



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
- 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.



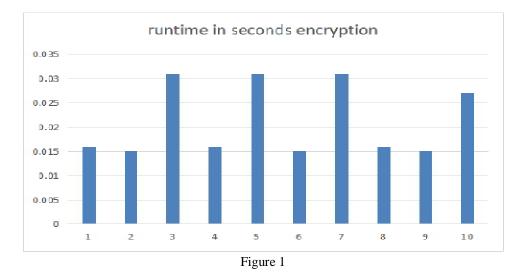
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429 Volume 8 Issue VII July 2020- Available at www.ijraset.com

## **IV. METHODOLOGY**

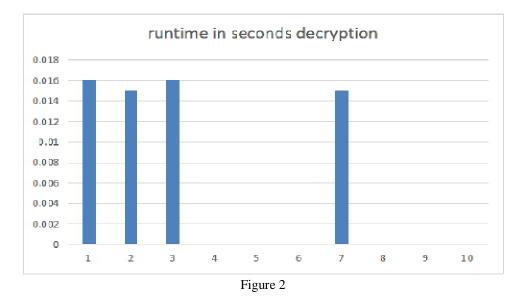
- A. The Configurations of The Computer Under Study
- 1) Windows 10 home edition
- 2) Intel i5 8<sup>th</sup> gen
- 3) GTX 1050ti
- 4) 8gb ddr4 ram
- 5) 1tb hdd
- 6) 128 gb ssd

## B. Algorithm Implementation

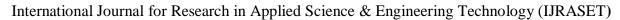
1) Using C



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.



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.





ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429 Volume 8 Issue VII July 2020- Available at www.ijraset.com

📢 File Edit Selection View Go Run Terminal He	lp					1.	.txt - Visu	ual Studio (	Code						-	٥	×
E 1.txt ×																	••••
D: > patents > mannacipherjul20 > tsting >  ≡ 1.txt																	-
P 1 hello world																	
P																	
¢¢																	
·B <sup>C</sup>																	
8														The 'Remote - WSL' extension is recomm Windows Linux Subsystem (WSL) installe			×
- 																Informatio	m
\$°5 ⊗ 0 ≜ 0																	(
♥ 0 ▲ 0	0	⊟i		-	<b>A</b>		0	6	-	0	•			Ln 1, Col 12 Spaces: 4 UTF		24	4
- Type here to search	U	HI	C				-	uro 3		-		0,	<u> </u>		19-07	-2020	4

Figure 3

#### The plain text before encrypting

Edit Selection View Go Run Terminal Help l.txt - Visual Studio Code ≣ 1.txt Ch 31884240772702026170176982105729515422821792240911323503174224481260811115519803232631419114680143383616415979271702960837513407641076728674162181239814282271671263423208 32326286443720828612233232264426812357394142113562173034173030703411632757917683108843429228625408042562835533109093077436416322092035539151251041322841034155632769135734 1182327016395651510426899293843770719599382222012821610103671941321313143752705032622405511717810454128213409842172356283932713874412563812430621168321846237982103713189 4023923486254522726333379238191050410339232392532639537148984237227516355153243932262156134028426791135711098218248356333141742760274822171832375294463839027771100783431 35039408313608729624103411132725852123102669718141231773339820047395753026129225413023184531845102521755726926170763234822565133712984917100170873121235652242773501610922 35274107301086414428352202678818489379753580131857423003157434571316302100833179113181878832967153663162126882239451796633288214512316328336421641034829413321994010817938 1284/202211860/230764.359401505310512540055534452727120200135762700003670150172727575125727001032945505571372574270013294505571725412720013707100170412722001357650124204165411502 242992528931694251083217622592139061255210135244571376434320298651665812069223263369024150341374246437383309871728840870271323138838597167318617204413556512420416541150 365621604826852198573368919330131103417623393308962979213611356222568439647303812147623943172093865742751182262445412147187224022530767729524401660213271263429011661426540 Ln 1, Col 153656 Spaces: 4 UTF-8 CRLF PI -P Type here to search O Hì 💽 🦬 💼 💼 🚺 🧃 🗊 🗊 🙂 🕓 🚱 🕼 🖾 🐨 🖉 🖉 🖉 🖉 🖉 🖉 🖉 🖉 🖉 🕅 1132 19-07-2020 Figure 4



## 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

The plain text after encrypting

Variations of cipher text for same password (i)

>	File Edit	Selection	View Go	Run Termin	ial Help					1.t	ct - Visual St	udio Code										-	٥	×
Ch	≣ 1.txt																							
	COUS	ers > neela >	OneDrive >	Desktop > ijra	set > ≣ 1 t																			
Q		22517252 59927355	6526982278 2834725568	95279072516 26881281112 26587185992	425366278 691725568	89512067 82738618	823275772	25669185	992778727	57726275	27285267	972746725	577018599	92789526	80725568	185992703	12691726	37625972	22789526	03727083	25972273	5527		
နစ		23725568	269821882	26275262752 27577264771 18599278952	859926059	92757726	376266792	28003281	272556826	88127787	20427238	512587126	52751888	72314425	16427247	274672516	41859922	60326917	2667925	87126275	27907185	9927		
å				18887253662 25366265992																		200		
₿		16426707 47726477	2746726982 185992800	26257259722 27083258432 28017259722	713725972 647726491	22647726 11888727	491272472 083258712	27588185 26275188	992616726 872627525	91725669 16427895	25669267 26477269	072625727 322708318	718426275 38232801	52789518 72718426	88727083. 57926275:	265781882 279071859	32625726 92536627	88125164 35527357	12605927 72667927	13718599 18427895	25568281 26477268	1126 8126		
		88716377	2657827247	25871267072 18887270832 25568276791	587126275	51888726	679262752	25843269	172647718	59927895	26477274	372708318	8232812	72587125	56818823	279072556	82698228	00327247	2708325	16427247	28127185	9925		
		34725568	185992584	18887256692	516426707	72790718	599259722	26167264	772516418	59925843	26147265	782718427	8951888	72708325	87126275	188872688	12516427	24726367	2657826	37627247	26477269	8226		
		72708326	5782649127	90725164266	792659928	86771859	919811188	32327357	251642708	32659926	47726376	251642789	5269172	53662516	42703118	887253662	59722746	32680725	5682688	11882327	35726578	2546		
				81118823282 5772647716																				
				47726167188																				
		92778726	9172577025	87127895188	872657825	56691882	327577271	18427083	277872691	72546725	56827679	280171859	92536625	58432724	72627525	568261671	88872556	82647726	52752735	72597225	56827787	2042		
				24718599276 08327355266																				
				03726477254 59926923264																				
		72647725	5682767926	03726275185	992638327	79072657	826376188	32327687	255682688	12800328	01725972	264772649	11888720	56792688	12670728	347251642	70832627	51888726	3762556	82778728	01725164	2577		-
				159922711269 120718599256																				
				81118823269																				
		92811126	9172708325	16427031188	872708326	65781882	326257271	18426881	276792647	72647727	08318823	262572688	31275882	74632812	72657825	770276792	60372667	92587128	84351888	72698227	08325843	2746		
8		72670728 72556826	0172708320 8812778718	36726982200 98218823260 88726578256 47726491202	372708318 691882326	85992789 60372688	526807255 125972278	56818599 39526807	260592757	72647727	28526275 91725366	279072577 198111882	702556823 232801720	72472625 55782566	72556818 92789528	599273552 457251642	65871859 68812627	92708326 51888725	55992647 55682647	71859926 72649126	57827679 91726477	2636 2556		
633 ⊗0	A 0.	72667926	5782724726	36725568264 56820335188	772605926	6477 <u>1</u> 859	926982266	95926917	255682647	72605926	47719811	185992584	13274672	54671859	92713926	037270832	55682767 76872708	92691725 32657826	51642627 54912790	51882328 72516426	01725366 67926599	2597 2867	ext &	۵
		pe here to s	search			0	at 🕐	-	<b>Ê</b>		0	8	0	0	<b>%</b> (			9 O			ITF-8 CRLF <i>(</i> 虎 印) EN	201	39	

#### Actual data

	File Edit	Selection	View	Go Rur		al Help								Studio	Code														٥	
Ð	≣ 1.txt																											ab- c⊄		
Q v		sers > neela Abstract uses the painstal on the p	— This numbe cingly	docume ring sy difficu	nt gives stem to lt to cr	an ove represe ack eve	rview o nt ciph n using	ers rat the la	her thar test sup	n alph Der co	anumeric mputers.	charac This d	ters.Tl	ne aim : wil	is to 1 be fo	create						lues o	on comp	outers.	.The M	Manna (	Cipher			
₽ ₽		Keywords I.Introc Cryptogr security cryptogr of crypt of a scr Alice (' the appr II. OBJE A.Manna B.Time p	luction raphy, raphy i , for raphy e cograph raphy p rambled 'A") for roach o CTIVES cipher	is the s tied example xists a y incorp receding message r the su f PCs in OF THE random	training in with , inform t the co porate e g the cu e shares ender, B n World STUDY ness vis	and in buildin ation s nvergen lectron tting e the un ounce ( War II, ualisat	vestiga g and i ecrecy, ice of t ic busi dge age ravelin "B") fo the te	tion of nvestig inform he orde ness, cl was ad g strat r the e	methods ating co ation re rs of ar hip-base equately egy just xpected	s for onvent espect rithme ed ins / equi t with benef	secure o ions tha ability, tic, sof tallment valent w planned iciary,	correspo at keep valida tware e cards, vith enc benefi and Eve	ondence outside tion, a engineer comput compution ciaries e ("mede	withi ers or and no ring, cerize a, the s to b iler")	people n-revoc electri d monet change lock ac for th	e in ger cation a ical bui cary for e of dat ccess fr ne foe.	neral fi are vita ilding, rms, PC ta from rom ener Since	rom pe al to corre passw an in mies. the im	rusing curren sponde ords, tellig The cr provem	priva t cryp nce so and mi ible so yptogr ent of	ite mes itograp ience, litary itate t aphy w	ssages ohy st , and / corr to obv writin r figu	andaro materi respond vious n ng regu ure mag	ferent ds. Pre ial sci dences. rubbish ularly chines	angle esent ience n. The utili in Wo	es in o day . Util: e orig izes tl orld Wa	data ization inator ne name ar I an	s		
		<ul> <li>c. Ident</li> <li>III.HYPC</li> <li>A. Null</li> <li>1) H01:</li> <li>2) H02:</li> <li>3) H03:</li> <li>B. Alter</li> <li>1) H11:</li> <li>2) H12:</li> </ul>	ifying OTHESES hypoth For th The pl Run ti rnative For th	whether eses ain tex me vari Hypothe same	r the ti encrypti t and ci es by a eses encrypti	me take on key pher te huge de on key	the res the res gree du the res	ultant always e to va ultant	cipher i same in rying le cipher i	is the lengt engths is not	same h of ciph same			gree d	ue to i	increase	e in th	e leng	th of	the ci	pher.									
@		3) H13: IV.METHC	DOLOGY						e to var	rying	lengths	of ciph	ier text							0						istalled o	ded as ye on your s nstall	/stem.	چي nformati	
⊗ 0.	▲ 0	pe here to					0	H	<b>a</b> =		<b>A</b> 🔿		0	1		0	0	R	0	2	-	Lr	n 40, Col	12 Spa			CRLF	20:4	4	¢
-	~ Iy	pe nere to	scarell				0				-	- WY		0	A.	~		6	<u> </u>		-	101	•	~			LING	21-07-2	2020	2



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

Online Tools			
SHA256	Hash	File Hash	
	CRC-16	CRC-16	
SHA256 online hash function	CRC-32	CRC-32	
neel	MD2	MD2	
	MD4	MD4	
	MD5	MD5	
	SHA1	SHA1	
	SHA224	SHA224	
	SHA256	SHA256	
h	SHA384	SHA384	
Input type Text 🗸	SHA512	SHA512	
Hash ZAuto Update	SHA512/224	SHA512/224	
	SHA512/256	SHA512/256	
983d3dc41c81113f13375728ff0dd5ca33d5d2f4c0c29c0df126a030627c3fcb	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	Show a

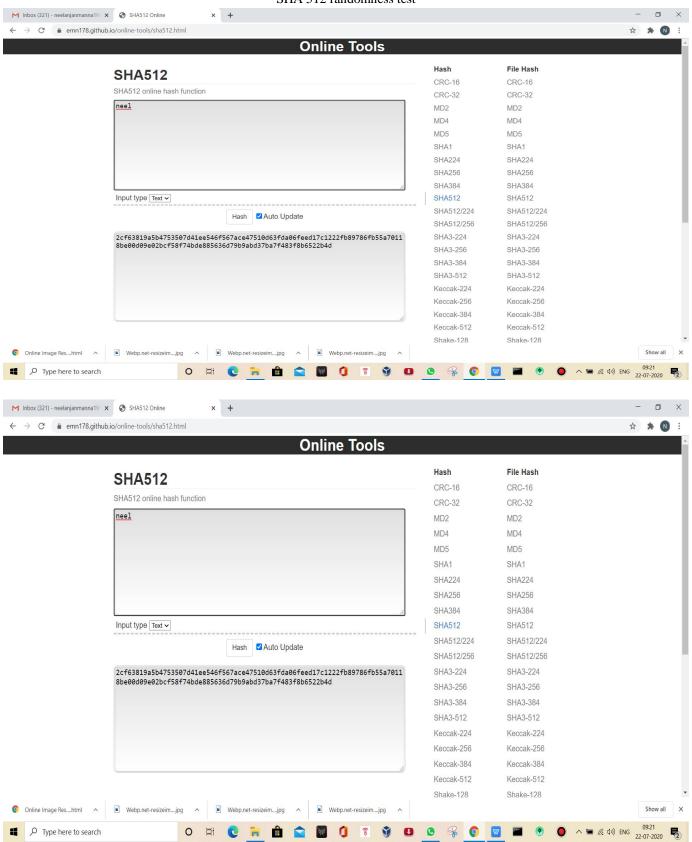


neel	MD2	MD2		
	MD4	MD4		
	MD5	MD5		
	SHA1	SHA1		
	SHA224	SHA224		
	SHA256	SHA256		
	SHA384	SHA384		
Input type Text 🗸	SHA512	SHA512		
Hash ZAuto Update	SHA512/224	SHA512/224		
	SHA512/256	SHA512/256		11
983d3dc41c81113f13375728ff0dd5ca33d5d2f4c0c29c0df126a030627c3fcb	SHA3-224	SHA3-224		
	SHA3-256	SHA3-256		
	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 Image Reshtml       Image Webp.net-resizeimjpg       Image Webp.net-resizeimjpg			Show all	×
📫 🔎 Type here to search O 🛱 💽 🚞 🏦 😭 🕥 🧊 💲	0 9 % 0	💟 🖬 🙆 🔵	へ 🍽 🦟 (小)) ENG 09:21   22-07-2020	<b>P</b> 2



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



ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429 Volume 8 Issue VII July 2020- Available at www.ijraset.com

emin / s.gith	ub.io/online-tools/sha512.html			
				Ť
	Online Tools			
	SHA512	Hash	File Hash	
		CRC-16	CRC-16	
	SHA512 online hash function	CRC-32	CRC-32	
	neel	MD2	MD2	
		MD4	MD4	
		MD5	MD5	
		SHA1	SHA1	
		SHA224	SHA224	
		SHA256	SHA256	
	Insuthing Texture	SHA384	SHA384	
	Input type Text •	SHA512	SHA512	
	Hash Z Auto Update	SHA512/224	SHA512/224 SHA512/256	
	1,620010,EM7E0E07441,0,EM6E627,0,0,47E1040,254,0,654, 447,4000,26,057,0,764	SHA512/256 SHA3-224	SHA512/256 SHA3-224	
	2cf63819a5b4753507d41ee546f567ace47510d63fda06feed17c1222fb89786fb55a7011 8be00d09e02bcf58f74bde885636d79b9abd37ba7f483f8b6522b4d	SHA3-224 SHA3-256	SHA3-224 SHA3-256	
		SHA3-250 SHA3-384	SHA3-250	
		SHA3-504 SHA3-512	SHA3-512	
		Keccak-224	Keccak-224	
		Keccak-256	Keccak-256	
		Keccak-384	Keccak-384	
		Keccak-512	Keccak-512	
		Shake-128	Shake-128	
e Reshtml 🔨	🔹 Webp.net-resizeimjpg 🧄 🔹 Webp.net-resizeimjpg 🔿			
e here to search neelanjanmanna19 emn178.gith	ubio/online-tools/sha512.html			9 <i>(</i> 虎 句)) ENG 5
neelanjanmanna19	x SHA512 Online x +			
neelanjanmanna19	x SHA512 Online x + ab.io/online-tools/sha512.html Online Tools	Hash	File Hash	
neelanjanmanna19	x SHA512 Online x + ub.io/online-tools/sha512.html Online Tools SHA512 SHA512	Hash CRC-16	File Hash CRC-16	
neelanjanmanna19	x SHA512 Online x + ab.io/online-tools/sha512.html Online Tools SHA512 SHA512 online hash function			
neelanjanmanna19	x SHA512 Online x + ub.io/online-tools/sha512.html Online Tools SHA512 SHA512	CRC-16 CRC-32 MD2	CRC-16 CRC-32 MD2	
neelanjanmanna19	x SHA512 Online x + ab.io/online-tools/sha512.html Online Tools SHA512 SHA512 online hash function	CRC-16 CRC-32 MD2 MD4	CRC-16 CRC-32 MD2 MD4	
neelanjanmanna19	x SHA512 Online x + ab.io/online-tools/sha512.html Online Tools SHA512 SHA512 online hash function	CRC-16 CRC-32 MD2 MD4 MD5	CRC-16 CRC-32 MD2 MD4 MD5	
neelanjanmanna19	x SHA512 Online x + ab.io/online-tools/sha512.html Online Tools SHA512 SHA512 online hash function	CRC-16 CRC-32 MD2 MD4 MD5 SHA1	CRC-16 CRC-32 MD2 MD4 MD5 SHA1	
neelanjanmanna19	x SHA512 Online x + ab.io/online-tools/sha512.html Online Tools SHA512 SHA512 online hash function	CRC-16 CRC-32 MD2 MD4 MD5 SHA1 SHA224	CRC-16 CRC-32 MD2 MD4 MD5 SHA1 SHA224	
neelanjanmanna19	x SHA512 Online x + ab.io/online-tools/sha512.html Online Tools SHA512 SHA512 online hash function	CRC-16 CRC-32 MD2 MD4 MD5 SHA1 SHA224 SHA256	CRC-16 CRC-32 MD2 MD4 MD5 SHA1 SHA224 SHA256	
neelanjanmanna19	x SHA512 Online x + abio/online-tools/sha512.html Conline Tools SHA512 online hash function neel	CRC-16 CRC-32 MD2 MD4 MD5 SHA1 SHA224 SHA226 SHA384	CRC-16 CRC-32 MD2 MD4 MD5 SHA1 SHA224 SHA226 SHA384	
neelanjanmanna19	x SHA512 Online x + ab.io/online-tools/sha512.html Online Tools SHA512 SHA512 online hash function	CRC-16 CRC-32 MD2 MD4 MD5 SHA1 SHA224 SHA226 SHA384 SHA512	CRC-16 CRC-32 MD2 MD4 MD5 SHA1 SHA224 SHA226 SHA384 SHA512	
neelanjanmanna19	x SHA512 Online x + abio/online-tools/sha512.html Conline Tools SHA512 online hash function neel	CRC-16 CRC-32 MD2 MD4 MD5 SHA1 SHA224 SHA226 SHA384 <b>SHA512</b> SHA512/224	CRC-16 CRC-32 MD2 MD4 MD5 SHA1 SHA224 SHA226 SHA384 SHA512 SHA512/224	
neelanjanmanna19	x ♥ SHA512 Online x + abjo/online-tools/sha512.html Conline Tools SHA512 SHA512 online hash function neel Input type Text ▼ Hash ♥ Auto Update	CRC-16 CRC-32 MD2 MD4 MD5 SHA1 SHA224 SHA256 SHA384 SHA512 SHA512/224 SHA512/226	CRC-16 CRC-32 MD2 MD4 MD5 SHA1 SHA224 SHA256 SHA384 SHA384 SHA512 SHA512/224 SHA512/226	
neelanjanmanna19	x SHA512 Online x + abio/online-tools/sha512.html Conline Tools SHA512 online hash function	CRC-16 CRC-32 MD2 MD4 MD5 SHA1 SHA224 SHA256 SHA384 <b>SHA512</b> SHA512/224 SHA512/226 SHA3-224	CRC-16 CRC-32 MD2 MD4 MD5 SHA1 SHA224 SHA256 SHA384 SHA512 SHA512/224 SHA512/226 SHA3-224	
neelanjanmanna19	x SHA512 Online x + abio/online-tools/sha512.html Conline Tools SHA512 online hash function neel Input type Text > Hash 2 Auto Update 2cf63819a5b4753507d41ee546f567ace47510d63fdae0feed17c1222fb89786fb55a7e11	CRC-16 CRC-32 MD2 MD4 MD5 SHA1 SHA224 SHA256 SHA384 SHA512 SHA512/224 SHA512/256 SHA3-224 SHA3-256	CRC-16 CRC-32 MD2 MD4 MD5 SHA1 SHA224 SHA256 SHA384 SHA512 SHA512/224 SHA512/226 SHA3-224 SHA3-226	
neelanjanmanna19	x SHA512 Online x + abio/online-tools/sha512.html Conline Tools SHA512 online hash function neel Input type Text > Hash 2 Auto Update 2cf63819a5b4753507d41ee546f567ace47510d63fdae0feed17c1222fb89786fb55a7e11	CRC-16 CRC-32 MD2 MD4 MD5 SHA1 SHA224 SHA256 SHA384 <b>SHA512</b> SHA512/224 SHA512/256 SHA3-224 SHA3-256 SHA3-384	CRC-16 CRC-32 MD2 MD4 MD5 SHA1 SHA224 SHA256 SHA384 SHA512 SHA512/224 SHA512/226 SHA3-224 SHA3-256 SHA3-384	
neelanjanmanna19	x SHA512 Online x + abio/online-tools/sha512.html Conline Tools SHA512 online hash function neel Input type Text > Hash 2 Auto Update 2cf63819a5b4753507d41ee546f567ace47510d63fdae0feed17c1222fb89786fb55a7e11	CRC-16 CRC-32 MD2 MD4 MD5 SHA1 SHA224 SHA256 SHA384 <b>SHA512</b> SHA512/224 SHA512/256 SHA3-224 SHA3-256 SHA3-384 SHA3-512	CRC-16 CRC-32 MD2 MD4 MD5 SHA1 SHA224 SHA256 SHA384 SHA512 SHA512/224 SHA512/226 SHA3-224 SHA3-226 SHA3-384 SHA3-512	
neelanjanmanna19	x SHA512 Online x + abio/online-tools/sha512.html Conline Tools SHA512 online hash function neel Input type Text > Hash 2 Auto Update 2cf63819a5b4753507d41ee546f567ace47510d63fdae0feed17c1222fb89786fb55a7e11	CRC-16 CRC-32 MD2 MD4 MD5 SHA1 SHA224 SHA256 SHA384 SHA512 SHA512/224 SHA512/256 SHA3-224 SHA3-226 SHA3-384 SHA3-512 Keccak-224	CRC-16 CRC-32 MD2 MD4 MD5 SHA1 SHA224 SHA256 SHA384 SHA512 SHA512/224 SHA512/226 SHA3-226 SHA3-226 SHA3-256 SHA3-384 SHA3-512 Keccak-224	
neelanjanmanna19	x SHA512 Online x + abio/online-tools/sha512.html Conline Tools SHA512 online hash function neel Input type Text > Hash 2 Auto Update 2cf63819a5b4753507d41ee546f567ace47510d63fdae0feed17c1222fb89786fb55a7e11	CRC-16 CRC-32 MD2 MD4 MD5 SHA1 SHA224 SHA256 SHA384 SHA512/224 SHA512/2256 SHA3-224 SHA3-226 SHA3-256 SHA3-384 SHA3-512 Keccak-224 Keccak-256	CRC-16 CRC-32 MD2 MD4 MD5 SHA1 SHA224 SHA256 SHA384 SHA512 SHA512/224 SHA512/226 SHA3-224 SHA3-226 SHA3-256 SHA3-384 SHA3-512 Keccak-224 Keccak-256	
neelanjanmanna19	x SHA512 Online x + abio/online-tools/sha512.html Conline Tools SHA512 online hash function neel Input type Text > Hash 2 Auto Update 2cf63819a5b4753507d41ee546f567ace47510d63fdae0feed17c1222fb89786fb55a7e11	CRC-16 CRC-32 MD2 MD4 MD5 SHA1 SHA224 SHA256 SHA384 <b>SHA512</b> SHA512/224 SHA512/2256 SHA3-224 SHA3-224 SHA3-256 SHA3-256 SHA3-512 Keccak-224 Keccak-256 Keccak-384	CRC-16 CRC-32 MD2 MD4 MD5 SHA1 SHA224 SHA256 SHA384 SHA512 SHA512/224 SHA512/226 SHA3-224 SHA3-226 SHA3-256 SHA3-256 SHA3-256 SHA3-384 SHA3-512 Keccak-226 Keccak-226	5
neelanjanmanna19	x SHA512 Online x + abio/online-tools/sha512.html Conline Tools SHA512 online hash function neel Input type Text > Hash 2 Auto Update 2cf63819a5b4753507d41ee546f567ace47510d63fdae0feed17c1222fb89786fb55a7e11	CRC-16 CRC-32 MD2 MD4 MD5 SHA1 SHA224 SHA256 SHA384 SHA512/224 SHA512/2256 SHA3-224 SHA3-226 SHA3-256 SHA3-384 SHA3-512 Keccak-224 Keccak-256	CRC-16 CRC-32 MD2 MD4 MD5 SHA1 SHA224 SHA256 SHA384 SHA512 SHA512/224 SHA512/226 SHA3-224 SHA3-226 SHA3-256 SHA3-384 SHA3-512 Keccak-224 Keccak-256	



RSA 512 randomness test

CrypTool 1.4.41 - RSA encryption of <unnamed1> for <bob sidechannelattack=""></bob></unnamed1>	- 0
File Edit View Encrypt/Decrypt DigitalSignatures/PKI Indiv. Procedures Analysis Options Window Help	
neel	
GH RSA encryption of <unnamed1> for <bob sidechannelattack=""></bob></unnamed1>	
00000000 BC CE 8D CF 21 FE 65 C5 D2 FB 95 40 EA 61 FA 15 F2 6E 54 06 84 CF E8 77 24 E8 4A 4A 2D 09 E4 DC 6F 4D 8A 5E	
ress F1 to obtain help. Η Ο Type here to search Ο Η CO 🛱 🔂 🙀 🛍 🕿 🖬 🧊 🕼 🕄 😻 💶 🏠 😪 🔯 🔟 🖉 Ο C. Α 🛥 🤅 div ENG	0VR NUM 10:22
📫 🔎 Type here to search O 🗄 C 🚔 💼 🚖 📓 <table-cell> 🚳 0 🕏 🥸 🖳 <table-cell> 🚱 🖓 🖉 🖉 🖉 🖉 🖉 🌘 🕵 🔨 🕬 🗛</table-cell></table-cell>	22-07-2020
CrypTool 1.4.41 - RSA encryption of <unnamed1> for <bob sidechannelattack=""></bob></unnamed1>	- 0
File Edit View Encrypt/Decrypt Digital Signatures/PKI Indiv. Procedures Analysis Options Window Help	
Re Unnamed	
RSA encryption of <unnamed1> for <bob sidechannelattack=""></bob></unnamed1>	)
00000000 1C CE 8D CF 21 FE 65 C5 D2 FB 95 40 EA 61 FA 15 F2 6E 54 06 84 CF E8 77 24 E8 4A 4A 2D 09 E4 DC 6F 4D 8A 5E	
00000024 6D 0F 86 B3 EF E5 56 61 DE B0 A7 82 1B 0F D0 A9 CC 90 73 AF 01 CC E2 8E 01 8E 60 BA mVa	
Y <del>res F1 to obtain help.</del> I C1 P.1 I C1 P.1	OVR NUM 10:22



## 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

		encryption of <unnamed1> for <bob sidechann<="" th=""><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th>o ×</th></bob></unnamed1>										o ×
		ypt/Decrypt Digital Signatures/PKI Indiv. Proc & 🕲 💼 🐻 🖓 曜	edures Analysis Op	tions Window Help								
•	🚰 Unnamed1											
	neel											
	1	<u></u>										
		ST RSA encryption of <unnamed1> for <bob s<="" td=""><td></td><td>FA 61 FA 15 F2 61</td><td>F 54 06 84 CF</td><td>F8 77 24 F8 44</td><td>44 2D 09 E4 DC</td><td>6F 4D 8A 5F</td><td>10 83</td><td>nT wî Li- c</td><td></td><td></td></bob></unnamed1>		FA 61 FA 15 F2 61	F 54 06 84 CF	F8 77 24 F8 44	44 2D 09 E4 DC	6F 4D 8A 5F	10 83	nT wî Li- c		
		000000000 CCE 8D CF 21 FE 65 00000024 6D 0F 86 B3 EF E5 56	61 DE BO A7 82	1B OF DO A9 CC 9	0 73 AF 01 CC	E2 8E 01 8E 60	BA		mVa	nTw\$.JJo		
	l											
	1 to obtain help.		~ ~ ~		• m <		0			L:1 C:1 P:1	OVR	
-	€ Type h	ere to search	O H C	P 🧮 🖻 🕯		<b>i i</b>	0 🚯 😵		<b>•</b> •	<u> </u>	ENG 22-0	07-2020
C Cryp	pTool 1.4.41 - RSA	encryption of <unnamed1> for <bob sidechann<="" td=""><td>nelAttack&gt;</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>-</td><td>o ×</td></bob></unnamed1>	nelAttack>								-	o ×
		ypt/Decrypt Digital Signatures/PKI Indiv. Proc	edures Analysis Op	tions Window Help								
		<u>x @ @ _ 77 ? ? ?</u>										
	Cr Unnamed1											
	1001											
												_
		ST RSA encryption of <unnamed1> for <e< td=""><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></e<></unnamed1>										
		000000000 C CE 8D CF 21 FE 00000024 6D 0F 86 B3 EF E5	65 C5 D2 FB 95 56 61 DE B0 A7	40 EA 61 FA 15 F 82 1B 0F D0 A9 C	2 6E 54 06 84 C 90 73 AF 01	CF E8 77 24 E CC E2 8E 01 8	8 4A 4A 2D 09 E4 E 60 BA	DC 6F 4D 8A 51	El.e mVa	9.anTw\$.JJ-	oM.^	
Ľ												
Press F1	1 to obtain help.									L:1 C:1 P:1	OVP	NUM
	P Type h	ere to search	O H C	) 🖬 💼 🕯		î 🧊	0 6 %	o 🔽 I	<b>•</b> 📀 🔵	<u> </u>		
									-		22-0	. 2020

## 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 .



ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429 Volume 8 Issue VII July 2020- Available at www.ijraset.com

### 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, <u>The Code Book</u>. 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







# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 🕓 (24\*7 Support on Whatsapp)