iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 8 **Issue:** VII **Month of publication:** July 2020

DOI: https://doi.org/10.22214/ijraset.2020.30556

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 8 Issue VII July 2020- Available at www.ijraset.com

Randomness of Manna Cipher with respect to RSA 512 SHA 512 and SHA 256

Neelanjan Manna
BCA ,The Heritage Academy . MCA , Vellore Institute of Technology

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 randomness and compare the randomness of SHA 512 SHA 256 and RSA 512.
Keywords: Manna Cipher , cryptography , mathematical cipher model , uncrackable cipher.

I. INTRODUCTION

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.

II. OBJECTIVES OF THE STUDY

A. Manna cipher randomness visualisation
B. The randomness of SHA 256
C. The randomness of SHA 512
D. The randomness of RSA 512
E. Comparison with Manna cipher

III. HYPOTHESES

A. Null Hypotheses

1) H01: The encrypted value of RSA 512 is highly random for the same plain text
2) H02: The encrypted value of SHA 256 is highly random for the same plain text
3) H03: The encrypted value of SHA 512 is highly random for the same plain text
4) H04: The Manna Cipher invented by Neelanjan Manna is less secure than RSA 512 , SHA 256 and SHA 512.

B. Alternative Hypotheses

1) H11: The encrypted value of RSA 512 is not at all random for the same plain text
2) H12: The encrypted value of SHA 512 is not at all random for the same plain text
3) H13: The encrypted value of SHA 256 is not at all random for the same plain text
4) H14 : The newly invented Manna Cipher by Neelanjan Manna is much more random and secure than RSA 512 SHA 256 and SHA 512, combined ,for the same plain text .

IV. METHODOLOGY

A. *The Configurations of The Computer Under Study*

1) Windows 10 home edition
2) Intel i5 8th gen
3) GTX 1050ti
4) 8gb ddr4 ram
5) 1tb hdd
6) 128 gb ssd

B. *Algorithm Implementation*

1) Using C

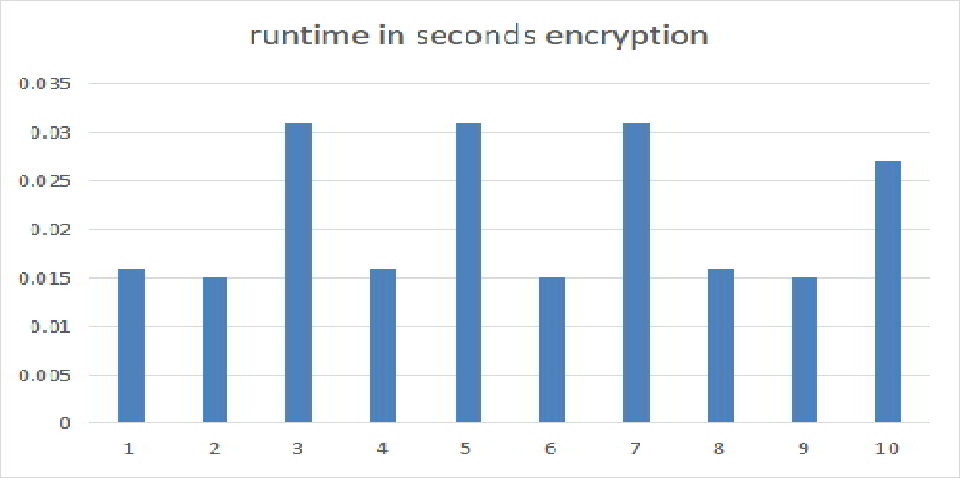


Figure 1

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.

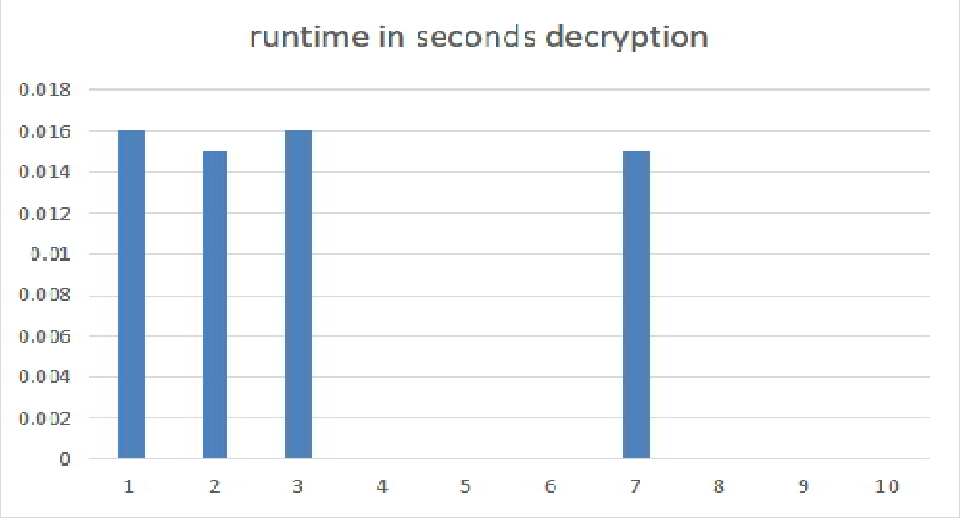


Figure 2

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.

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 8 Issue VII 2020- Available at www.ijraset.com

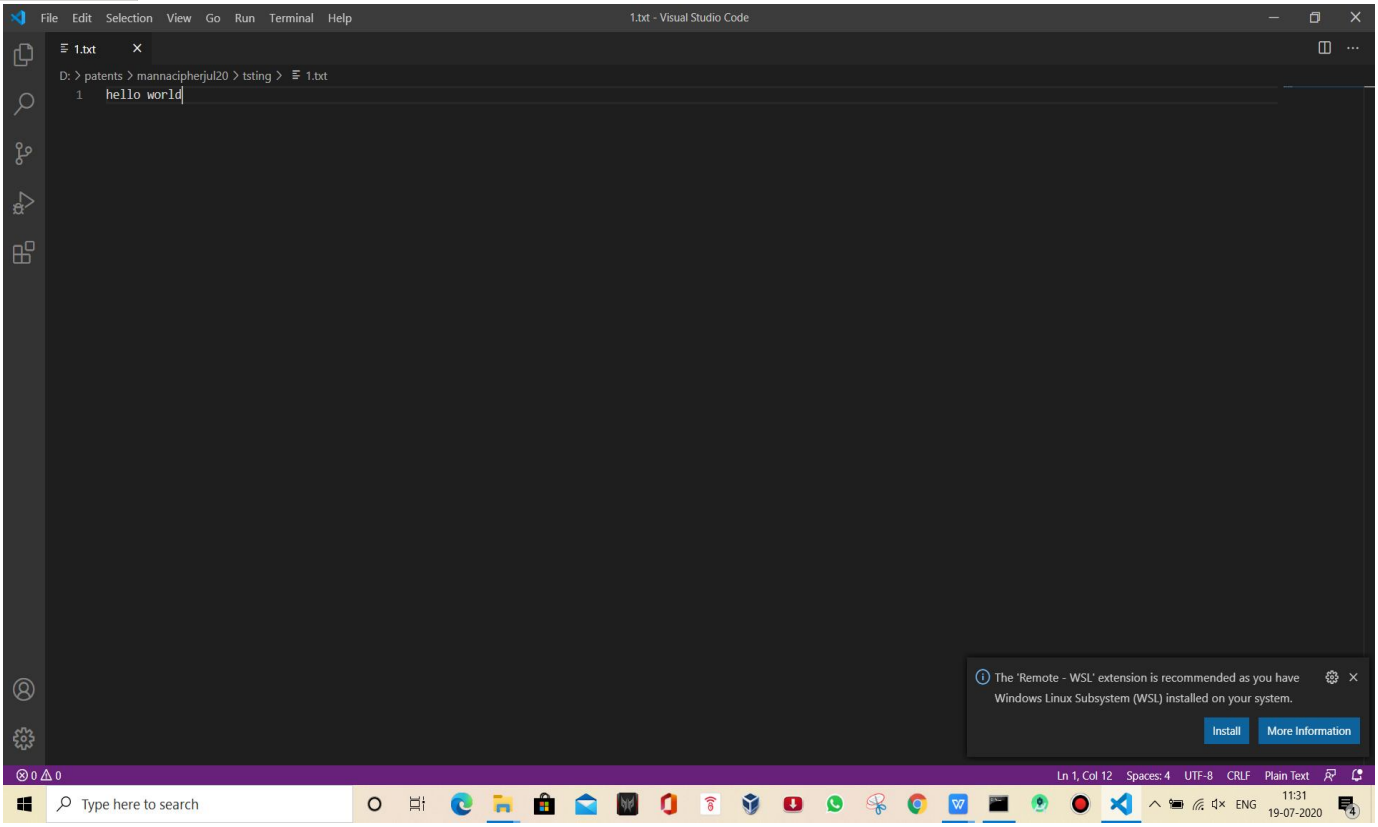


Figure 3

The plain text before encrypting

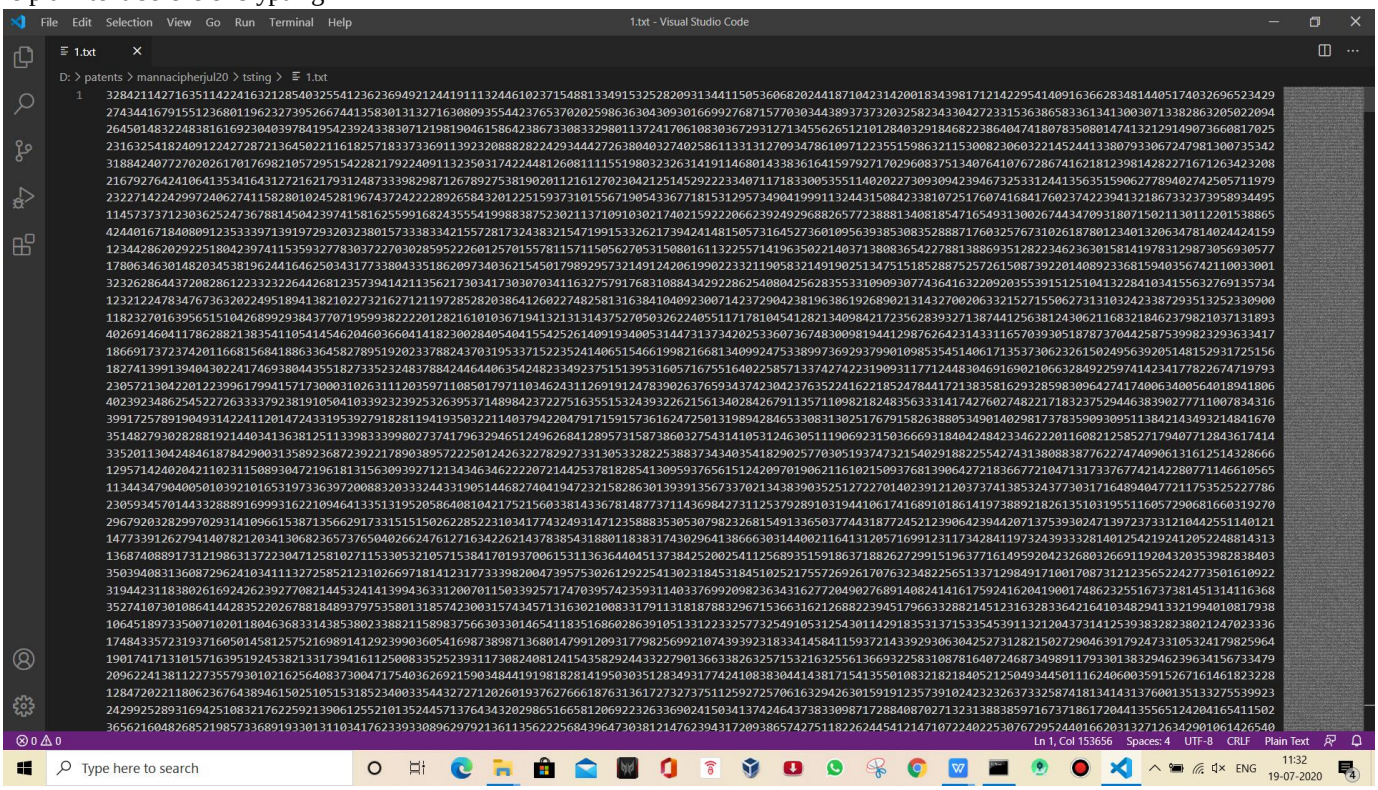
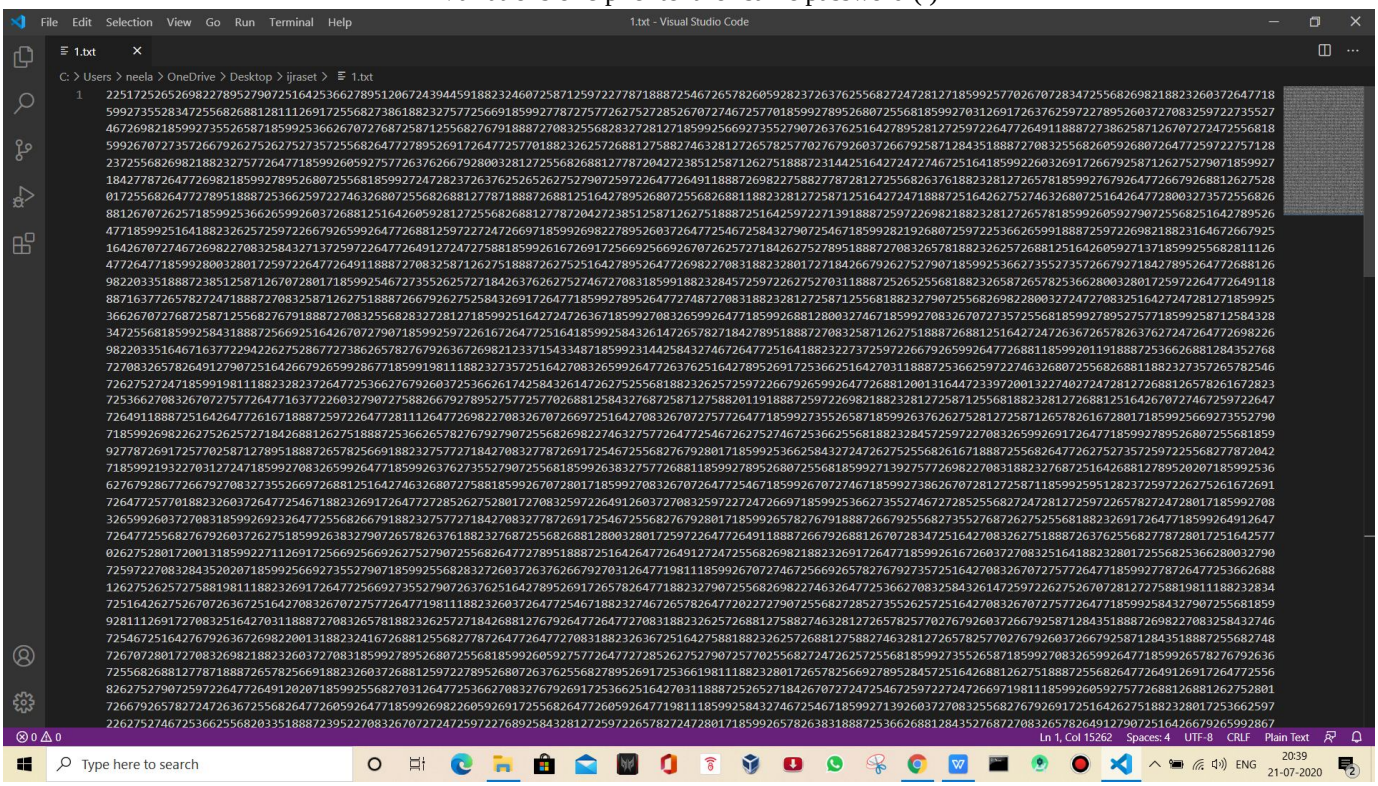


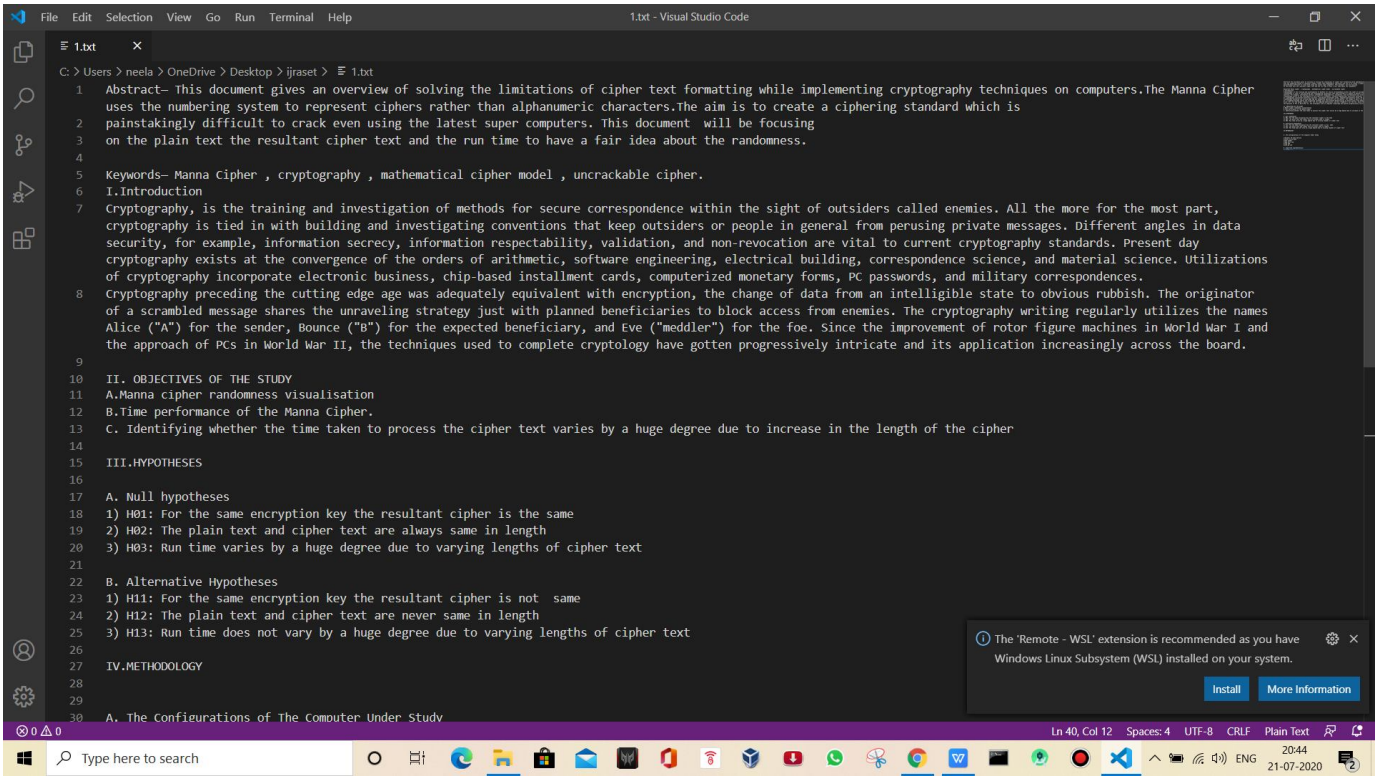
Figure 4

The plain text after encrypting

Variations of cipher text for same password (i)

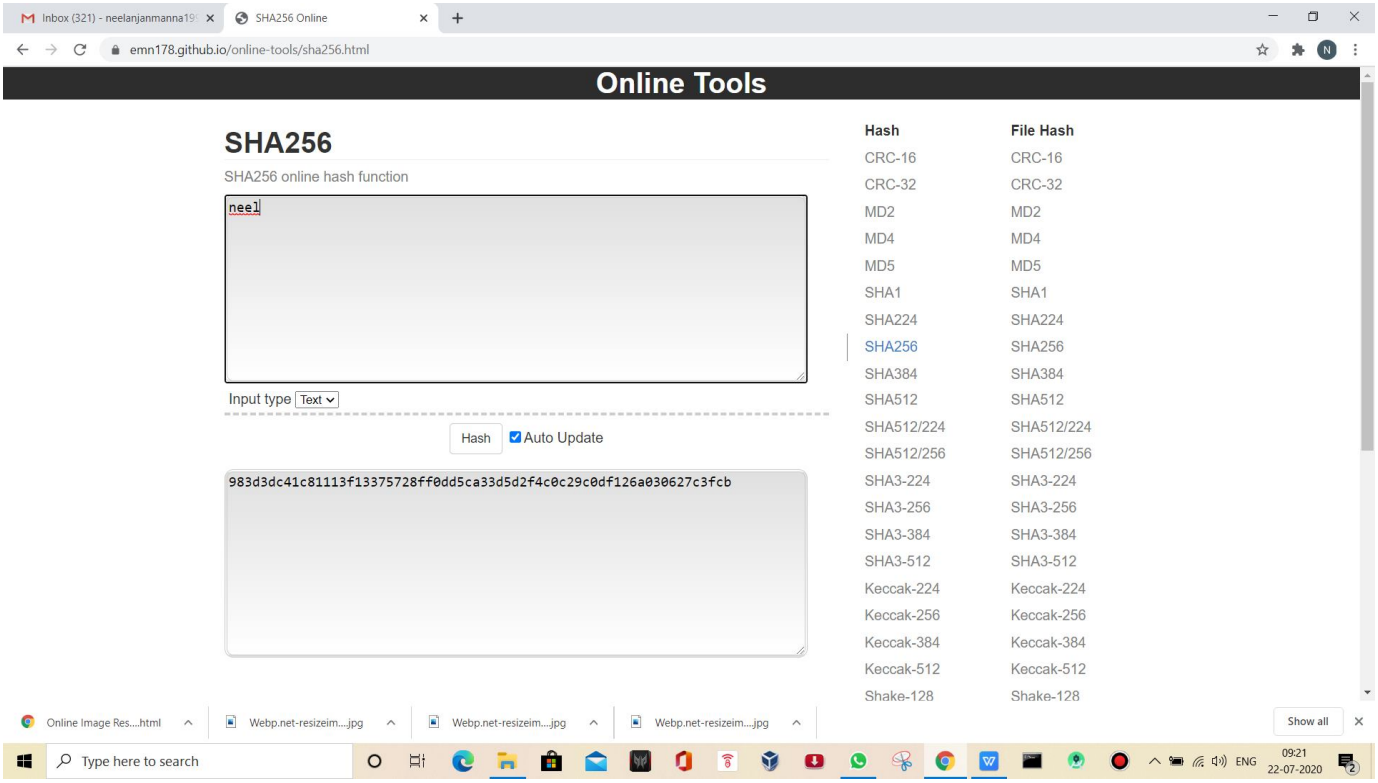


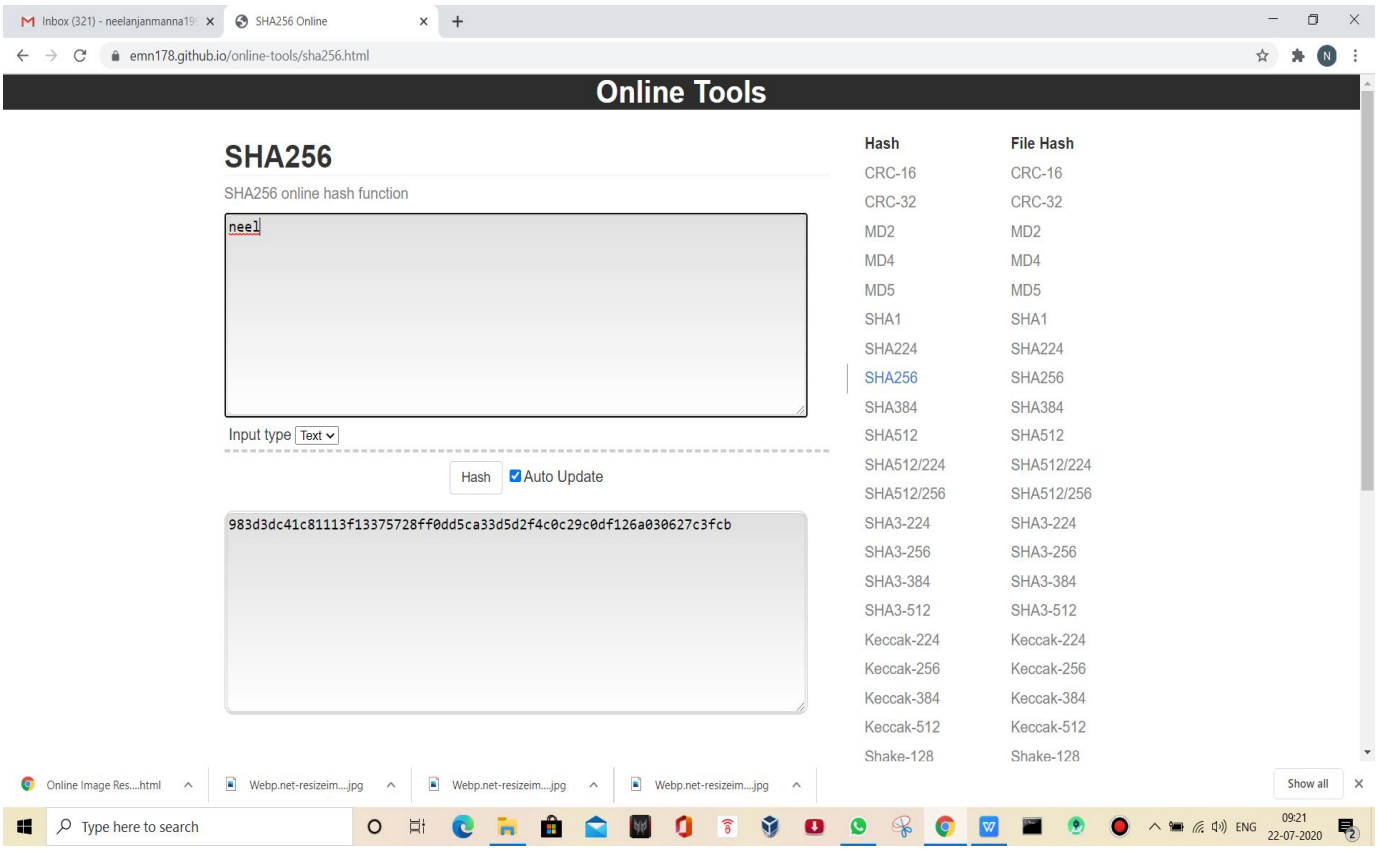
Actual data



International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 8 Issue VII July 2020- Available at www.ijraset.com

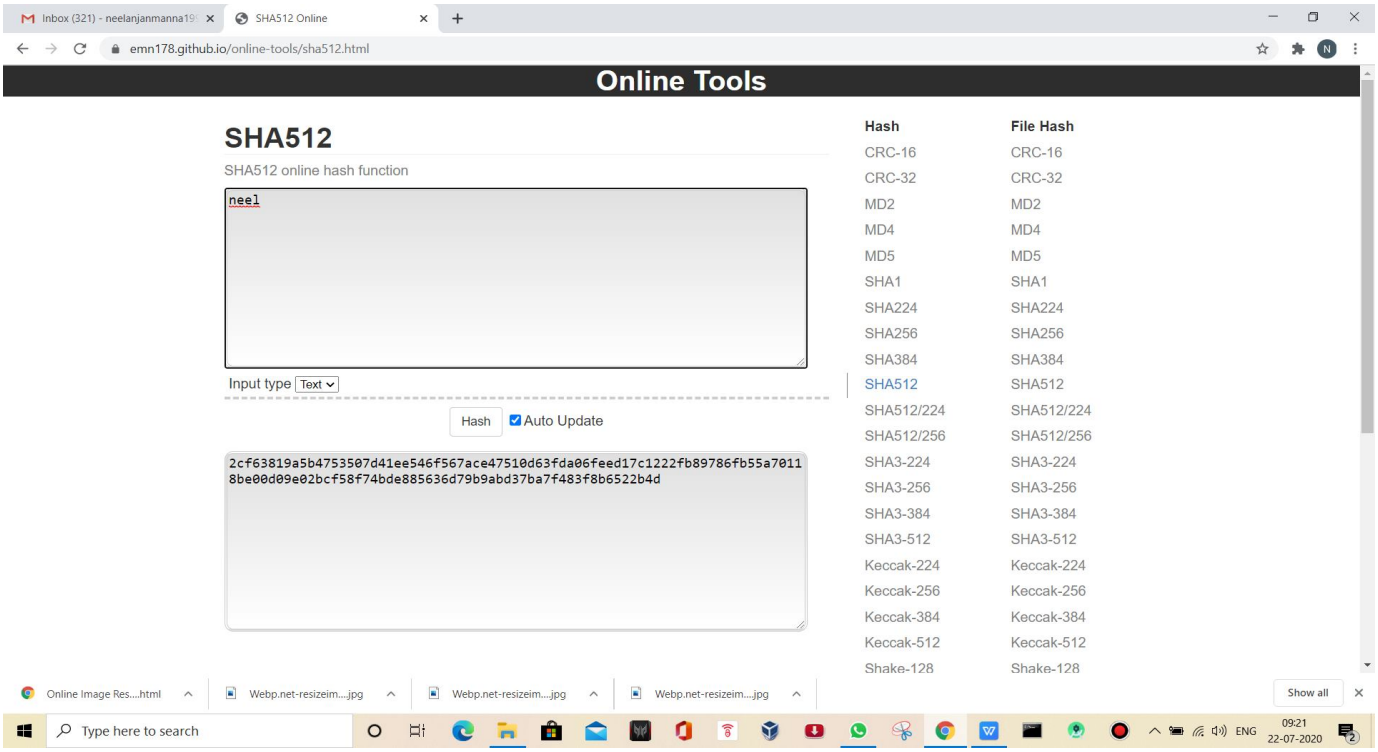
SHA 256 randomness test

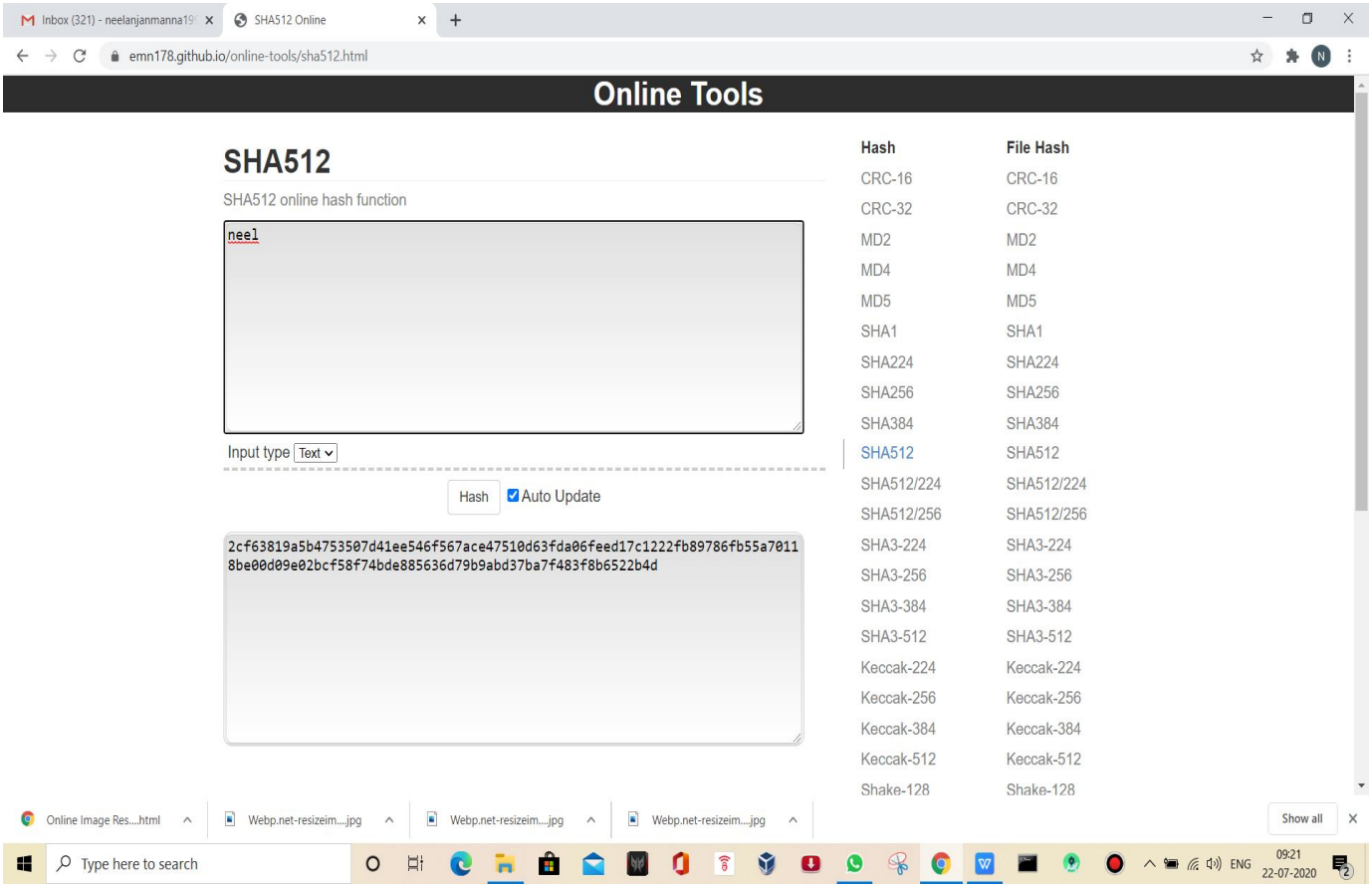




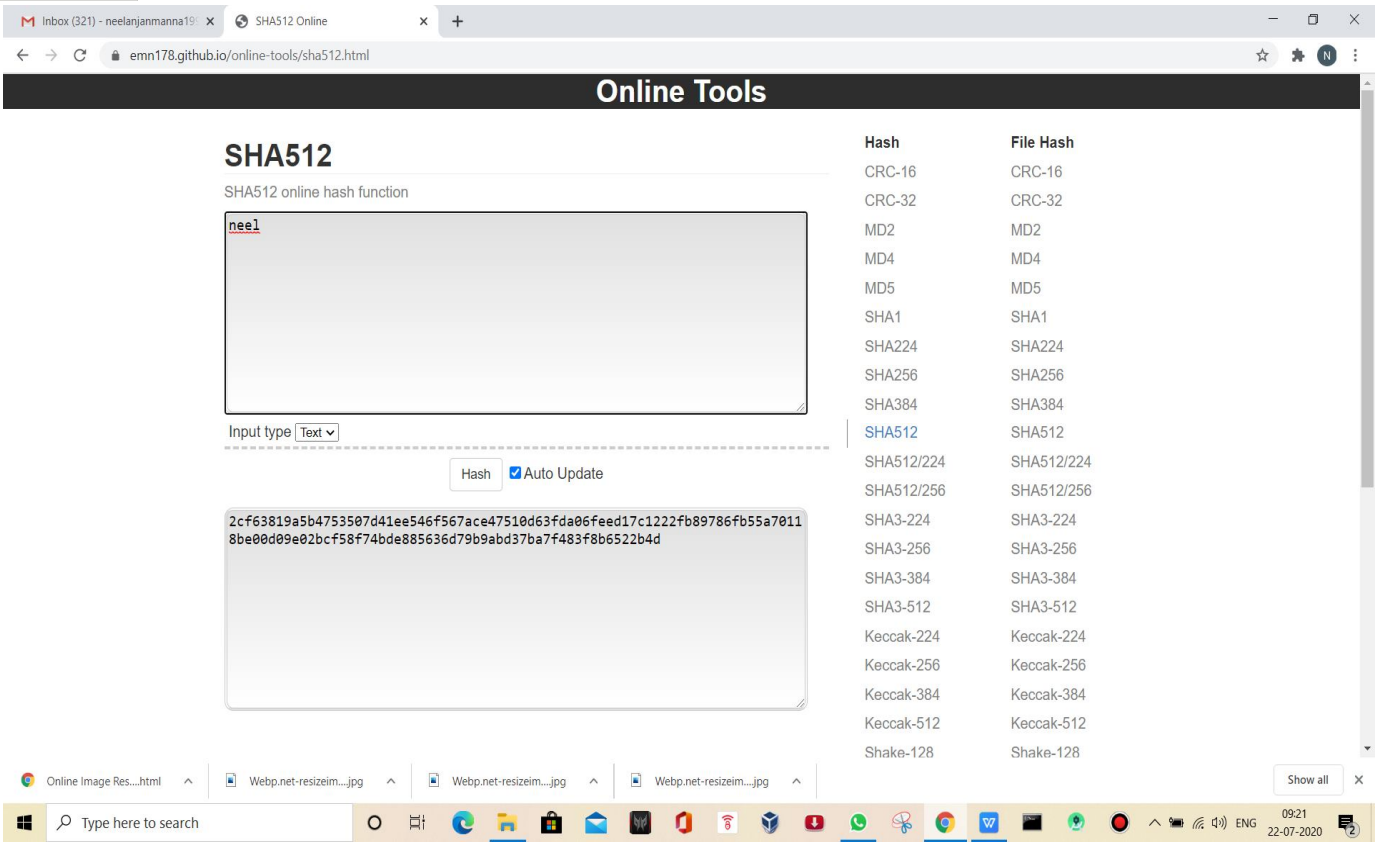
International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 8 Issue VII July 2020- Available at www.ijraset.com

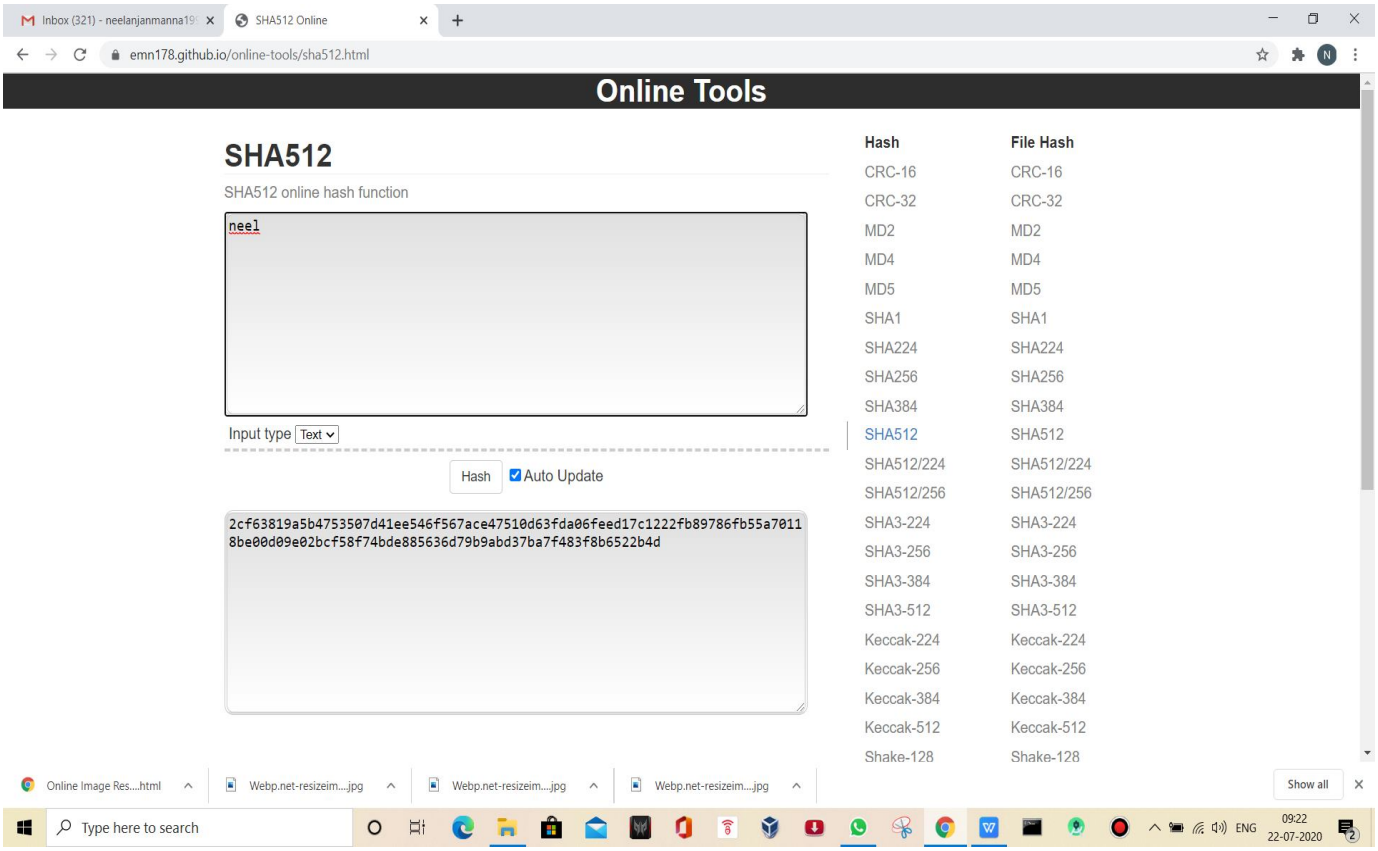
SHA 512 randomness test





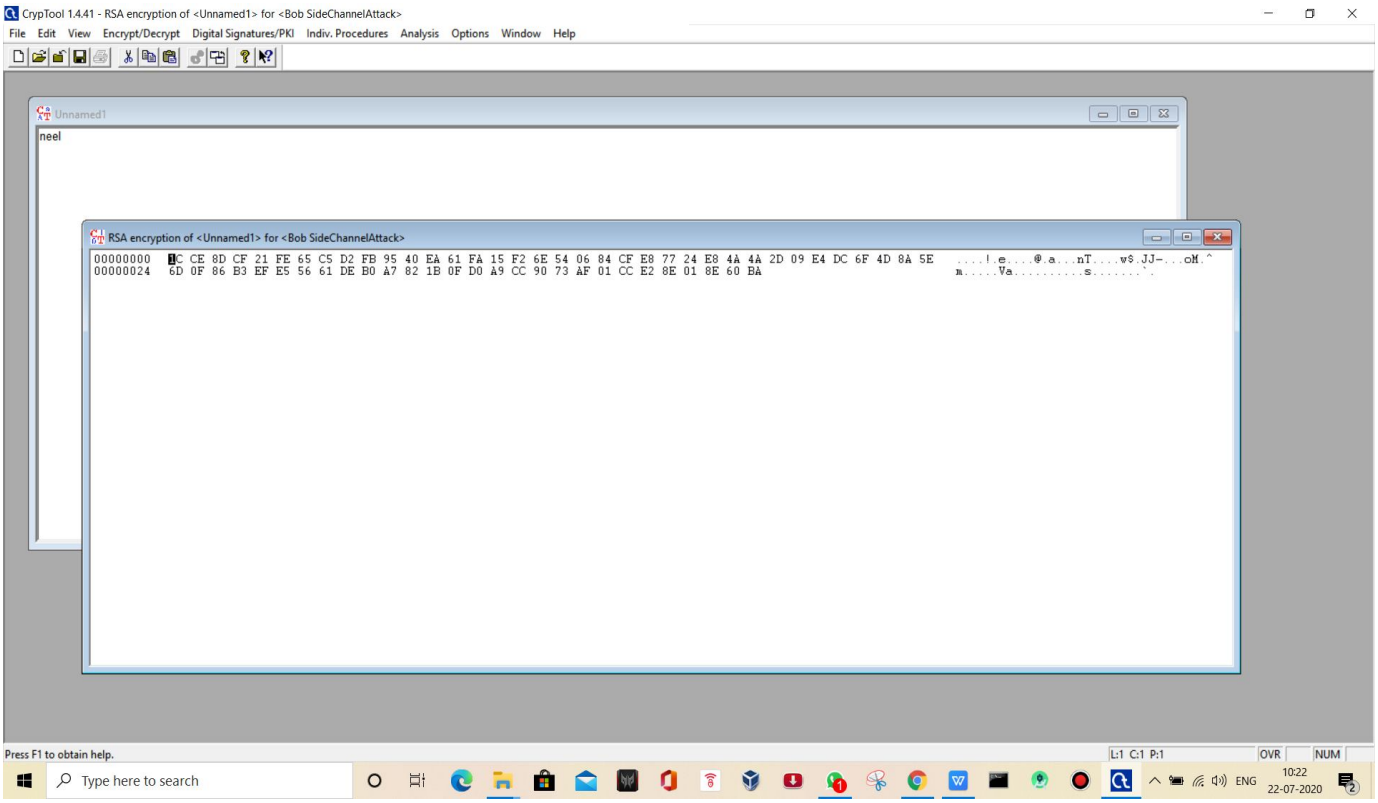
International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 8 Issue VII July 2020- Available at www.ijraset.com

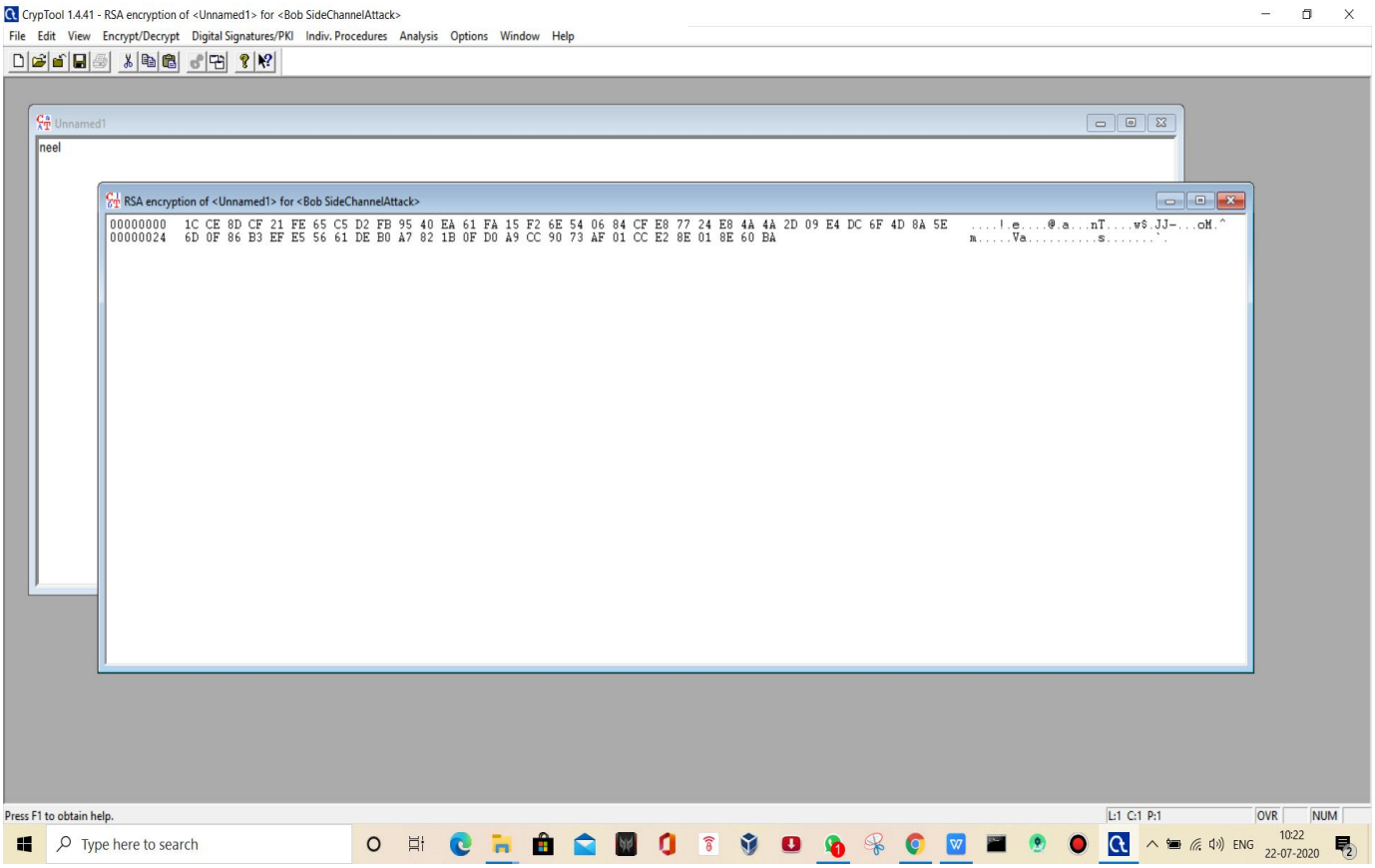


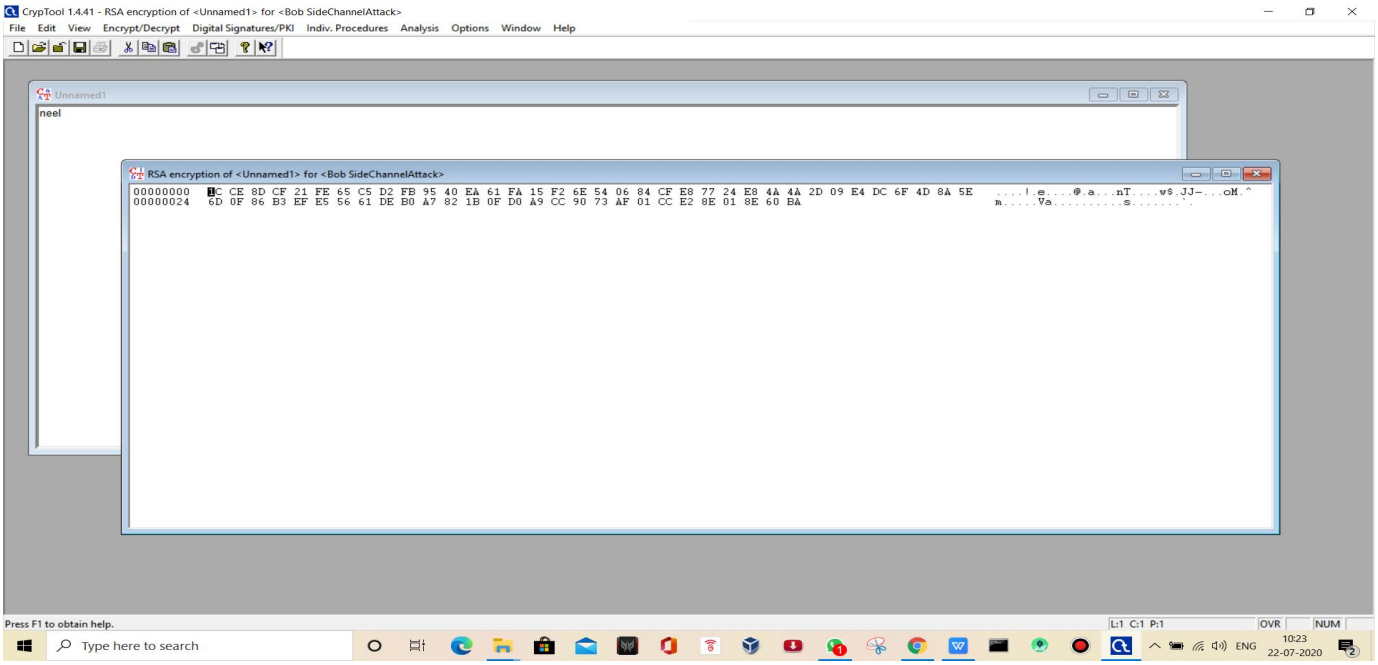


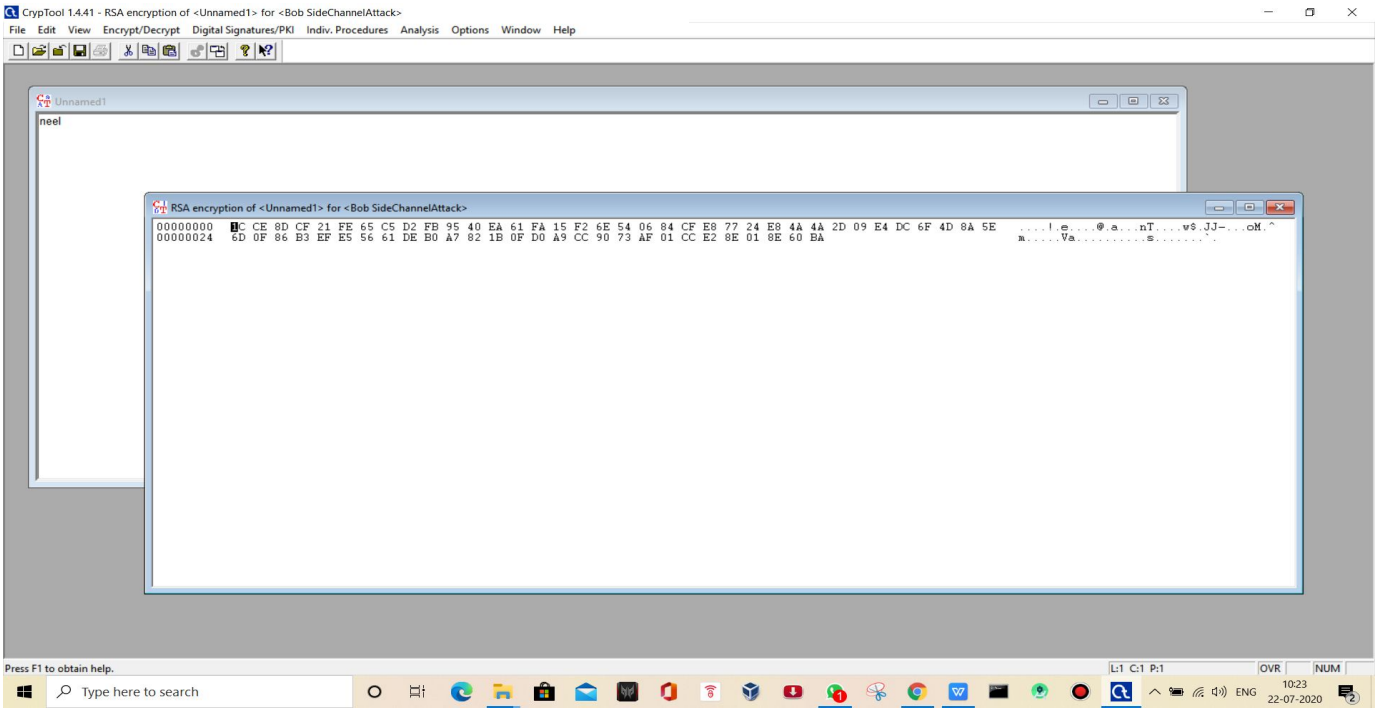
International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 8 Issue VII July 2020- Available at www.ijraset.com

RSA 512 randomness test







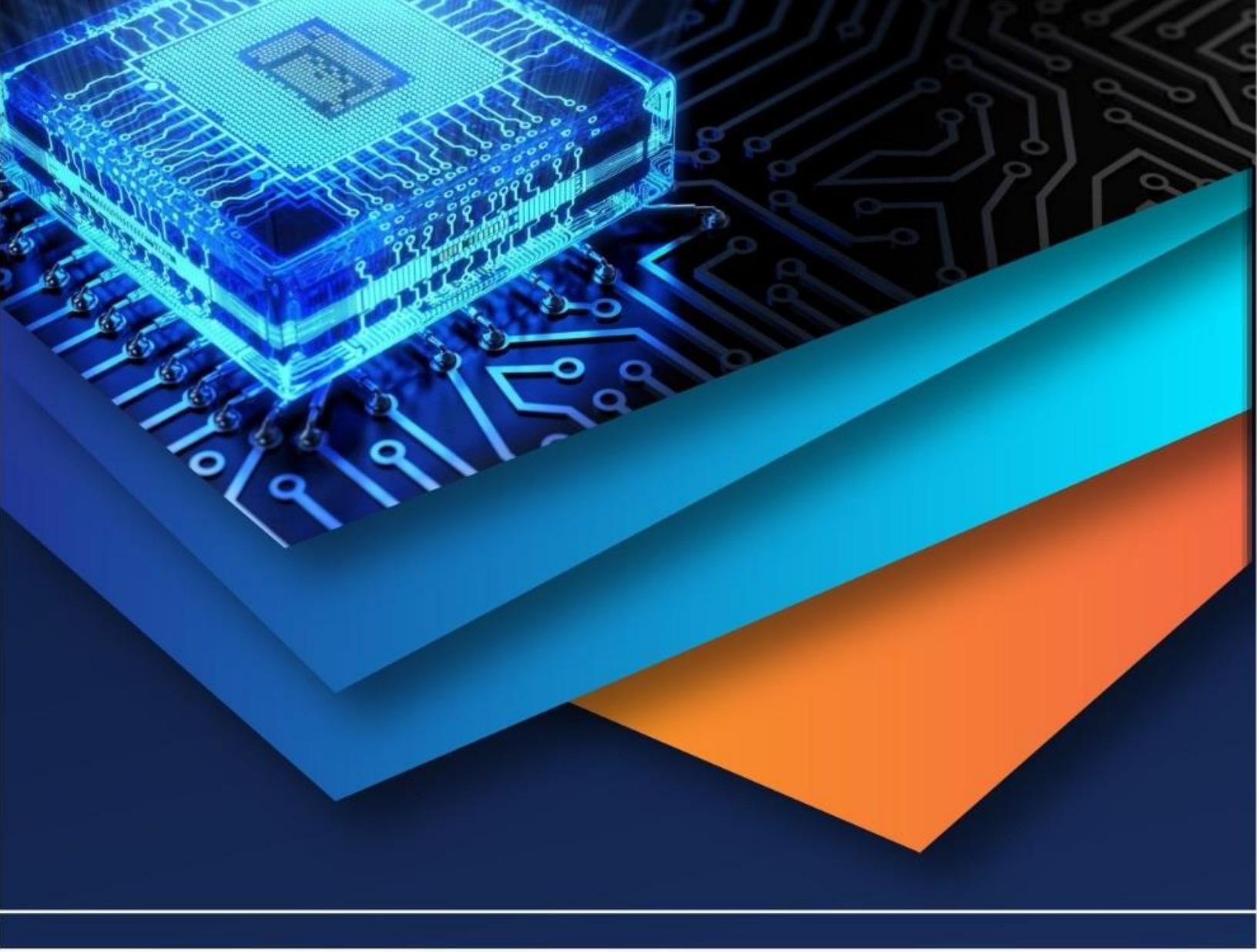


V. CONCLUSION

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 has been done in this document where the variations in cipher text for same password can be seen as well as the comparison with randomness of RSA 512 SHA 256 and SHA 512.As it can be seen the encrypted form of the plain text is static for all SHA 256 , SHA 512 and RSA 512 whereas Manna Cipher is highly random and secure .

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.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY