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.2020.30542>

www.ijraset.com

Call: 08813907089

E-mail ID: ijraset@gmail.com

Randomness of Manna Cipher for Larger Plain Texts

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.*

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. Time performance of the Manna Cipher.
- 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

III. HYPOTHESES

A. Null hypotheses

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

B. Alternative Hypotheses

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

The screenshot shows the Visual Studio Code editor interface. The file explorer on the left shows a file named '1.txt'. The editor window displays the content of '1.txt', which is 'hello world'. The status bar at the bottom indicates 'Ln 1, Col 12, Spaces: 4, UTF-8, CRLF, Plain Text'.

Figure 3: The plain text before encrypting

The screenshot shows the Visual Studio Code editor interface. The file explorer on the left shows a file named '1.txt'. The editor window displays the encrypted content of '1.txt', which is a long string of hexadecimal characters. The status bar at the bottom indicates 'Ln 1, Col 15366, Spaces: 4, UTF-8, CRLF, Plain Text'.

Figure 4: The plain text after encrypting

```
1 385224127043792441324288641848422643088821321729220643482840612418764271244022346044217243582413714400843362415734325244132346044249642922432904228044022346044184843472
3460443360443524157343684435241977428044462346044336042592346044379435824228844116429224248242496348924308842604424823460443036429224321427124413241169439004292242583
43254402234604433604259234604420644292242684426044248242886434828441324157343244132346044238843582428864314442042430884390042922424824249634892433914260442922428042280
348924197743144436924228042804362415734325244132419774325242702346044206443912435934368444132425834249643912411694346842812435933482844132415734260442812424824271243802
4318942280440223460443360434723460442064435824238143684442423088422804391242987363400642187642280348923914941848434724248241848348923813942712436924187642280439124604
4008440224157343792438924308842604424823460443254424242381419564282428864427124347241347243892442359343792441324157343144346843088436034892428864228043622488642280
400224157343252441323460442064429224268442604424824288643792348924288641848441324187642280439123460443900428124116943252348924116943036436924187641848434724318941341442482
428864271242623460442064428124116943684420424137143900424824288643792364323985642604424823460441848429224238134828429224298734828441324258334828426242886422804204243088
42280348924116934828426241977434684281241573436844292242482424963489242987439004204248242712420424886417234892433914260442922431743923489243238243468
42042419774325244022430884184843142419774325242702428044403489241472427124259241674427124262431894303644132346044390043582346044206443912411694206443142346044280443582
415734325234892431894379242922424824249634892430884260442482346044303642042430884228044022430883482844022431894346842482428863482842624262425834144436924318943900424824286
437923642346044044428124197743792348924147243360422624318943144424824248243900348923460444224429224228043036348924127042280348924167443360422624318943792429224248242496
3489232382436043472346044390042812415733482843692422804184842922424823482844132415734325244132346044390042812415733482843912415734379244242422482434824390034892
41371427124369241876422804391234604439004248243492439003489241169432524272346044390042812415733482843912418943252348924308842712433641573348284413242583348284281241169
441164282346044184834892416744184842922428863482842922414724228042042346044184842152483440084413234604439004281241573348284391241169432524272425834144434724157343792
440223238243604347234604429224280442433914336043912414724379228071284441978834892391494184843472424824184834892381394271243692418764228043912346043612434892413714368444682
42684439004358241775436844204242684426044468234604361243489242381418484413241876422804336241169439004292243171418484325234604420644292242684426044248242886348284336242583
4242413714390042922425834325234272381394684468242684390043582417754368442042426844260444682358163482842922429873482844132418764228034892430884368442042419774325242922
424242496348924116943252342723460442712437423904280440224308842712427024116943900429224258343252348924258342388348924238142804441324187643360437242987348284259242583
348924348924298742280426243189436844248243460442064435824288643684424824298743468435824288642712427482424824206442482346044422442922430884260442922424823482841324187642280
329842987427124270241876439003489242583423883489242583440084413242987427124237743568440224260442064420424280430364248241472384284262424228043624197742248044022
360183482838522422804303643489243088426044248234604431444358242886422803489241674433604391234604439004281241573348284336242583437924413234604434684204242886439003621234604
420644391243593434684413242583424964391241169434684281243593348284284292242987348284413241977422804232346044271243472346044422442922430884260434892412704400842922428042172
4224248242496348924116943252423734604427124374239042804402243088427124270241169439004292242583423883489242583440084413242987427124237743568440224260442064420424280430364248241472384284262424228043624197742248044022
348924348924298742280426243189436844248243460442064435824288643684424824298743468435824288642712427482424824206442482346044422442922430884260442922424823482841324187642280
329842987427124270241876439003489242583423883489242583440084413242987427124237743568440224260442064420424280430364248241472384284262424228043624197742248044022
360183482838522422804303643489243088426044248234604431444358242886422803489241674433604391234604439004281241573348284336242583437924413234604434684204242886439003621234604
420644391243593434684413242583424964391241169434684281243593348284284292242987348284413241977422804232346044271243472346044422442922430884260434892412704400842922428042172
4224248242496348924116943252423734604427124374239042804402243088427124270241169439004292242583423883489242583440084413242987427124237743568440224260442064420424280430364248241472384284262424228043624197742248044022
348924348924298742280426243189436844248243460442064435824288643684424824298743468435824288642712427482424824206442482346044422442922430884260442922424823482841324187642280
329842987427124270241876439003489242583423883489242583440084413242987427124237743568440224260442064420424280430364248241472384284262424228043624197742248044022
360183482838522422804303643489243088426044248234604431444358242886422803489241674433604391234604439004281241573348284336242583437924413234604434684204242886439003621234604
420644391243593434684413242583424964391241169434684281243593348284284292242987348284413241977422804232346044271243472346044422442922430884260434892412704400842922428042172
4224248242496348924116943252423734604427124374239042804402243088427124270241169439004292242583423883489242583440084413242987427124237743568440224260442064420424280430364248241472384284262424228043624197742248044022
348924348924298742280426243189436844248243460442064435824288643684424824298743468435824288642712427482424824206442482346044422442922430884260442922424823482841324187642280
329842987427124270241876439003489242583423883489242583440084413242987427124237743568440224260442064420424280430364248241472384284262424228043624197742248044022
360183482838522422804303643489243088426044248234604431444358242886422803489241674433604391234604439004281241573348284336242583437924413234604434684204242886439003621234604
420644391243593434684413242583424964391241169434684281243593348284284292242987348284413241977422804232346044271243472346044422442922430884260434892412704400842922428042172
4224248242496348924116943252423734604427124374239042804402243088427124270241169439004292242583423883489242583440084413242987427124237743568440224260442064420424280430364248241472384284262424228043624197742248044022
348924348924298742280426243189436844248243460442064435824288643684424824298743468435824288642712427482424824206442482346044422442922430884260442922424823482841324187642280
329842987427124270241876439003489242583423883489242583440084413242987427124237743568440224260442064420424280430364248241472384284262424228043624197742248044022
360183482838522422804303643489243088426044248234604431444358242886422803489241674433604391234604439004281241573348284336242583437924413234604434684204242886439003621234604
420644391243593434684413242583424964391241169434684281243593348284284292242987348284413241977422804232346044271243472346044422442922430884260434892412704400842922428042172
4224248242496348924116943252423734604427124374239042804402243088427124270241169439004292242583423883489242583440084413242987427124237743568440224260442064420424280430364248241472384284262424228043624197742248044022
348924348924298742280426243189436844248243460442064435824288643684424824298743468435824288642712427482424824206442482346044422442922430884260442922424823482841324187642280
329842987427124270241876439003489242583423883489242583440084413242987427124237743568440224260442064420424280430364248241472384284262424228043624197742248044022
360183482838522422804303643489243088426044248234604431444358242886422803489241674433604391234604439004281241573348284336242583437924413234604434684204242886439003621234604
420644391243593434684413242583424964391241169434684281243593348284284292242987348284413241977422804232346044271243472346044422442922430884260434892412704400842922428042172
4224248242496348924116943252423734604427124374239042804402243088427124270241169439004292242583423883489242583440084413242987427124237743568440224260442064420424280430364248241472384284262424228043624197742248044022
348924348924298742280426243189436844248243460442064435824288643684424824298743468435824288642712427482424824206442482346044422442922430884260442922424823482841324187642280
329842987427124270241876439003489242583423883489242583440084413242987427124237743568440224260442064420424280430364248241472384284262424228043624197742248044022
360183482838522422804303643489243088426044248234604431444358242886422803489241674433604391234604439004281241573348284336242583437924413234604434684204242886439003621234604
420644391243593434684413242583424964391241169434684281243593348284284292242987348284413241977422804232346044271243472346044422442922430884260434892412704400842922428042172
4224248242496348924116943252423734604427124374239042804402243088427124270241169439004292242583423883489242583440084413242987427124237743568440224260442064420424280430364248241472384284262424228043624197742248044022
348924348924298742280426243189436844248243460442064435824288643684424824298743468435824288642712427482424824206442482346044422442922430884260442922424823482841324187642280
329842987427124270241876439003489242583423883489242583440084413242987427124237743568440224260442064420424280430364248241472384284262424228043624197742248044022
360183482838522422804303643489243088426044248234604431444358242886422803489241674433604391234604439004281241573348284336242583437924413234604434684204242886439003621234604
420644391243593434684413242583424964391241169434684281243593348284284292242987348284413241977422804232346044271243472346044422442922430884260434892412704400842922428042172
4224248242496348924116943252423734604427124374239042804402243088427124270241169439004292242583423883489242583440084413242987427124237743568440224260442064420424280430364248241472384284262424228043624197742248044022
348924348924298742280426243189436844248243460442064435824288643684424824298743468435824288642712427482424824206442482346044422442922430884260442922424823482841324187642280
329842987427124270241876439003489242583423883489242583440084413242987427124237743568440224260442064420424280430364248241472384284262424228043624197742248044022
360183482838522422804303643489243088426044248234604431444358242886422803489241674433604391234604439004281241573348284336242583437924413234604434684204242886439003621234604
420644391243593434684413242583424964391241169434684281243593348284284292242987348284413241977422804232346044271243472346044422442922430884260434892412704400842922428042172
4224248242496348924116943252423734604427124374239042804402243088427124270241169439004292242583423883489242583440084413242987427124237743568440224260442064420424280430364248241472384284262424228043624197742248044022
348924348924298742280426243189436844248243460442064435824288643684424824298743468435824288642712427482424824206442482346044422442922430884260442922424823482841324187642280
329842987427124270241876439003489242583423883489242583440084413242987427124237743568440224260442064420424280430364248241472384284262424228043624197742248044022
360183482838522422804303643489243088426044248234604431444358242886422803489241674433604391234604439004281241573348284336242583437924413234604434684204242886439003621234604
420644391243593434684413242583424964391241169434684281243593348284284292242987348284413241977422804232346044271243472346044422442922430884260434892412704400842922428042172
4224248242496348924116943252423734604427124374239042804402243088427124270241169439004292242583423883489242583440084413242987427124237743568440224260442064420424280430364248241472384284262424228043624197742248044022
3489243489242
```

3) Actual data

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.The performance analysis regarding randomness of SHA 256 SHA 512 and RSA 512 with the Manna ciphering standard shall be the part of future research work.

REFERENCES

- [1] F. L. Bauer, *Decrypted Secrets*. Springer, 2010. 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

Call : 08813907089 (24*7 Support on Whatsapp)