Journal of Theoretical and Applied Information Technology

31st October 2023. Vol.101. No 20

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

NEW CRYPTOSYSTEM USING ENHANCED AUTOMATIC THEOREM PROVING AND ENHANCED CIPHERS

[1]K. KANTHI SOWJANYA, [2]SURENDRA TALARI, [3]GEESALA YOJANA, [4]PRASAD VANGAPANDU

[2]Associate Professor, Department of Mathematics, GITAM Deemed to be University, Visakhapatnam - 45, Andhra Pradesh, India

[1,3,4]Research Scholar, Department of Mathematics, GITAM Deemed to be University, Visakhapatnam - 45, Andhra Pradesh, India

ABSTRACT

Almost every sector in India has been influenced constructively and positively by globalization. In the present digitalized world, the safety and conduct of information in the cyber space is quite pivotal. In the secure and safe exchange of information, the multitudinous dimension of cryptography plays a major role. Using Automatic Theorem Proving concept, this article proposes a new cryptosystem technique by allocating various enhanced ciphers to the enhanced antecedent and consequent rules. Using plaint text and connective symbols, the sequent is formed; then this plain text is encrypted into various levels using enhanced antecedent rules, consequent rules and the corresponding allocated enhanced ciphers. It involves multiple levels of encryptions and decryptions with more security thus making it harder to the attacker to decipher the plain text. The security levels are infeasible in spite of the feasibility of encryption and decryption run time of the proposed technique.

Keywords: *Sequent, Connectives, Enhanced antecedent rules & consequent rules, Enhanced ciphers, Encryption, Decryption.*

1. INTRODUCTION:

This paper discusses a new encoding and decoding method using enhanced Automatic Theorem Proving **[6,14]**, in which different enhanced ciphers are allocated to the enhanced antecedent and consequent rules. Since different enhanced ciphers are assigned to the enhanced antecedent and consequent rules, we get level-1, level-2…level-k cipher texts, where k is the number of connectives used in the encoding process. Firstly, the sender and the receiver agree with the enhanced ciphers list. This system constitutes one public key **[9]** with a set of variables obtained in the level-k encryption sequent and these variables take in the same order obtained in the level-k encryption sequent. This system constitutes two secret keys; the first secret key is the set of connectives used in the encoding sequent to get final cipher text that is level-k cipher text and the second secret key contains set of ciphers used to get level-1, level-2…level-k cipher texts **[10,13,17]**. Due to these different levels of cipher texts, it is difficult for the attacker to decode the original plain text from the public key. Even if the secret keys are found by the attacker, he would get the plain text only up to some extent and it is highly difficult to find it completely **[21].** The cryptosystem proposed in an enhanced cipher based Automatic Theorem Proving Technique for Encryption and Decryption **[21]** used existing antecedent & consequent rules as well as existing ciphers. In the proposed new cryptosystem, enhanced antecedent and consequent rules and enhanced ciphers like Triangular cipher, Jelly cipher, Slash fair cipher and Tree fence Technique are developed. So, the cryptosystem described in this paper is more secure and efficient than the previous methods and the procedures of techniques of encryption and decryption **[23]** are included in this system.

The ECC is asymmetric- key algorithm, which used 256-bit key for encrypting and decrypting the 128-bit original data. RSA algorithm is a public key encryption algorithm and which is used 3024-bit key for encrypt and decrypt the 128-bit size of information. In AES algorithm, substitution bytes (S-Box) plays crucial role and it offer confusion in cipher text and battle against the unauthorized access, but it is not completely satisfy the unauthorized access.

1.1 Description of Automatic Theorem Proving:

To check whether a given statement is valid or not from the set of premises, Automatic Theorem

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Proving **[4]** is used. Antecedent rules, consequent rules, sequent, axioms, statements, premises are included in it. It contains a set of rules and procedure that allows one to construct each step of derivation in a particular manner without any barrier to any ingenuity and arrive at the final step. Though this procedure is mechanical, it is an authentic process for the validity of the statement/conclusion more than any other previously available methods. This system includes the procedures of techniques of derivation and works more effectively than the previous methods. This system of derivation consists of 10 rules, an axiom schema and rules of well-formed sequent & formulas **[2,10]**.

1. Variables: the capital letters A, B, C… P, Q, R…. are used as statement variables and statement formulas.
2. Connectives: The connectives appear in the formulas in the order of given precedence.
3. String of formulas: A string of formulas is defined as follows:
   (a) Any formula is a string of formulas
   (b) If alpha and beta are strings of formulas, then alpha-beta and beta-alpha are strings in that.
   (c) Only those strings that are obtained by steps (a) and (b) are strings of formulas, with the exception of the empty string which is also a string of formulas.
   Note: The strings A, B, C; B, C, A; A, C, B; etc., are the same as the order in which the formulas appear in any string is immaterial.
4. Sequent: If alpha and beta are strings of formulas, then they together form a *sequent* in which alpha is denoted as the antecedent and beta as the consequent of the sequent.
   Thus, A, B, C, D, E, F is true only when A B C D E F is true. i.e., A sequent is true if and only if either at least one of the formulas of the antecedent is false or at least one of the formulas of the consequent is true. In this sense, the symbol is a generalization of the connection to strings of formulas. Similarly, we use the symbol applied to strings of formulas as a generalization of the symbol. Thus A⇒B means "A implies B" or is a tautology which means that is true. Ex: P, Q, R $\Rightarrow^{S}$ P, N hence, the empty antecedent is interpreted as the logical constant "true" (T) and the empty consequent is interpreted as the logical constant "false" (F).
5. Axiom Schema: If alpha and beta are strings of formulas such that every formula in both alpha and beta is a variable only, then the sequent is an axiom if and only if alpha and beta have at least one variable in common.
   Ex: A, B, C$\Rightarrow^{S}$P, B, R is an axiom, where A, B, C, P & R are variables
6. Theorem: The following sequent are the theorems of our system:
   (a) Every axiom is a theorem.
   (b) If a sequent alpha is a theorem and a sequent beta result from alpha through the use of one of the above rule s of the system which are given below, then beta is a theorem.
   (c) Sequent obtained by (a) and (b) are the only theorems.

1.2 Rules:

To combine formulas within strings by introducing connectives {@,Θ,®,©,ö}. Corresponding to each of the connectives there are two rules, one for the introduction of the connective in the antecedent and the other for its introduction in the consequent. The strings of formulas while P and Q are formulas to which the connectives are applied **[24]** in the description of these enhanced antecedent and consequent rules.

Antecedent Rules:

1. Rule ¬ ⇒ : If ξ,ϑ ⇒ P, η, then ξ, ¬P, β ⇒ η
2. Rule ∧ ⇒ : If P, Q, ξ, ϑ ⇒ η, then ξ, P ∧ Q, ϑ ⇒ η
3. Rule ∨ ⇒ : If P, ξ, ϑ ⇒ η and Q, ξ, ϑ ⇒ η, then ξ, P∨Q, ϑ ⇒ η
4. Rule → ⇒ : If Q, ξ, ϑ ⇒ η and ξ, ϑ ⇒ P, η, then ξ, P→Q, ϑ⇒ η
5. Rule ↔ ⇒ : If P, Q, ξ, ϑ⇒ η and ξ, ϑ ⇒ P, Q, η, then ξ, P↔Q, ϑ⇒ η

Consequent Rules:

1. Rule ⇒ ¬: If P, ξ ⇒ ϑ, η, then ξ⇒ ϑ, ¬P, η
2. Rule ⇒ ∧: If ξ⇒ P, ϑ, η and ξ⇒ Q, ϑ, η, then ξ⇒ ϑ, P∧Q, η
3. Rule ⇒ ∨: If ξ⇒ P, Q, ϑ, η, then ξ ⇒ ϑ, P∨Q, η

4. Rule $\Rightarrow \rightarrow$: If P, $\xi \Rightarrow$ Q, ϑ, η, then $\xi \Rightarrow \vartheta$, $P \rightarrow Q$, η
5. Rule $\Rightarrow \leftrightarrow$: If P, $\xi \Rightarrow$ Q, ϑ, η and Q, $\xi \Rightarrow$ P, ϑ, η, then $\xi \Rightarrow \vartheta$, $P \leftrightarrow Q$, η

Proposed new /enhanced antecedent and consequent rules:

Enhanced Antecedent Rules:

1. Rule @ $\Rightarrow$: If ξ,PQ,$\vartheta \Rightarrow$ Q,η then ξ,P@Q,$\vartheta \Rightarrow \gamma$
2. Rule Θ $\Rightarrow$: If ξ,P,$\vartheta \Rightarrow_{PQ}$,$\eta$, then ξ,PΘQ,$\vartheta \Rightarrow \eta$
3. Rule ® $\Rightarrow$: If ξ,Q,$\vartheta \Rightarrow_{QP}$,$\eta$ then ξ,P®Q,$\vartheta \Rightarrow \eta$
4. Rule © $\Rightarrow$: If ξ,QP,$\vartheta \Rightarrow_{P}$,$\eta$ then ξ,P©Q,$\vartheta \Rightarrow \eta$
5. Rule ö $\Rightarrow$: If ξ,Q,$\vartheta \Rightarrow_{PQ}$,$\eta$ then ξ,PöQ,$\vartheta \Rightarrow \eta$

Enhanced Consequent Rules:

5. Rule $\Rightarrow$@: If ξ,Q $\Rightarrow$ P,ϑ, η then $\xi \Rightarrow \vartheta$,P@Q,$\eta$
6. Rule $\Rightarrow$Θ: If ξ,P $\Rightarrow$ ϑ,QP,η then $\xi \Rightarrow \vartheta$,PΘQ,$\eta$
7. Rule $\Rightarrow$®: If ξ,Q $\Rightarrow$ ϑ,PP,η then $\xi \Rightarrow \vartheta$,P®Q,$\eta$
8. Rule $\Rightarrow$©: If $\xi \Rightarrow$ ϑ,QP,η then $\xi \Rightarrow \vartheta$,P©Q,$\eta$
5. Rule $\Rightarrow$ö: If $\xi \Rightarrow \vartheta$,PQ,$\eta$ $\xi \Rightarrow$ P, ϑ, η, then $\xi \Rightarrow \vartheta$,PöQ,$\eta$

2. LITERATURE SURVEY:

2.1 Tree fence Technique:

In this cipher first divide the plain text into two equal even length blocks. If we will not get even length blocks then add the dummy alphabets x's at the end the plain text, in such a way that to get even length blocks. Say these two blocks as P1 and P2. Say (E1, P1B) is 1st alphabet of the P1 block, (E2, P1B) is 2nd alphabet of the P1 block, … (Er, P1B) is rth alphabet of the P1 block. Similarly Say (E1, P2B) is 1st alphabet of the P2 block, (E2, P2B) is 2nd alphabet of the P2 block, … (Er, P2B) is rth alphabet of the P2 block. Then for encryption table is as follows:

(E1, P1B)	(E(r-1), P2B)	(E3, P1B)	….	(E1, P2B)
(Er, P2B)	(E2, P1B)	(E(r-2), P2B)	….	(Er, P1B)

To get the cipher text take the elements in the order that (E1, P1B) (E(r-1), P2B) (E3, P1B) …. (E1,P2B)(Er,P2B) (E2,P1B) (E(r-2),P2B) ….(Er,P1B).

For decryption again divide the cipher text into two blocks C1 and C2 as per the agreement of sender and receiver. Then for decryption table is as follows:

(E1, C1B)	(E2, C2B)	(E3, C1B)	(E4, C2B)	….	(E(r-1), C1B)	(Er, C2B)
(Er, C1B)	(E(r-1), C2B)	(E(r-2), C1B)	(E(r-3), C2B)	….	(E2, C1B)	(E1, C2B)

Where (E1, C1B) is 1st alphabet of the C1 block, (E2, C1B) is 2nd alphabet of the C1 block, … (Er, C1B) is rth alphabet of the C1 block. Similarly Say (E1, C2B) is 1st alphabet of the C2 block, (E2, C2B) is 2nd alphabet of the C2 block, … (Er, C2B) is rth alphabet of the C2 block.

Example: Take the plain text as 'happybirthday' then divide into two blocks as happybi|rthday. To make both the blocks as even length fill the alphabet x at the end the plain text, then the plain text becomes 'happybi|rthdayxxx' after making two blocks. Applying Tree fence technique encryption procedure, we get cipher text 'hxpyyditxaxpabhr'. Applying decryption procedure of we get required plain text 'happybirthday'.

2.2 Slash fair cipher:

Contract 5×5 table contain 25 position T1, T2, T25. Take any key word of non-repeated alphabet with length $\leq$ 10. Divide this key word into two equal parts and place 1st part alphabet in 3rd row of the table and place the 2nd parts alphabet in the 4th row corresponding below places of alphabet of 1st part occupied in 3rd row then fill the remaining alphabets. Then If keyword contains repeated alphabets their corresponding only the alphabets.

Apply the following rules for encryption. Here some rules are followed as play fair cipher.

1. Divide the plain text into 2 letter blocks, to make any single letter block as two letter block fill with x.
2. If 2 letters contain in the same row then take the alphabets below of corresponding alphabets circularly.
3. If two letters contain in same column then take immediate right elements of alphabets circularly.
4. Otherwise follow play fair cipher.

For decryption apply following rules.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

1. Divide the plain text into 2 letter blocks, to make any single letter block as two letter blocks fill it with x.
2. If 2 letters contain in the same row then take the alphabets above of corresponding alphabets circularly.
3. If two letters contain in same column then take proceeding element in a row of that element.
4. Otherwise follow play fair cipher.

Example: Take the key word 'ACTION' and frame the 5X5 table which contain 25 positions. First divide the key word into two equal parts as ACT and ION then place 1st part alphabet in 3rd row of the table and place the 2nd parts alphabet in the 4th row corresponding below places of alphabet of 1st part occupied in 3rd row then fill the remaining alphabets.

B	R	D	E	F
G	H	S	M	K
L	A	C	T	P
Q	I/J	O	N	U
V	W	X	Y	Z

Take the plaint text as 'goodmorning' and divide it into two letter blocks as go|od|mo|rn|in|gx. To make any single letter block as two letter blocks fill it with x. Then the cipher text is 'sqnesneiwysv'.

Divide the cipher text into two letter blocks in decryption as 'sq|ne|sn|ei|wy|sv' then applying decryption procedure of slash fair cipher we get required plain text 'goodmorning'.

2.3 Jelly cipher: In this cipher take key word and write its numerical values and then add all these numerical values we get one number say 'n' then write its equivalent alphabet say 'g' then find modulus of that number under modulo 24 as here we are taking 24 constantly, instead of 24 we can take any positive number. Then we get one value say 'g^1' then apply '$(x+g^1)$ (mod 26)' which is having similarity of shift cipher finally we get cipher text 'c'.

In decryption procedure to get plain text p: c-n (mod 26) we get required plain text.

Example: Take key word 'action', its numerical equivalent is '0 2 19 8 14 13' and its sum is 56. Find 56 under modulo 24 we get 8. Then apply x+8 (mod 26) where x is the plain text. Consider the plain text as 'today' its numerical equivalent is '19 14 3 0 24' applying addition 8 mod 26 for this we get '1 22 11 8 6' final cipher text is 'bwlig'.

In decryption procedure to get plain text p: c-n (mod 26) that is p: c-8 (mod 26) we get '19 14 3 0 24' equivalent to 'today' which is required plain text.

2.4 Triangular cipher: First n letter plain text convert into n number of numerical values. Then divide this 'n 'number of numerical strings into 4 letter blocks. If any block does not contain 4 number of numerical then make it as 4 number of numerical blocks by filling with one's label the number in this letter block as l_{11}, l_{21}, l_{22} and u_{12} respectively. Then form the matrices L and U as $L=\begin{bmatrix} l_{11} & 0 \\ l_{21} & l_{22} \end{bmatrix}$ and $U=\begin{bmatrix} 1 & u_{12} \\ 0 & 1 \end{bmatrix}$ and multiply LU we get new 2x2 matric.

Then write it corresponding alphabets of this matrix row wise. So, we get first 4 letter block of cipher text. Repeat the process for the remaining 4 letter block of the 'n' numbered string. We get 'n' number cipher text. Here we can divide the n number of string into finite block where each block may contain 4 numerals, 9 numerals,16 numerals etc. Such that we can form a square matrix with these numerals of order 2x2 ,3x3,4x4 etc.

For decryption divide the n numeral cipher text string into 4 numeral blocks as a in secret key will mention that each block contains 4 numerals. Then form 2x2 with 4 numerals of each block, say any 2x2 matrix is A. Then write $A=\begin{bmatrix} l^1_{11} & 0 \\ l^1_{21} & l^1_{22} \end{bmatrix}\begin{bmatrix} l_{11} & 0 \\ l_{21} & l_{22} \end{bmatrix}$ and solve this we get as $l^1_{11}=l_{11}$, $l^1_{21}=l_{21}$, $l^1_{22}=l_{22}$ and $u^1_{12}=u_{12}$. We get the plain text. So, we write the one block plain text as $l^1_{11}\ l^1_{21}\ l^1_{22}\ u^1_{12}$. Repeat this process for all blocks we get required plaint text.

Example: Take the plain text as 'bcde' and write its corresponding numerals '1234'. Then write it in 2X2 matrix as $\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$. Write this 2X2 matrix as product of two matrices as $\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}=\begin{bmatrix} 1 & 0 \\ 2 & 3 \end{bmatrix}\begin{bmatrix} 1 & 4 \\ 0 & 1 \end{bmatrix}$. Then multiply right side two matrices we get new 2X2 matrix $\begin{bmatrix} 1 & 4 \\ 2 & 11 \end{bmatrix}$ then writing its corresponding alphabets we get $\begin{bmatrix} b & e \\ c & l \end{bmatrix}$, so the cipher text is 'becl'. After applying above decryption

Input: Plain Text (COVID VACCINE IS READY) **Output:** Cipher Text (TNWQILGFVAM QKMQZTNWQBXIO)
Step 1: Start *Step 2: The plain text is taken as input in the initial phase (COVID VACCINE IS READY)* *Step 3: The plain text is divided into 'm' blocks where each block contains 'k' number of alphabets* *Step 4: The blocks are labeled with A1, A2…Am* *Step 5: The 1st encryption sequent is formed with A1, A2, … Am* *Step 6: Antecedent and Consequent rules are applied on the Encryption sequent until all the connectives are eliminated, to get level-1, level-2…level-k cipher texts* *Step 7: Level-k cipher is the final cipher text* *Step 8: Stop*

procedure of Triangular cipher, we get required plain text 'abcd'.

2.5 Passing key cipher: In the plain text take odd position alphabets as new plain text and even numbered position alphabets as key. Let the plain text be 'p1p2p3p4…pk' where its length is even number. If its length is odd number then make it an even numbered length by adding the alphabet 'a' at the end of the plain text. Now its new plain text becomes p1p3…p(k-1) by considering the length is even number and key becomes p2p4p6…p(k-2). Let these corresponding numerals be n1n3n5…n(k-1) and n2n4n6…n(k-2). Now perform addition for these numerals as following way under modulus 26 say t12t34…t(k-1) (k-2).

New plain text numerals	n1n3n5…n(k-1)
Key numerals	n2n4n6…n(k-2)
Total	t12t34…t(k-1) (k-2) [mod 26]

Then write corresponding alphabets for t12t34…t(k-1) (k-2) we get required cipher text.

In the decryption, to get required plain text perform subtraction for these numerals of cipher text and key numerals as following way under modulus 26 we get p1p3…p(k-1).

Cipher text numerals	c1c3c5…c(k-1)
Key numerals	n2n4n6…n(k-2)
Total	n1n3n5…n(k-1)[mod 26]

Then place key alphabets in the even places of above cipher text we get 'p1p2p3p4…pk' which is required plaint text.

Example: Take plain text 'todayisveryhot', consider the new plain text as 'tdyseyo' and key as 'oaivrht'. Then its corresponding numerals are '19 3 24 18 4 24 14' and '14 0 8 21 17 7 19'. Now perform addition for these numerals by the procedure of passing key cipher under modulo 26 we get '7 3 6 13 21 5 7' and required cipher text is 'h d g n v f h'. In decryption procedure perform subtraction for these numerals of cipher text and key numerals as following way under modulus 26 we get '19 3 24 18 4 24 14'. Then place key alphabets in the even places of above cipher text we get 'todayisveryhot' which is required plaint text.

P.A. Kameswari et al. [20] solved DLP using pollard Rho algorithm, the cryptosystem based on above DLP useful for transmitting the data securely, but security levels are weak.

Surendra, T et al. [21] developed cryptosystem based on ATP and antecedent and consequent rules assigned to the ciphers. In this cryptosystem as the ciphers used already known there is a possibility for attacks.

The present developed cryptosystem which is based on Automatic Theorem Proving and new sequent rules assigned with new defined ciphers overcomes above limitations.

3. PROPOSED ALGORITHMS:

3.1 Encryption process:

[17] First the plain text is divided into 'm' blocks where each block contains k number of alphabets. Now these blocks are labeled as A1, A2, A3 …. Am, where 'm' is the finite value. The blanks are filled with the alphabet z, if Am block does not contain k number of alphabets. The sequent is formed with these labels and connective symbols {@,Θ,®,©,ö} using Automatic Theorem Proving **[2,10]** concept and it is important that the statement formula contains the consequent part only in the encryption sequent $\alpha,\beta,\chi \Rightarrow^{Sn} \beta,\delta$ for n=1,2,… finite value the statement formulas may contain in the antecedent and consequent part or may contain in antecedent part only or may contain in consequent part only in the encryption sequent $\alpha,\beta,\chi \Rightarrow^{Sn} \beta,\delta$ for n=1,2,… finite value where α,β,χ,β & δ are simple atomic variables or compound statements. Then the antecedent and consequent rules are applied to get level-1, level-2 …level-k cipher texts where k is number of

connectives in the first encryption sequent until all the connective symbols were eliminated in the sequent. The level-k cipher text is the final cipher text which will be sent to the receiver. Since different levels cipher texts occur in each level, it is very difficult to the attacker to recover the plain text, hence security is more. Here the first secret key is the set of ciphers used in antecedent and consequent rules **[11,14,15]**; public key set contain two parts, first part contains the variables to be used in antecedent part while forming first decryption sequent. Similarly, variables in the second part of the public key are to be used in consequent part while forming first decryption sequent. In the public key, **[7]** these two parts were separated by the symbol **';'**. The second secret key is the set of "antecedent and consequent rules used in order to get level-1 to level-k cipher texts". The second secret key contains the order of the connective symbols removed in the encryption sequents. In the second secret key one connective symbol is to be applied to two variables or two statement formulas only in the process of decryption. The public key is set of "variables A_i^j with 1≤i≤m & 1≤j≤k in the final encryption sequent" where all the connectives were eliminated.

3.2 Encryption algorithm:

3.3 Decryption process:

The cipher text obtained from the sender contain any particular 'k[th]' number block followed by any numeric value, its means that k[th] block is to be repeated that many number of times of the numeric value represented in the cipher text. For instance, the cipher text contains the numeric 'l' then that particular k[th] block has to be repeat 'l' times. Then cipher text is divided into the m letter blocks and labeled with the variables X_i^j with 1≤i≤m & 1≤j≤m from the public key. The decryption sequent $\alpha^j,\beta^j,\Rightarrow^{SDn}\chi^j,\delta^j$ for 1≤j≤k and n=1, 2, finite value where $\alpha^j,\beta^j,\chi^j\&\delta^j$ are the variables from the public key is formed **[7]**. The decryption sequent are written using private key. The connectives in the secret key are used in reverse order i.e., from backward direction to decode the cipher text. The implications in the secret key are used from the right and 'R followed by connective symbol' represents rules that has to be applied in decryption consequent part. Similarly, 'L followed by connective symbol' represents that rule to be applied in decryption antecedent part'. With one connective symbol in the secret key, compound statement is formed by taking two variables or two compound statements by considering the order. The process is repeated until all the connectives are used in the secret key. In this process we get plain text–k, plain text– (k-1), plain text–1, from level-k, level–k-1, level-1 cipher texts. Level -1 plain text is the required plain text **[16,23]**.

3.4 Decryption algorithm:

Input: Cipher Text (TNWQIL GFVAM QKM QZTNWQBXIO)
Output: Plain Text (COVID VACCINE IS READY)

Step 1: Start
*Step 2: Cipher text is taken as input in the final phase (*TNWQILGFVAMQKMQZTNWQBXIO*)*
Step 3: The cipher text is divided into blocks where each block contains k number of alphabets.
Step 4: The blocks are labeled with A_i^j *with 1≤i≤m & 1≤j≤m in the same order as in the public key'*
Step 5: The decryption sequent's is formed using L-connectives or R-connectives in private key from backward direction. Repeat the process until all the L- connectives or R-connectives used.
Step 6: plain text-k, plain text–(k-1), …. plain text-1is obtained
Step 7: The required plain text is obtained
Step 8: Stop

4. IMPLEMENTATION OF ENCRYPTION AND DECRYPTION:

Symbol	Name
X@Y	Jelly cipher
XΘY	Slash fair cipher
X®Y	Passing key cipher
X©Y	Tree fence cipher
XöY	Triangular cipher
a-0, b-1, c-2, z-25	Alphabets and its values in encryption sequent
$\Rightarrow^{Sn}$	n- decryption sequent
a-connective	connective symbol used in antecedent part
c-connective	connective symbol used in consequent part

4.1 Implementation 1.

- Plain text: **COVID VACCINE IS READY**
- COVI | DVAC | CINE | ISRE| ADYx
- Say (COVI | DVAC | CINE | ISRE| ADYx) =(A1|A2|A3|A4|A5)

Now for the sequent with the above variables A1, A2, A3, A4, A5 using connective symbols {@,Θ,®,©,ö} statement formulas may contain in the antecedent and consequent part or may contain in antecedent part only or may contain in consequent part only. (A1ΘA2)$\Rightarrow^{S1}$[(A3©A4)@A5], by using rule 'implies a→' the sequent 1is changed to $A_1^1 \Rightarrow^{S2} A_1^1\ A_2^1$,[(A3©A4)@A5] where A_1^1=TNWQ & A_2^1 =BXIO, a level-1 cipher text. To get level-2 cipher text, 'rule →c' is applied and the sequent 2 changes to $A_1^1, A_5^1 \Rightarrow^{S3} A_1^1\ A_2^1, (A_3^1 © A_4^1)$ where A_3^1=KQVM, A_4^1=QAZM & A_5^1=ILGF. Again apply rule '⇒©' on the sequent 3 then we get the sequent 4 as $A_1^1, A_5^1 \Rightarrow^{S3} A_4^{11}\ A_3^{11}, A_1^1\ A_2^1$ where A_3^{11}=KQVM & A_4^{11}=MQAM which is level-4 cipher text. Since all connective symbols are eliminated in the sequent 4, the process can be stopped and concluded that it is final cipher text **[12,16]**. The final cipher text is **TNWQILGFVAMQKMQ ZTNWQBXIO**. The public key is $(A_1^1, A_5^1; A_4^{11}\ A_3^{11}, A_1^1\ A_2^1)$ and secret key1 is (@:Jelly, **Θ:** Slash fair, ©: Tree fence) & secret key2 is (a**Θ,c@,c©).**

In the second secret key, one connective symbol has to be applied to two variables or two statement formulas only. In the decryption procedure first the cipher text is considered as 4 letter blocks as (**TNWQ|ILGF |VAMQ |KMQZ |TNWQ |BXIO**) and label it as $(A_1^1 | A_5^1 | A_4^{11} | A_3^{11} | A_1^1 |)$ using public key **[25]**. The sequent is formed from the public key by choosing the variables before symbol ';' for antecedent part and after the symbol ';' for consequent part for decryption such as $A_1^1, A_5^1 \Rightarrow^{SD1} A_4^{11}, A_3^{11}, A_1^1, A_2^1$ which is level-1 sequent in decryption process. Here $\Rightarrow^{SDk}$ represents k-level sequent for decryption process. Further level sequent steps are formed using secret keys by applying one connective symbol to two variables or two statement formulas at a time as $A_1^1, A_5^1 \Rightarrow^{SD1} A_3^1 © A_4^1, A_1^1, A_2^1$ where A_3^1=KQVM & A_4^1=QAZM , $A_1^1 \Rightarrow^{SD1}$ (A3©A4)@A5, A_1^1, A_2^1 where A3=CINE, A4=ISRE & A5=ADYX & (A1ΘA2)$\Rightarrow^{SD1}$ [(A3©A4)@A5] where A1=COVI & A2=DVAC. So, we got the required plain text as '**COVID VACCINE IS READY'.**

4.2 Implementation 2:

Consider the plain the text '**declare war on neighbour country'**. This plain text is divided as 4 letter blocks as 'decl|arew|aron|neig|hbou|rcou|ntry' and labeled as B1, B2, …B7 where B1= decl, B2=arew, B3=aron, B4=neig, B5=hbou, B6=rcou, B7=ntry. So, the divided plain text blocks equivalent to (B1|B2|B3|B4| B5|B6|B7). For the first sequent with these variables as (B3öB4)@B1$\Rightarrow^{S1}$(B2ΘB5)© (B6®B7), the first 'rule @⇒' is applied and $(B_3^1$ ö $B_4^1)\ B_1^1 \Rightarrow^{S2} B_1^1$,(B2ΘB5)© (B6® B7) is obtained where B_3^1=izwv, B_4^1=vmq o, B_1^1=lmkt. Now again 'rule ö ⇒' is applied on the above sequent and $B_4^{11}\ B_1^1 \Rightarrow^{S3} B_3^{11}\ B_4^{11}, B_1^1$ (B2ΘB5)©(B6®B7) is obtained where B_3^{11}=bcde, B_4^{11}=fghi. Now again, 'rule ⇒©' is applied on the above sequent then $B_4^{11}\ B_1^1 \Rightarrow^{S4} B_3^{11}\ B_4^{11}, B_1^1$ $(B_6^1$ ® $B_7^1)(B_2^1$ Θ $B_5^1)$ is obtained where B_6^1=yrtw, B_7^1=ubcu, B_2^1=aren & B_5^1=hoor. Now again 'rule ⇒®' is applied on the above sequent then $B_4^{11}\ B_1^1, B_7^{11} \Rightarrow^{S5} B_3^{11}\ B_4^{11}$, $B_1^1, B_6^{11}\ B_6^{11}$ $(B_2^1$ Θ $B_5^1)$ is obtained where B_6^{11}=ppvw & B_7^{11}= ppvw. Now again 'rule ⇒Θ' is applied on the above sequent then $B_4^{11}\ B_1^1, B_7^{11}, B_2^{11} \Rightarrow^{S6} B_3^{11}\ B_4^{11}$, $B_1^1, B_6^{11}\ B_6^{11}$, $(B_5^{11}\ B_2^{11})$ is obtained where B_2^{11}=cdfu & B_5^{11}=siid. The process is ceased since all the connective symbols were eliminated in the last sequent. So, the final level cipher text **[12,16]** is "**ovqmlmktppvwcdfuviwzovqmlmktppvw2siid cdfu**". The public key **[25]** is

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

$\{B_4^{11}\ B_1^1, B_7^{11}, B_2^{11}; B_3^{11}\ B_4^{11}, B_1^1, B_6^{11}\ B_6^{11}, B_5^{11}\ B_2^{11}\}$ and secret key1 is similar as in implementation 1 which is (@:Jelly, Θ: Slash fair, ©: Tree fence) & secret key2 is (a@,aö;c©,c®,cΘ). The 'k' number block is to be repeated that many number of times of the numeric value represented in the cipher text. For instance, the cipher text contains the numeric 3 and agreed as 4 letter block, then that particular block has to be repeat 3 times.

In the decryption procedure first write the cipher text in expanded form as **(ovqmlmktppvwcdfuviwzovqmlmktppvwppvwsiidcdfu)** then divide into four letter blocks as **(ovqm|lmkt|ppvw|cdfu |viwz|ovqm|lmkt|ppvw|ppvw|siid|cdfu)** and using public key equate these blocks to $(B_4^{11}|B_1^1|\ B_7^{11}|B_2^{11}|\ |B_4^{11}|B_1^1|\ B_6^{11}|B_6^{11}|\ B_5^{11}|)$.The decryption first sequent is formed with the variables using private key as $B_4^{11}\ B_1^1, B_7^{11}, B_2^{11} \Rightarrow^{SD1} B_3^{11}\ B_4^{11},\ B_1^1, B_6^{11}\ B_6^{11}, (B_5^{11}\ B_2^{11})$. Further level sequent steps are formed using secret key and public key by applying one connective symbol to two variables or two statement formulas at a time as $B_4^{11}\ B_1^1, B_7^{11} \Rightarrow^{SD2} B_3^{11}\ B_4^{11},\ B_1^1, B_6^{11}\ B_6^{11}\ (B_2^1 \Theta B_5^1)$ where B_2^1=aren & B_5^1=hoor, $B_4^{11}\ B_1^1 \Rightarrow^{SD3} B_3^{11}\ B_4^{11},\ B_1^1\ (B_6^1 ® B_7^1)(B_2^1 \Theta B_5^1)$ where B_6^1=yrtw & B_7^1=ubcu, $B_4^{11}\ B_1^1 \Rightarrow^{SD4} B_3^{11}\ B_4^{11},\ B_1^1$ (B2 Θ B5) ©(B6®B7) where B2=arew, B5=hb ou, B6=rcou & B7=ntry, $(B_3^1 \ddot{o} B_4^1)\ B_1^1 \Rightarrow^{SD5} B_1^1$, (B2ΘB5)© (B6®B7) where B_3^1=izwv & B_4^1=vmqo, (B3öB4)@B1 $\Rightarrow^{SD6}$ (B2ΘB5)©(B6®B7) where B1= decl, B3=aron & B4=neig. By writing these in order like B1B2B3B4B5B6B7 we get required plain text as **declarewaronneighbourcountry.**

5. RESULTS AND DISCUSSION:

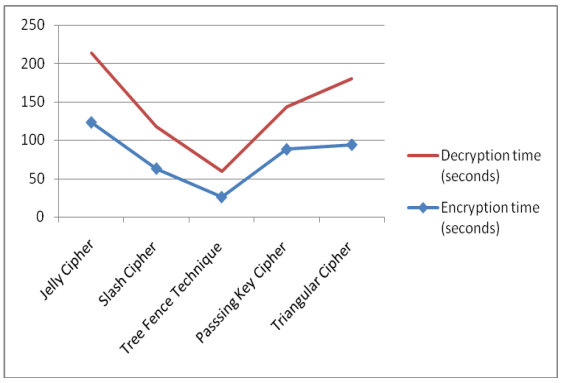

Fig 1: The Execution Time Of Encryption & Decryption

6. CRYPTANALYSIS:

As we proposed new public key cryptosystem which was developed by using new antecedent, consequent rules and enhanced sequent, here we developed new ciphers and assigned these ciphers to the developed antecedent and consequent rules. So that will have different levels of encryptions. When the attacker tries to decrypt the message using available sources, he can decrypt the message up to some levels only and cannot decrypt the original plain text easily which is very difficult to get it **[14, 21]**.

Also in some cipher text, size of the cipher text becomes double the size the plain text which occupies more space and required a greater number of public and private keys to perform entire encryption and decryption process which affects the performance of cryptosystems. But the proposed crypto system overcomes this problem, that is the size of the cipher text less than or equal to size of the plain text. Hence it improves the performance of the encryption and decryption process.

7. OPEN RESEARCH ISSUES(FUTURE SCOPE):

We can develop in future new cryptosystems with automatic theorem proving with novel encryption and decryption rules using three or more variables assigned to different methods.

8. CONCLUSION:

This paper discusses the development of a new public key cryptosystem method using Enhanced Automatic Theorem Proving with new ciphers and enhanced antecedent and consequent rules;

different ciphers are allocated in antecedent and consequent rules. To present an effective data encryption and decryption algorithm based on automatic theorem proving and sequent rules. To incorporate better data security and facilitate secure data interchange using effective encryption and decryption rules. To introduce ATP based cryptosystem model for enhancing the data security. The expected outcome is the performances will be compared with different existing approaches to prove the model superiority.

Limitation is delays the execution time. Since different levels of encryptions are there, it is very difficult to the attacker to retrieve the plain text from the public key. Even if the attacker gets the public key, using this public key he can decode the text upto some levels only and it is infeasible to decode the plain text completely. Hence higher security levels are achieved in this method. One more advantage of this method is that for 'n' size plaint text we get 'n+q' size cipher text where q is finite number. Where as in Elliptic curve crypto system we get '2n' size cipher text for encryption of 'n' size plain text, so that it is somewhat feasible to the attacker to decode the plain text. But in our proposed new public key cryptosystem we get more 'n+q' size cipher text for n size plain text, so if it very difficult to the attacker to retrieve the required plain text. So, the security is more for this crypto system. applying programming concept to the proposed technique, A feasible run time of encryption and decryption with infeasible security levels is achieved with the application of programming concept to the proposed technique. Therefore, the proposed method is obviously a better choice than the other existing encryption and decryption methods. Thus, the new cipher, new antecedent rules & consequent rules can be defined and applied to this cryptosystem method in future also.

ACKNOWLEDGEMENTS:

The authors would like to express their gratitude for the support extended by the Department of Mathematics, GIS, and GITAM Deemed to be University.

REFERENCES:

[1] A.J. Menezes, P.C. Van Oorschot, and S.A. Vanstone, "Hand book of Applied Cryptography." CRC Press Series on Discrete Mathematics and its Applications. CRC Press, Boca Raton, FL, 1997. With a foreword by Ronald L. Rivest.

[2] Bhishma Rao, "A text of Mathematical Foundations of Computer Science", SciTech Publications (India) Pvt Ltd., ISBN-10: 8183710433.

[3] Douglas R. Stinson "Cryptography theory and practice" Second edition.

[4] Geoff Sutcliffe, "Automated Theorem Proving: Theory and Practice A Review", AI Magazine Volume 23 Number 1 (2002) (© AAAI).

[5] Gerhard Frey "The arithmetic behind cryptography" AMS volume 57, Number 3.

[6] Hans Delfs Helmut Knebl "Introduction to cryptography" Principles and its applications, second edition.

[7] Harry Yosh "The key exchange cryptosystem used with higher order Diophantine equations" IJNSA VOL.3, 15. No.2, March 2011.

[8] I. Niven, H.S. Zuckerman and J.H. Silverman "An Introduction to the Theory of Numbers", 5th ed., John Wiley and Sons, New York, 1991.

[9] J. Buchmann "Introduction to cryptography", Springer Verlag 2001.

[10] J.P. Tremblay & R. Manohar, "A text book of Discrete Mathematical Structures with Applications to Computer Science', McGraw Hill Education (India) Edition 1997.

[11] Keith M. Martin, Rei Safavi-Naini, Huaxiong Wang and Peter R.Wild "Distributing the encryption and decryption of a block cipher".

[12] K.H. Rosen, "Elementary number theory and its applications" Third edition, Addison-Wesley.

[13] Menzes A. and Vanstone S. "Hand book of applied cryptography", The CRC-Press eries of Discrete Mathematics and its Applications CRC-Press, 1997.

[14] Neal Koblitz "A course in number theory and cryptography" ISBN 3-578071-8, SPIN 10893308.

[15] Peter J. Smith and Michael J.J. Lennon, "A New Public Key System" LUC Partners, Auckland UniServices Ltd, The University of Auckland, Private Bag92019m Auckland, New Zealand.

[16] Phillip Rogaway Mihir Bellare John Black Ted Krovetz "OCB: A block-cipher mode of

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

operation for efficient authenticated encryption".

[17] P.Rogaway, M-Bellare, J. Black,T-Korvetz "A Block Cipher mode of operation for efficient authenticated encryption" Eighth ACM conference on computer and communication security (CCS-8) ACM Press, 2001.

[18] Serge Vaudenay "A classical introduction to cryptography applications for communication security" Springer International Edition.

[19] Song Y. Yan, "Number Theory for computing", 2nd edition, Springer, ISBN: 3-540-43072-5.

[20] Surendra Talari & P. Anuradha Kameswari, Pollard RHO algorithm implemented to Discrete Log with Lucas sequences, International Journal on Recent and Innovation Trends in Computing and Communication, ISSN: 2321-8169 Volume: 4, Issue: 3.

[21] Surendra Talari, S.S. Amiripalli, P. Sirisha, D.S. Kumar and V.K. Deepika, An Improved Cipher Based Automatic Theorem Proving Technique for encryption and Decryption, "Advances in Mathematics: Scientific Journal", page numbers 3121-3134, volume 9/5, June, 2020.

[22] W. Diffi and M. E. Helman "New directions in Cryptography." IEEE Transactions on Information theory, 22, 644654, 1976.

[23] William Stallings "Cryptography and network security principals and practice" 5th ed.