



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

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

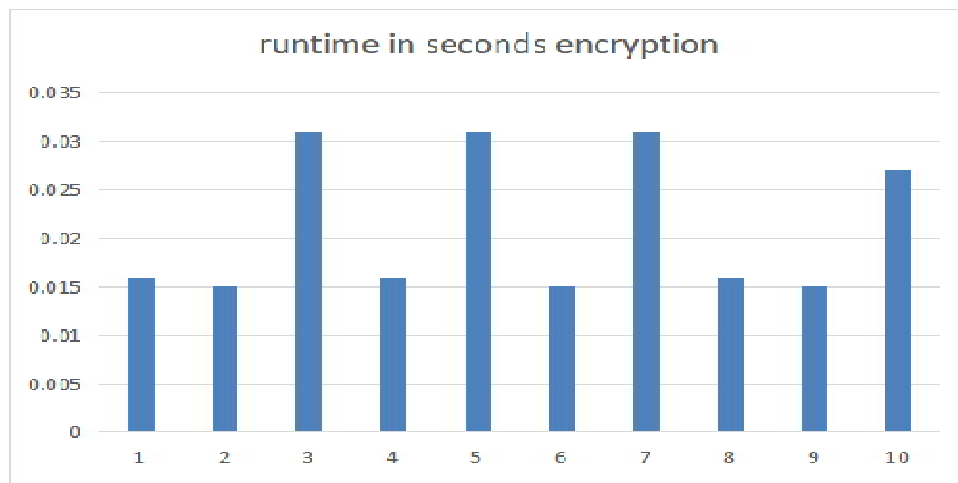


Figure 1

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.

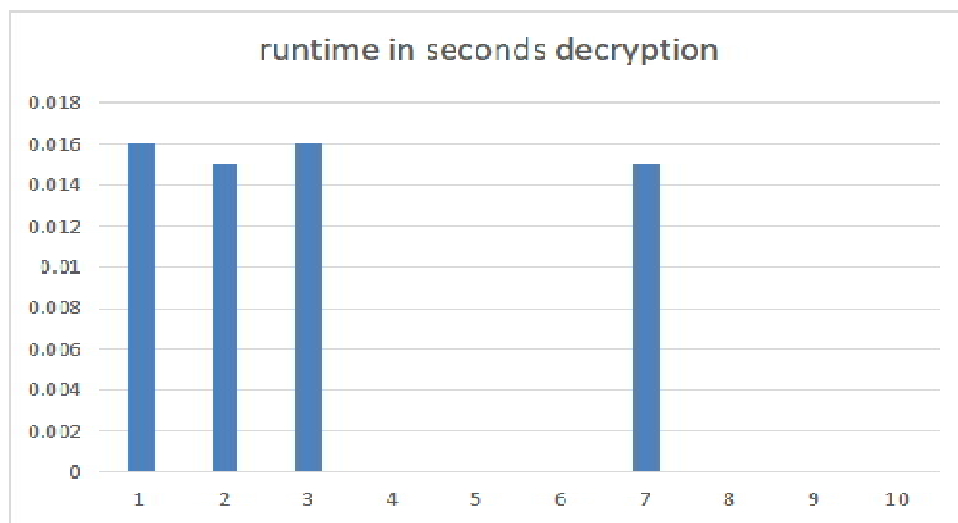


Figure 2

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.

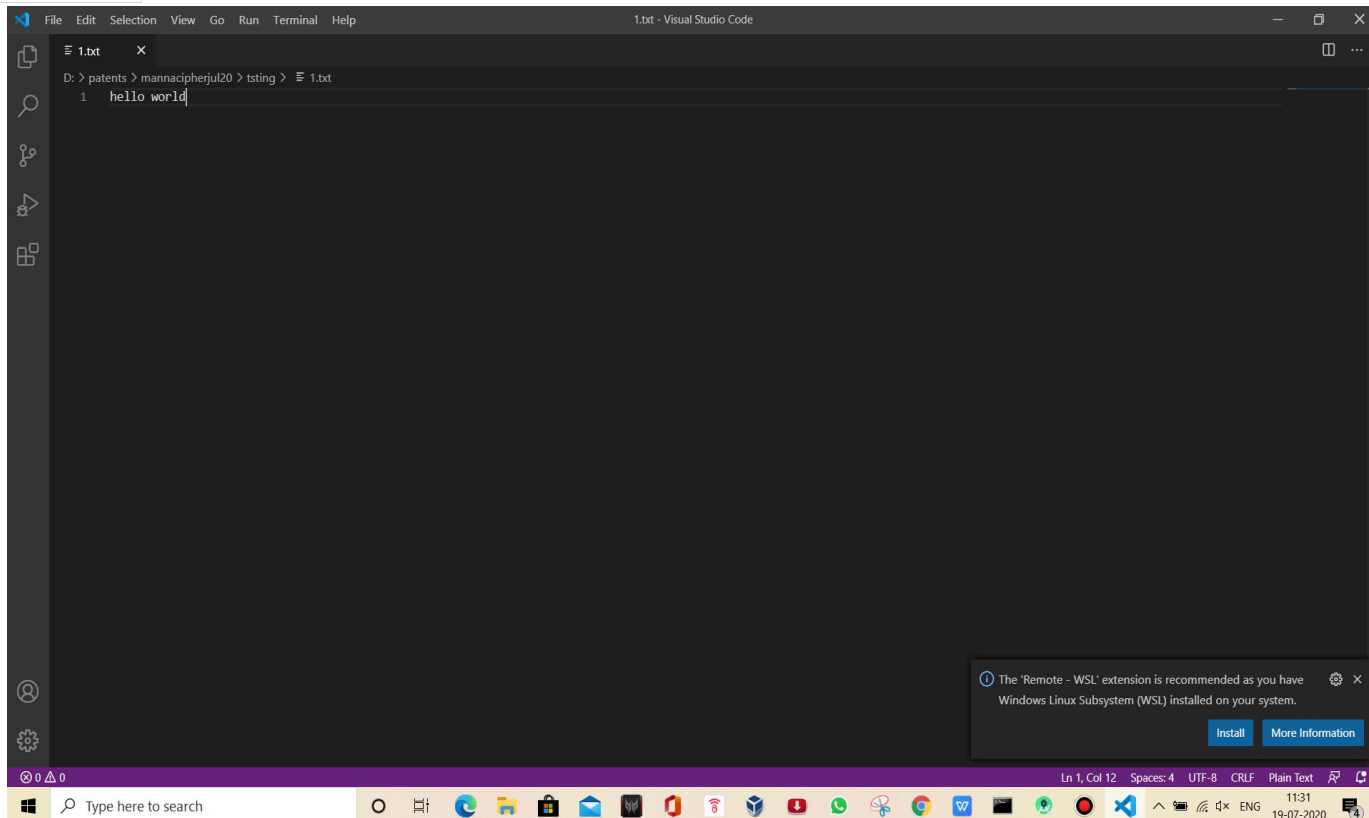


Figure 3

The plain text before encrypting

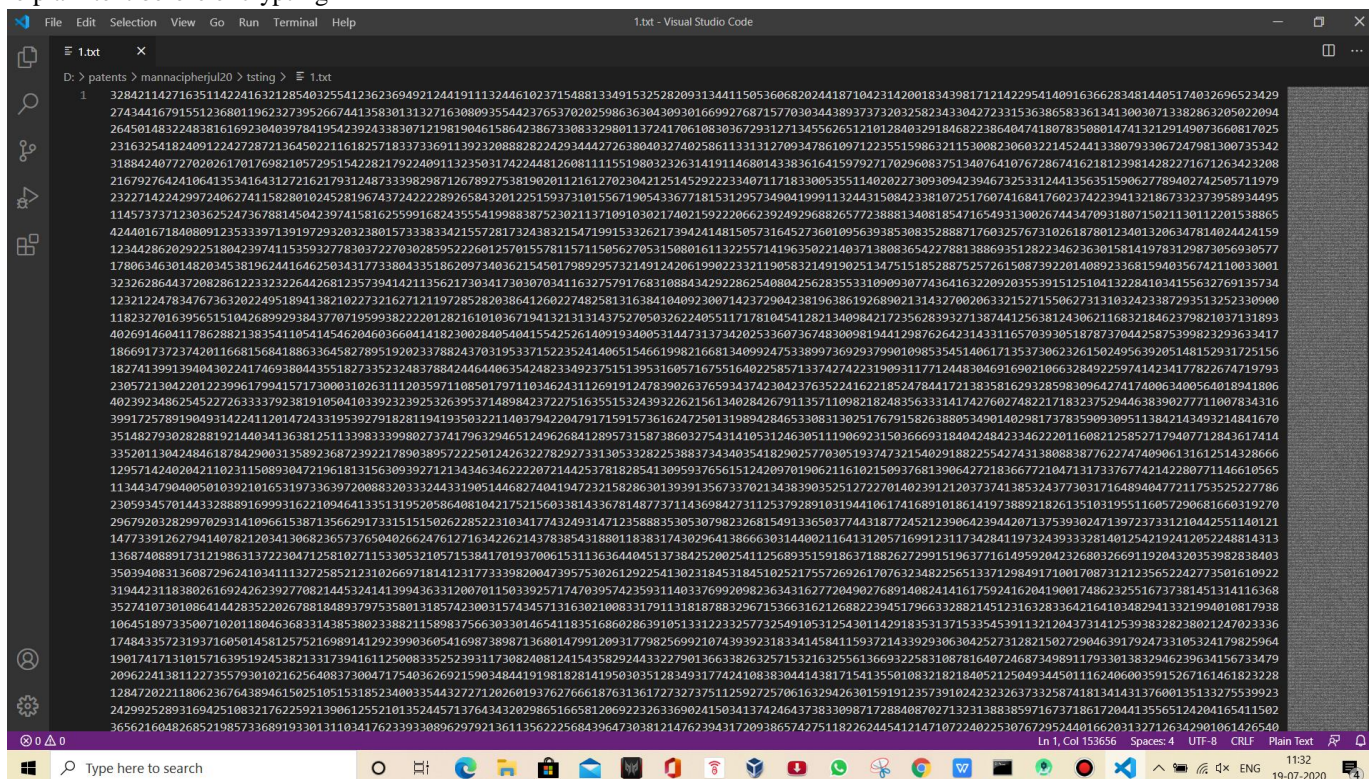
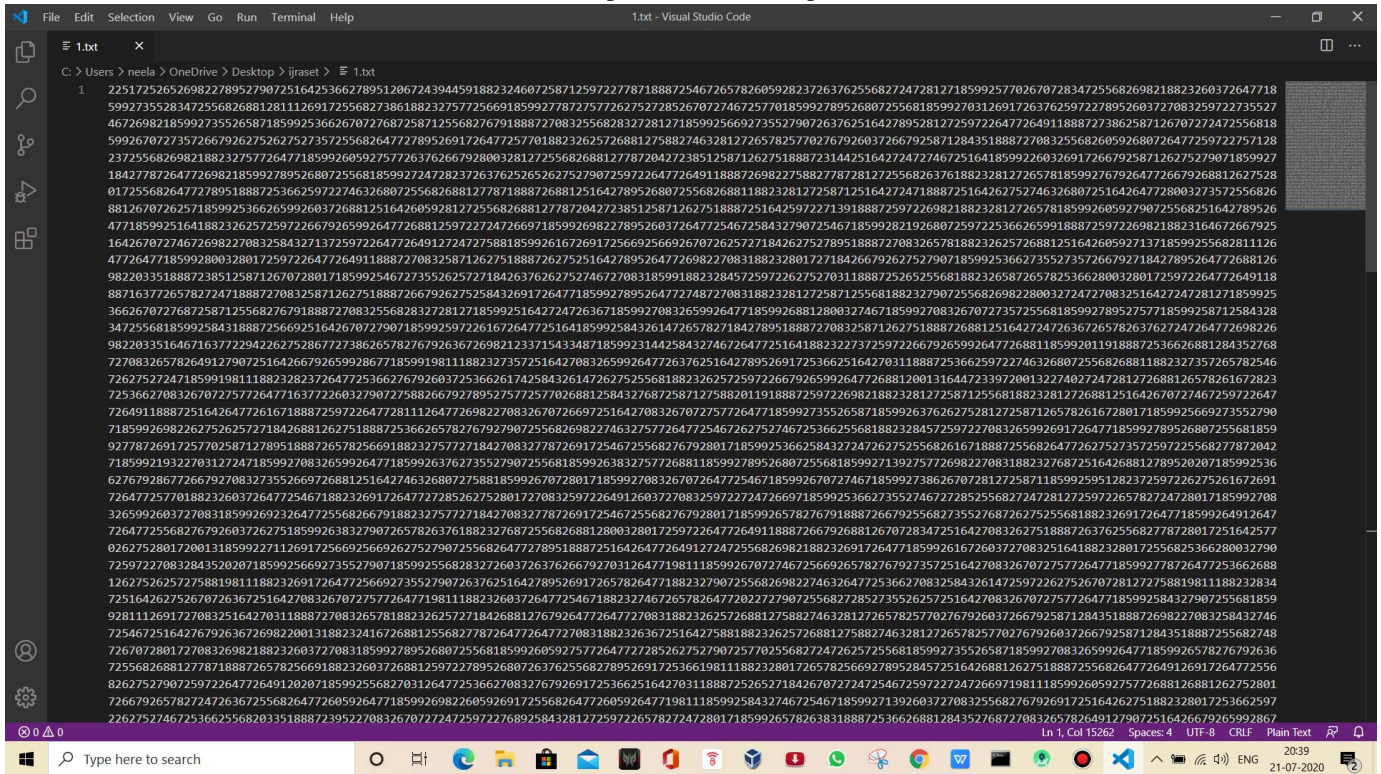


Figure 4

The plain text after encrypting

Variations of cipher text for same password (i)

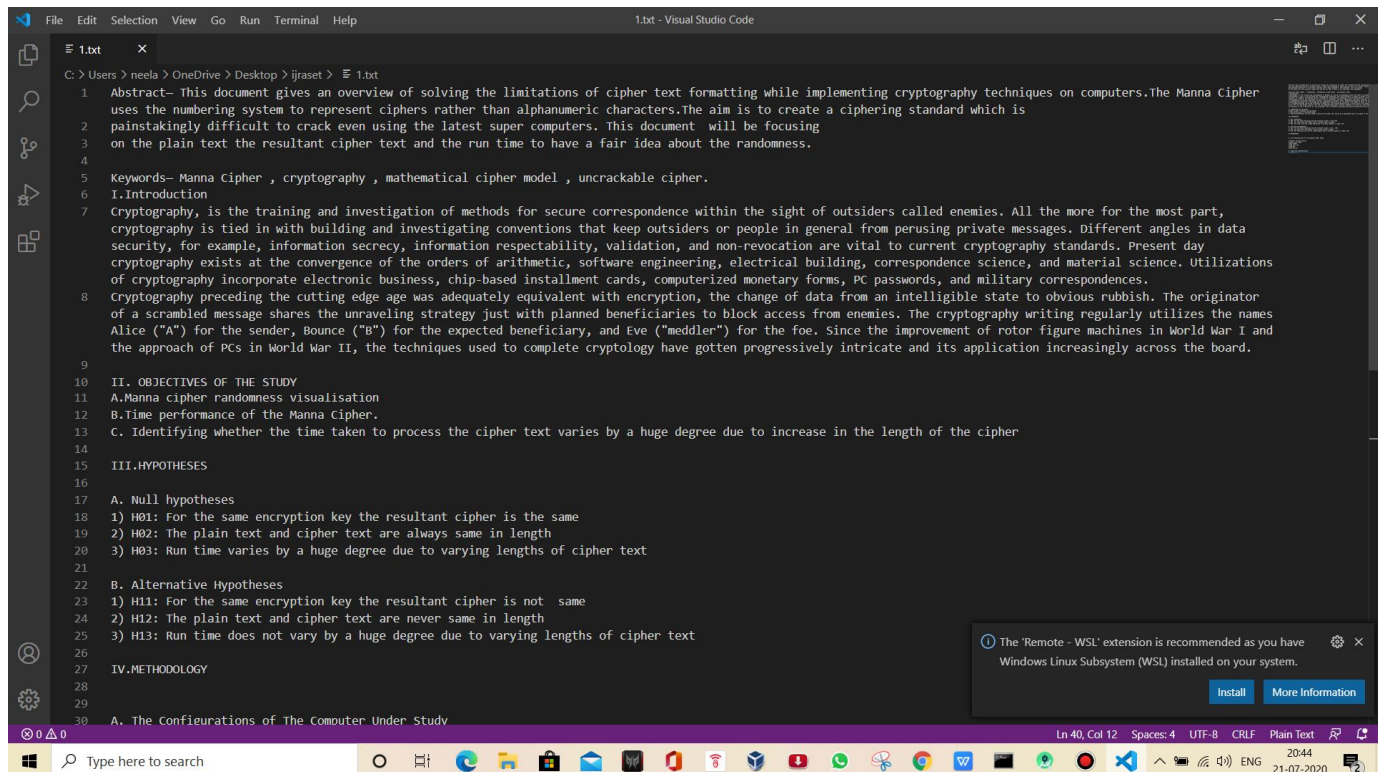


```

1 2251725265269822789527907251642536627895120672439445918823246072587125972778188872546726578260592823276376255682724728121718599257702670728347255682698218823260372647718
59927352834725568268812811126912556827386188232757256691859927787257272825670727467257018599278952680725568185992703126912637625972278952603727083259722735527
467269821859927355265871859925366267072687258112556827679188872708325568283272812185992566927355279072637625164278952812725972264772649118887273862587126707274272556818
599267072735726679262752627527357255682647727895269172647725701882326257268812758827463281272657825770276792603726679258712843518887270832556826952680726477259722757128
2372556826982188232757264771859926959275772637626679280032812725568268812778720427238512587126275188872314425164272472746725164185992260326917266792587126275299071859927
1842778726477269821859927895268072556818599272472823763762562675279072597226477264911888726982275882778728127255682637618823281272657818599276792647726679268812627528
017255682647727895188872536625972746326807255682688127781888726881251642789526807255682688118823281272587125164272471888725164262752746326807251642647728003273572556826
8812670726257185992536626992603726881251642680528127255682688127787204272385125871262751888725164259722731391888725972698218823281272657818599269592790725568251642789526
47718599251641882326257259722667926599264772688125972272472669718599269827895260372647725467258437907254671859928127068072597225366265918887259722698218823164672667925
164267072746726982708325843271372597264772649127247275881859926167269172566925669267072625727184267257895188872708326257818823262572688125164260592713718599255682811126
47726477185992800328017259722647726491188872708325871262751888726275251642789526477269822708318823280172718426679262752790718599253662735527357266792718427895264772688126
982203351888723851258712670728017185992546727355262572718426376262572467278318599188232845725972262757031888725262556818823265872657825366280032801725972264772649118
8871637726578272471888727083258712627518887266792627525843269172647718599278952647724872708318823281272587125568188232790725568269822800327247270832516427247281271859925
366267072687258125568276791888727083255682832728127185992516427247263671859927083265992647718599268812800327467185992708326707273572556818599278952757718599258712584328
34725568185992584318887256692516426707279071859925972261672647725164185992584326147265782718427895188872708325871262751888726881251642724726367265782637247264772698226
9822033516467163772294226275286727386265782767926367269821233715433487185992314425843274672647725164188232273725972266792659926477268811859920119188872536626881284352768
7270832658264912790725164266792659928677185991981188232735725164270832659926477263762516427895269172536625164270318887253662597224632680725568268811882327357265782546
72625727471859919811882328237264772536627679260372536626147258432614726275256818823262572597226679265992647726881200131644723397200132274027247281272688126578261672823
725366270832670727572647716377226032790727588266792789527572577026881258432768725871275882011918887259722698218823281272587125568188232812726881251642670727467259722647
72649118887251642647726167188872597226477281112647726982270832670726697251642708326707275726477185992735526587185992637626275281272587126578261672801718599256692735527907
7185992698226275262572718426881262751888725366265782769279072556826982274632757264772546725662556818823284572597227083265992691726477185992789526807255681859
92778726917257702587127895188872657826691882375772718427083277872691725467255682767928017185992536625843272472627556826167471888725568264772627573572597225568277872042
1859921932270312724718599270832659926477185992637627355279072556818599268823757268811859927895268072556818599271392757726982270831882327687251642688127895202071859925843
62767928677266792708327355266972688125164274632680727588185992670728017185992708326707264772546718599267072467185992738626707281272587185992595128237597226275261672691
726747577018823260372647725467188232691726477272852627528017208325972724726697185992536627355274672728556827247281272597226578264727280171859927083
326592603727083185992692326477255682667918823275727184270832778726917254672556827679280171859926578267918887266792556827355276872627556818823269172647718599264912647
7264772556827679260372627518599263827907265782637618823276872556826881280032801725972264772649118887266792688126707283472516427083262751888726376255682778728017251642572
06275280172801318599227112691725669256692627527907255682647727895188872516426477264911274272556826982188232691726477185992616726037270832516418823280172556825366280032790
725972270832843250280185992692735527907185992556828327260372637626679270312647719811859926070724672566926578276792735725164270832670727572647718599278726477253662688
1262752625727588198118823269172647725467188232691726477198118823260372647725467274672657826477202272790725568272852735526257251642708326707275726477185992584327907255681859
9281112691720832516427031188872708326578188232625727184268812767926477264772708318823262572688127588227463281272657825770276926037266792637266792587128435188872698227083258432746
725467251642767926367269822001188232416726881255682778726477264772708318823263672516427588188232625726881275882746328127265782577027692603726679258712843518887255682748
7267072801727083269821882326037270831859927895268072556818599269592757726477272852627527907257702568272472625725568185992735526587185992708326599264771859926578276792636
72556826881277818887265782669188232603726881259722789526807263762556827895269172536619811882328017265782566927895284572516426881262751888725568264772649126917264772556
82627527907259722647726491202071859925568270312647725366270832767926917253662516427031188872565271842670727247266971981185992695927572688126881262752801
7266792657827247263672556826477269592647718599269822605926917255682647726959264771981185992584327467254671859927139260372708325568276792691725164262751882328017253662597
226275274672536625568203518887239522708326707272472597227689258432812725972265782724728017185992657826381888725366268812843527687270832657826491279072516426679265992867

```

Actual data

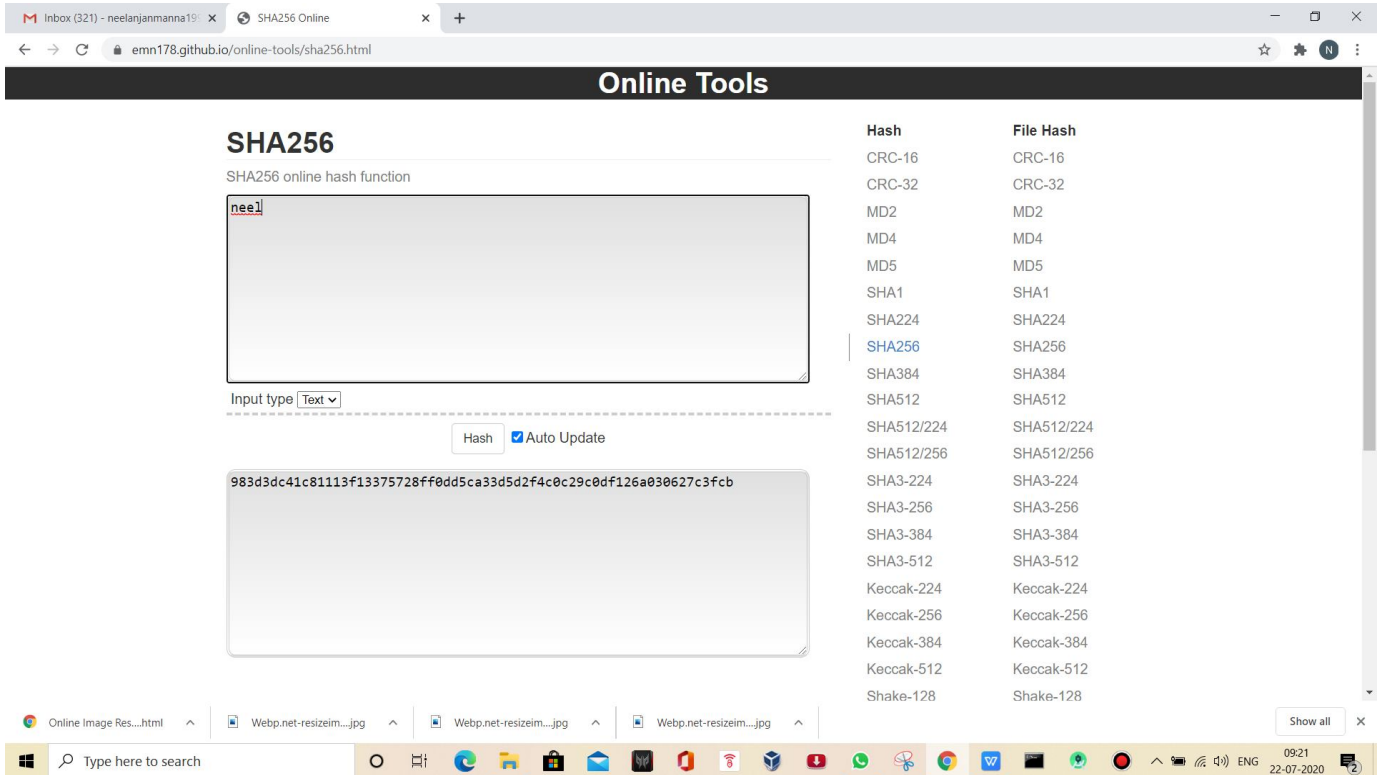


```

1 Abstract—This document gives an overview of solving the limitations of cipher text formatting while implementing cryptography techniques on computers. The Manna Cipher
2 uses the numbering system to represent ciphers rather than alphanumeric characters. The aim is to create a ciphering standard which is
3 painstakingly difficult to crack even using the latest super computers. This document will be focusing
4 on the plain text the resultant cipher text and the run time to have a fair idea about the randomness.
5
6 Keywords— Manna Cipher , cryptography , mathematical cipher model , uncrackable cipher.
7 I. Introduction
8 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,
9 cryptography is tied in with building and investigating conventions that keep outsiders or people in general from perusing private messages. Different angles in data
10 security, for example, information secrecy, information respectability, validation, and non-revocation are vital to current cryptography standards. Present day
11 cryptography exists at the convergence of the orders of arithmetic, software engineering, electrical building, correspondence science, and material science. Utilizations
12 of cryptography incorporate electronic business, chip-based installment cards, computerized monetary forms, PC passwords, and military correspondences.
13 Cryptography preceding the cutting edge age was adequately equivalent with encryption, the change of data from an intelligible state to obvious rubbish. The originator
14 of a scrambled message shares the unraveling strategy just with planned beneficiaries to block access from enemies. The cryptography writing regularly utilizes the names
15 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
16 the approach of PCs in World War II, the techniques used to complete cryptography have gotten progressively intricate and its application increasingly across the board.
17
18 II. OBJECTIVES OF THE STUDY
19 A. Manna cipher randomness visualisation
20 B. Time performance of the Manna Cipher.
21 C. Identifying whether the time taken to process the cipher text varies by a huge degree due to increase in the length of the cipher
22
23 III. HYPOTHESES
24
25 A. Null hypotheses
26 1) H01: For the same encryption key the resultant cipher is the same
27 2) H02: The plain text and cipher text are always same in length
28 3) H03: Run time varies by a huge degree due to varying lengths of cipher text
29
30 B. Alternative Hypotheses
31 1) H11: For the same encryption key the resultant cipher is not same
32 2) H12: The plain text and cipher text are never same in length
33 3) H13: Run time does not vary by a huge degree due to varying lengths of cipher text
34
35 IV. METHODOLOGY
36
37 A. The Configurations of The Computer Under Study

```

SHA 256 randomness test



Online Tools

SHA256

SHA256 online hash function

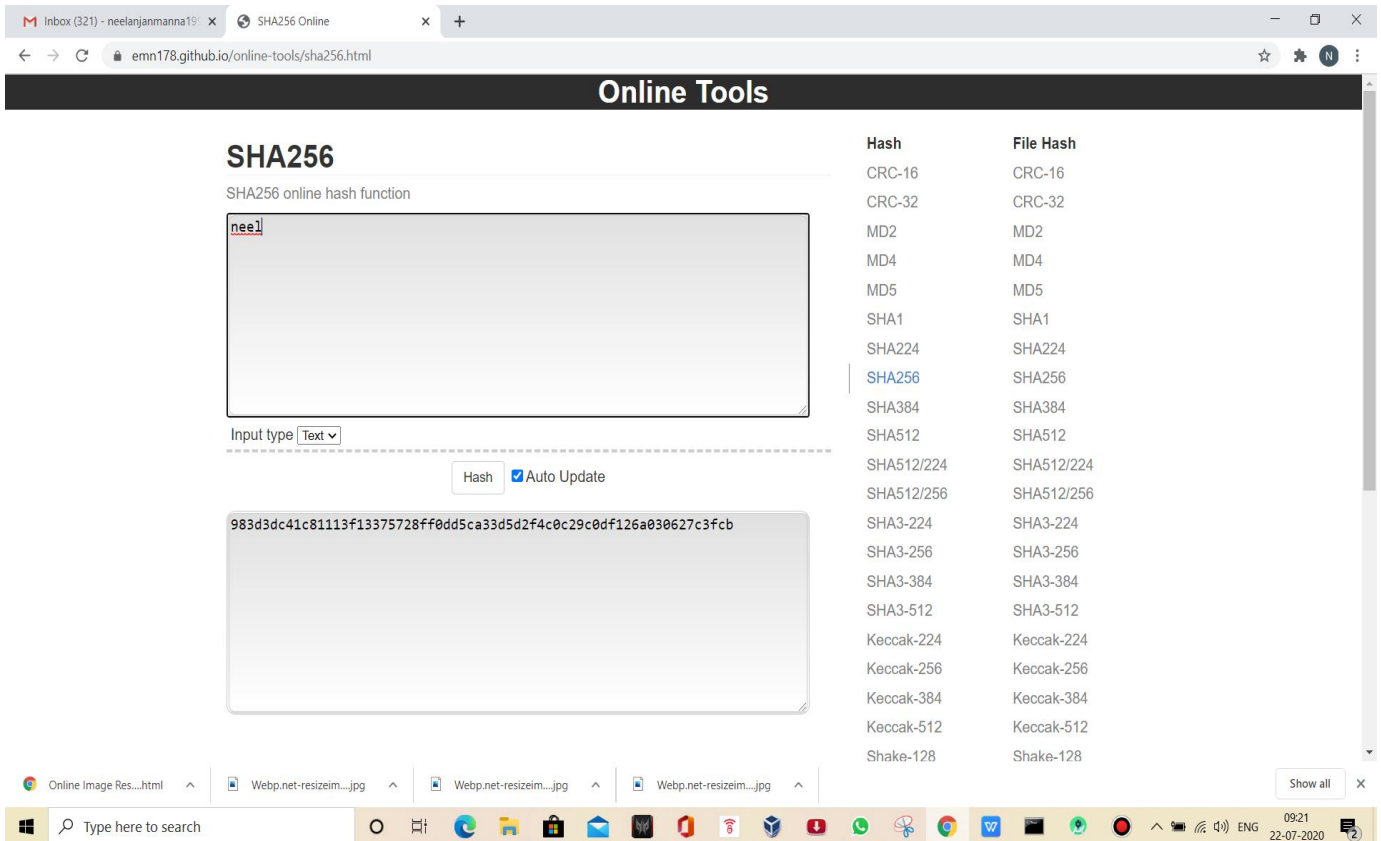
Input: nee1

Input type: Text

Hash: Auto Update

Output: 983d3dc41c81113f13375728ff0dd5ca33d5d2f4c0c29c0df126a030627c3fcb

Hash	File Hash
CRC-16	CRC-16
CRC-32	CRC-32
MD2	MD2
MD4	MD4
MD5	MD5
SHA1	SHA1
SHA224	SHA224
SHA256	SHA256
SHA384	SHA384
SHA512	SHA512
SHA512/224	SHA512/224
SHA512/256	SHA512/256
SHA3-224	SHA3-224
SHA3-256	SHA3-256
SHA3-384	SHA3-384
SHA3-512	SHA3-512
Keccak-224	Keccak-224
Keccak-256	Keccak-256
Keccak-384	Keccak-384
Keccak-512	Keccak-512
Shake-128	Shake-128



Online Tools

SHA256

SHA256 online hash function

Input: nee1

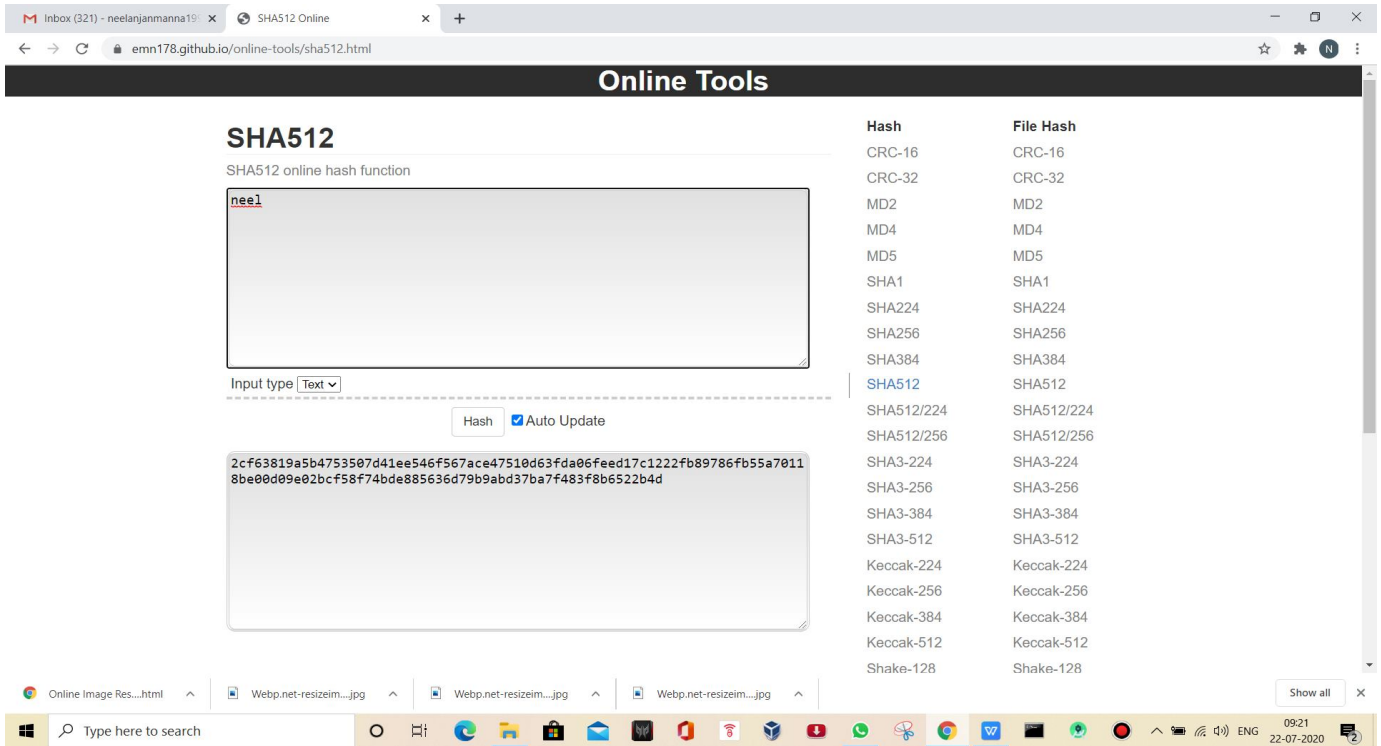
Input type: Text

Hash: Auto Update

Output: 983d3dc41c81113f13375728ff0dd5ca33d5d2f4c0c29c0df126a030627c3fcb

Hash	File Hash
CRC-16	CRC-16
CRC-32	CRC-32
MD2	MD2
MD4	MD4
MD5	MD5
SHA1	SHA1
SHA224	SHA224
SHA256	SHA256
SHA384	SHA384
SHA512	SHA512
SHA512/224	SHA512/224
SHA512/256	SHA512/256
SHA3-224	SHA3-224
SHA3-256	SHA3-256
SHA3-384	SHA3-384
SHA3-512	SHA3-512
Keccak-224	Keccak-224
Keccak-256	Keccak-256
Keccak-384	Keccak-384
Keccak-512	Keccak-512
Shake-128	Shake-128

SHA 512 randomness test



Online Tools

SHA512

SHA512 online hash function

Input: `neel`

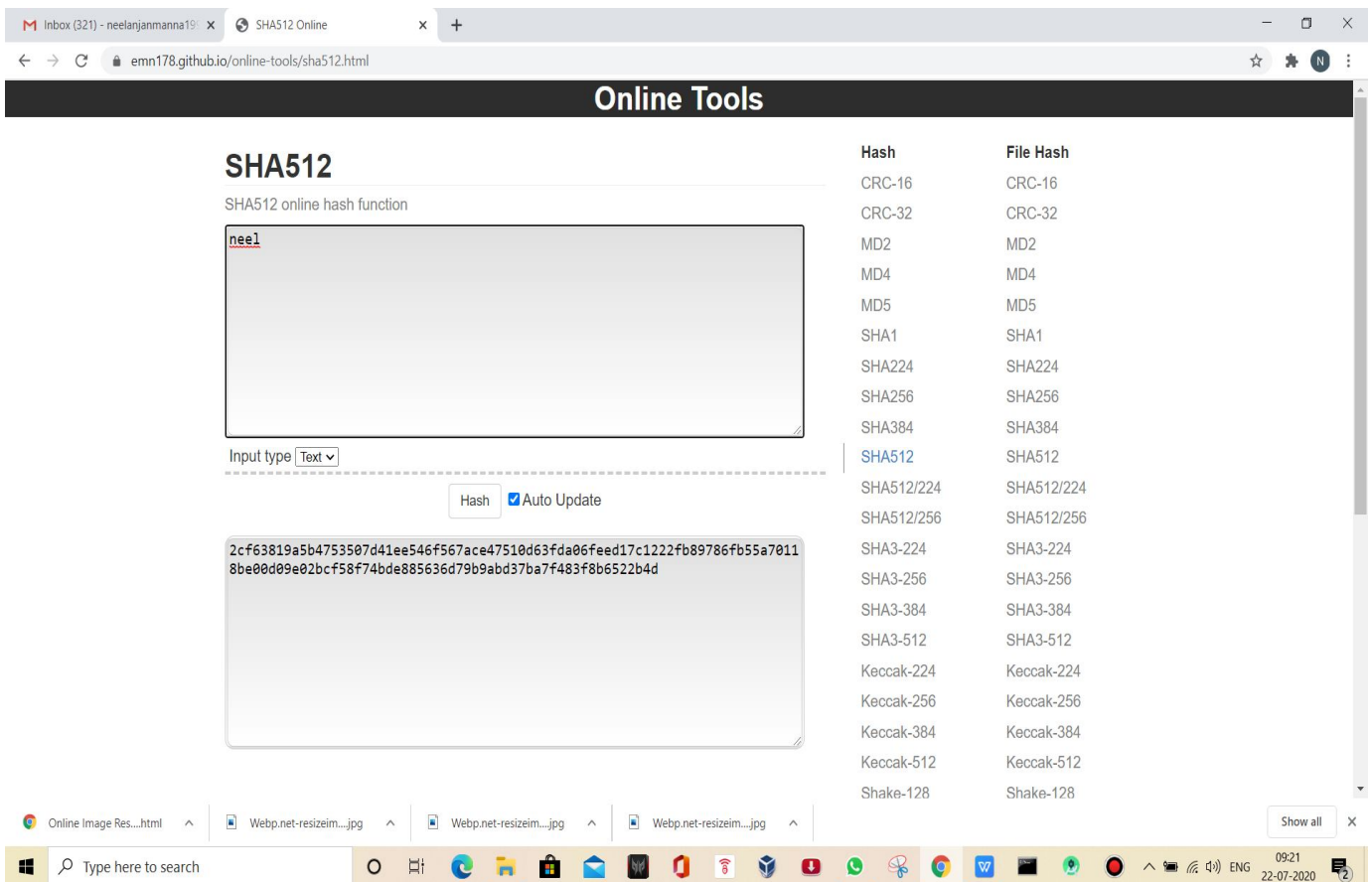
Input type:

Hash: Auto Update

Output Hash:

```
2cf63819a5b4753507d41ee546f567ace47510d63fda06feed17c1222fb89786fb55a70118be00d09e02bcf58f74bde885636d79b9abd37ba7f483f8b6522b4d
```

Hash	File Hash
CRC-16	CRC-16
CRC-32	CRC-32
MD2	MD2
MD4	MD4
MD5	MD5
SHA1	SHA1
SHA224	SHA224
SHA256	SHA256
SHA384	SHA384
SHA512	SHA512
SHA512/224	SHA512/224
SHA512/256	SHA512/256
SHA3-224	SHA3-224
SHA3-256	SHA3-256
SHA3-384	SHA3-384
SHA3-512	SHA3-512
Keccak-224	Keccak-224
Keccak-256	Keccak-256
Keccak-384	Keccak-384
Keccak-512	Keccak-512
Shake-128	Shake-128



Online Tools

SHA512

SHA512 online hash function

Input: `neel`

Input type:

Hash: Auto Update

Output Hash:

```
2cf63819a5b4753507d41ee546f567ace47510d63fda06feed17c1222fb89786fb55a70118be00d09e02bcf58f74bde885636d79b9abd37ba7f483f8b6522b4d
```

Hash	File Hash
CRC-16	CRC-16
CRC-32	CRC-32
MD2	MD2
MD4	MD4
MD5	MD5
SHA1	SHA1
SHA224	SHA224
SHA256	SHA256
SHA384	SHA384
SHA512	SHA512
SHA512/224	SHA512/224
SHA512/256	SHA512/256
SHA3-224	SHA3-224
SHA3-256	SHA3-256
SHA3-384	SHA3-384
SHA3-512	SHA3-512
Keccak-224	Keccak-224
Keccak-256	Keccak-256
Keccak-384	Keccak-384
Keccak-512	Keccak-512
Shake-128	Shake-128

SHA512 Online

emn178.github.io/online-tools/sha512.html

Online Tools

SHA512

SHA512 online hash function

neel

Input type

Hash Auto Update

```
2cf63819a5b4753507d41ee546f567ace47510d63fda06feed17c1222fb89786fb55a70118be00d09e02bcf58f74bde885636d79b9abd37ba7f483f8b6522b4d
```

Hash	File Hash
CRC-16	CRC-16
CRC-32	CRC-32
MD2	MD2
MD4	MD4
MD5	MD5
SHA1	SHA1
SHA224	SHA224
SHA256	SHA256
SHA384	SHA384
SHA512	SHA512
SHA512/224	SHA512/224
SHA512/256	SHA512/256
SHA3-224	SHA3-224
SHA3-256	SHA3-256
SHA3-384	SHA3-384
SHA3-512	SHA3-512
Keccak-224	Keccak-224
Keccak-256	Keccak-256
Keccak-384	Keccak-384
Keccak-512	Keccak-512
Shake-128	Shake-128

09:21 22-07-2020

SHA512 Online

emn178.github.io/online-tools/sha512.html

Online Tools

SHA512

SHA512 online hash function

neel

Input type

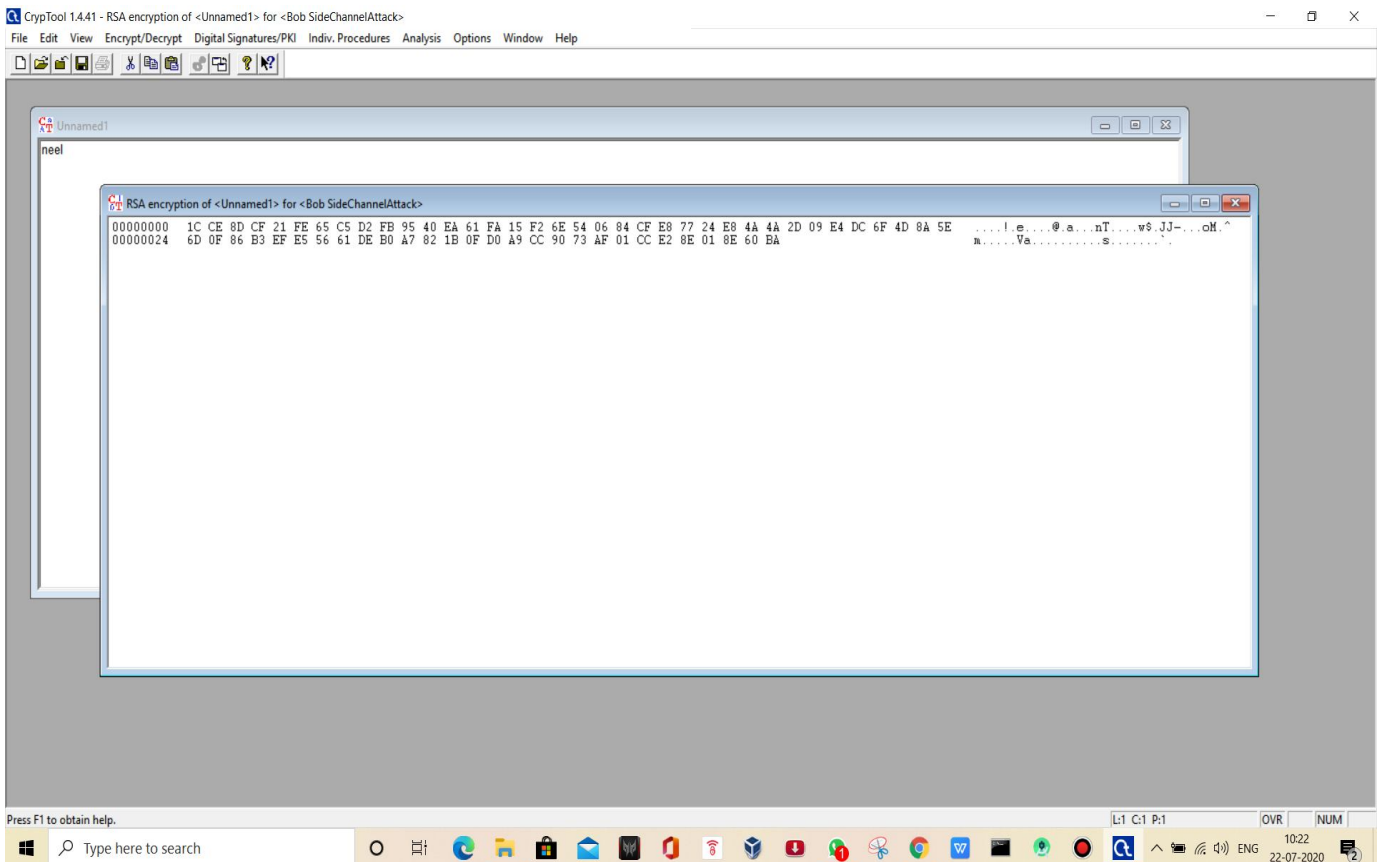
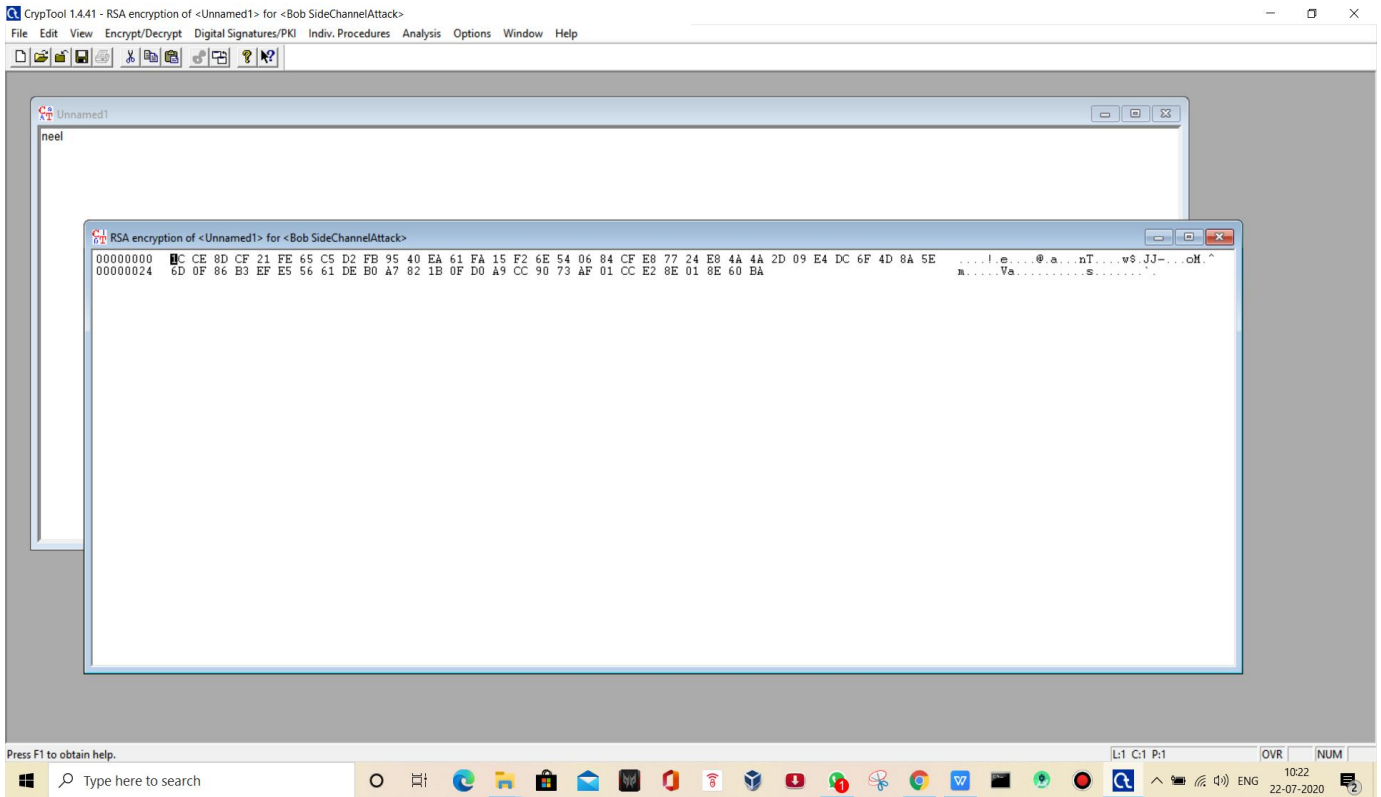
Hash Auto Update

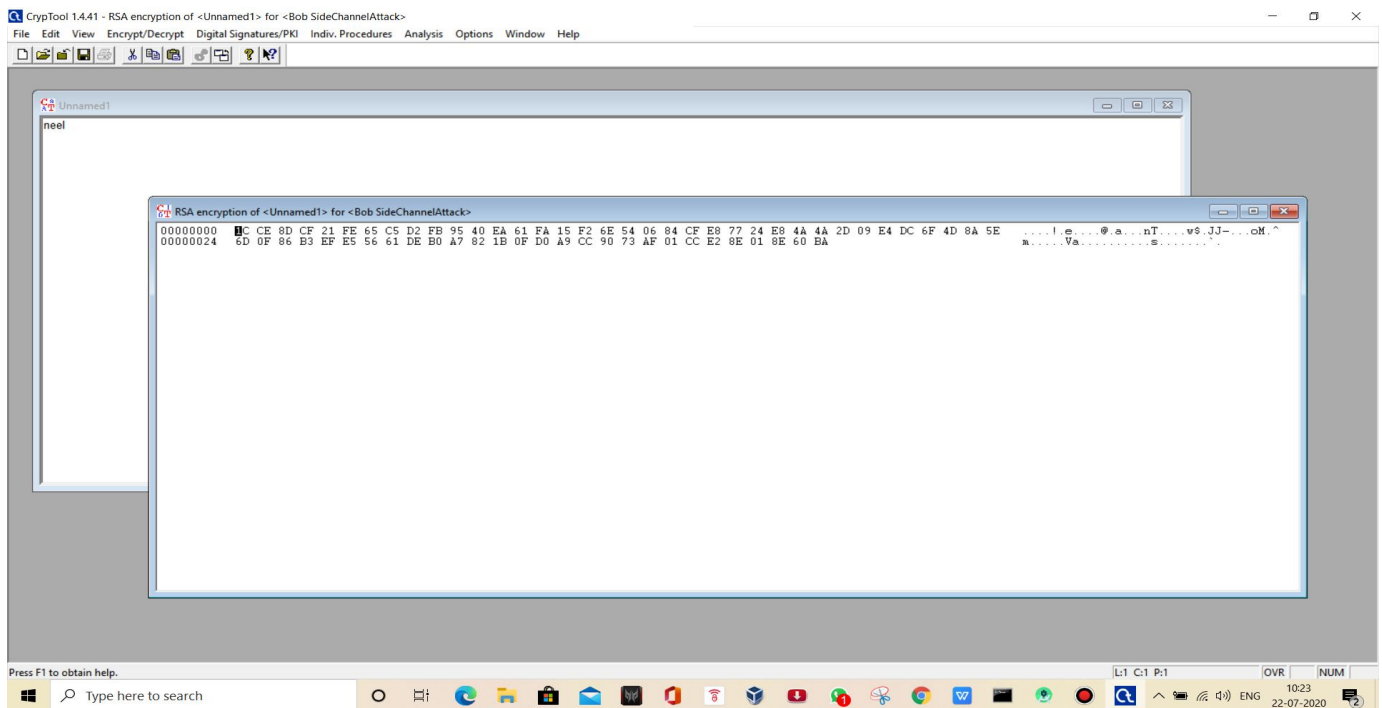
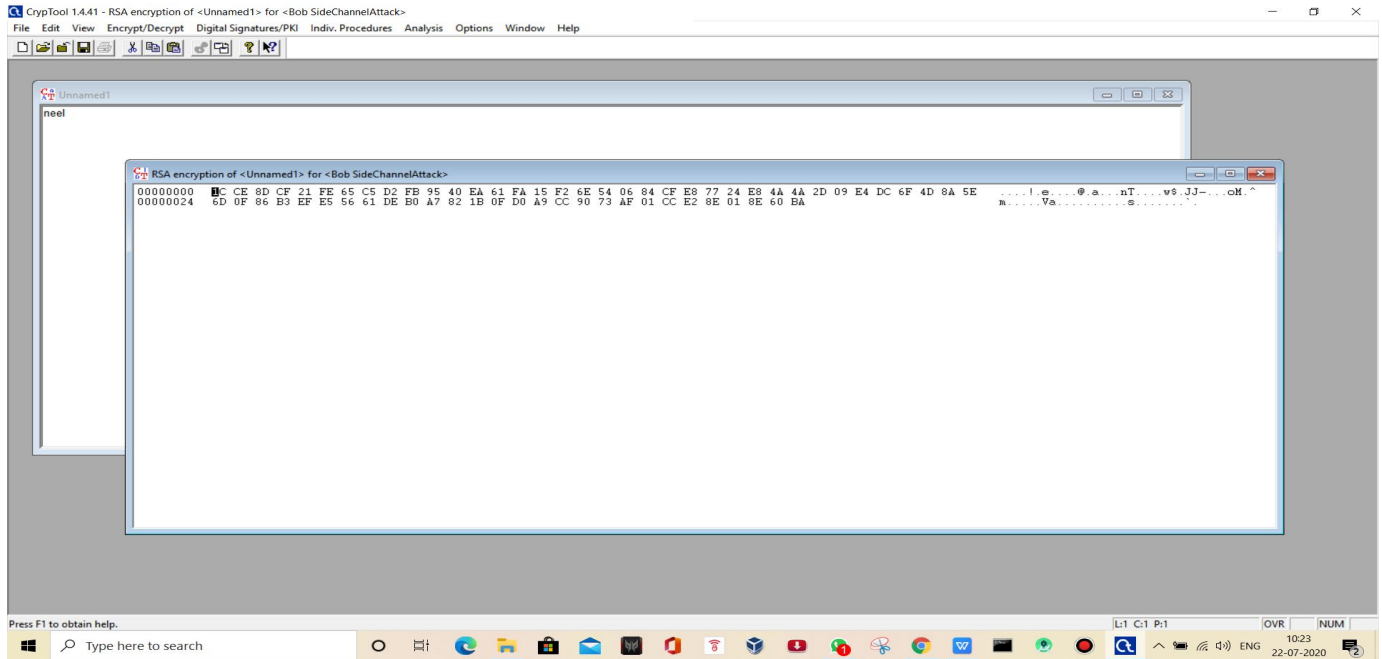
```
2cf63819a5b4753507d41ee546f567ace47510d63fda06feed17c1222fb89786fb55a70118be00d09e02bcf58f74bde885636d79b9abd37ba7f483f8b6522b4d
```

Hash	File Hash
CRC-16	CRC-16
CRC-32	CRC-32
MD2	MD2
MD4	MD4
MD5	MD5
SHA1	SHA1
SHA224	SHA224
SHA256	SHA256
SHA384	SHA384
SHA512	SHA512
SHA512/224	SHA512/224
SHA512/256	SHA512/256
SHA3-224	SHA3-224
SHA3-256	SHA3-256
SHA3-384	SHA3-384
SHA3-512	SHA3-512
Keccak-224	Keccak-224
Keccak-256	Keccak-256
Keccak-384	Keccak-384
Keccak-512	Keccak-512
Shake-128	Shake-128

09:22 22-07-2020

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. ISBN 978-3-642-06383-1.
- [2] Ciphcr 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

Call : 08813907089  (24*7 Support on Whatsapp)