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.2020.30439

www.ijraset.com

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

Manna Cipher

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 performance.

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 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

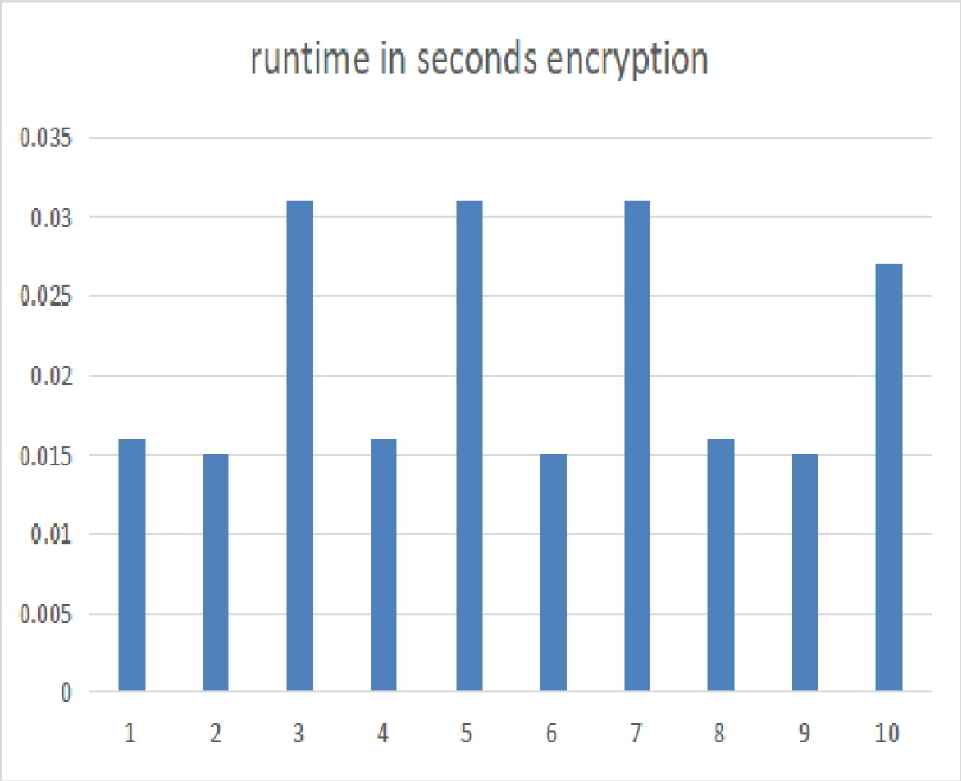


Figure 1:

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.

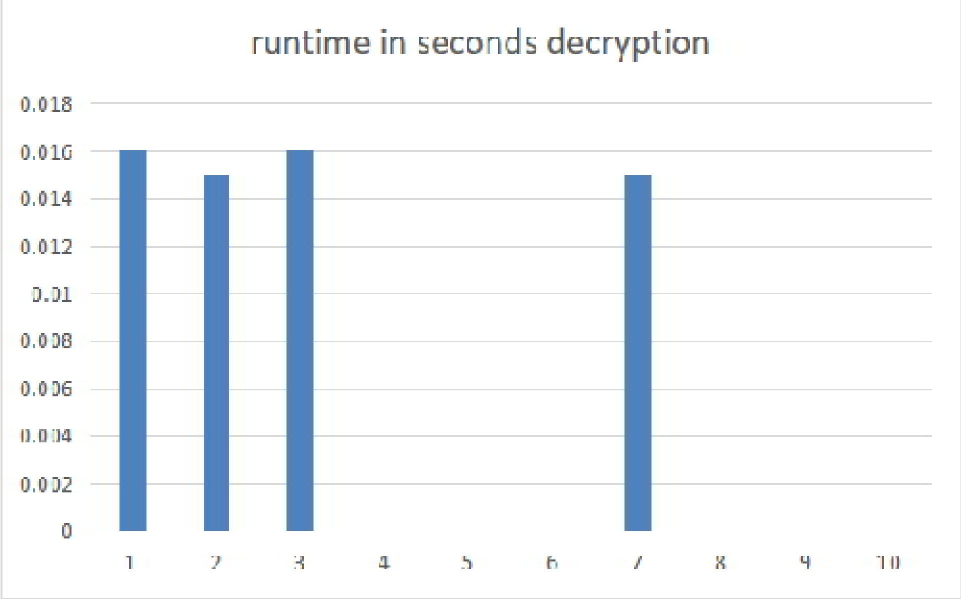
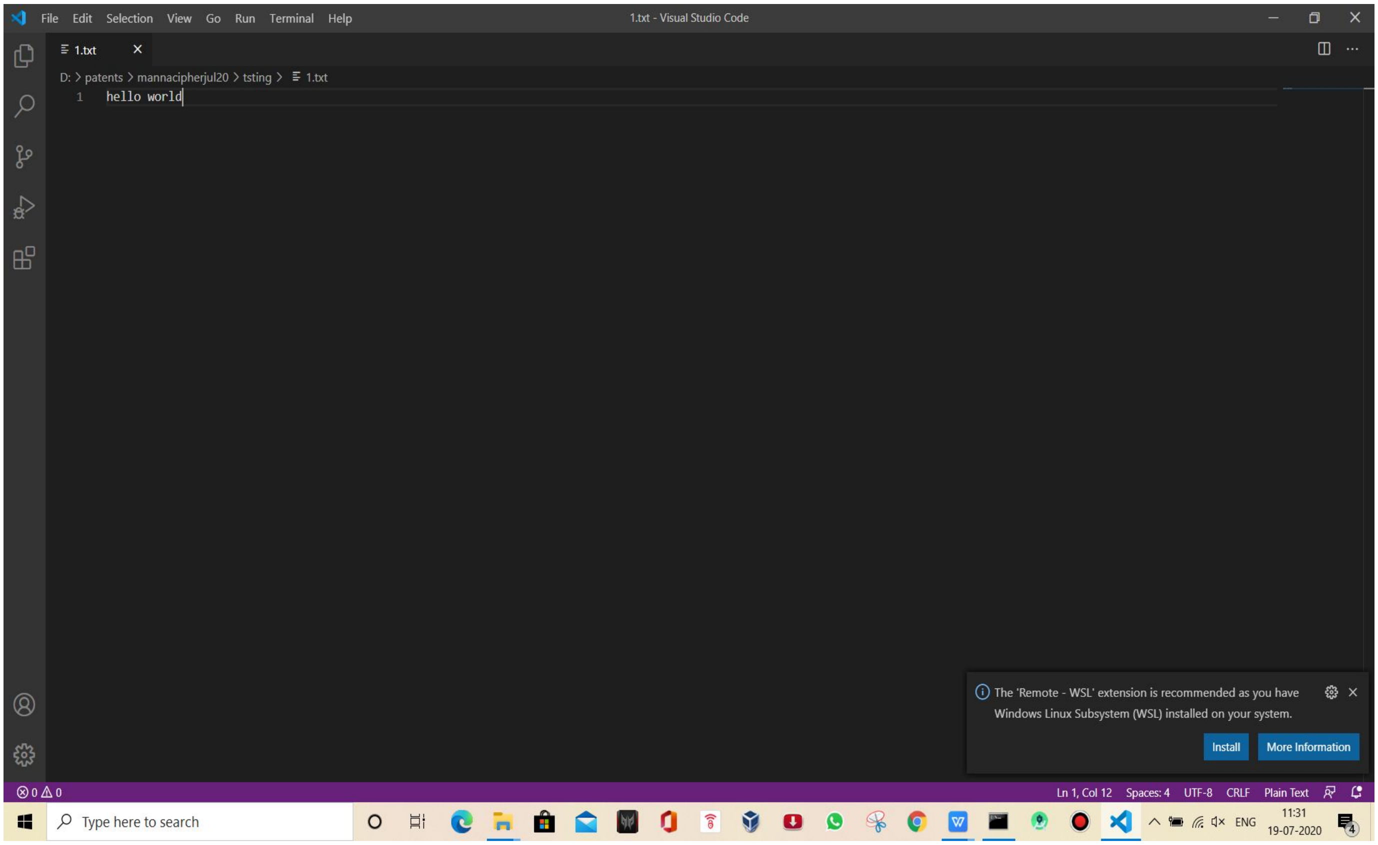


Figure 2:

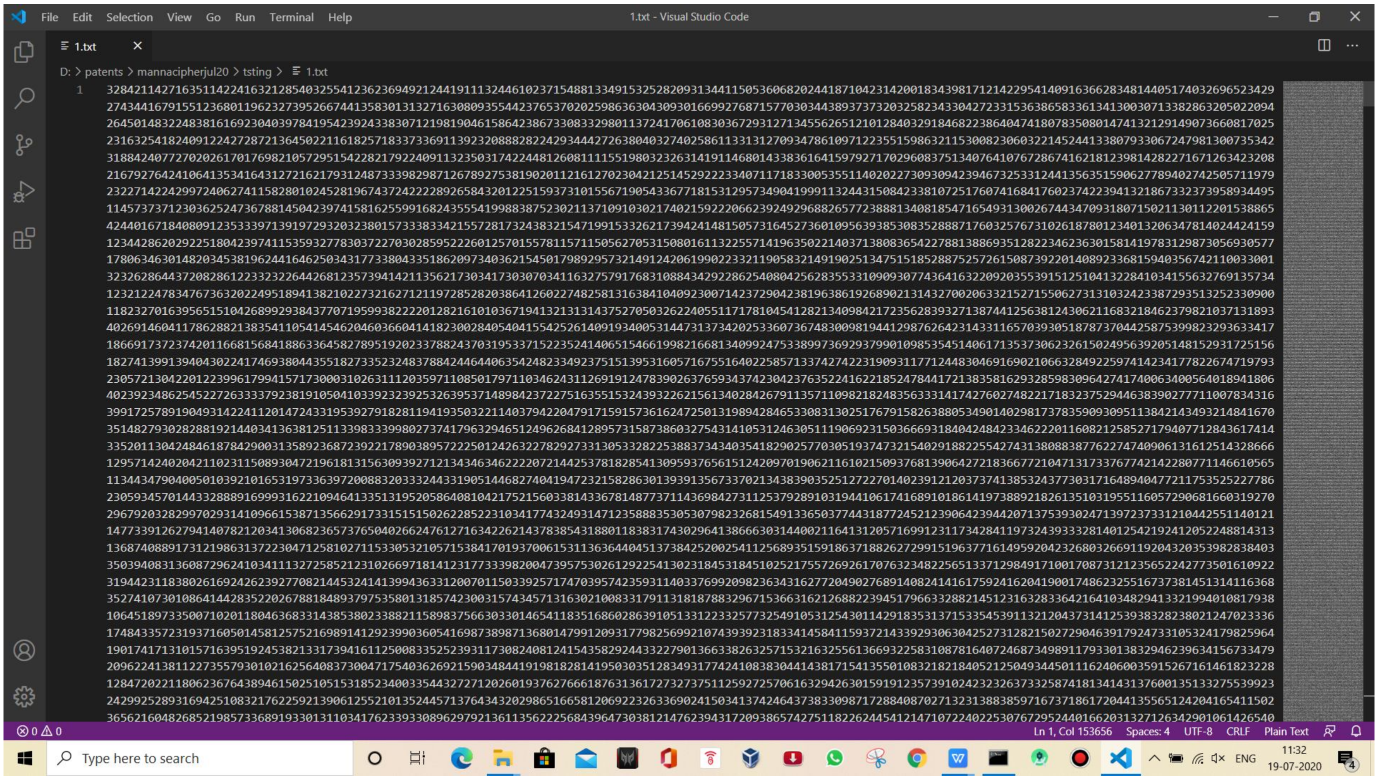
In figure 2 the run time is depicted to decrypt a text file containing the Manna cipher with the password neel .The time taken to decrypt in seconds is depicted along y axis and the serial number of the decryption round is depicted along x axis.


File Edit Selection View Go Run Terminal Help
1.txt - Visual Studio Code
1.txt
D: > patents > mannacipherjul20 > tsting > 1.txt
Install
More Information
⊗ 0 ⚠ 0
Ln 1, Col 12 Spaces: 4 UTF-8 CRLF Plain Text
Type here to search
ENG
11:31
19-07-2020

```
hello world
```

The 'Remote - WSL' extension is recommended as you have Windows Linux Subsystem (WSL) installed on your system.

Figure 3:The plain text before encrypting


File Edit Selection View Go Run Terminal Help
1.txt - Visual Studio Code
1.txt
D: > patents > mannacipherjul20 > tsting > 1.txt
⊗ 0 ⚠ 0
Ln 1, Col 153656 Spaces: 4 UTF-8 CRLF Plain Text
Type here to search
ENG
11:32
19-07-2020

```
32842114271635114224163212854032554123623694921244191113244610237154881334915325282093134411505360682024418710423142001834398171214229541409163662834814405174032696523429
27434416791551236801196232739526674413583013132716308093554423765370202598636304309301669927687157703034438937373203258234330427233153638658336134130030713382863205022094
26450148322483816169230403978419542392433830712198190461586423867330833298011372417061083036729312713455626512101284032918468223864047418078350801474132129149073660817025
23163254182409122427287213645022116182571833733691139232088828224293444272638040327402586113313127093478610971223551598632115300823060322145244133807933067247981300735342
31884240772702026170176982105729515422821792240911323503174224481260811115519803232631419114680143383616415979271702960837513407641076728674162181239814282271671263423208
21679276424106413534164312721621793124873339829871267892753819020112161270230421251452922233407117183300535511402022730930942394673253312441356351590627789402742505711979
23227142242997240627411582801024528196743724222289265843201225159373101556719054336771815312957349041999113244315084233810725176074168417602374223941321867332373958934495
11457373712303625247367881450423974158162559916824355541998838752302113710910302174021592220662392492968826577238881340818547165493130026744347093180715021130112201538865
42440167184080912353339713919729320323801573338334215572817324383215471991533262173942414815057316452736010956393853083528887176032576731026187801234013206347814024424159
12344286202922518042397411535932778303722703028595222601257015578115711505627053150801611322557141963502214037138083654227881388693512822346236301581419783129873056930577
17806346301482034538196244164625034317733804335186209734036215450179892957321491242061990223321190583214919025134751518528875257261508739220140892336815940356742110033001
32326286443720828612233232264426812357394142113562173034173030703411632757917683108843429228625408042562835533109093077436416322092035539151251041322841034155632769135734
12321224783476736320224951894138210227321627121197285282038641260227482581316384104092300714237290423819638619268902131432700206332152715506273131032423387293513252330900
11823270163956515104268992938437707195993822220128216101036719413213131437527050326224055117178104541282134098421723562839327138744125638124306211683218462379821037131893
40269146041178628821383541105414546204603660414182300284054041554252614091934005314473137342025336073674830098194412987626423143311657039305187873704425875399823293633417
18669173723742011668156841886336458278951920233788243703195337152235241406515466199821668134099247533899736929379901098535451406171353730623261502495639205148152931725156
18274139913940430224174693804435518273352324837884244644063542482334923751513953160571675516402258571337427422319093117712448304691690210663284922597414234177822674719793
23057213042201223996179941571730003102631112035971108501797110346243112691912478390263765934374230423763522416221852478441721383581629328598309642741740063400564018941806
40239234862545227263333792381910504103392323925326395371489842372275163551532439322621561340284267911357110982182483563331417427602748221718323752944638390277711007834316
39917257891904931422411201472433195392791828119419350322114037942204791715915736162472501319894284653308313025176791582638805349014029817378359093095113842143493214841670
35148279302828881921440341363812511339833399802737417963294651249626841289573158738603275431410531246305111906923150366693184042484233462220116082125852717940771284361741 4
33520113042484618784290031358923687239221789038957222501242632278292733130533282253883734340354182902577030519374732154029188225542743138088387762274740906131612514328666
12957142402042110231150893047219618131563093927121343463462222072144253781828541309593765615124209701906211610215093768139064272183667721047131733767742142280771146610565
11344347904005010392101653197336397200883203332443319051446827404194723215828630139391356733702134383903525127227014023912120373741385324377303171648940477211753525227786
23059345701443328889169993162210946413351319520586408104217521560338143367814877371143698427311253792891031944106174168910186141973889218261351031955116057290681660319270
29679203282997029314109661538713566291733151515026228522310341774324931471235888353053079823268154913365037744318772452123906423944207137539302471397237331210442551140121
14773391262794140782120341306823657376504026624761271634226214378385431880118383174302964138666303144002116413120571699123117342841197324393332814012542192412052248814313
13687408891731219863137223047125810271153305321057153841701937006153113636440451373842520025411256893515918637188262729915196377161495920423268032669119204320353982838403
35039408313608729624103411132725852123102669718141231773339820047395753026129225413023184531845102521755726926170763234822565133712984917100170873121235652242773501610922
31944231183802616924262392770821445324141399436331200701150339257174703957423593114033769920982363431627720490276891408241416175924162041900174862325516737381451314116368
35274107301086414428352202678818489379753580131857423003157434571316302100833179113181878832967153663162126882239451796633288214512316328336421641034829413321994010817938
10645189733500710201180463683314385380233882115898375663033014654118351686028639105133122332577325491053125430114291835313715335453911321204373141253938328238021247023336
17484335723193716050145812575216989141292399036054169873898713680147991209317798256992107439392318334145841159372143392930630425273128215027290463917924733105324179825964
19017417131015716395192453821331739416112500833525239311730824081241543582924433227901366338263257153216325561366932258310878164072468734989117933013832946239634156733479
20962241381122735579301021625640837300471754036269215903484419198182814195030351283493177424108383044143817154135501083218218405212504934450111624060035915267161461823228
12847202211806236764389461502510515318523400335443272712026019376276661876313617273273751125927257061632942630159191235739102423232637332587418134143137600135133275539923
24299252893169425108321762259213906125521013524457137643432029865166581206922326336902415034137424643738330987172884087027132313883859716737186172044135565124204165411502
36562160482685219857336891933013110341762339330896297921361135622256843964730381214762394317209386574275118226244541214710722402253076729524401662031327126342901061426540
```

Figure 4:The plain text after encrypting

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 will be the scope of my future research work.

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.

I. CONCLUSIONS

The version of this template is V2. Most of the formatting instructions in this document have been compiled by Causal Productions from the IEEE LaTeX style files. Causal Productions offers both A4 templates and US Letter templates for LaTeX and Microsoft Word. The LaTeX templates depend on the official IEEEtran.cls and IEEEtran.bst files, whereas the Microsoft Word templates are self-contained. Causal Productions has used its best efforts to ensure that the templates have the same appearance.

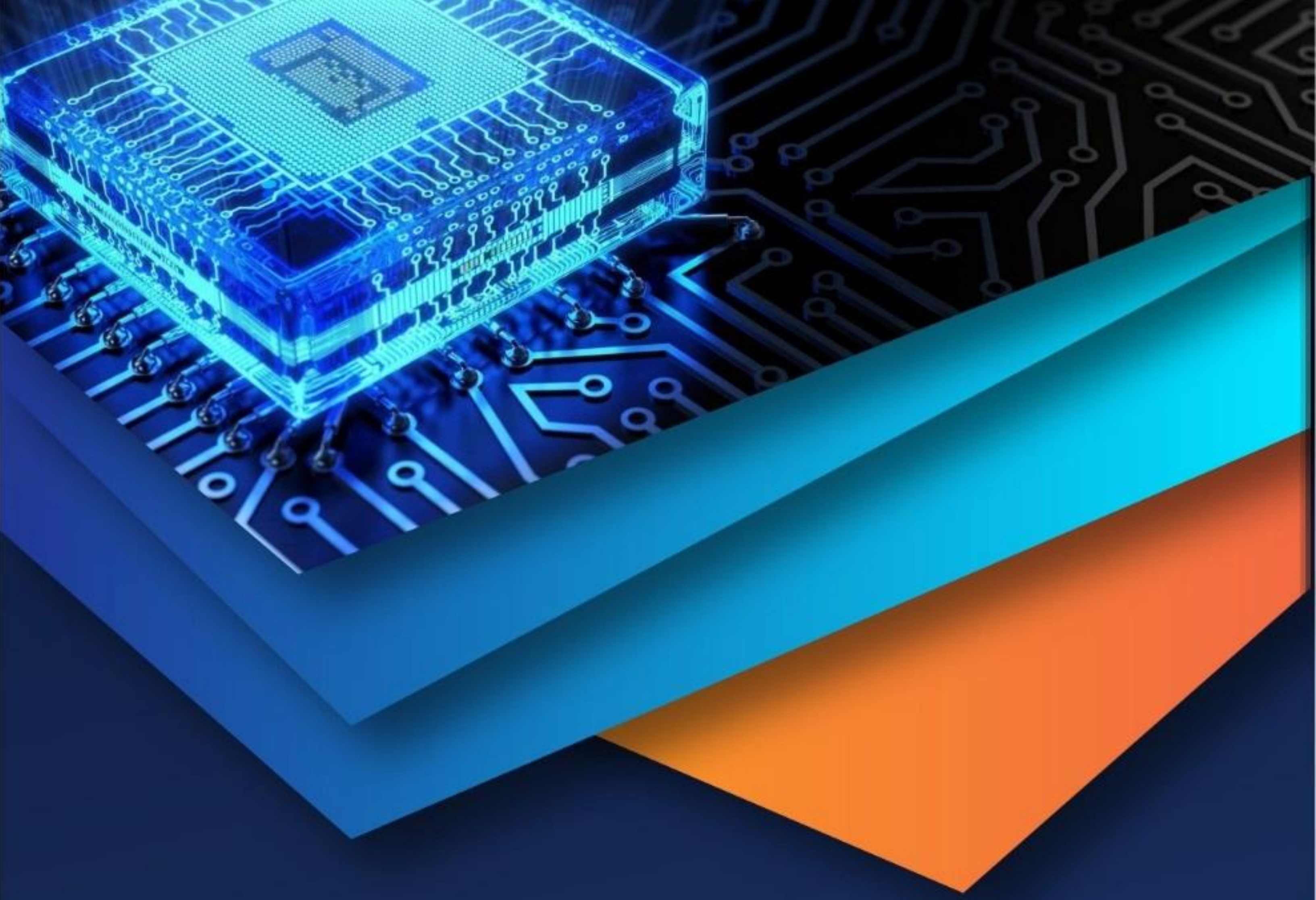
Causal Productions permits the distribution and revision of these templates on the condition that Causal Productions is credited in the revised template as follows: "original version of this template was provided by courtesy of Causal Productions (www.causalproductions.com)".

II. ACKNOWLEDGMENT

The heading of the Acknowledgment section and the References section must not be numbered.Causal Productions wishes to acknowledge Michael Shell and other contributors for developing and maintaining the IEEE LaTeX style files which have been used in the preparation of this template. To see the list of contributors, please refer to the top of file IEEETran.cls in the IEEE LaTeX distribution.

REFERENCES

[1] S. M. Metev and V. P. Veiko, Laser Assisted Microtechnology, 2nd ed., R. M. Osgood, Jr., Ed. Berlin, Germany: Springer-Verlag, 1998.
[2] J. Breckling, Ed., The Analysis of Directional Time Series: Applications to Wind Speed and Direction, ser. Lecture Notes in Statistics. Berlin, Germany: Springer, 1989, vol. 61.
[3] S. Zhang, C. Zhu, J. K. O. Sin, and P. K. T. Mok, "A novel ultrathin elevated channel low-temperature poly-Si TFT," IEEE Electron Device Lett., vol. 20, pp. 569–571, Nov. 1999.
[4] M. Wegmuller, J. P. von der Weid, P. Oberson, and N. Gisin, "High resolution fiber distributed measurements with coherent OFDR," in Proc. ECOC'00, 2000, paper 11.3.4, p. 109.
[5] R. E. Sorace, V. S. Reinhardt, and S. A. Vaughn, "High-speed digital-to-RF converter," U.S. Patent 5 668 842, Sept. 16, 1997.
[6] (2002) The IEEE website. [Online]. Available: http://www.ieee.org/
[7] M. Shell. (2002) IEEEtran homepage on CTAN. [Online]. Available: http://www.ctan.org/tex-archive/macros/latex/contrib/supported/IEEEtran/
[8] FLEXChip Signal Processor (MC68175/D), Motorola, 1996.
[9] "PDCA12-70 data sheet," Opto Speed SA, Mezzovico, Switzerland.
[10] A. Karnik, "Performance of TCP congestion control with rate feedback: TCP/ABR and rate adaptive TCP/IP," M. Eng. thesis, Indian Institute of Science, Bangalore, India, Jan. 1999.
[11] J. Padhye, V. Firoiu, and D. Towsley, "A stochastic model of TCP Reno congestion avoidance and control," Univ. of Massachusetts, Amherst, MA, CMPSCI Tech. Rep. 99-02, 1999.
[12] Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specification, IEEE Std. 802.11, 1997.



doi crossref

10.22214/IJRASET

INDEX COPERNICUS

45.98

ISRA JIF

IMPACT FACTOR: 7.129

SJIFactor Scientific Journal Impact Factor TOGETHER WE REACH THE GOAL

IMPACT FACTOR: 7.429

ISI

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 ✆ (24*7 Support on Whatsapp)