ADV MATH SCI JOURNAL
Advances in Mathematics: Scientific Journal **9** (2020), no.5, 3121–3134
ISSN: 1857-8365 (printed); 1857-8438 (electronic)
https://doi.org/10.37418/amsj.9.5.71

AN IMPROVED CIPHER BASED AUTOMATIC THEOREM PROVING TECHNIQUE FOR ENCRYPTION AND DECRYPTION

SURENDRA TALARI[1], S. S. AMIRIPALLI, P. SIRISHA, D. SATEESH KUMAR, AND V. KRISHNA DEEPIKA

ABSTRACT. Globalization has positively influenced almost every sector in India. In the present digital world, security and management of information in the cyber space is quite crucial. The multifarious dimension of cryptography plays an important role in exchange of information securely. In this paper we propose one new crypto system technique using Automatic Theorem Proving concept by assigning various ciphers to the antecedent and consequent rules. Here we form the sequent using plaint text, connective symbols then encrypt this plain text into various levels using antecedent rules and consequent rules and the corresponding assigned ciphers. Since it involves various levels of encryptions and decryptions, it is difficult to the attacker to decrypt the plain text, so that security is more. Though the encryption and decryption run time of the proposed technique is feasible, the security levels are infeasible.

1. INTRODUCTION

In this paper we discuss new encryption and decryption method using Automatic Theorem Proving [6, 14] in which we assigned different ciphers to the antecedent and consequent rules. Before forming encryption sequent we obtain level-1 cipher text using another cipher which was not used in the antecedent

[1]*corresponding author*

2010 *Mathematics Subject Classification.* 68P25, 94D05.

Key words and phrases. sequent's, connectives, antecedent rules and consequent rules, ciphers, encryption and decryption.

and consequent rules. Here we used vigenere cipher to obtain level-1 cipher. Since we assigned different ciphers to the antecedent and consequent rules, we get level-2, level-3, ..., level-k cipher texts, where k is the number of connectives used in the encryption process. This system contains one public key [9] with a set of variables obtained in the level-k encryption sequent. Here these variables take in the same order obtained in the level-k encryption sequent. Also this system contains two secret keys; the first secret key is the set of connectives used in the encryption sequent to get final cipher text that is level-k cipher text. The second secret key contains set of ciphers used to get level-1, level-2, ..., level-k cipher texts [10, 13, 17]. Since we get different levels of cipher texts, it is difficult to the attacker to decrypt the original plain text from the public key. Even if the attacker finds the secret keys, he will get the plain text only up to some levels and it is very difficult to find the plain text. The crypto system described in this paper is more secure and good than the previous methods and this system includes the procedures of techniques of encryption and decryption [22].

1.1. **Description of automatic theorem proving.** Automatic theorem proving [8] is used to check whether given statement is valid or not from the set of premises. It includes antecedent rules, consequent rules, sequent, axioms, statements, premises. It contains a set of rules and procedure which allows one to construct each step of derivation in a specified manner without any barrier to any ingenuity and finally to arrive at a last step. Even though this procedure is mechanical, it is a full decision process for validity of the statement/conclusion more than any other previous available methods. The system described is more efficient than the previous methods and this system includes the procedures of techniques of derivation. This system of derivation consists of 10 rules, an axiom schema and rules of well-formed sequent and formulas [6, 14].

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 with the order of precedence as given.
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 of formulas;

(c) Only those strings which 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 order in which the formulas appear in any string is not important and so the strings A, B, C; B, C, A; A, C, B; etc., are the same [3, 5].

Sequent: If alpha and beta are strings of formulas, then they are called a sequent in which alpha is denoted the antecedent and beta the consequent of the sequent. Thus A, B, C, D, E, F is true if and only if 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 $A \Rightarrow B$ means "A implies B" or is a tautology while means that is true. Ex: $P, Q, R \Rightarrow^S P, N$ 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. For example: $A, B, C \Rightarrow^S P, B, R$ is an axiom, where A, B, C, P, R are variables
6. Theorem: The following sequences are theorems of our system:
   (a) Every axiom is a theorem.
   (b) If a sequent alpha is a theorem and a sequent beta results from alpha through the use of one of the above rules of the system which are given below, then beta is a theorem.
   (c) Sequences obtained by (a) and (b) are the only theorems [2, 4].

1.2. **Rules.** The following rules are used to combine formulas within strings by introducing connectives $\{\urcorner, \wedge, \vee, \rightarrow, \leftrightarrow\}$. 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. In the description of these rules, there are strings of formulas while X and Y are formulas to

which the connectives are applied [23].

Antecedent Rules:

Rule 1: $\rceil \Rightarrow$: If $\alpha, \beta \Rightarrow X, \gamma$, then $\alpha, \rceil X, \beta \Rightarrow \gamma$

Rule 2: $\wedge \Rightarrow$: If X, Y, $\alpha, \beta \Rightarrow \gamma$, then $\alpha, X \wedge Y, \beta \Rightarrow \gamma$

Rule 3: $\vee \Rightarrow$: If X, $\alpha, \beta \Rightarrow \gamma$ and $Y, \alpha, \beta \Rightarrow \gamma$, then $\alpha, X \vee Y, \beta \Rightarrow \gamma$

Rule 4: $\rightarrow\Rightarrow$: If $Y, \alpha, \beta \Rightarrow \gamma$ and $\alpha, \beta \Rightarrow X, \gamma$, then $\alpha, X \rightarrow Y, \beta \Rightarrow \gamma$

Rule 5: $\leftrightarrow\Rightarrow$: If X, Y, $\alpha, \beta \Rightarrow \gamma$ and $\alpha, \beta \Rightarrow X, Y, \gamma$, then $\alpha, X \leftrightarrow Y, \beta \Rightarrow \gamma$

Consequent Rules:

Rule 1: $\Rightarrow\rceil$: If $X, \alpha \Rightarrow \beta, \gamma$, then $\alpha \Rightarrow \beta, \rceil X, \gamma$

Rule 2: $\Rightarrow \wedge$: If $\alpha \Rightarrow X, \beta, \gamma$ and $\alpha \Rightarrow Y, \beta, \gamma$, then $\alpha \Rightarrow \beta, X \wedge Y, \gamma$

Rule 3: $\Rightarrow \vee$: If $\alpha \Rightarrow X, Y, \beta, \gamma$, then $\alpha \Rightarrow \beta, X \vee Y, \gamma$

Rule 4: $\Rightarrow\rightarrow$: If X, $\alpha \Rightarrow Y, \beta, \gamma$, then $\alpha \Rightarrow \beta, X \rightarrow Y, \gamma$

Rule 5: $\Rightarrow\leftrightarrow$: If X, $\alpha \Rightarrow Y, \beta, \gamma$ and $Y, \alpha \Rightarrow X, \beta, \gamma$, then $\alpha \Rightarrow \beta, X \leftrightarrow Y, \gamma$

2. PRELIMINARIES

2.1. **Play fair Cipher:** Here we use the key word CHARLES (Charles Stone invented this cipher). Draw 5x5 matrix with the key word, first removing any repeated letters, as follows [18, 19]:

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

For example the plain text is 'meet me at the bridge', write this as 'me et me at th eb ri dg ex' and to make the even number of letters fill the space with 'x'. If any repeated letter is there in the plain text, the same pair is separated by filler. Suppose if the plain text is 'balloon' then we write this as 'ba lx lo on'. If the plain text letters are in the same row, each is replaced by the letter to the right with the first element of the row circularly. That is 'eb' is replaced by 'sd' and 'ng' is replaced by 'gi' or 'gj'. If the plain text letters are in the same column, then each letter is replaced by the letter beneath and with the top element of the column circularly. That is 'dt' would be replaced by 'my' and 'ty' would be replaced by 'yr'. If the plain text pair is not in the same row or column then each plain text letter in a pair is replaced by the letter that lies in its own row and column occupied by the other plain text letter. Suppose 'me' becomes 'gd' for the plain text 'meet me at the bridge' the corresponding cipher text is 'gd do gd rq pr sd hm em bv'.

2.2. **Vigenere Cipher:** It [15, 19] is a substation cipher also known as polyalphabetic cipher. While moving through the plain text, we use different mono alphabetic substitutions. Here plain text and cipher text is equal to $(Z26)^m$ where 'm' is a positive integer. Also key space is $(Z26)^m$, that is $k = (k_1, k_2, ...k_m) \in K^m$ and number of possible key words of length m is $(26)^m$. For encryption $e_k(x_1, x_2, ...x_m) = (x_1 + k_1, x_2 + k_2, ...x_m + k_m)$ under the modulo 26 and decryption is $d_k(y_1, y_2, ...y_m) = (y_1 - k_1, y_2 - k_2, ...y_m - k_m)$ under the modulo 26.

2.3. **Rail fence technique:** In this [15, 18, 19] cipher a different kind of mapping is achieved using transportation technique. Here plain text is writing down as sequence of columns and cipher text is read as sequence of rows. For example, consider the plain text 'meet me after the party over'; by applying rail fence technique of depth 2, we get the cipher text by the following steps. First write the plain text as sequence of columns of dept 2, now the cipher text is 'mematrhprysvretefeteatioe'. To decrypt this again we have to apply reverse of rail fence technique with dept 2 we will get required plain text.

m	e	m	a	t	r	h	p	r	y	s	v	r
e	t	e	f	e	t	e	a	t	i	o	e	

2.4. **Permutation cipher:** It is also known as transportation cipher. Here plain text and cipher text is equal to $(26)^m$ which is same as Viginere cipher. Key space

is a set of all possible permutations of $\{1, 2, ...m\}$. For each permutation $\pi \in k$, the encryption is $e_\pi(x_1, x_2, ...x_m) = [x_{\pi(1)}, x_{\pi(2)}, ..., x_{\pi(m)}]$ and the decryption is $d\pi(y_1, y_2, ..., y_m) = [y_{\pi^{-1}(1)}, y_{\pi^{-1}(2)}, ..., y_{\pi^{-1}(m)}]$ where π^{-1} is the inverse permutation of π [20, 25].

2.5. **Substitution Cipher:** In this plain text and cipher text are equal to all twenty-six English alphabets. Here k is the key space which is a set of all possible permutations of 26 alphabet characters. For each permutation $\phi \in k$, $e\phi(x) = \phi(x)$ where x is from the plain text set, the decryption is $d\phi(y) = \phi^{-1}(y)$ where y is from the cipher text set [1, 7].

3. Proposed algorithms

3.1. **Encryption process:** In this part [21] first we find level-1 cipher text from the plain text using Vigenere cipher. Then divide this level-1 cipher text into blocks where each block contain p number of alphabets where p is the length of the word in the vigenere cipher. Now label these blocks as $X_1, X_2, X_3, ..., X_m$, where 'm' is the finite value. If X_m block does not contain p number of alphabets then fill the blanks with the alphabet x. Form the sequent with these labels and connective symbols $\{\urcorner, \wedge, \vee, \rightarrow, \leftrightarrow\}$ using automatic theorem proving [6, 14] concept and make sure that the statement formula will contain in the consequent part only in the encryption sequent $\alpha, \beta, \chi \Rightarrow^S n\beta, \delta$ for $n = 1, 2, ...$ finite value where $\alpha, \beta, \chi, \beta\&\delta$ are simple atomic variables or compound statements. Then apply antecedent and consequent rules and we get level-2, level-3, ..., level-k cipher texts where k is number of connectives in the first encryption sequent. We stop applying the rules 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 retrieve the plain text, so that security is more. Here the first secret key is the set of ciphers used in antecedent and consequent rules and to obtain level-1 cipher text [15, 18, 19]. That is public key set contain two parts, first part contain the variables have to be use in antecedent part while forming first decryption sequent. Similarly, variables in the second part of the public key have to be used in consequent part while forming first decryption sequent. In the public key [11] 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-2 to level-k cipher texts". That is second secret key contains the order of the connective symbols we removed in the encryption sequents. In the second secret key one connective symbol has to apply to two variables or two statement formulas only in the process of decryption. The public key is set of "variables X_i^j with $1 \leq i \leq m$ and $1 \leq j \leq k$ in the final encryption sequent" where all the connectives were eliminated.

3.2. **Encryption algorithm:**

Input: Plain Text (MILITARY IS READY TO ATTACK) Output: Cipher Text (KVDPZRYJWEYCQFMNURAMWPAQ)
1. Start 2. In initial phase plain text is taken as input (MILITARY IS READY TO ATTACK) 3. Apply Vigenere cipher to get level-1 cipher text [1, 7] 4. Divide level-1 cipher text into p blocks 5. Label blocks with $X_1, X_2...X_m$ 6. Formation of 1st encryption sequent with $X_1, X_2, ...X_m$ 7. Apply antecedent and consequent rules on the 1st Encryption sequent until all the connectives are eliminated, then we get level-1, level-2...level-k cipher texts 8. Level-k cipher is the Final cipher text 9. Stop

3.3. **Decryption process:** The final cipher text obtained from the Alice has to be divided into the p letter blocks. Label these blocks with the variables X_i^j with $1 \leq i \leq m$ and $1 \leq j \leq k$ from the public key. Form the decryption sequent $\alpha^j, \beta^j, \Rightarrow^{SDn} \chi^j, \delta^j$ for $1 \leq j \leq k$ and $n = 1, 2, ...$ finite values where a_j, b_j, c_j, d_j are the variables from the public key [11]. Using private key, write the decryption sequens. Use the connectives in the secret key in reverse order i.e. from backward direction to decode the cipher text. Use the implications in the secret key from the right and 'R followed by connective symbol' represents rules that has to apply in decryption consequent part. Similarly, 'L followed by connective symbol' represents that rules has to apply in decryption antecedent part'. With one connective symbol in the secret key we have formed compound statement by taking two variables or two compound statements by considering the order. Repeat the process 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'. For the plain text-1 apply Vigenere cipher decryption process and we get required plain text [20, 25].

3.4. **Decryption algorithm:**

Input: Cipher Text (KVDPZRYJWEYCQFMNURAMWPAQ) Output: Plain Text (MILITARY IS READY TO ATTACK)
1. Start 2. In final phase cipher text is taken as input (KVDPZRYJWEYCQFMNURAMWPAQ) 3. Divide cipher text into blocks where each block contain p number of alphabet 4. Label the blocks with X_i^j with $1 \leq i \leq m$ and $1 \leq j \leq k$ in the same order as in the public key 5. Form the decryption sequent's using L-connectives or R-connectives in private key from backward direction. Repeat the process until all the L-connectives or R-connectives used 6. We get plain text-k, plain text-$(k-1)$, ... plain text-1 7. Apply decryption process of Vigenere cipher to the plain text-1 [1, 7] 8. We get required plain text 9. Stop

4. IMPLEMENTATION OF ENCRYPTION AND DECRYPTION

Symbol	Name
$X \wedge Y$	caser cipher
$X \vee Y$	permutation cipher
$X \rightarrow Y$	play fair cipher
$X \leftrightarrow Y$	substitution cipher
7X	rail fence technique
a-0, b-1, c-2, ...z-25	alphabets and its values in
$\Rightarrow^{Sn}$	encryption sequent
$\Rightarrow^{SDn}$	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: **MILITARY IS READY TO ATTACK**
- Using Vigenere cipher with key work: DOPE = (3, 10, 14, 15, 4)
- MILI| TARY| ISRE| ADYT| OATT| ACKx
- Level -1 cipher text: PWAM| WOGC| LGGI| DRNX| ROIX| DQZx
- Say (PWAM| WOGC| LGGI| DRNX| ROIX| DQZx)= $(X_1|X_2|X_3|X_4|X_5|X_6)$

Now for the sequent with the above variables $X_1, X_2...X_6$ using connective symbols $\{\rceil, \wedge, \vee, \rightarrow, \leftrightarrow\}$ make sure that the statement formula completely lies on consequent part only. $\Rightarrow^{S1}$ $(X_6 \wedge X_3) \rightarrow ((X_1 \wedge X_2) \rightarrow (X_5 \vee X_4))$, by using rule 'implies $\rightarrow$c' then the sequent 1 changes to $(X_6^1 \wedge X_3^1) \Rightarrow^{S2} ((X_1^1 \wedge X_2^1) \rightarrow (X_5^1 \wedge X_4^1)$ where X_6^1= TBVY, X_3^1= NCJK, X_1^1= WHKR, X_2^1= PVOE, X_5^1= TCWK, X_4^1= MDZK which is level-2 cipher text. To get level-3 cipher text apply the rule 'rule $\rightarrow$c' to then the sequent 2 changes to $(X_1^{11} \wedge X_2^{11})$, $(X_6^1 \wedge X_3^1) \Rightarrow^{S3} (X_5^{11} \wedge X_4^{11})$ where X_1^{11}= HSAM, X_2^{11}= WO VG, X_5^{11}= TM XN, X_4^{11}= ROXI. Again applying rule $'\wedge \Rightarrow'$ and $' \Rightarrow \vee'$ on the sequent 3 then we get the sequent 4 as X_1^{111}, X_2^{111}, X_6^{11}, $X_3^{11} \Rightarrow^{S4}$ where X_1^{111}= KVDP, X_2^{111}= ZRYJ, X_6^{11}= WEYC, X_3^{11}= QFMN, X_5^{111}= URAM, X_4^{111}= WPAQ which is level-4 cipher text. Since all connective symbols are eliminated in the sequent 4, we can stop the process and conclude that it is final cipher text [12, 16]. The final cipher text is **KVDPZRYJWEYCQFMNURAMWPAQ**. The public key is $(X_1^{111}, X_2^{111}, X_6^{11}, X_3^{11}; X_5^{111}, X_4^{111})$ and secret key1 is (level-1: Vigenere, $\wedge$:caser, $\vee$: permutation, $\rightarrow$: play fair, $\leftrightarrow$: substitution, $\rceil$: Rail fence) & secret key2 is $(c\rightarrow, c\rightarrow, a\wedge^2, c\vee)$ where $\wedge^2$ represents that the connective $\wedge$ has to apply twice and similarly for other connectives. In the second secret key one connective symbol has to apply to two variables or two statement formulas only. Consider the cipher text as 4 letter blocks as **(KVDP| ZRYJ| WEYC| QFMN| URAM| WPAQ)** and label it as $(X_1^{111}|X_2^{111}|X_6^{11}|X_3^{11}|X_5^{111}|X_4^{111})$ using public key [24]. Then form the sequent from the public key by choosing the variables before symbol ';' for antecedent part and after the symbol ';' for consequent part for decryption such as $X_1^{111}, X_2^{111}, X_6^{11}, X_3^{11} \Rightarrow^{SD1} X_5^{111}, X_4^{111}$, which is level-1 sequent in decryption process. Here $\Rightarrow^{SDk}$ represents k-level sequent for decryption process. Using secret keys form further level sequent steps by applying one connective symbol to two variables or two statement formulas at a time as $(X_1^{11} \wedge X_2^{11}), (X_6^1 \wedge X_3^1) \Rightarrow SD2\ X_5^{11} \vee X_4^{11}$ where X_1^{11}= HSAM, X_2^{11}= WOVG,

X_5^{11}= TMXN, X_4^{11}= ROXI, $(X_6^1 \wedge X_3^1) \Rightarrow SD3\ (X_1^1 \wedge X_2^1) \rightarrow (X_5^1 \vee X_4^1)$ where X_6^1= TBVY, X_3^1= NCJK, X_1^1= WHKR, X_2^1= PVOE, X_5^1= TCWK, X_4^1= MDZK & $\Rightarrow^{SD4} (X_6 \wedge X_3) \rightarrow ((X_1 \wedge X_2) \rightarrow (X_5 \vee X_4))$ where X_6= DQZx, X_3= LGGI, X_1= PWAM, X_2= WO GC, X_5= ROIX & X_4= DRNX. For this applying the decryption process of Vigenere cipher we obtain the plain text as **'MILITARY IS READY TO ATTACK'**.

4.2. **Implementation 2:** Consider the plain the text **'government has declared the war on enemy country'**. In Viginer [24, 25] cipher the key word is 'FIGHT' which is numerically equivalent to (58 6 7 19), after applying Vigenere cipher on plain text the level-1 cipher text is **'miykxhtgoxirnlpfpuuxsms fvtctakdfdeq'**. Divide this level-1 cipher text into letter blocks as **miykx| htgox| irnlp| fpuux| smsfv| tctak| dfdeqand** equivalent to $(X_1|X_2|X_3|X_4|X_5|X_6|X_7)$. For the first sequent with these variables as $\Rightarrow^{S1} (\neg((X_3 \rightarrow X_7) \wedge \neg(X_2 \vee X_5)) \rightarrow (X_1 \rightarrow (X_6 \vee X_4)))$. Apply 'rule implies $\rightarrow$' on the above sequent we get $(\neg(X_3^1 \rightarrow X_7^1) \wedge \neg(X_2^1 \vee X_5^1)) \Rightarrow^{S2} (X_1^1 \rightarrow (X_6^1 \vee X_4^1))$ where X_3^1= mhutq, X_7^1= fefst, X_2^1= provy, X_5^1= dibew, X_1^1= nkmxy, X_6^1= rorqm & X_4^1= usz(q)zq. On the second sequent apply the 'rule implies$\rightarrow$' we get, $X_1^{11}, (\neg(X_3^1 \rightarrow X_3^1) \wedge \neg(X_2^1 \vee X_5^1)) \Rightarrow^{S3} (X_6^{11} \vee X_4^{11})$ where X_1^{11}= gmykz, X_6^{11}= tctan & X_4^{11}= fpu(x)ux. After applying 'rule $\wedge$ implies' & 'rule implies $\vee$' on the third sequent we get $\neg(X_3^{11} \rightarrow X_7^{11})$, $\neg(X_2^{11} \rightarrow X_5^{11})$, $X_1^{11} \Rightarrow^{S4} X_6^{111}, X_4^{111}$ where X_3^{11}= pkyit, X_7^{11}= ihivw, X_2^{11}= suryb, X_5^{11}= glehz, X_6^{111}= rmroq & X_4^{111}= zzqu, sq. On the fourth sequent apply the 'rule $\neg$ implies' we get, $X_1^{11} \Rightarrow^{S5} X_3^{111} \rightarrow X_7^{111}, X_2^{111} \vee X_5^{111}, X_6^{111}, X_4^{111}$ where X_3^{111}= pytki, X_7^{111}= iiwhv, X_2^{111}= srbuy & X_5^{111}= gezlh. Apply the rule 'implies $\vee$' on the fifth sequent we get $\Rightarrow^{S6} X_2^{iv}, X_5^{iv}, X_3^{111} \rightarrow X_7^{111}, X_6^{111}, X_4^{111}$ where X_2^{iv}= bysru & X_5^{iv}= zhgel. On the sixth sequent apply the rule 'implies$\rightarrow$' we get $X_3^{iv}, X_1^{11} \Rightarrow^{S7} X_7^{iv}, X_2^{iv}, X_5^{iv}, X_6^{111}, X_4^{111}$ where X_3^{iv}= wtmqk(w) & X_7^{iv}= w(k)phwc stop the process since all the connective symbols were eliminated the sixth sequent. So the final level cipher text [12, 16] is "wtmqk(w)gmykzw(k)phw cbysruzhgelrmroqzzqu, sq". The public key [24] is $\{X_3^{iv}, X_1^{11}; X_7^{iv}, X_2^{iv}, X_5^{iv}, X_6^{111}, X_4^{111}\}$ and secret key1 is same as in implementation 1 & secret key 2 is $\{c \rightarrow, a\wedge, c \rightarrow, a\neg^2, c\vee^2, c \rightarrow\}$ where $\neg^2$ represents that the connective negation $\neg$ has to apply twice and similarly for other connectives. Divide the above cipher text into five letter blocks as (**wtmqk(w)| gmykz| w(k)phwc| bysru| zhgel| rmroq| zzqu, sq**) and using public key

equate these blocks to $\{X_3^{iv}|X_1^{11}|X_7^{iv}|X_2^{iv}|X_5^{iv}|X_6^{111}|X_4^{111}\}$. Now form the decryption first sequent with the variables using private key as $X_3^{iv}, X_1^{11} \Rightarrow^{SD1} X_7^{iv}, X_2^{iv}, X_5^{iv}, X_6^{111}, X_4^{111}$. Using secret key and public key form further level sequent steps by applying one connective symbol to two variables or two statement formulas at a time as $X_1^{11} \Rightarrow^{SD2} (X_3^{111} \rightarrow X_7^{111}), X_2^{iv}, X_5^{iv}, X_6^{111}, X_4^{111}$ where X_3^{111}= pytki & X_7^{111}= iiwhv, $X_1^{11} \Rightarrow^{SD3} (X_3^{111} \rightarrow X_7^{111}), (X_2^{111} \vee X_5^{111}), (X_6^{11} \vee X_4^{11})$ where X_2^{111}= srbuy, X_5^{111}= gezlh, X_6^{11}= tctan & X_4^{11}= fpu(x)ux, $\rceil(X_3^{11} \rightarrow X_7^{11})$, $\rceil(X_2^{11} \vee X_5^{11})$, $X_1^{11} \Rightarrow^{SD4} (X_6^{11} \vee X_4^{11})$ where X_3^{11}= pkyit, X_7^{11}= ihivw, X_2^{11}= suryb & X_5^{11}= glehz, $\rceil(X_3^{11} \rightarrow X_7^{11})$, $\rceil(X_2^{11} \vee X_5^{11}) \Rightarrow^{SD5} (X_1^{1} \rightarrow X_6^{1} \vee X_4^{1})$ where X_1^1= nkmxy, X_6^1= rorqm & X_4^1= usz(q)zq, $\rceil(X_3^1 \rightarrow X_7^1)$, $\rceil(X_2^1 \vee X_5^1) \Rightarrow^{SD5} (X_1^1 \rightarrow X_6^1 \vee X_4^1)$ where X_3^1= mhutq, X_7^1= fefst, X_2^1= provy & X_5^1= dibew, $\Rightarrow^{SD6}(\rceil(X_3 \rightarrow X_7) \wedge \rceil(X_2 \vee X_5)) \rightarrow (X_1 \rightarrow (X_6 \vee X_4))$ where X_3= irnlp, X_7= dfdeq, X_2= htgox, X_5= smsfv, X_1= miykx, X_6= tctak & X_4= fpuux. By writing these in order like $X_1X_2X_3X_4X_5X_6X_7$ we get level-1 cipher text as **miykxhtgoxirnlpfpuuxsmsfvtc takdfdeq**. Applying Vigenere cipher [24, 25] decryption process with the 5-letter word we get required plain text as **'government has declared the war on enemy country'**.

5. Results and discussion

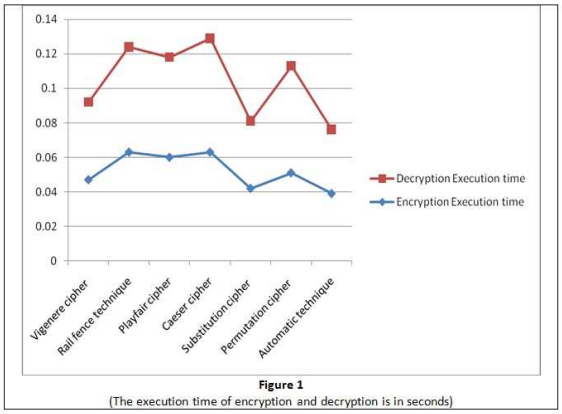

Figure 1
(The execution time of encryption and decryption is in seconds)

6. Conclusion

In this paper we developed a new crypto system method using Automatic theorem proving; we assigned different ciphers at level-1 encryption and in antecedent and consequent rules. 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 public key, using this public key he can decrypt the text up to some levels only and it is infeasible to decrypt the plain text. So security levels are more in this method. After applying programming concept to the proposed technique we got feasible run time of encryption and decryption with infeasible security levels. Hence the proposed method is better than the other existing encryption and decryption methods. For future scope, we can define new cipher, new antecedent rules and consequent rules and can apply to this crypto system method.

Acknowledgment

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

References

[1] A. J. Menezes, P. C. Van Oorschot, S. A. Vanstone: *Hand book of Applied Cryptography*, CRC Press Series on Discrete Mathematics and its Applications. CRC Press, Boca Raton, FL, 1997.

[2] S. S. Amiripalli, V. Bobba: *An Optimal TGO Topology Method for a Scalable and Survivable Network in IOT Communication Technology*, Wireless Personal Communications, **107**(2) (2019), 1019–1040.

[3] S. S. Amiripalli, V. Bobba: *Impact of trimet graph optimization topology on scalable networks*, Journal of Intelligent and Fuzzy Systems, **36**(3) (2019), 2431–2442.

[4] S. S. Amiripalli, V. V. R. Kollu, B. J. Jaidhan, L. S. Chakravarthi, V. A. Raju: *Performance improvement model for airlines connectivity system using network science*, International Journal of Advanced Trends in Computer Science and Engineering, **9**(1) (2020), 789–792.

[5] S. S. Amiripalli, V. Bobba: *Research on network design and analysis of TGO topology*, International Journal of Networking and Virtual Organisations, **19**(1) (2018), 72–86.

[6] B. Rao: *Mathematical Foundations of Computer Science*, SciTech Publications (India) Pvt Ltd, 2005.

[7] D. R. STINSON: *Cryptography: theory and practice*, CRC Press, 2002.

[8] G. SUTCLIFFE: *Automated Theorem Proving: Theory and Practice A Review*, AI Magazine, **23**(1) (2002), 121–122.

[9] A. A. ABD EL-AZIZ: *An extended data protection model based on cipher-text-policy attribute based encryption model and an XACML framework in cloud computing*, International Journal of Advanced Science and Technology, **28**(16) (2019), 1021–1033.

[10] G. FREY: *The arithmetic behind cryptography*, Notices of the American Mathematical Society, **57**(3) (2010), 366–374.

[11] H. DELFS, H. KNEBL: *Introduction to Cryptography- Principles and Applications*, Springer Verlag, 2015.

[12] H. YOSH: *The key exchange cryptosystem used with higher order Diophantine equations*, IJNSA, **3**(2) (2011), 43–50.

[13] I. NIVEN, H. S. ZUCKERMAN, J. H. SILVERMAN: *An Introduction to the Theory of Numbers*, 5th ed., John Wiley and Sons, New York, 1991.

[14] J. BUCHMANN: *Introduction to cryptography*, Springer Verlag, 2001.

[15] J. P. TREMBLAY, R. MANOHAR: *A text book of Discrete Mathematical Structures with Applications to Computer Science*, McGraw Hill Education (India) Edition, 1997.

[16] S. M. A. ALI, H. F. HASAN: *Novel encryption algorithm for securing sensitive information based on feistel cipher*, Test Engineering and Management, Sept-Oct 2019, 10–16.

[17] K. M. MARTIN, R. SAFAVI-NAINI, H. WANG, P. R. WILD: *Distributing the encryption and decryption of a block cipher*, Designs Codes and Cryptography, **36**(3) (2005), 263–287.

[18] K. H. ROSEN: *Elementary number theory and its applications*, Third edition, Addison-Wesley, 1993.

[19] H. SYED, A. KUMAR: *A concrete security framework model for cloud computing security issues*, International Journal of Control and Automation, **12**(5) (2019), 261–270.

[20] A. MENZES, S. VANSTONE: *Handbook of applied cryptography*, The CRC-Press series of Discrete Mathematics and its Applications CRC-Press, 1997.

[21] N. KOBLITZ: *A course in number theory and cryptography*, Springer Verlag, 1994.

[22] P. ROGAWAY, M. BELLARE, J. BLACK, T. KROVETZ: *OCB: A block-cipher mode of operation for efficient authenticated encryption*, ACM Transactions on Information and System Security, **6**(3) (2001), 196–205.

[23] 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.

[24] S. VAUDENAY: *A classical introduction to cryptography applications for communication security*, Springer, 2006.

[25] S. Y. YAN: *Number Theory for computing*, 2nd edition, Springer, 2002.

Department of Mathematics
GIS, GITAM Deemed to be University
Visakhapatnam, AP, India
E-mail address: surendrat.bw@gmail.com

Department of Computer Science
GIS, GITAM Deemed to be University
Visakhapatnam, AP, India

Faculty of Mathematics
Indian Maritime University
Visakhapatnam, AP, India

Department of Mathematics
Koneru lakshmaiah Education Foundation
Vaddeswaram, Guntur, AP, India

Department of Computer Science
GIS, GITAM Deemed to be University
Visakhapatnam, AP, India