OPEN ACCESS

International Journal of Innovations in Science & Technology

IJIST
P ISSN : 2618-1630
E ISSN : 2909-6130

A Survey Paper on ASCII-Based Cryptographic Techniques

Abid Sultan[1], Yao Lin[2], Azhar Mushtaq[3]

[1,2] School of Software, Dalian University of Technology, China.

[3]Deparment of CS&IT University of Sargodha

* **Correspondence**: Abid Sultan and abidsultan006@gmail.com

Citation |Sultan. A Lin. Y, Mushtaq. A, "A Survey Paper on ASCII-Based Cryptographic Techniques," Int. J. Innov. Sci. Technol., vol. 4, no. 4 pp.1087-1098, 2022.

DOI: https://doi.org/ 10.33411/IJIST/2022040411

Received| Aug 31, 2022, **Revised**| Dec 13, 2022, **Accepted**| Dec 15, 2022, **Published**| Dec 17, 2022.

With the passage of time networking field has become much more advanced. Because of this advancement, the communicating parties don't want to rely on the third party for communication because a third party may misuse or share their personal information with someone else. That's why there is a need for such a method at which we can rely on secure communication. In recent years a lot of cryptographic techniques based on ASCII values have been proposed, but selecting an efficient and effective technique from them is a big task. In this paper, we have made a comparison among several techniques based on certain parameters to find out the best one for the ease of the users.

Keywords: Symmetric; Asymmetric; Encryption; Decryption; Memory Consumption and Complexity.

Introduction

Cryptography has become a major part of making our data secure. It has been used for several decades to secure and conceal important data. Some clues to the usage of cryptography were found in an engraving carved around 1900 BC in Egypt. The scribe used different hieroglyphic symbols. Their intention was not to hide the message but maybe they wanted to change its form anyway.

The authors got motivated by the papers of Udepal Singh, Upasna Garg [1], and Akanksha Mathur [2]. The reason behind the author's motivation is that the author wanted to find a secure technique for the process of communication. The author studied about 50 papers to compare which technique will be an efficient and effective one. The author aims to provide ease to people who want to perform secure communication.

Security has been a major concern for the last few years. A lot of researchers have proposed various techniques for improving security while utilizing the cryptographic technique. To some extent, cryptography came as a solution for secure communication. Cryptography plays an important role in securing crucial data from hackers or any third party. It enables the protection of the data by converting it into an unintelligible format so that only authorized users can be able to approach the data by changing it into the initial form [3]. Cryptography enables us to protect susceptible or sensitive data and to transmit it through unassured networks just like the internet so that the shared data can't be read by anybody besides the supposed recipients [4]. Cryptography includes encryption and decryption processes. The conversion of plain text to cipher text with the help of a key is known as encryption, while the conversion of cipher text to plain text by using a key is known as decryption. Cryptography is of two types Symmetric Encryption and Asymmetric Encryption.

In symmetric encryption, only a single key is used for both encryption and decryption processes. Encryption and decryption key is kept secret from intruders and is accessible to only authorized users [1]. The secrecy of encryption and decryption keys defines how strong the symmetric encryption is.

In asymmetric encryption, two different keys are used for encryption and decryption processes. The key which is used for encryption is known as the public key. While the key which is used for decryption is known as a private key and it must be kept secret from Intruders[1]. The asymmetric key is granted to the users through message authentication detection which is a safe method.

Gradually, the intruders or hackers became enough smart to break the old techniques that were used to secure the data, so it brought a need for such techniques that could be used to secure the data from that intruder. Then as a result some new and efficient techniques were invented such as AES (Advanced Encryption Standard), and DES (Data Encryption Standard), which have increased the difficulty level for intruders in the process of stealing data or decoding it. DES provides generally less security as compared to AES. DES shorts for Data Encryption Standard. It is an asymmetric key encryption algorithm that uses a key that is 56 bits in size. The encryption is done in 16 rounds in this technique. This technique is comparatively considered a weaker one because it can easily be broken by a Brute-force attack [5]. AES shorts for Advanced Encryption Standard. AES provides more security as compared to DES because it uses blocks and keys of greater length. In AES block size is fixed which is 128 bits [5]. The size of the key can be different which are 128, 192, and 256 bits. There are three different rounds in AES 10, 12, and 14 which can be used depending on the size of the key. Although these techniques are quite efficient and hard to break still it does not ensure 100% safety of the data.

ASCII shorts for American Standard Code for Information Interchange. ASCII codes were standardized in 1982 as a source of storing and transmitting data like English texts. That standard code consists of 32 non-displayed control characters and 96 displayed alphanumeric and other characters. Every letter or other symbol has been given a number from 0 to 128, for example, 33 for! 36 for $, 65 for A, 66 for B, 97 for a, and 98 for b. The main aim of ASCII codes is to produce adaptability among electronic networks or devices so that data can be shared and received successfully. ASCII codes were not compatible with complex texts or data that's why an Extended ASCII has been developed which contains some advanced symbols that are suitable for complex texts. An ASCII art is just like a matrix of ASCII codes that will combine to produce an original image. The main aim of ASCII art is to interact as a substitute for graphics in such conditions where graphics communication is impossible [6].

This paper has been organized into the following sections. The first section describes the introduction of cryptography and ASCII. The proposed work based upon certain parameters has been defined in the second section. The third section defines the comparative analysis among different values based on certain parameters. While the fourth section represents the results based on the comparison that the authors have made in this paper.

Through this paper, we should be able to achieve certain contributions which are defined below.

1. There is no need to waste your time searching for which technique is best for cryptography.
2. As this paper comes up with an efficient technique, so by using this technique people will be able to do secure communication.
3. Resulted technique comes with the trusted method to perform effective communication and is generally much stronger than any other technique.

Literature Review

As the ASCII-based cryptographic techniques have been mainly focused on in recent years, so we have made a comparison of ASCII-based cryptographic techniques to find out which technique will be efficient for secure communication. We have defined certain parameters here on which cryptography is mainly based. A lot of authors proposed various aspects of cryptography but still, there were some limitations in their algorithms.

Dur-E-Shawar Agha et al. [7] came up with a technique based on symmetric key encryption that uses ASCII codes, ROT13, and modulus functions to develop a key of any random size. For encryption plain text is converted into ASCII values then apply modulus function and XOR generates the ciphertext.

Veerpal Kaur and Ramanpreet Kaur [8] worked on an efficient technique for data compression which involves ASCII codes, binary codes, numeric codes, and symbols for generating the ciphertext.

Akanksha Mathur [9] defined an algorithm using ASCII values which are asymmetric encryption algorithms. It uses only one key for encryption and decryption but with a little bit of change in it. The limitation is that it only executes when the plain text's length and the key's length will be the same.

M.Lavanya et al. [10] came up with a technique known as RANS_ASC encryption that performs substitution cipher based on ASCII values. It is an asymmetric key encryption algorithm. The plain text is converted into a floating number. The main benefit of floating numbers is that it makes the Brute Force attack impossible because of their key which is the floating-point number. That's why the probability to predict the key is almost impossible, which is its strength.

Er. Suraj Arya and Dr. Ankit Kumar [11] proposed an algorithm in which the length of the input string will be incrementally added to the ASCII values, then it will produce symbols based on the resultant added ASCII value.

Deepak and Parveen [12] proposed an algorithm for making data secure. It involves writing the words at an odd position first and then writing the words that are at an even position. The key length does not rely on the plain text's length. It includes taking the binary of ASCII values then adding the binary of key and PT and finally taking 2's complement.

Mahmudul Hasan Moon, Md. Palash Uddin et al. [13] defined an algorithm for making the data secure. This algorithm performs three-level encryption. This technique can't be broken through a Brute-force attack because of increased unprintable characters. Thus, this algorithm ensures the high-level security of our data. The only flaw of this algorithm is that it consumes greater memory as compared to the original data.

In this paper [14], Yuki Nanjo, Md. Al-Amin Khandaker et al clarified the techniques for pairing implementation on BN (Barreto-Naehrig) curve for 128-bit security level in IoT. To increase, the level of security authors also describes the scalar multiplication in G1 and G2 groups along with G3 exponentiation.

Shijie Yan, Ping Zhen, et al. [15] proposed an efficient technique PS-CPPKC that depends on a random oracle that is a productive technique to assess the security of CPPKC (Chebyshev polynomials-based public key cryptosystem). The authors make use of the one-way hash function to improve the security of CPPKC, which is its advantage.

Proposed work

To decide the best ASCII-based cryptography techniques, this paper has proposed the following four parameters on which previous techniques will be evaluated.

1. Execution time
2. Complexity
3. Memory Consumption
4. Data Limit
5. Shifting operation

Execution time

Execution time is the time during which plain text is converted into Cipher text. Execution time has a major impact on cryptography. If the execution time is greater, then it will not be efficient while on the other hand if the execution time is less then it will be considered an efficient technique [13]. By increasing the complexity, the execution time will also increase.

Complexity

Complexity refers to how complex or strong the cryptographic technique is. Security directly relies on complexity. If we increase the steps of the cryptographic technique the complexity will also increase. The lesser the number of steps lesser will be the less complex it will be easy for the cryptographic analyst to break that technique [13].

Memory consumption

Memory consumption refers to the memory that is consumed by the system while performing the process of cryptography. Memory consumption also plays a vital role in the cryptographic technique. It is inversely proportional to the cryptographic technique. If it consumes greater memory of the system, then it possibly slows down your system's speed and vice versa.

Data limit

The data limit represents how much data a cryptographic technique can encrypt. Whether it can encrypt a single line, a paragraph, or a file. The technique which will be able to encrypt large data such as files will be considered an efficient technique.

Shifting operation

The shifting operation involves the shifting of bits based on the nature of that technique. Shifting can either be left or right. In right shifting the number of specific bits will be shifted to the left side, while in the left shifting the number of specific bits will be shifted to the right side. Shifting enhances the security of the techniques by creating random results. Due to this, the intruders can't be able to crack the techniques

Results

According to the table.2, we conclude that paper No.1 [3] is one of the best papers that makes use of almost four parameters, which we chose for the evaluation of the defined schemes.

The proposed scheme [3] uses XOR and One Time padding computation for encryption. The most efficient point of this scheme is two randomly generated used for encryption. The key length is dependent on the size or length of plaintext and is used XOR operation and One-time padding. These mentioned computations are used in this paper for encryption.

The execution time of the proposed system [3] was compared with the other system and its less than other schemes. Encryption time Comparison: DES & AES, Fixed length System, Proposed System (sec) [3]

Length of Plain text	DES	Fixed Key length	Proposed System
40	0.0672	0.0035	0.0032
60	0.0829	0.0042	0.0043
80	0.1098	0.0068	0.0052
100	0.1372	0.0071	0.0062

Length of Plain text	AES	Fixed Key length	Proposed System
40	0.58	0.0032	0.0033
60	0.87	0.0052	0.0042
80	1.15	0.0064	0.0053
100	1.44	0.0069	0.0064

In order to enhance the security of the system three levels of security are utilized, XOR Operation, One Time padding, and Watermarking. The advantages of the mentioned method are as follows

1. A more secure system.
2. Less vulnerable to attacks by a cryptanalyst.
3. Key-length changes iteration by iteration make it difficult to guess key length.
4. The main and most important strength is system has very less execution as compared to others.

Table 1. Comparative Analysis of Selected Parameters

<table>
<tr><th>Paper No.</th><th>Execution Time</th><th>Complexity</th><th>Memory Consumption</th><th>Data Limit</th><th>Shifting Operation</th></tr>
<tr><td>Paper 1[3]</td><td><table><tr><td>Length of PT</td><td>Fixed key length</td><td>Execution Time(sec)</td></tr><tr><td>40</td><td>0.0035</td><td>0.0032</td></tr><tr><td>60</td><td>0.0042</td><td>0.0043</td></tr><tr><td>80</td><td>0.0068</td><td>0.0052</td></tr><tr><td>100</td><td>0.0071</td><td>0.0062</td></tr></table></td><td>The techniques used in this paper for encryption are Modulus operation, right shifting, and XOR operation.</td><td>It has not been defined by the author.</td><td>Can encrypt audio files, video files as well as images</td><td>The right Shifting of keys needs to be done one time.</td></tr>
<tr><td>Paper 2 [1]</td><td>The author did not mention the execution time.</td><td>This paper involves Modulus operation and right-shifting methods for encryption.</td><td>This attribute was not in consideration by the author.</td><td>The author did not consider a data limit.</td><td>The right Shifting of keys needs to be done one time.</td></tr>
<tr><td>Paper 3[7]</td><td><table><tr><td>Input size in(Kb)</td><td>Execution Time in(sec)</td></tr><tr><td>20</td><td>0.00600</td></tr><tr><td>36</td><td>0.01002</td></tr><tr><td>45</td><td>0.02003</td></tr><tr><td>59</td><td>0.04207</td></tr><tr><td>69</td><td>0.07037</td></tr></table></td><td>For encryption, this method involves applying ROT 13, modulus operation, and then performing XOR of the key.</td><td>It was not defined by the author.</td><td>No clue is given about this parameter.</td><td>No attention was given to this parameter.</td></tr>
<tr><td>Paper 4[8]</td><td>, The author did not take this attribute as an important one.</td><td>In this paper authors assigned numerical codes to unique symbols, adding 0's in MSB bits until it is divisible by 8 for making secure communication.</td><td>Less memory consumption (consumes less memory while cryptography is being performed).</td><td>No limit on data length (The amount of data to be encrypted is not specified).</td><td>This one was not focused on by the author.</td></tr>
</table>

<table>
<tr>
<td>Paper 5[2]</td>
<td><table><tr><td>Size of PT</td><td>Execution Time</td></tr><tr><td>2</td><td>322</td></tr><tr><td>4</td><td>3679</td></tr><tr><td>6</td><td>3861</td></tr><tr><td>8</td><td>4748</td></tr><tr><td>10</td><td>5543</td></tr></table></td>
<td>The operations used for encryption in this paper are taking modulus, after that converting it into binary values, and then finally performing the right circular shifting of binary values.</td>
<td>This parameter was not specified by the author.</td>
<td>There is no clarification about this parameter.</td>
<td>It includes performing the right circular shifting of binary values(n times where n is the length of input).</td>
</tr>
<tr>
<td>Paper 6[13]</td>
<td>This one is not mentioned by the author.</td>
<td>This paper only uses a vigenere table with a key for increasing security.</td>
<td>Less memory consumption</td>
<td>, The author took no interest in this parameter.</td>
<td>The author did not use this parameter in the paper.</td>
</tr>
<tr>
<td>Paper 7[16]</td>
<td><table><tr><td>Size of PT</td><td>Execution time in ms</td></tr><tr><td>2</td><td>15</td></tr><tr><td>4</td><td>15</td></tr><tr><td>6</td><td>16</td></tr><tr><td>8</td><td>16</td></tr><tr><td>10</td><td>30</td></tr></table></td>
<td>The proposed method involves operations of taking modulus for each value with min value of character ASCII codes, then the same for KEY.</td>
<td>The author paid no attention to this parameter.</td>
<td>This attribute was not relevant to the author's work.</td>
<td>Not discussed by the author.</td>
</tr>
<tr>
<td>Paper 8[17]</td>
<td><table><tr><td>Size</td><td>Execution Time /Kb</td></tr><tr><td>27.8</td><td>0</td></tr><tr><td>69.5</td><td>0</td></tr><tr><td>81.8</td><td>0.000672</td></tr><tr><td>103</td><td>0.000533</td></tr><tr><td>599</td><td>0.000367</td></tr></table></td>
<td>Not properly determined by the author.</td>
<td>This was not defined in the paper.</td>
<td>Only specific files can be encrypted</td>
<td>, The author did not put it to use.</td>
</tr>
<tr>
<td>Paper 9[18]</td>
<td>, The author did not properly show this parameter.</td>
<td>The most efficient operations involved in the proposed method are adding random characters at the start and end of the text and then taking the modulus.</td>
<td>Not considered by the author of the paper.</td>
<td>Can encrypt messages as well as files</td>
<td>The author paid no consideration to this parameter.</td>
</tr>
</table>

<table>
<tr>
<td>Paper 10[19]</td>
<td><table><tr><td>Size of PT</td><td>Execution Time for 16 bits</td><td>Execution Time for 32 bits</td></tr><tr><td>2</td><td>15</td><td>31</td></tr><tr><td>4</td><td>16</td><td>33</td></tr><tr><td>6</td><td>26</td><td>42</td></tr><tr><td>8</td><td>37</td><td>67</td></tr><tr><td>10</td><td>52</td><td>98</td></tr></table></td>
<td>The technique proposed by the authors involves the process of generating the key and adding a key in plain text. After that right shifting is done then finally taking 2's complement.</td>
<td>No consideration by the author about this parameter.</td>
<td>It is not mentioned in the paper.</td>
<td>It performs the right shifting of the output of step 5 one time.</td>
</tr>
<tr>
<td>Paper 11[20]</td>
<td><table><tr><td>File size in (kb)</td><td>Execution time in (msec)</td></tr><tr><td>50</td><td>512</td></tr><tr><td>100</td><td>1064</td></tr><tr><td>250</td><td>2462</td></tr><tr><td>512</td><td>2834</td></tr></table></td>
<td>The major methods used in this paper include the generation of the magic rectangle, mapping with the magic rectangle, and encryption with RSA and N-prime RSA</td>
<td>This parameter was not described in the paper.</td>
<td>It is not mentioned by the author.</td>
<td>This parameter was not related to the author's work.</td>
</tr>
<tr>
<td>Paper 12[21]</td>
<td>This parameter was not examined by the author of the paper.</td>
<td>The proposed method involves the main operations of generating an OTP having a length corresponding to a single digit, generating ASCII for each OTP, a Key is generated by performing an XOR operation, and finally, the resulted value is further XORED with a predefined XOR Constant</td>
<td>This parameter was not defined in the paper.</td>
<td>This technique can be used to encrypt not only a single word but also messages with n number of words</td>
<td>This one was not focused on in the paper.</td>
</tr>
<tr>
<td>Paper 13[22]</td>
<td><table><tr><td>Text size</td><td>Execution time in (sec)</td></tr><tr><td>1.2 Mb.txt</td><td>0:01:03</td></tr><tr><td>440 kb.txt</td><td>0:01:11</td></tr></table></td>
<td>It was not clarified by the author.</td>
<td>This parameter was not mentioned in the paper.</td>
<td>This technique can work efficiently with a 2 Mb file</td>
<td>This was not included by the author.</td>
</tr>
</table>

	150 kb.txt 0:00:06 28 kb.txt 0:00:02				

Table 2. Parameters Highlighted in Papers

Execution time	Complexity	Memory consumption	Data Limit	Shifting Operation
Execution time is given by the Paper No. 2[3], 5[2], 10[19], 11[20], 13[22], 17[23],18[24],20[25]	Paper No. 1[1], 2[3], 3[8], 4[16], 5[2], 9[18], 10[19], 11[20], 12[21],14[26], 15[27], clarified about complexity.	The author mentioned memory consumption in Paper No. 3[2], 16[28],22[29]	A description of the data limit is given in paper no. 2[3], 3[8], 12[21], 13[22], 21[30]	Shifting operations have been used in paper no. 1[1], 2[3], 19[31]

Conclusion

Our focus is to make communication secure to prevent the data from intruder attacks and to perform efficient communication. By comparing previous papers based on certain parameters that we have defined, we can find the best technique for secure communication. We have studied around 50 ASCII-based papers, but we find that only 20 papers were relevant to our proposed parameters. It has been a challenging task for us to find which technique is the best. Finally, we came up with an efficient technique. Based on certain circumstances with regards to execution time, complexity, data limit, and shifting operations, we have concluded that paper No. 1[3] "An ASCII Value-based Optimized Text data Encryption System" of Roofee Sultana will be the most efficient while making efficient and effective communication. Because as compared to other techniques its security, and execution time is much more efficient than other techniques and supports multiple types of data. It clarifies the maximum number of parameters due to which it shows effective results. The plus point of using this technique will be that it will be faster, more securer, and supports multiple types of data.

References

[1] U. Singh and U. Garg, "An ASCII value based text data encryption System," vol. 3, no. 11, pp. 1–5, 2013.

[2] A. Mathur, "A Research paper: An ASCII value based data encryption algorithm and its comparison with other symmetric data encryption algorithms," undefined, 2012.

[3] R. Sultana and T. M. Kumari, "An ASCII Value based Optimized Text data," pp. 6650–6656, 2016, doi: 10.15662/IJAREEIE.2016.0508008.

[4] C. J. et al S.G. Rohini, "ASCII BASED SYMMETRIC KEY ALGORITHM FOR DATA SECURITY," vol. 116, no. 5, pp. 75–80, 2017.

[5] H. O. Alanazi, B. B. Zaidan, A. A. Zaidan, H. A. Jalab, M. Shabbir, and Y. Al-Nabhani, "New Comparative Study Between DES, 3DES and AES within Nine Factors," vol. 2, Mar. 2010, doi: 10.48550/arxiv.1003.4085.

[6] Y. Takeuchi, D. Takafuji, Y. Ito, and K. Nakano, "ASCII art generation using the local exhaustive search on the GPU," Proc. - 2013 1st Int. Symp. Comput. Networking, CANDAR 2013, pp. 194–200, 2013, doi: 10.1109/CANDAR.2013.35.

[7] D.-E.-S. Agha, S. Ali Khan, H. Fakhruddin, and H. H. Rizvi, "Security Enhancing by using ASCII Values and Substitution Technique for Symmetric Key Cryptography," Indian J. Sci. Technol., vol. 10, no. 36, pp. 1–6, Sep. 2017, doi: 10.17485/IJST/2017/V10I36/119181.

[8] R. K. Veerpal Kaur, "An Advanced Text Encryption &amp; Compression System Based on ASCII Values &amp; Arithmetic Encoding to Improve Data Security," vol. 3, no. 4, 2015, Accessed: Sep. 13, 2022. [Online]. Available: https://www.academia.edu/8628575/An_Advanced_Text_Encryption_and_Compression_System_Based_on_ASCII_Values_and_Arithmetic_Encoding_to_Improve_Data_Security

[9] M. Lavanya, R. Vijay Sai, A. Festina, J. Eshwari, T. Manopriya, and V. Vaithiyanathan, "An encryption algorithm functioning on ASCII values and random number generation," Indian J. Sci. Technol., vol. 8, no. 35, Dec. 2015, doi: 10.17485/IJST/2015/V8I35/86673.

[10] E. S. Arya and A. Kumar, "Ascii Based Encryption Decryption Technique for Information Security and Communication," 3rd Int. Conf. Innov. trends Sci. Eng. Manag. YMCA connaught place, New Delhi, 7th January, pp. 25–33, 2017.

[11] D. D. and P. P., "Modern Encryption and Decryption Algorithm based on ASCII Value and Binary Operations," Int. J. Comput. Appl., vol. 172, no. 1, pp. 30–34, 2017, doi: 10.5120/ijca2017915060.

[12] M. H. Moon, M. P. Uddin, M. I. Afjal, M. Al Mamun, M. A. Marjan, and M. Nitu, "A Cryptographic Algorithm Based on ASCII and Number System Conversions along with a Cyclic Mathematical Function," 5th Int. Conf. Comput. Commun. Chem. Mater. Electron. Eng. IC4ME2 2019, Jul. 2019, doi: 10.1109/IC4ME247184.2019.9036706.

[13] K. Goyal, T. Kumar, D. Garg, and P. Thakral, "Cryptography : A Game Play Using ASCII Conversion," no. March 2019, 2018.

[14] Y. Nanjo, M. A. A. Khandaker, T. Kusaka, and Y. Nogami, "Efficient pairing-based cryptography on raspberry Pi," J. Commun., vol. 13, no. 2, pp. 88–93, 2018, doi: 10.12720/jcm.13.2.88-93.

[15] S. Yan, P. Zhen, and L. Min, "Provably secure public key cryptosystem based on chebyshev polynomials," J. Commun., vol. 10, no. 6, pp. 380–384, 2015, doi: 10.12720/jcm.10.6.380-384.

[16] S. R. Shinge and R. Patil, "An Encryption Algorithm Based on ASCII Value of Data," Int. J. Comput. Sci. Inf. Technol., vol. 5, no. 6, pp. 7232–7234, 2014.

[17] M. M. Rahman, "Any File Encryption by Translating ASCII Value of Characters," Int. J. Adv. Res. Comput. Sci., vol. 3, no. 2, pp. 41–43, 2012, doi: 10.26483/IJARCS.V3I2.1032.

[18] D. Vegad, "Character Based Encryption and Decryption using Modulo Arithmatic," vol. 1, no. 10, pp. 57–60, 2015.

[19] F. Qazi, F. H. Khan, K. N. Kiani, S. Ahmed, and S. A. Khan, "Enhancing the Security of Communication Using Encryption Algorithm Based on ASCII Values of Data," Int. J. Secur. Its Appl., vol. 11, no. 2, pp. 59–68, 2017, doi: 10.14257/ijsia.2017.11.2.06.

[20] V. G. et al Hardik Gandhi, "A Research on Enhancing Public Key Cryptography by the Use of MRGA with RSA and N-Prime RSA," vol. 1, no. 12, 2015, Accessed: Sep. 13, 2022. [Online]. Available: https://www.academia.edu/16075924/A_Research_on_Enhancing_Public_Key_Cryptography_by_the_Use_of_MRGA_with_RSA_and_N_Prime_RSA

[21] A. Olkar, "ASCII Based Text Encryption and Decryption With Check For Data Integrity," vol. 4, no. 12, pp. 10–12, 2015, doi: 10.17148/IJARCCE.2015.412109.

[22] K. KumarPandey, V. Rangari, and S. Kumar Sinha, "An Enhanced Symmetric Key Cryptography Algorithm to Improve Data Security," Int. J. Comput. Appl., vol. 74, no. 20, pp. 29–33, 2013, doi: 10.5120/13028-0215.

[23] W. Zhang, Y. Zhao, and S. Fan, "Cryptosystem Identification Scheme Based on ASCII Code Statistics," Secur. Commun. Networks, vol. 2020, 2020, doi: 10.1155/2020/8875864.

[24] B. Dhanuja, B. Prabadevi, K. Bhavani Shankari, and G. Sathiya, "E-REA Symmetric Key Cryptographic Technique," Int. Conf. Emerg. Trends Inf. Technol. Eng. ic-ETITE 2020, Feb. 2020, doi: 10.1109/IC-ETITE47903.2020.38.

[25] K. Gupta and S. Singh, "DNA Based Cryptographic Techniques: A Review," Int. J. Adv. Res. Comput. Sci. Softw. Eng., vol. 3, no. 3, p. 2277, 2013, doi: 10.6633/IJNS.201811.

[26] N. A. N. Abdullah et al., "a Theoretical Comparative Analysis of Dna Techniques Used in Dna Based Cryptography," J. Sustain. Sci. Manag., vol. 17, no. 5, pp. 165–178, 2022, doi: 10.46754/jssm.2022.05.014.

[27] M. Faheem, S. Jamel, A. Hassan, Z. A., N. Shafinaz, and M. Mat, "A Survey on the Cryptographic Encryption Algorithms," Int. J. Adv. Comput. Sci. Appl., vol. 8, no. 11, 2017, doi: 10.14569/ijacsa.2017.081141.

[28] D. Garg, K. K. Bhatia, and S. Gupta, "A novel Genetic Algorithm based Encryption Technique for Securing Data on Fog Network Using DNA Cryptography," Proc. 2nd

Int. Conf. Innov. Pract. Technol. Manag. ICIPTM 2022, pp. 362–368, 2022, doi: 10.1109/ICIPTM54933.2022.9754031.

[29] P. Dixit, A. K. Gupta, M. C. Trivedi, and V. K. Yadav, "Traditional and hybrid encryption techniques: A survey," Lect. Notes Data Eng. Commun. Technol., vol. 4, no. June, pp. 239–248, 2018, doi: 10.1007/978-981-10-4600-1_22.

[30] N. Saqib and S. S. Shekhawat, "Securing Wireless Sensor Networks Using Elliptic Curve Cryptography," Int. J. Eng. Trends Technol., vol. 56, no. 1, pp. 7–11, 2018, doi: 10.14445/22315381/ijett-v56p202.

[31] S. Kumar, M. S. Gaur, P. Sagar Sharma, and D. Munjal, "A Novel Approach of Symmetric Key Cryptography," Proc. 2021 2nd Int. Conf. Intell. Eng. Manag. ICIEM 2021, pp. 593–598, Apr. 2021, doi: 10.1109/ICIEM51511.2021.9445343.