INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 6.078
(Volume 6, Issue 4)
Available online at: https://www.ijariit.com

Manna cipher

Neelanjan Manna
neelanjanmanna1997@gmail.com
Vellore Institute of Technology, Vellore, Tamil Nadu

ABSTRACT

This document gives an overview of solving the limitations of cipher text formatting while implementing cryptography techniques on computers. The Manna Cipher uses the numbering system to represent ciphers rather than alphanumeric characters.The aim is to create a ciphering standard which is painstakingly difficult to crack even using the latest super computers. This document will be focusing on the plain text the resultant cipher text and the run time to have a fair idea about the performance.

Keywords— *Manna Cipher, cryptography , mathematical cipher model , uncrackable cipher.*

1. INTRODUCTIO

Cryptography is the training and investigation of methods for secure correspondence within the sight of outsiders called enemies. All the more for the most part, cryptography is tied in with building and investigating conventions that keep outsiders or people in general from perusing private messages. Different angles in data security, for example, information secrecy, information respectability, validation, and non-revocation are vital to current cryptography standards. Present day cryptography exists at the convergence of the orders of arithmetic, software engineering, electrical building, correspondence science, and material science. Utilizations of cryptography incorporate electronic business, chip-based installment cards, computerized monetary forms, PC passwords, and military correspondences.

Cryptography preceding the cutting edge age was adequately equivalent with encryption, the change of data from an intelligible state to obvious rubbish. The originator of a scrambled message shares the unraveling strategy just with planned beneficiaries to block access from enemies. The cryptography writing regularly utilizes the names Alice ("A") for the sender, Bounce ("B") for the expected beneficiary, and Eve ("meddler") for the foe. Since the improvement of rotor figure machines in World War I and the approach of PCs in World War II, the techniques used to complete cryptology have gotten progressively intricate and its application increasingly across the board.

2. OBJECTIVES OF THE STUDY

- Manna cipher visualisation
- Time performance of the Manna Cipher.
- Identifying whether the time taken to process the cipher text varies by a huge degree due to increase in the length of the cipher

3. HYPOTHESES

3.1 Null hypotheses

H01: For the same encryption key the resultant cipher is the same
H02: The plain text and cipher text are always same in length
H03: Run time varies by a huge degree due to varying lengths of cipher text

3.2 Alternative Hypotheses

H11: For the same encryption key the resultant cipher is not same
H12: The plain text and cipher text are never same in length
H13: Run time does not vary by a huge degree due to varying lengths of cipher text

4. METHODOLOGY

4.1 The Configurations of The Computer Under Study

a) Windows 10 home edition
b) Intel i5 8th gen

c) GTX 1050ti
d) 8gb ddr4 ram
e) 1tb hdd
f) 128 gb ssd

4.2 Algorithm implementation
Using C

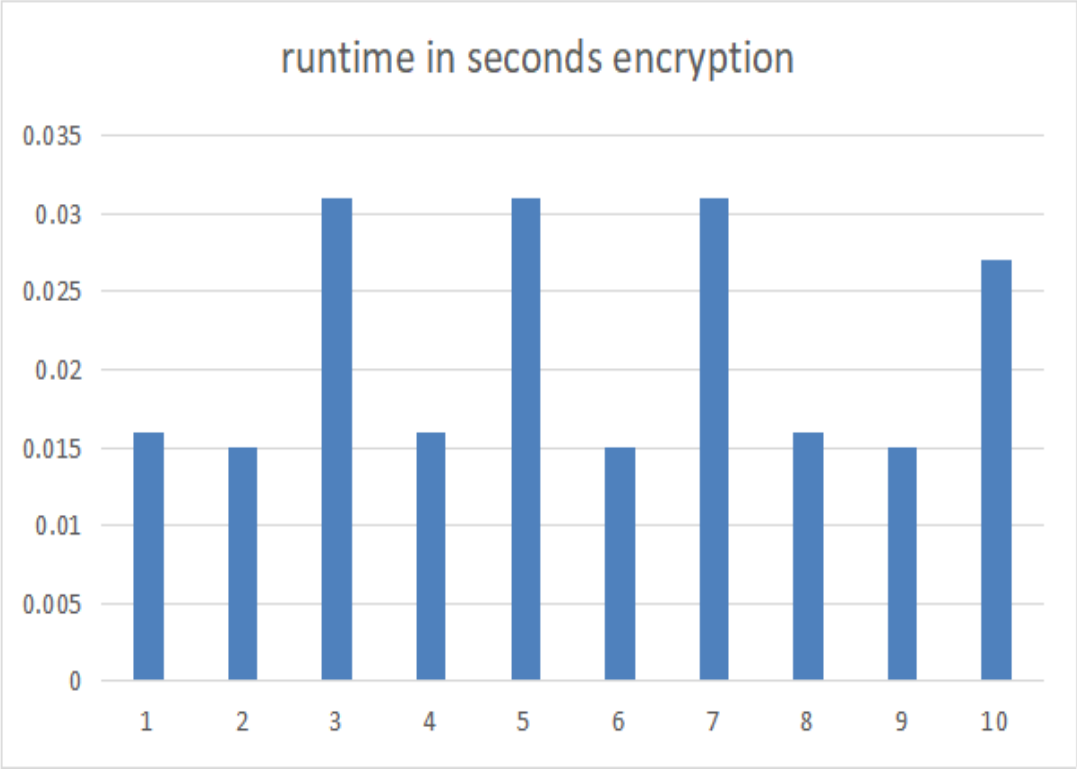

Fig. 1: Runtime in seconds encryption

In figure 1 the run time is depicted to encrypt a text file containing the text “hello world” with the password neel .The time taken to encrypt in seconds is depicted along y axis and the serial number of the encryption round is depicted along x axis.

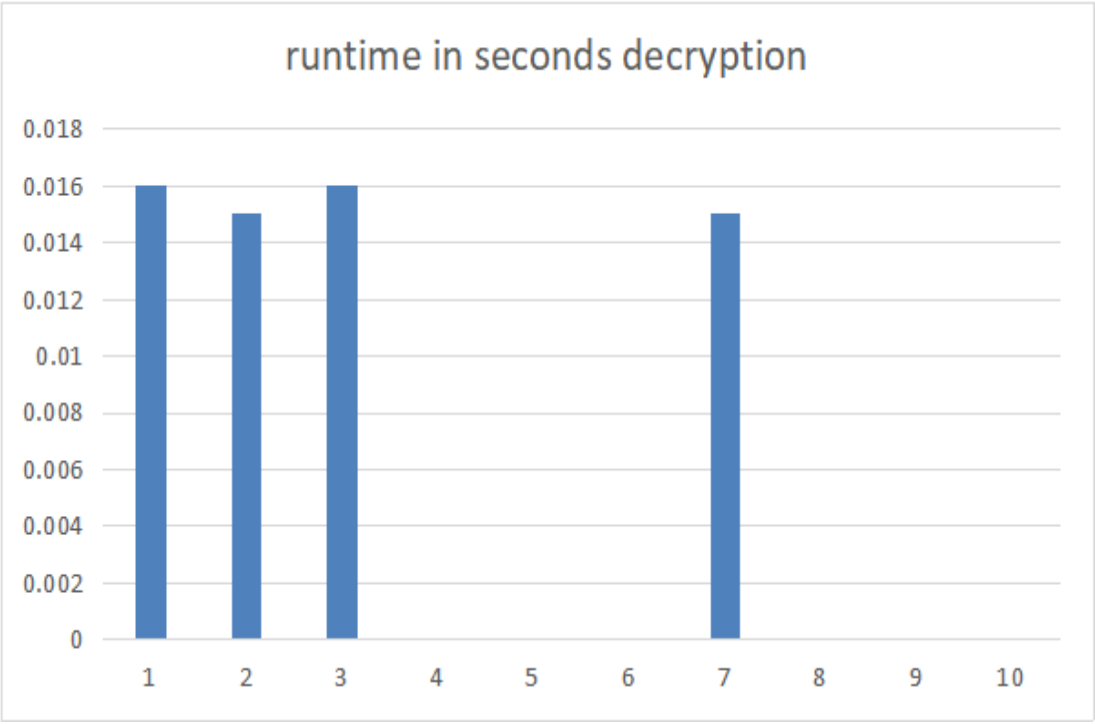

Fig. 2: Runtime in seconds decryption

In figure 2 the run time is depicted to decrypt a text file containing the Manna cipher with the password neel .The time taken to decrypt in seconds is depicted along y axis and the serial number of the decryption round is depicted along x axis.

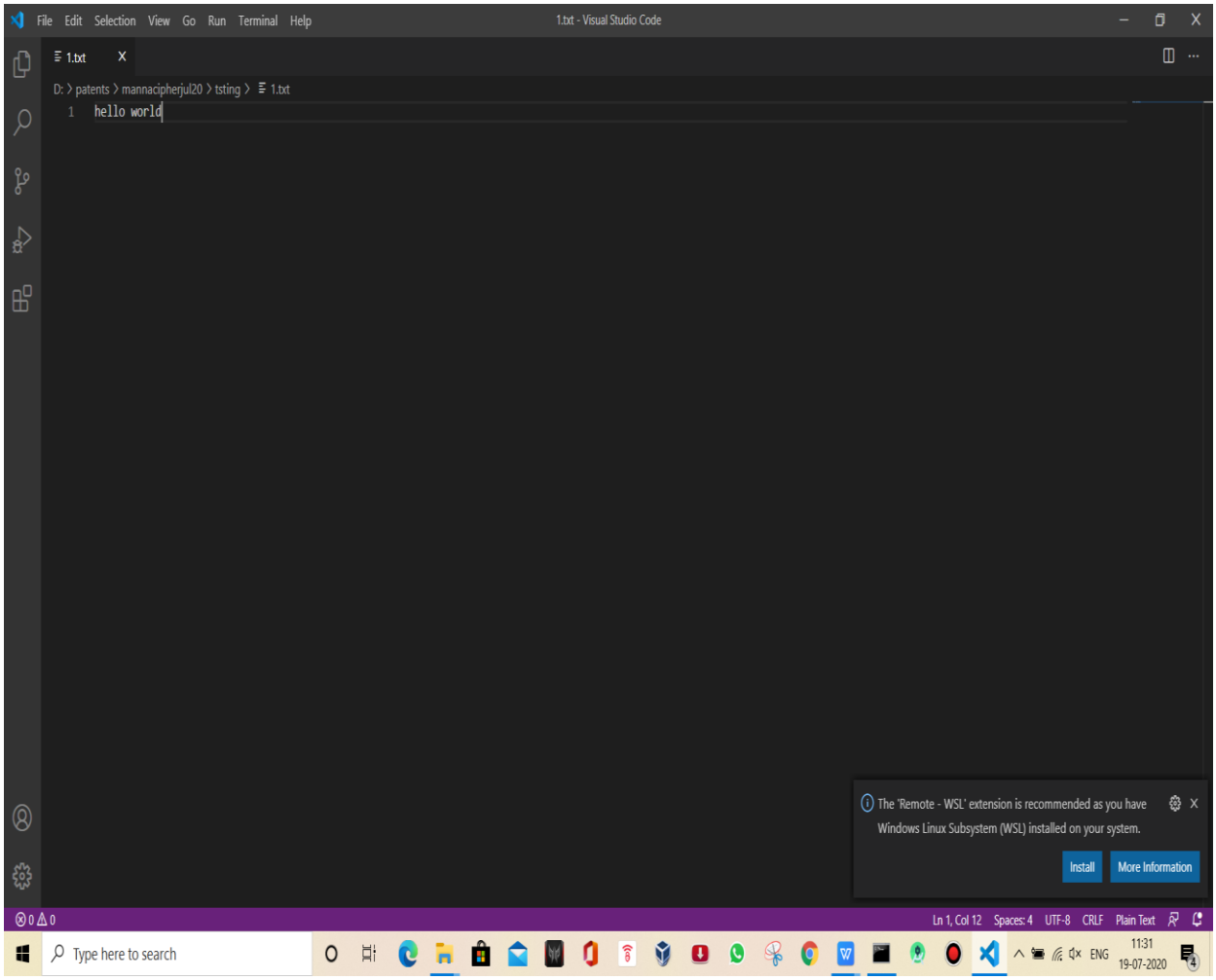

Fig. 3: The plain text before encrypting

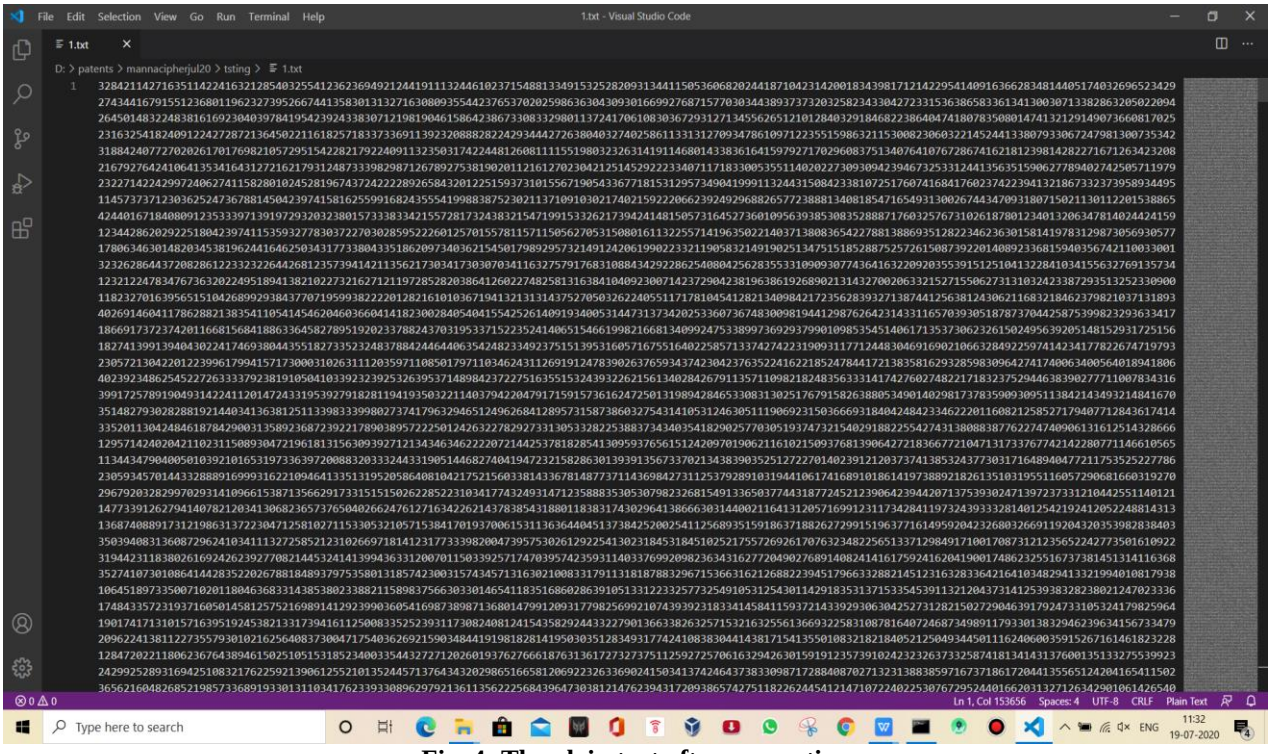

Fig. 4: The plain text after encrypting

6. CONCLUSION

From the above figures(Figure 1 and Figure 2) we can observe that the performance of the laptop used in the study the encryption algorithm is very fast to perform the encoding process and the decryption algorithm after running for three consecutive times using the same pass code takes only 0.015 seconds at maximum in the later decryption stages to decode the cipher. The plain text is given in Figure 3 and the cipher text is given in Figure 4.The performance analysis for larger plain texts will be the scope of my future research work.

7. REFERENCES

[1] F. L. Bauer, Decrypted Secrets. Springer, 2010<sup4< sup="">. ISBN 978-3-642-06383-1.
[2] Cipher A. Deavours/Louis Kruh, Machine Cryptography and Modern Cryptanalysis. Artech House, Norwood 1985. ISBN 0-89006-161-0.
[3] William F. Friedman, Elements of Cryptanalysis. Aegean Park Press, Laguna Hills 1976. ISBN 0-89412-002-6.
[4] William F. Friedman, Military Cryptanalysis, Part I, II, III, IV. 1938. Reprint: Aegean Park Press, Laguna Hills 1980. ISBN 0-89412-044-1, 0-89412-064-6, 0-89412-196-0, 0-89412-198-7.
[5] Helen Fouché Gaines, Cryptanalysis. Dover Publications, New York 1939, 1956(6). ISBN 0.486-20097-3.
[6] Walt Howe: Basic Cryptanalysis. US Army Field Manual 34-40-2. Aegean Park Press, Laguna Hills 1997.
[7] David Kahn, The Codebreakers. Macmillan, New York, 1967. ISBN 0-02-560460-0. 2. Auflage: Scribner, New York 1996.
[8] Simon Singh, The Code Book. Fourth Estate, London 1999.
[9] Solomon Kullback, Statistical Methods in Cryptanalysis. Aegean Park Press, Laguna Hills 1976. ISBN 0-89412-006-9.
[10] Randall K. Nichols, Classical Cryptography Course, Volume I & II. Aegean Park Press, Laguna Hills 1996. ISBN 0-89412-263-0 & 0-89412-264-9.
[11] Abraham Sinkov, Elementary Cryptanalysis. The Mathematical Association of America, Washington 1966. ISBN 0-88385-622-0.

