ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 1, January 2018

Mathematical Logic and Logical equivalence implementation to find the intermediate key Management for DES Encryption Algorithm

[1] Mohanesh B M, [2] Anil Kumar C J, [3] Dr Putte Gowda D
[1] Assistant Profesor,Computer Science and Engineering. ,A.T.M.E, Mysuru ,
[2] Associate professor ,C.S and Engg ,A.T.M.E,Mysuru, [3] Professor,C.S and Engg ,A.T.M.E,Mysuru

Abstract: **- The objective of the study is to look into a new method to generate an intermediate key for a symmetric key given in the DES encryption algorithm. Using the concept of Mathematical Logic and Logical Equivalence an intermediate key is generated.An intermediate key used at sender and the receiver side.There are two equations used one on the sender side and another on the receiver side both giving the same intermediate key. Mathematical logic is the science dealing with the methods of reasoning; these are the statements that are called propositions. Propositions are the statement which in a given context said to be true or false .These propositions are connected by the logical connectives and they are "not", "and", "or", "if then", "if and only if". The propositions formed using these logical connectives is called compound propositions. Two propositions u and v are said to be logically equivalent whenever u and v have the same truth value. This is denoted by u⇐⇒v and it's represented as u and v are logically equivalent. During the generation of the intermediate key, u is used at the sender side and v is used at the receiver end to provide the same intermediate key.This paper proposes a new method for generating an intermediate key for DES algorithm.**

Index Terms**: - DES, DES encryption, Logical equivalence.**

I. INTRODUCTION

DES stands for Data Encryption standard and it is an Encryption method used for a security using a key to provide encryption and decryption. This algorithm involves carrying out permutation substitutions between the encrypted data and key. The main aim of the paper is to provide security for the key that is used in the DES algorithm[1][2], DES is an encryption standard used to provide security for the data by using symmetric key during the encryption and decryption, there has been a very less work in providing a security for the key that is being used. During encryption the data is divided into the blocks of 64 bit size and its put for the encryption, There are totally 16 rounds among which ,first being the initial permutation then 16 rounds of processing with the round key in each round and finally the final permutation, Key generator provides a key for each round. When the key has been given as an input, this key is processed with the mathematic logic to form an intermediate key, further this key is used as input for an encryption and decryption. Data Encryption Standard is a Symmetric key block cipher using the concept of Fiestel Cipher.It carries out 16 rounds of Fiestel rounds ,in each block 64 bit of key length is reduced to 56 bits before use.Figure 1 shows the DES algorithm with 16 rounds .

(i) Initial and Final Permutations

Initial and final permutations are the straight permutation that changes the pin location, Initial permutation is done before the first round and the final permutation is done after the 16 th round.

(ii) Round Functions

In each round of the DES cipher, It uses the fiestel cipher and the steps involved in these rounds are.

Step 1: The initial input is 32 bit and it is expanded to 48 bit, using expansion p box.

Step 2: XOR with the 48 bit key,represented as round key 1.

Step 3: S Boxes.

In S Boxes it uses the 8 S boxs and each 6 bit is converted into the 4 bit.

Step 4: Straight P-box,

The output of the 8 S-boxes is given to the straight P-box.

(iii) Key Generation.

For every round a key is generated, It is converted into 48 bits from the 56 bits[1][2]. For the round 1,2,9,16 there is 1 bit shift and for the others there is two bit shift. Figure 1 shows initial permutation and final permutation with 16 rounds of encryption or decryption.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 1, January 2018

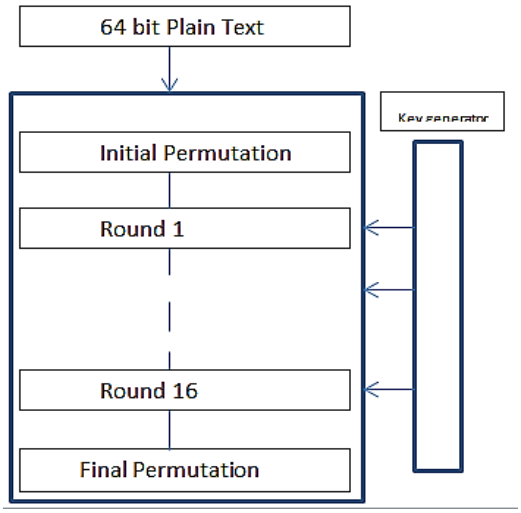

Fig 1. DES Algorithm with 16 rounds

II. RELATED LITRATURE

A.Mathematical Logic

Mathematical logic is the science dealing with the methods of reasoning, consider a statement "three is a prime number" "Seven is divisible by 3". These are the statements that are called propositions. Propositions are the statement which in a given context said to be true or false. The above two statements each is true and false respectively. These propositions are connected by the logical connectives and they are "not", "and", "or", "if then", "if and only if". The propositions formed using this logical connectives is called compound propositions. From the above 2 statements we get Three is a prime number and Seven is not divisible by 3 which is true. Some of logical connectives are.

(i) Conjunction.

The logical connectives "and" referred earlier is called conjunction of a given proposition. Let p and q be two propositions, the conjunction "p^q" is true only when p is true and q is true and all other cases are false. Table 1 explains truth table of the Conjunction.

p	q	P^q
0	0	0
0	1	0
1	0	0
1	1	1

Table 1. Truth Table of the Conjunction

(ii) Disjunction

A compound proposition obtained by combining two given proposition by inserting a word "or" between them is called Disjunction. The disjunction pvq is false only when p is false and q is false; in all other cases it is true. Table 2 explains truth table of the Disjunction.

p	q	P^q
0	0	0
0	1	1
1	0	1
1	1	1

Table 2 .Truth table of the Disjunction.

(iii) Negation

The proposition obtained by inserting the word 'not' at an appropriate place .The negation of p is denoted by ¬ p read as not of p. Table 3 explains the truth table of the negation.

p	¬ p
0	1
1	0

Table 3 .Truth table of the Negation

(iv) Conditional

Conditional proposition obtained by combining two given propositions by using the words "if" and "then" at appropriate places is called a conditional. The notation of p and q is denoted by p→q represents conditional. Table 4 explain truth table of conditional proposition.

p	q	P→q
0	0	1
0	1	1
1	0	0
1	1	1

Table 4. Truth table of the conditional proposition.

(v) Biconditional

Let p and q be two propositions. Then the conjunction of the conditional p→q and q→p is called bi-conditional of p and q. Table 5 explain Truth table of the Bi-conditional.

p	q	q→p	p→q	P↔ q
0	0	1	1	1
0	1	0	1	0
1	0	1	0	0
1	1	1	1	1

Table 5. Truth table of the Bi-conditional proposition.

B.DES Algorithm

DES algorithm Data Encryption Standard is a Symmetric key block cipher uses concept of Fiestel Cipher. It carries out 16 rounds of Fiestel rounds.For a block of 64 bit with a key length of 56 bits out of 64 bits. For the round 1,2,9,16 there is 1 bit shift and for the others there is two bit shift.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 1, January 2018

C. Logical Equivalence.

Two propositions u and v are said to be logically equivalent whenever u and v have the same truth value. This is denoted by u⟸⟹v and its represented as u and v are logically equivalent. Lets consider an example, there are p and q then (p→q) ⟸⟹(¬p)vq and Table 6 explains truth table for logical equivalence.

p	q	(p→q)	¬p	(¬p)vq
0	0	1	1	1
0	1	1	1	1
1	0	0	0	0
1	1	1	0	1

Table 6 .Truth table of the Logical Equivalence

D. Triple DES

Triple DES is a method of providing encryption by repeating DES encryption for 3 times. There are 48 rounds for the triple DES Similarly an encryption is made stronger when we use different intermediate key at every level of DES encryption.

E. Observation and Need for Intermediate key.

In the present method, the symmetric key used in the encryption and the decryption of DES algorithm is same and is passed over the network. The key passed over the network is directly used in the encryption and decryption, so it is not very sure to tell the key was not watched by the middle man. This motivates the need of an intermediate key. An intermediate key formed from the given key and used for encryption and decryption of a DES algorithm. Triple DES is an encryption algorithm to run DES for 3 times[1], and it uses the same key in all 3 rounds hence this can be draw back so This paper proposes extension of intermediate key For second and third round using logical equivalence equations[10].

F. Present Key exchange algorithms

Diffie Hellman algorithm and RSA algorithm[1][2] is the method used in present days for key exchange. This provides security to the key being shared. One of the drawback of using this algorithm is the data passed over the network will be very big. This paper explains the need of intermediate key and method of creating an intermediate key and passing a small amount of information of data over the network which helps in generating the intermediate key.

III METHOD AND DESIGN CONCEPTS.

A. Logical Equivalence

The key used in the Des algorithm is easily known in the network and this key is directly used for first round of encryption. This paper proposes a secured intermediate key and is used for the first round, using the concept of logical Equivalence. Key generated using combination of given key and truth table value of logical equivalence from the equation used is called intermediate key. This intermediate key is passed to the first round of DES encryption. Consider a key "AABB09182736CCDD"[1] combine it with truth table value of logical equivalence obtained from an equation. Key generated represented as a new intermediate key it is passed to the first round of DES encryption. Considering a statement (p→q) ⟸⟹(¬p)vq[6] which is logically equivalent for generating an intermediate key. Table 7 shows the Truth table for the Logical equivalence.

p	q	(p→q)	¬p	(¬p)vq
0	0	1	1	1
0	1	1	1	1
1	0	0	0	0
1	1	1	0	1

Table 7.Truth table for Logical equivalence.

B. Intermediate key generation at the sender side

Consider the key AABB09182736CCDD given for the DES Algorithm, At the sender end intermediate key is generated by using the truth table values obtained from the logical equivalence. Now we consider a notation (p→q) which has truth values of 1,1,0,1.Using this truth values we form an intermediate key.In the table below 1,1,0,1 is taken in the multiple of 4 and is mapped with the given key ,the letters of the key matching with the 1 is kept and letters matched with 0 is made 0.Table 8 shows key and an Intermediate key from the truth table[8].

Truth table values	1	1	0	1	1	1	0	1	1	1	0	1	1	1	0	1
key	A	A	B	B	0	9	1	8	2	7	3	6	C	C	D	D
I.key	A	A	0	B	0	9	0	8	2	7	0	6	C	C	0	D

Given key	AABB09182736CCDD
Intermediate key	AA0B09082706CC0D

Table 8 Truth table for intermediate key.

(i) Algorithm

Initialize to Accept the plain text and the key
Generate an intermediate key
Using this intermediate key generate the first round key
Apply for the Des algorithm
Encrypted text is formed.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 1, January 2018

C. Architecture ,Data Flow Diagram and Uml table

Figure 2 explains the architecture of intermediate key, it has logical equivalence term ,truth table ,given key ,intermediate key and DES module as Architectural module. Figure 3 explains dataflow diagram, Flow starts by accepting the key ,taking equation for truth table, Intermediate key, an equation is sent over the network ,checks the list of equation selects the equation and finally decrypt. Figure 4 explains the U.M.L diagram, The U.M.L diagram consists of classes being implemented Laws of Logic ,Rule of Inference, List of Equations, Pattern Matching, Truth Table and DES.

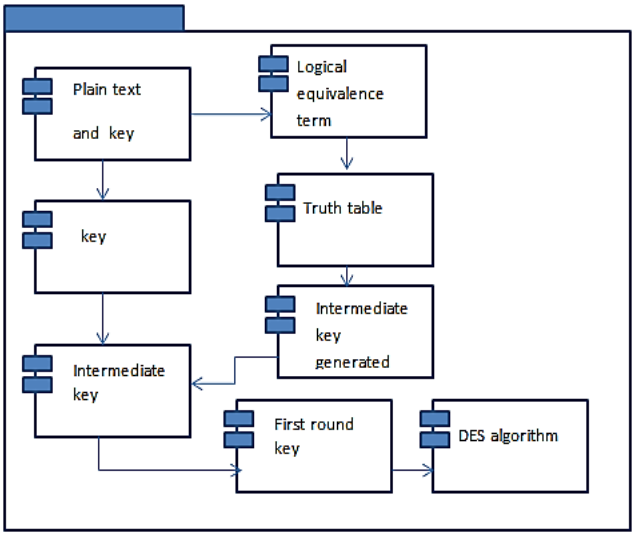

Figure 2.Architecture of an Intermediate key algorithm.

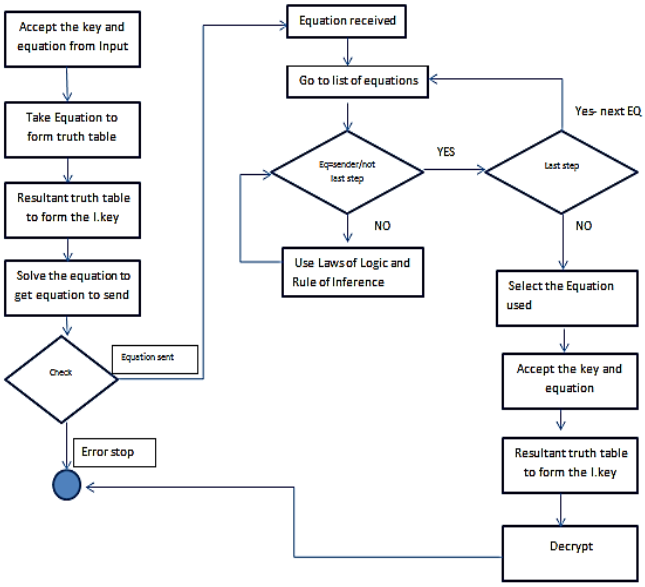

Figure 3.Data Flow diagram.

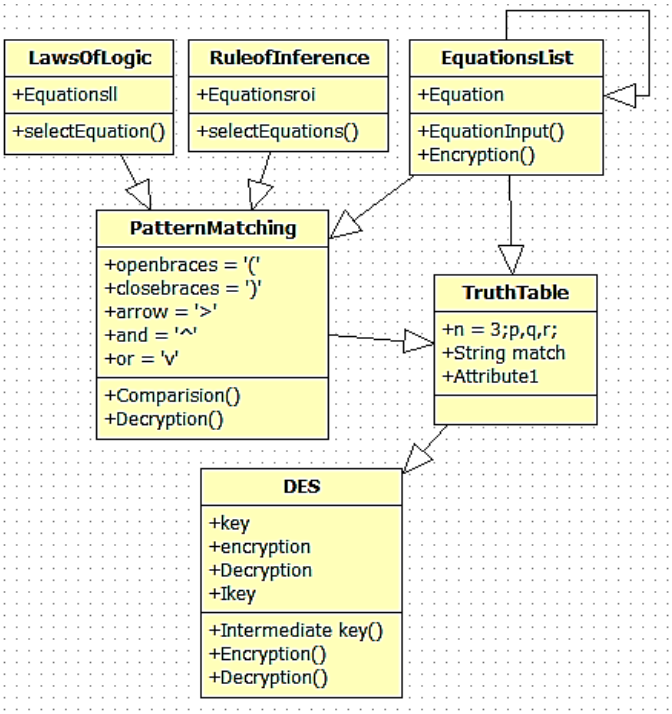

Figure 4. UML diagram

D .Intermediate key generation at the receiver end.

Consider the key AABB09182736CCDD given for the DES Algorithm[4][9], intermediate key is generated by finding a truth table values of the equation obtained from the list of equation. Selecting Equation from the list of equation is done, when the equation solved should result into the equation passed over the network. This is termed as Receiver equation which is logically equivalent to the equation at the sender end. From table 7 we consider a notation (¬p)vq as a receiver equation for (p→q).

E Logical Equivalence as a key and laws of logic.

Logical Equivalence of two equations is obtained by solving laws of logic and Rule of Inference. Let's consider an example in equation 1, it is applied with all different laws of logic to get its equivalent. The equation 2 is got by applying the commutative law which is logically equivalent, this statement is more simplified to get equation 3,for equation 3 absorption law is applied and we get equation 4,similarly applying these laws we get equations 5,6,7,8,9,10,11,12 respectively.

$(p \rightarrow q) \wedge [\neg q \wedge (r \vee \neg q)]$ (1)
$(p \rightarrow q) \wedge [\neg q \wedge (r \vee \neg q)] \Longleftrightarrow (p \rightarrow q) \wedge [\neg q \wedge (\neg q \vee r)]$ (2)
$(p \rightarrow q) \wedge [\neg q \wedge (r \vee \neg q)] \Longleftrightarrow (p \rightarrow q) \wedge [\neg q \wedge (\neg q \vee r)]$ (3)
$(p \rightarrow q) \wedge [\neg q \wedge (r \vee \neg q)] \Longleftrightarrow (p \rightarrow q) \wedge \neg q$ (4)
$(p \rightarrow q) \wedge [\neg q \wedge (r \vee \neg q)] \Longleftrightarrow (p \rightarrow q) \wedge \neg q$ (5)
$(p \rightarrow q) \wedge [\neg q \wedge (r \vee \neg q)] \Longleftrightarrow \neg [(p \rightarrow q) \rightarrow q]$ (6)
$(p \rightarrow q) \wedge [\neg q \wedge (r \vee \neg q)] \Longleftrightarrow \neg [\neg (p \rightarrow q) \vee q]$ (7)

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 1, January 2018

$(p \rightarrow q) \wedge [\neg q \wedge (r \vee \neg q)] \Longleftrightarrow \neg [(p \wedge \neg q) \vee q]$ (8)

$(p \rightarrow q) \wedge [\neg q \wedge (r \vee \neg q)] \Longleftrightarrow \neg [q \vee (p \wedge \neg q)]$ (9)

$(p \rightarrow q) \wedge [\neg q \wedge (r \vee \neg q)] \Longleftrightarrow \neg [(q \vee p) \wedge (q \vee \neg q)]$ (10)

$(p \rightarrow q) \wedge [\neg q \wedge (r \vee \neg q)] \Longleftrightarrow \neg [(q \vee p) \wedge T0]$ (11)

$(p \rightarrow q) \wedge [\neg q \wedge (r \vee \neg q)] \Longleftrightarrow \neg (q \vee p)$ (12)

The above statements are logically equivalent. Similarly we can see more logically equivalent statements.

These Logical Equivalence is obtained by applying the laws of logic. some of laws of logic are Laws of double negation,Idempotent,Laws,identity,Laws,inverse,Laws,domination,Laws,Commutative laws, Absorption laws, De-morgans law, Associative Law, Distributive law.

F. Rules of Inference

Logical Equivalence is obtained by extending the solving method by using Rules of Inference.

Consider a set of propositions p1,p2,p3 …pn and a proposition then the compound proposition of the form $(p1 \wedge p2 \wedge p3 \ldots\ldots \wedge pn) \rightarrow Q$ is called argument. Some of rules of Inference are as shown below[7].

i)Rule of Conjunctive simplification: $(p \wedge q) \Rightarrow p$

ii)Rule of Disjunctive Amplification: $p \Rightarrow p \vee q$

iii)Rule of Syllogism: $\{(p \rightarrow q) \wedge (q \rightarrow r)\} \Rightarrow (p \rightarrow r)$

iv)Modus Pones : $\{p \wedge (p \rightarrow q)\} \Rightarrow q$

v) Modus Tollens : $\{(p \rightarrow q) \wedge \neg q\} \Rightarrow (\neg p)$

vi)Rule of disjunctive syllogism :$\{(p \vee q) \wedge \neg p\} \Rightarrow q$

vii)Rule of Contradiction $(\neg p \rightarrow F0) \Rightarrow p$.

G. Method to implement

To generate an intermediate key in the DES algorithm .Consider an example from equation 13 and an attempt is made to solve with the combination of both laws of logic and rules of inference. Now the equation 14,15 gives logically equivalent, then by applying the laws of inference equation 16 is obtained by law of syllogism and this equation 16 is not logically equivalent to equation 13. Similarly by applying the laws we get a simplified equation 17 and 18.

$(p \rightarrow q) \wedge (r \rightarrow s) \wedge (p \vee r)$ (13)

$\Longleftrightarrow (p \rightarrow q) \wedge (r \rightarrow s) \wedge (\neg p \rightarrow r)$ (14)

$\Longleftrightarrow (p \rightarrow q) \wedge (\neg p \rightarrow r) \wedge (r \rightarrow s)$ (15)

$\Rightarrow (p \rightarrow q) \wedge (\neg p \rightarrow s)$ (16)

$\Longleftrightarrow (\neg q \rightarrow \neg p) \wedge (\neg p \rightarrow s)$ (17)

$\Rightarrow (\neg q \rightarrow s)$ (18)

$\Longleftrightarrow q \vee s.$ (19)

From the above problem the logically equivalent equations are (13) and equation (14) then using laws of logic and rule of inference [6]it is derived to equation 19.For the example being discussed in table 9,Equation 19[6] is got by solving the equation 15.During the encryption of the DES algorithm equation13 is used and intermediate key is generated. Then equation 19 which is not logically equivalent is passed over the network to represent the equation used in generating the intermediate key. At the decryption side of the DES algorithm there are list of equations which are logically equivalent and not logically equivalent. These equation need to be solved one by one to identify required logically equivalent equation used in the encryption. Table 9 shows the equations used in encryption, in the network, and in decryption.

Sender uses for encryption	$(p \rightarrow q) \wedge (r \rightarrow s) \wedge (p \vee r)$
Equation sent **in network**	$(q \vee s)$
Receiver solves the equation To get (qvs)	$(p \rightarrow q) \wedge (\neg p \rightarrow r) \wedge (r \rightarrow s)$

Table 9 Equation used at sender ,network and receiver.

H. Implementation steps

Rules of Inference and logic of laws is shown and is compared while encrypting and decrypting the statements. The laws of logic used during the encryption and decryption used are.

1. Double negation $(\neg \neg p) = p$.
2. Idempotent laws $(p \vee p) = p$, $(p \wedge p) = p$
3. Identity law $(p \vee F0) = p$,$(p \wedge T0) = p$
4. Inverse law $(p \vee \neg p) = T0$,$(p \wedge \neg p) = F0$,
5. Domination laws $(p \vee T0) = T0$, $(p \wedge F0) = F0$
6. Commutative laws $(p \vee q) = (q \vee p)$,$(p \wedge q) = (q \wedge p)$
7. Absorption Laws $(p \vee (p \wedge q)) = p$,$(p \wedge (p \vee q)) = p$.
8. Demorgans laws $\neg(p \vee q) = \neg p \wedge \neg q$, $\neg(p \wedge q) = \neg p \vee \neg q$,
9. Associative laws $p \vee (qvr) = (pvq)vr$, $p \wedge (q \wedge r) = (q \wedge q) \wedge r$
10. Distributive laws

$p \vee (q \wedge r) = (pvq) \wedge (pvr)$,$p \wedge (qvr) = (p \wedge q) v (p \wedge r)$

Rules of Inference used in encryption and decryption are.

1.Modus Ponens
2.Law of syllogism
3.Modus Tollens
4.Rule of Disjunctive syllogism
5.Rule of contradiction
6.Rule of conjunctive simplification
7.Rule of disjunctive amplification
8.Rule of conditional proof
9.Rule of proof cases
10 Rule of Constructive dilemma and rule of destructive dilemma used in future enhancement.

IV. RESULTS AND DISCUSSION.

A. Test Case 1

First test case was conducted, at the encryption side the equation 20 was used and decryption is done using same equation. Total number of terms used is 3 that is p,q,r.

$(p \rightarrow q) \wedge (q \rightarrow r)$ (20)

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 1, January 2018

The equation expected to pass over the network is p→r now the equation is got by solving equation 20 by law of inference.

Table 10 explains the first Test case study.

Equation at sender	(p→q)^(r→s)^(p v r)
Equation at network	(q v s)
Equation at receiver end	(p→q)^(¬p→r)^(r→s)

Table 10 explains the first Test case study.

B. Test Case 2

During the test case 2, The program is made as specified in figure 4 (which is the UML diagram of the classes). In this test case encryption is made by selecting one of list of equations. Then during decryption, to identify the equation which is used in the encryption all the equation in the equation list is solved which ever equation results in the equation which is passed over the network is selected. This result to say which equation is used in the encryption.

C. Test Case 3

In this test case 3 A large equations is used during encryption and a very small solved equation is used to pass over the network, then during decryption this large equation is identified and used during the decryption. Table 11 shows which uses a separate equation for encryption and a separate equation that has to be transferred over the network and a separate equation at a decryption side.

Equation at sender	(p→q)^(r→s)^(p v r)
Equation at network	(q v s)
Equation at receiver end	(p→q)^(¬p→r)^(r→s)

Table 11 equations used at the test case 3

D. Performance

This paper proposes a new method of generating intermediate key. Using this method of generating an intermediate key improves the standard of encryption .As the length of the equation increases the complicated encryption is made and the advantage of this encryption is that the data sent over the network to represent this equation can be very small. Even if there is a middle man attack intruder cannot find which key has been used to form the intermediate key. In the present day it is known to use a triple des, If the intermediate key is used during the triple des then the encryption becomes more strong. As a pros and cons , The equations that is used has to be present in the sender end and the receiver end defined previously if this equation is accessed by any attacker this will become a very much draw back to this encryption.

E. Improved performance with Triple DES and intermediate key

Triple DES is a method of providing encryption by repeating the encryption for 3 times. There are 48 rounds for the triple DES[3][5]. Similarly an encryption can be made stronger when it uses different intermediate key at every level of DES encryption. As there is a constant effort made to break the encrypted message, there is a need to provide improvements in giving up gradation of the des system and triple des, This paper can provide an attempt to make this encryption stronger and hard to break by any attacks.

F. Comparing the present and the proposed algorithms.

RSA and diffie Hellman[11][12] is used to provide security for the key being exchanged and termed to be as a strongest algorithm. Now the drawback of these algorithms is that very big large context of data is passed over the network. This paper suggests an algorithm to provide a small data to big data which is to be passed over the network for encryption[3].

V. FUTURE ENHANCEMENTS

The security of the data can be given when encryption is very strong and this can be done by providing strong mathematical proofs for encryption. As future enhancements more data security can be provided by using the concepts of inclusion and exclusion.

VI. CONCLUSION

A new technique intermediate key using rule of inference and laws of logic in combination with logical equivalence is applied for DES algorithm. The main objective is to generate intermediate key .From test case 1,2,3 it is clearly observed that DES can be given a strong encryption technology by using in intermediate key .For further work it is planned to use rule of induction to provide more security.

ACKNOWLEDMENTS

Authors remain thankful to Dr S.K. Katti and Dr Anusuya M.A for helping and guiding us.We thank all the people who have helped us in preparation of this paper.

REFERENCES

1. Farouzan,B.A & Mukhopadhyay,D (2010). Cryptography and Network Security.New Delhi,India :Tata McGraw-Hill.

2. Stallings, W. (2011).Cryptography and Network Security: Principles and Practice.US,USA:Pearson.

3. Sindhu, G.,Krithika,P (2015).Analysis and comparison of symmetric key algorithm (Blowfish,DES,TEA,IDEA) in Cryptography.IJSART-Volume 1 Issue 11 NOVEMBER 2015.

4. H.Fiestel,W.A.Notz, and J.L Smith, "Some Cryptographic Techniques Machine to Machine Data Communications", Proceedings on the IEEE,v.63,n.11,1975,pp,1545-1554.
5. Karthik S,Muruganandam . A,(2014).Data Encryption and Decryption by using Triple DES and Performance Analysis of Crypto System, International Journal of Scientific Engineering and Research (IJSER).Vol. 2 (11).

6. Ralph P Grimaldi and Ramana B.V.(2009).Discrete and Combinatorial Mathematics.US,USA:Pearson

7. E.C Koenig , " Analysis for correct reasoning by robots: modus ponens modus tollens",Proceedings on the I.E.E.E. August 06 1989,pp,584-589.

8. Anupam Chattopadhyay,Zoltan Rakosi,"Combinational logic synthesis for material implication",Proceedings on I.E.E.E 2006,PP,200-203.

9. Ji Yao,Hongbo Kang, " FPGA Implementation of Dynamic Key Management for DES Encryption algorithm",Proceedings on the I.E.E.E .2011,pp,volume 9 ,4795-4798.

10. Mathhew Morrison , "Theory,Synthesis and Application of Adiabatic and Reversible logic Circuits for Security Applicaation".Proceedings on the I.E.E.E ,2014,pp,252-255.

11. Aqeel sahi Khader ,David Lai, "Preventing man in the middle attack in Deffie-Hellman key exchange protocol".Proceedings on the I.E.E.E ,2015,pp,204-208.

12. P.M.Aishwarya,Archana Raj,Dona John , "Binary RSA encryption Algorithm", Proceedings on the I.E.E.E ,2016,PP,178-181.