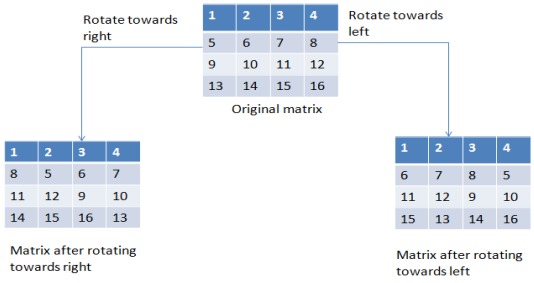

FIGURE 4. Row Switching

An example of row switching operation is shown in fig 1.4.

Shuffle and Exchange: Shuffle exchange network model is based on two routing functions, shuffle and exchange [3]. A perfect shuffle is shown in fig 5(a). It splits the data into two halves from the center and then inter mixes them evenly. Inverse perfect shuffle does the opposite to restore the original ordering as shown in fig 5(b).

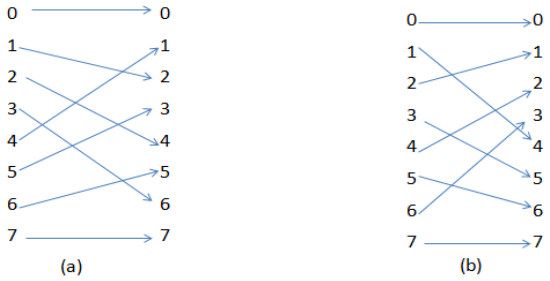

FIGURE 5. Shuffle Network

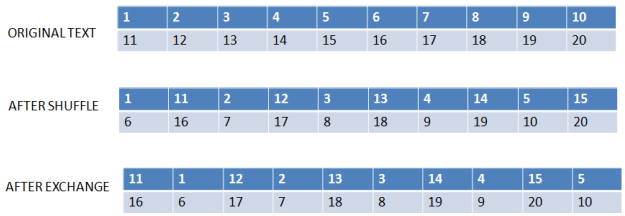

FIGURE 6. Example of Shuffle and Exchange

Exchange merely swaps two adjacent elements as shown in fig 6.

2. Existing Work

This section deals with the working of the existing work. The existing work refers in the paper Kumar Ramesh, Maram Balajee, Rao Lakshmana, "Encryption and Decryption Algorithm using 2-D Matrices", International Journal of Advanced Research in Computer Science and Software Engineering Research Paper,(IJARCSSE), Vol. 3, Issue 4, April-2013[5]. The existing work consists of the following steps under encryption and decryption. The steps are described below briefly.

Algorithm For Encryption: The following are steps used in encryption

- STEP 1: The SSK is shared between the sender and receiver.
- STEP 2: The Session Key is generated randomly.
- STEP 3: Intermediate Key is obtained as Shared Secret Key EX-OR Session Key.
- STEP 4: If number of characters in Plain Text is not a multiple of 16 then pad space as the default character.
- STEP 5: Obtain ASCII value of all characters.
- STEP 6: Double Reflecting Data Perturbation method is applied to all characters in the Plain Textexcept ".", here the delimiter is dot.
- STEP 7: All the characters will arranged in 4X4 matrices and transposed.
- STEP 8: DRDP is applied row wise.
- STEP 9: EX-OR the first 16 characters with Session Key, EX-OR next 16 characters with Intermediate-Key, and so on. Append the Intermediate-Key to cipher-text and transmit to the destination.

Algorithm for decryption: The following steps are followed in decryption

- STEP 1: Extract last 16 characters that constitute the Intermediate Key.
- STEP 2: The receiver calculates the Session Keyusing Intermediate-Key and Shared-Secret-Key as Intermediate-Key EX-OR Shared-Secret-Key.

- STEP 3: EX-OR the first 16 characters with Session Key, EX-OR next 16 characters with Intermediate Key, and so on.
- STEP 4: Obtain ASCII value of all the characters.
- STEP 5: DRDP is applied row wise.
- STEP 6: Transpose all the matrices.
- STEP 7: Double Reflecting Data Perturbation method is applied to all characters in the Plain Text except ".".
- STEP 8: Convert the ASCII value to their corresponding character.

3. Design of Proposed Work

This section deals with the modules in proposed work namely key generation, encryption and decryption.

Overview Of Proposed Work: To initiate transmission of data a Shared Secret Key is shared between the sender and receiver. Further the sender generates a onetime Session Key and obtains Intermediate Key as Session Key EX-OR Shared Secret Key. The data is encrypted as per the procedure discussed below and the decryption process is carried out at the receiver end. Keys Used In Proposed Work : The table 2. describes the keys used in proposed work. Keys may consist of Letters (both upper case and lower case), Numbers (0-9) and Symbols. All keys are of 16 bytes.

TABLE 2. Keys used in proposed work

Key	Description
Shared Secret Key (SSK)	It is agreed upon by both Sender and Receiver
Session Key (SK)	It is randomly generated each time
Intermediate Key (IK)	It can be obtained as SSK **EX-OR** SK

The description of keys used in proposed work is tabulated in table 2.

Determining The Number Of Key Matrices: Depending upon the length of the text, variable numbers of keys are generated. Let the length of Plain Text be denoted as 'L'. If 'L' is not divisible by 16, increment it to the next value divisible by 16. Two cases are possible since 'L'/16 can be an even number or odd number. Let L2 denote number of Session Key matrices and L3 denote number of Intermediate Key matrices If 'L'/16 is an even number, L2=L/32 and L3=L/32. If 'L'/16 is an odd number, L2=(L/32)+1 and L3=L/32 . This step is common for both encryption and decryption.

Encryption Module: The process of encryption consists of the following sub modules listed below. Each sub module is described briefly; each sub module acts as a pipeline structure, wherein output of one module is used as input of another. The Encryption process consists of following sub modules,

- Generation of variable number of SK
- Generation of variable number of IK
- Operations on Plain Text

Generation Of Variable Number Of SK: The following are the steps involved in generating variable number of SK

- STEP 1: Compute sum of digitsof LCM of sum of digits*position of every character in SSKas "sd".
- STEP 2: Randomly generate 16 characters for SK.
- STEP 3: For i from 1 to sk_n

  Sk[i]={
  Take hash of previous matrix as hash2
  Mod hash2with sd
  EXOR with permutation order
  Row switching
  DRDP rowwise
  Transpose
  Add delta A
  Cycle permutation order
  }

Generation of Variable Number of IK: The following are the steps involved in generating variable number of IK

- STEP 1: Compute sum of digits of LCM of sum of digits*position of every character in SSK as "sd".
- STEP 2: Compute 16 byte hash of SSK.
- STEP 3: Mod hash with sd, call it hash`.
- STEP 4: EX-OR hash` and SK[0] and store in IK[0]
- STEP 5: For i from 1 to ik_n, repeat step 3 in generation of variable number of SK.

Operations on Plain Text: The following are the steps performed on Plain Text

- STEP 1: Obtain ASCII value of PT.
- STEP 2: Perform padding if necessary.
- STEP 3: Perform DRDP on entire PT.
- STEP 4: Group into 16 characters.
- STEP 5: Compute LCM (Sumofdigit(SSK))%2.

- STEP 6: If LCM (Sumofdigit(SSK))%2==0 Arrange odd numbered matrix in row major order and even numbered matrix in column major order. Else. Arrange odd numbered matrix in column major order and even numbered matrix in row major order.
- STEP 7: For odd numbered matrix EX-OR with IK and for even numbered matrix EX-OR with SK.
- STEP 8: Perform Row switching.
- STEP 9: Perform DRDP row wise.
- STEP 10: Obtain 16 byte hash of CT matrix1.
- STEP 11: For all matrix except matrix1 EX-OR with previous matrix hash.
- STEP 12: EX-OR first matrix with hash of last matrix.
- STEP 13: For all matrixes except matrix1 EX-OR with previous matrix hash.
- STEP 14: Arrange every 16 characters according to the permutation order.
- STEP 15: Append IK changed according to permutation order.
- STEP 16: Append the number of padded bytes.
- STEP 17: Append the net hash.
- STEP 18: Perform shuffle and exchange for sum of digit of sum of all SSK values.

Decryption Module: The process of decryption performed on the receiver side, consists of the following sub modules listed below. Each sub module is described briefly; each sub module acts as a pipeline structure, wherein output of one module is used as input of another. It proceeds in reverse order of encryption. The Decryption process consists of following sub modules

- Extracting the digest, IK, number of padded bytes
- Generation of Variable Number of IK
- Generation of Variable Number of SK
- Operations on Cipher Text

Extracting The Digest, Ik, Number Of Padded Bytes: Since SHA 256 was used to create the digest would be of 32 bytes. Intermediate Key would be of 16 bytes and number of padded bytes would be of 2 byte. The length of Plain Text would be length (received Cipher Text) – 50.Perform reverse shuffle and exchange for sum of digit of sum of all SSK values. Leaving the last 32 bytes of digest, create the digest using rest of the bytes. Compare the digest with the digest received; if both the digest match then proceed with the following steps else discard the message.The 16 bytes preceding the digest constitute IK. Arrange it in reverse permutation order. Arrange every other group of 16 characters according to the reverse permutation order, it forms the CT.

Generation Of Variable Number Of Ik: Follow step 5 as in generation of variable number of IK in encryption module.

Generation Of Variable Number Of Sk: The following are the steps involved in generating variable number of SK

- STEP 1: Compute sum of digits of LCM of sum of digits*position of every character in SSK as ‘sd’.
- STEP 2: Compute 16 byte hash of SSK.
- STEP 3: Mod hash with sd, call it hash`.
- STEP 4: EX-OR hash` and IK[0] and store in SK[0].
- STEP 5: For i from 1 to sk_n, repeat step 3 in generation of variable number of SK in encryption module.

Operations on Cipher Text: The following are the steps performed on CT

- STEP 1: EX-OR from last to second the hash value of previous matrix.
- STEP 2: EX-OR first matrix with hash of last matrix.
- STEP 3: EX-OR from last to second the hash value of previous matrix.
- STEP 4: Perform DRDP row wise.
- STEP 5: Perform Reverse Row switching. if(LCM(Sumofdigit(SSK))%2!=0) rotate towards right else rotate towards left
- STEP 6: EX-OR with appropriate key matrix
- STEP 7: Compute LCM(Sumofdigit(SSK))%2
- STEP 8: If LCM(Sumofdigit(SSK))%2==0 Arrange odd numbered matrix in column major order and even numbered matrix in row major order Else Arrange odd numbered matrix in row major order and even numbered matrix in column major order.
- STEP 9: Perform DRDP on the entire CT. Obtain character corresponding to ASCII.

4. Comparison Of Proposed Work And Existing Work

This section deals with various factors taken under consideration for comparing proposed work and existing work.

Diffusion: The change of a single character in Plain Text changes multiple characters in Cipher Text. This is achieved in the proposed work by performing EX-OR through feedback network, which makes changes globally.But the existing work exhibits changes only locally among the group of 16 characters. Let Plain Text be of 64 consecutive a’s before change and b, followed by 63 a’s after change. The diffusion measurement is depicted in table 4.1. Figures 4.1 and 4.2 show the Plain Text and corresponding Cipher Text before and after changing the PT in existing work proposed work respectively.

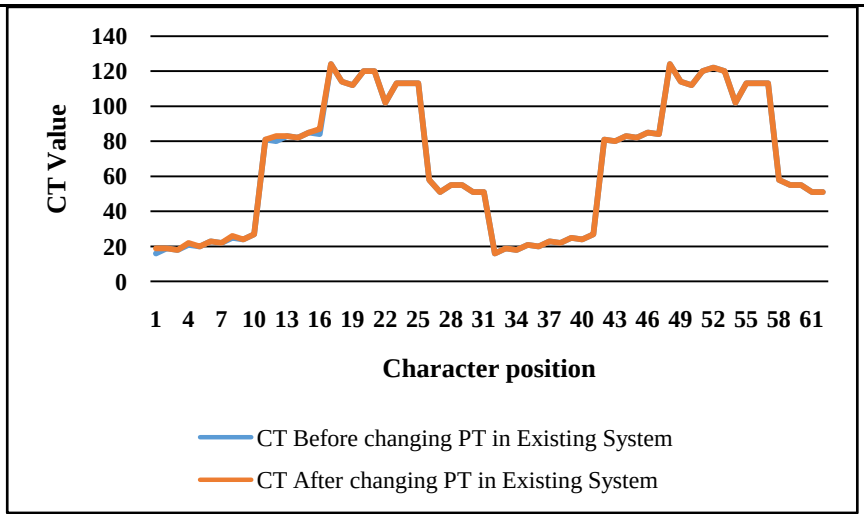

FIGURE 7. Diffusion in Existing Work

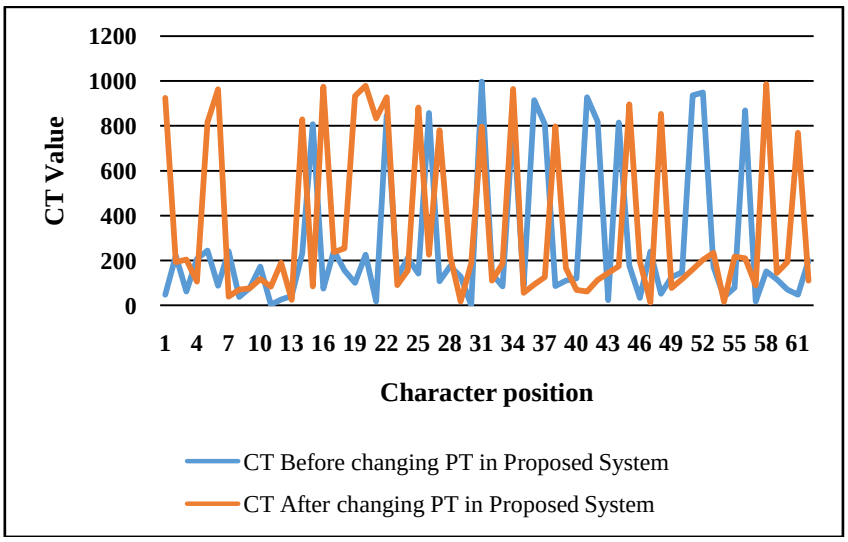

FIGURE 8. Diffusion in proposed work

TABLE 3. Diffusion measurement in both the works

Work	Number of Bits changed in Plain Text	Number of characters changed in Cipher Text	Percentage of change in CT
Existing	1	5	7.8125%
Proposed	1	100	100%

From table 3. it can be inferred that the diffusion is of higher measurement in proposed work than that of existing work. This stands as a proof of better diffusion rate in the proposed work.

Confusion: The change of one letter in the key introduces changes in many letters of Cipher Text. It is present even in existing work but it is still more existent in proposed work because of treating the hash value of SSK as base for key generation instead of using the SSK value directly.The usage of hash makes the CT to change entirely upon modification of even a single bit in SSK. Let the SSK before change be ‘labmnophijkcdefg’and the SSK after change be ‘labmnoqhijkcdefg’. Figures 7and 8 show the Plain Text and corresponding Cipher Text before and after changing the key in existing work and proposed work. The confusion measurement is depicted in table 3.

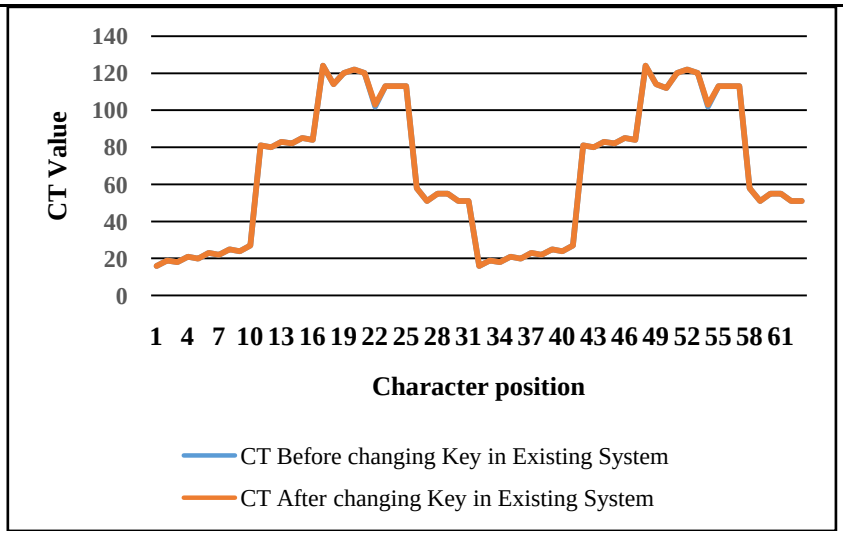

FIGURE 9. Confusion in existing work

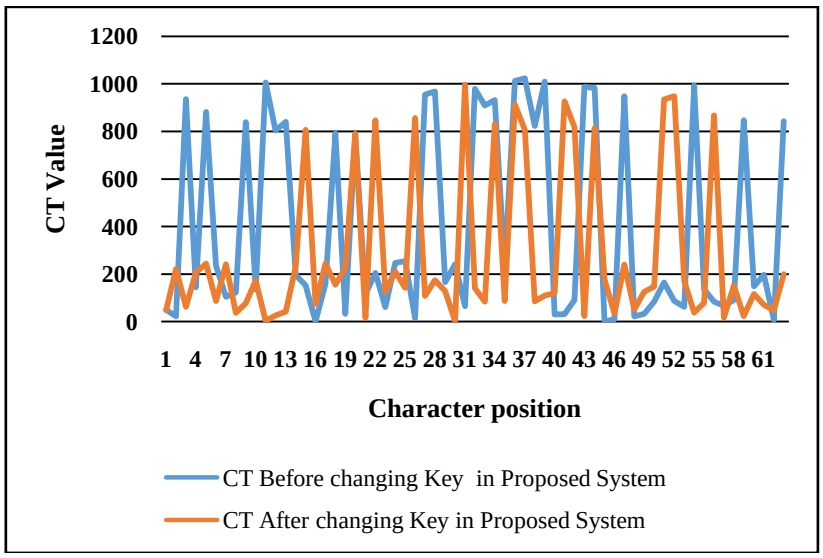

FIGURE 10. Confusion in proposed work

TABLE 4. Confusion measurement in both the works

Work	Number of Bits changed in Key	Number of characters changed in Cipher Text	Percentage of change in CT
Proposed	1	2	3.125%
Existing	1	64	100%

From table 4. it can be inferred that confusion rate of proposed work is higher than that of existing work. Since the hash of SSK is used in key generation, even a change of single letter in key contributes for change of entire Cipher Text. Thus key space of SSK will not exhaust.

Dot Is Not Treated As Delimiter: The proposed work does not treat dot as a delimiter, so the ASCII value of characters in one sentence affects another. But in the existing work the DRDP calculations are carried out locally within area bounded between delimiters.

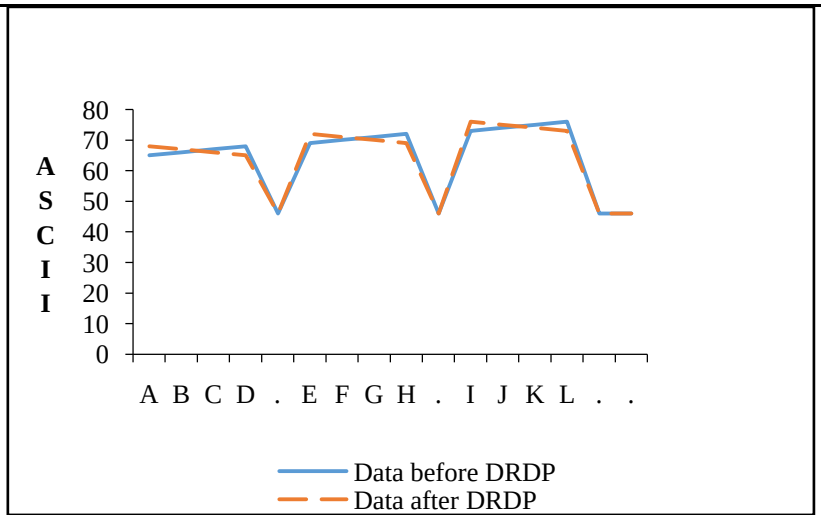

FIGURE 11. Chart depicting DRDP calculation of existing work

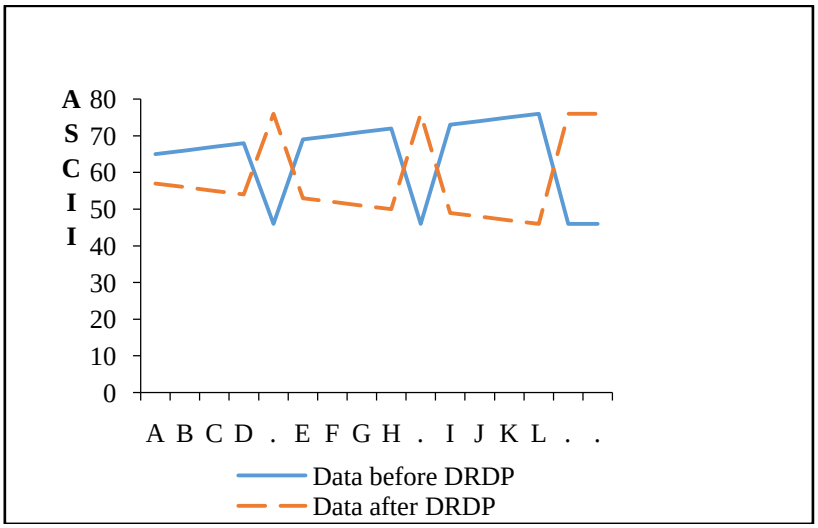

FIGURE 12. Chart depicting DRDP calculation of proposed work

Figures 11 and 12 represent the DRDP calculation in the existing work and proposed work respectively.

Unique Keys for Each Step: The proposed work aims to find unique keys for each step through key generation algorithms. But the existing work does not have that feature and employs same key for every subset, hence the confusion rate is very low.

Message Digest: The proposed work employs message digest which not only handle integrity but also authentication, since only the sender and receiver know the Shared Secret Key and only the unaltered messages are decrypted.But the existing work does not employ message digest, which leads to decryption of all the messages, which may sometime lead to fruitless decryption.

Padding Letter: The existing work use space as their default padding character. But the proposed Work uses the character corresponding to the average value of ASCII value of Plain Text. So the padding character varies from message to message, it is shown in fig 4.7 for the Plain Text “hello world hello world hello world”. The proposed work uses the average ASCII value of characters in Plain Text as padding byte, but the existing work uses space as the default padding byte. This leads to the same Plain Text getting padded differently in existing work and proposed work.

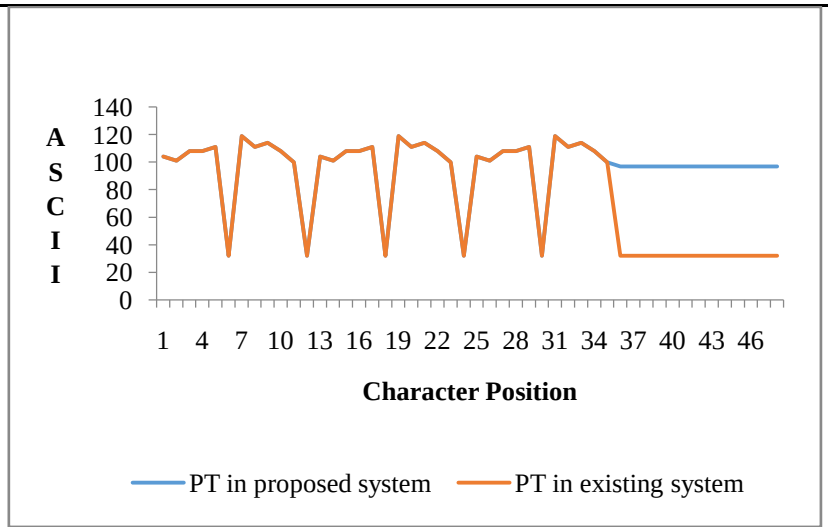

FIGURE 13. Chart depicting Plain Text ASCII values in existing and proposed work

Pattern In CT: There is no repeated pattern in CT of proposed work as each group of 16 characters are treated with different keys. The existing work uses same set of keys for treating group of 32 characters. So pattern gets repeated.Example consider the text, ”aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa”, it’s Cipher Text in existing workand proposed work is shown in figures 4.9 and 4.8.

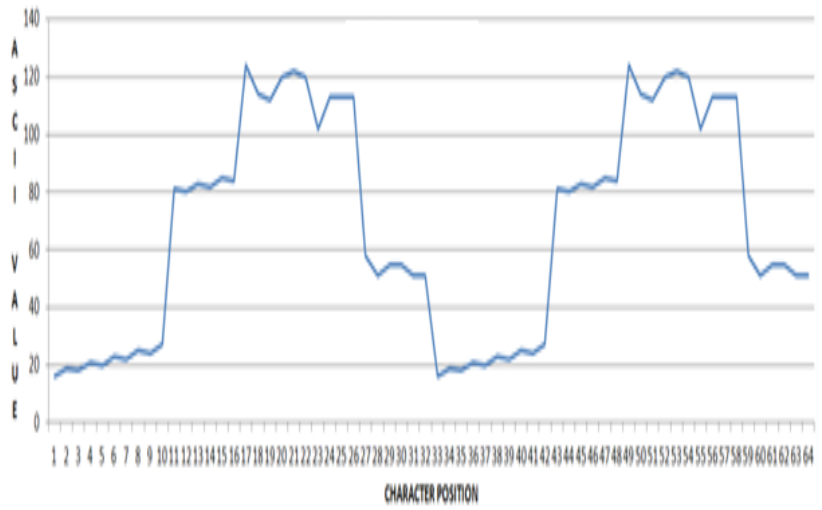

FIGURE 14. Chart depicting Cipher Text in existing work

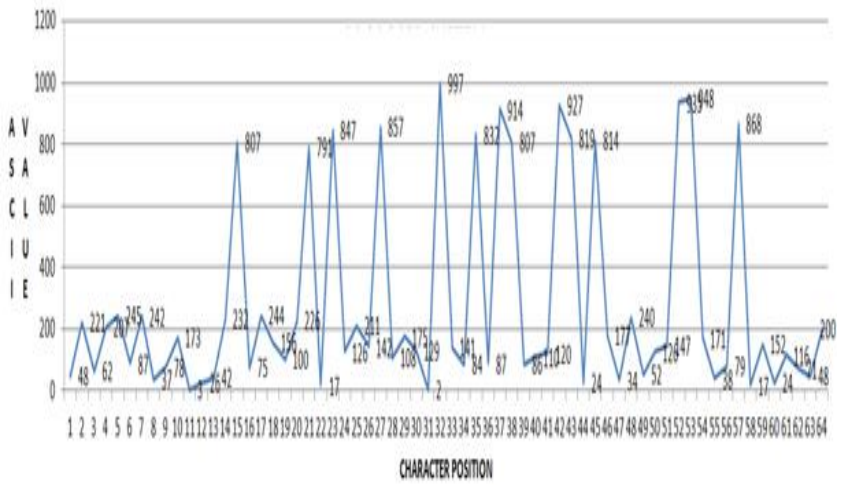

FIGURE 15. Chart depicting Cipher Text in proposed work

The rectangle portion in fig 4.8 shows the repeated portion of CT in existing work, which provides a rose bed for the

attacker. But the proposed work does not show off any such pattern.

Security Analysis: Traditionally, the privacy provided by a perturbation technique is measured by the variance between the actual and the perturbed values. This measure(S) is given by, S = Variance (X – X') / Variance (X), where X represents Plain Text ASCII value and X'represents the corresponding Cipher Text ASCII value.The higher S shows the higher protection level. [6] The variance of proposed work is 191.4223 and the variance of existing work is2.017213. Since the variance of proposed work is higher than that of existing work it can be inferred that the security level of proposed work is higher than that of existing workas shown in table 5.

TABLE 5. Variance calculation in existing work and proposed work

Work	Var(X)	Var(X-X')	Var(X-X') / Var(X)
Proposed	790.1025	151243.2	191.4223
Existing	1210.859	2442.561	2.017213

5. Conclusion

The security of information is of high concern and algorithms need to be powerful enough to serve all aspects of information security. In the past, hackers were highly skilled programmers who understood the details of the computer communications and how to exploit vulnerabilities. Today, anybody can hack by downloading tools from internet. These attacks have generated an increased need for network security and security policies. This research work has aimed to satisfy most of the aspect of information security in a vital way. The creation of digest for the Cipher Text makes out the decryption of messages to be carried out on receiver side only when the message is unaltered in transit and the Shared Secret Key provided by receiver must be same as the Shared Secret Key used by the sender, which only enables the creation of correct digest. The usage of EX-OR operation allows higher diffusion rate as the change in Plain Text is reflected in multiple places in Cipher Text. The work employs stream cipher which enables further confusion. Also the Cipher Text generation is dependent only on the Plain Text and no other external factors. The Cipher Text obtained for the message varies from time to time, since the Session Key is generated randomly each time. Thus by the above discussed features the proposed work poses to be more efficient than the existing work. The network security field may have to evolve to deal with the threats in future.

References

[1]. Abhilash G et al, "Advanced Symmetric Key Cryptography Using Extended MSA Method: BLZ Symmetric Key Algorithm", International Journal of Computer Science & Engineering Technology, Vol.2, issue 7, July 2012.

[2]. Bhandare Kumar Santosh, "Data Distortion Based Privacy Preserving Method for Data Mining Work", International Journal of Emerging Trends & Technology in Computer Science, Vol.2, issue 3, May -June 2013.

[3]. Ernastuti, "Perfect Shuffle Algorithm for Cryptography", ARPN Journal of Engineering and Applied Sciences, Vol.9, issue 12, December 2014.

[4]. Gupta Vishwa et al, "Advance Cryptography Algorithm for improving Data Security", International Journal of Advanced Research in Computer Science and Software Engineering, Vol.2, issue 1, January 2012.

[5]. Kumar Ramesh, Maram Balajee, Rao Lakshmana, "Encryption and Decryption Algorithm using 2-D Matrices", International Journal of Advanced Research in Computer Science and Software Engineering, Vol.3, Issue 4, April-2013.

[6]. Menezes Alfred et al,"Handbook of Applied Cryptography", CRC-Press, 1996.

[7]. Stallings William, "Cryptography and Network Security Principles and Practice", sixth edition, Pearson, 2014.