International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

Implementation of One Time Pad Cipher with Rail Fence and Simple Columnar Transposition Cipher, for Achieving Data security

Jawad Ahmad Dar[1], Sandeep Sharma[2]

[1]Research Scholar, Computer Science and Engineering, Kurukshetra University Kurukshetra, Haryana, India

[2]Research Scholar, Computer Science and Engineering, Kurukshetra University Kurukshetra, Haryana, India

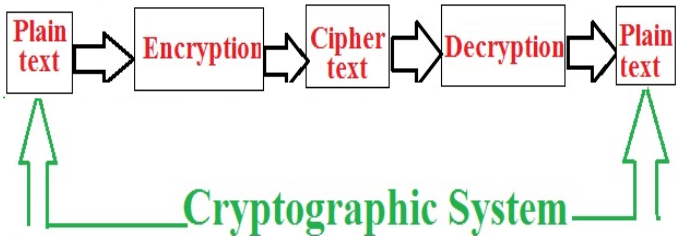
Abstract: ***Cryptography is an art and science of converting original message into no readable form. There are two techniques for converting data into no readable form. Transposition technique, Substitution technique. In recent years there is drastic progress in Internet world. Sensitive information can be shared through internet but this information sharing is susceptible to certain attacks. Cryptography was introduced to solve this problem. Cryptography is art for achieving security by encoding the plain text message to cipher text. Substitution and transposition are techniques for encoding. When Caesar cipher substitution, Rail fence cipher and Columnar Transposition Cipher techniques are used individually, cipher text obtained is easy to crack. This Paper will present a perspective on combination of techniques like Rail fence and colounar transposition with one time pad cipher. One Time Pad is an example of substitution method. In this paper I will presented how to improve security of One Time Pad Cipher to make it more secure and strong by Its implementation with Rail fence and columnar transposition cipher***

Keywords: Rail fence cipher, key, columnar transposition, cryptography, One Time Pad cipher, cryptanalysis.

1. Introduction

The dramatic rise of internet has opened the possibilities that no one had imagined. We can connect to any person, any organization or any computer, no matters how far we are from them This modern era is dominated by paperless offices-mail messages-cash transactions and virtual departmental stores. Due to this there is a great need of interchanging of data through internet.. Internet cannot be used only for browsing purpose. Sensitive information like banking transactions, credit card information and confidential data can be shared through internet. But still we are left with a difficult job of protecting network from variety of attacks. With the lots of efforts, network support staff came up with solution to our problem named "Cryptography". Cryptography is the art of achieving security by encoding the data into unreadable form. Data that can be read and understood without any difficulty is called plain text or clear text. The method of encoding Plain text in such a way as to hide its content is called encryption. Encrypting plain text results in unreadable gibberish called cipher text. You use Encryption to ensure that information is hidden from anyone for whom it is not intended, even those who can see the encrypted data. The process of reverting cipher text to its original plain text is called decryption . There are two primary ways in which plaintext can be codified to corresponding Cipher text: Substitution and Transposition. A Substitution technique is one in which the letters of Plain text are replaced by other letters or by numbers(Caesar Cipher

Hill Cipher, Monoalphabetic cipher etc).A Transposition technique is one in which the letters of the message are rearranged or permuted. (Rail Fence method, Columnar method etc.). One Time Pad is an example of substitution method. As One Time Pad has various limitations so this paper will present a perspective on combination of techniques rail fence and transposition. With the era of computer, need of automated tools became essential and the collection of tools designed to protect data and to protect data from hacker is known as Computer Security The use of networks and communication facilities for carrying data between users and computer to computer is done. So Network Security measures are needed to protect data during transmission For Network Security came the concept of Cryptography- meaning is „Secret Writing -is the most effective and strongest tool for controlling against many types of security attacks. So Encryption is the process to change data in a form that cannot be get easily. Symmetric and Asymmetric are the two types of encryption. In symmetric encryption techniques we use the same key for both encryption and decryption purpose. In symmetric method, there are two techniques (substitution and transposition) are used. Substitution technique maps the plaintext elements into cipher text elements and Transposition technique change the position of plaintext elements systematically into ciphertext elements.



2. One Time Pad and its Cryptanalysis

One Time Pad Algorithm :One-time pad encryption we need a key, called one-time pad. A one-time pad can be a singlesheet, a booklet or a strip or roll of paper tape that contains series of truly random digits. A one-time pad set consists oftwo identical one-time pads, one pad called OUT

and one called IN. To establish one-way communications,you only need one OUT pad for the sender and one IN pad for the receiver. To communicate in both directions, you need two different one-time pad sets: person A has an OUT pad of which person B has the IN copy, and person B has another OUT pad of which person A has the IN copy. Never use a single pad to communicate in both directions to avoid the risk of simultaneous use of the same pad sheet! The use of multiple IN copies of a pad, to enable more than one person to receive a message, is possible but not advisable. Multiple copies pose additional security risks and should only be used in a strictly controlled environment. Never use multiple OUT copies of a pad, as this will inevitable result in simultaneous use of the same pad and the risk of non destroyed copies of a pad.One-time pad encryption is only possible if both sender and receiver are in possession of the same key. Therefore, both parties must exchange their keys beforehand. This means that the secure communications are expected and planned within a specific period. Enough key material must be available for all required communications until a new exchange of keys is possible. Depending on the situation, a large volume of keys could be required for a short time period, or little key material could be sufficient for a very long period, up to several years.

2.1 Encryption And Decryption Using One Time Pad Algorithm

The one-time pad is a long sequence of random letters. These letters are combined with the plaintext message to produce the cipher text. To decipher the message, a person must have a copy of the one-time pad to reverse the process. A one time pad should be used only once and then destroyed . To encipher a message, you take the first letter in the plaintext message and add it to the first random letter from the one-time pad. For example, suppose you are enciphering the letter S (the 19th letter of the alphabet) and the one-time pad gives you C (3rd letter of the alphabet). You add the two letters and subtract 1. When you add S and C and subtract 1, you get 21 which is U. Each letter is enciphered in this method, with the alphabet wrapping around to the beginning if the addition results in a number beyond 26 (Z).To decipher a message, you take the first letter of the cipher text and subtract the first random letter from the one-time pad. If the number is negative you wrap around to the end of the alphabet. Army Signal Corp. Officer, Joseph Mauborgne, proposed an improvement to Vernam Cipher that was the ultimate in security, He suggested that we use a random key that is as long as the message means the key need not to be repeated. In additional key must be use once for encryption and decryption of a single message and then that key is discarded. So this technique is called as One Time Pad and there is relationship between key and plaintext and it is unbreakable. In this as advance of vignere cipher scheme we Can use 27 character in which 27th character is SPACE, so in this key will be as long as message. So table of Vignere cipher must be expanded to 27*27. If in case it is known that a given cipher text is One time pad cipher, then brute force cryptanalysis is easily performed: Try all the 27 keys.

3. Columnar Transposition Cipher

The columnar transposition cipher is a fairly simple, easy to implement cipher. It is a transposition cipher that follows a simple rule for mixing up the characters in the plaintext to form the ciphertext.Although weak on its own, it can be combined with other ciphers, such as a substitution cipher, the combination of which can be more difficult to break than either cipher on it's own.

3.1 Example

The key for the columnar transposition cipher is a keyword e.g. INDIAN. The row length that is used is the same as the length of the keyword. To encrypt a piece of text, e.g.defend the east wall of the castle,we write it out in a special way in a number of rows (the keyword here is INDIAN):

I	N	D	I	A	N
d	e	f	e	n	d
t	h	e	e	a	s
t	w	a	l	l	o
f	t	h	e	c	a
s	t	l	e		

In the above example, the plaintext has been padded so that it neatly fits in a rectangle. This is known as a regular columnar transposition. An irregular columnar transposition leaves these characters blank, though this makes decryption slightly more difficult. The columns are now reordered such that the letters in the key word are ordered alphabetically.

D	N	A	I	N	I
f	d	n	e	e	d
e	s	a	e	h	t
a	o	l	l	w	t
h	a	c	e	t	f
l			e	t	s

The ciphertext is read off along the columns:
Dttfsehwttfeahleeleenalcdsoa

4. Rail Fence Cipher

Similarly Rail Fence cipher is also a very weak cipher to Cryptanalyze. A code breaker simply has to try several depths until the correct one is found. It is very easy to find depth if you know some of the plain text. Letters break into rows according to certain fixed patterns based on the number of rows in the key . For example, if there are two rows, then letters 1, 3, 5, … of the message are in row one and letters 2, 4, 6, ... are in row two. Example shown below

Let plain text be " KURUKSHETRA UNIVERSITY KURUKSHETRA"

K R K H T A N V R I Y U U S E R

U U S E R U I E S T K R K H T A

Cipher text is "KRKHTANVRIYUUSERUUSERUIESTKRKHTA"

RAIL FENCE CIPHER

5. Proposed Algorithm

5.1 A. Encryption Algorithm

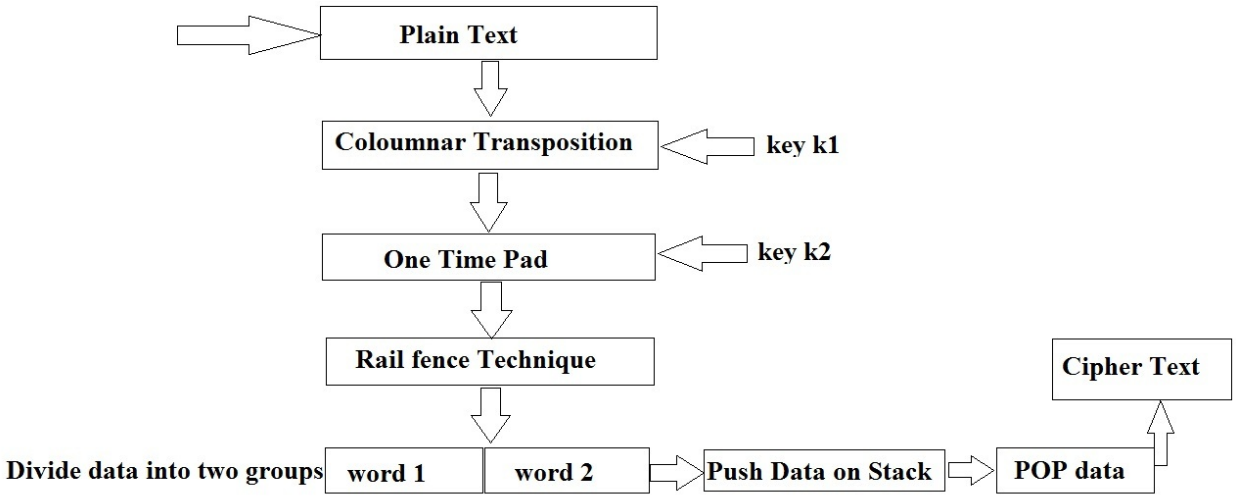
1) First take the plain text to be encrypted from sender.
2) write the plain text in rectangular format across rows, order is determined by key k1.(Columnar transposition technique).
3) Read off the message column by column in order using Key K1,we get cipher text CT1.
4) Perform Encryption Technique (one Time pad cipher) on CT1,using key k2,we get CT2
5) Perform Rail fence technique on CT2we get,CT3
6) Now divide the cipher text(CT3),into two halves, as Word 1,andWord 2.
7) To add more complexity put these different words, on different stacks using PUSH operations, now POP the Values from stack, we get two words. Let it be CT4.
8) Finally CT4 is our required Cipher Text.

5.2 B. Decryption Algorithm

1) Write the cipher text to be converted into plain text,(CT4)
2) write cipher text as two separate words Word 1,and Word
3) PUSH two words on to stacks, using different stacks
4) POP one element from stack one and second element from stack second.
5) Using Key K2 to decrypt CT3 by one time pad cipher ,we get CT2.
6) Arrange cipher text obtained in step 5(CT2),into rectangular format, as column by column using Key K1 and read of as rows.
7) Output of step 6 is our required plain text

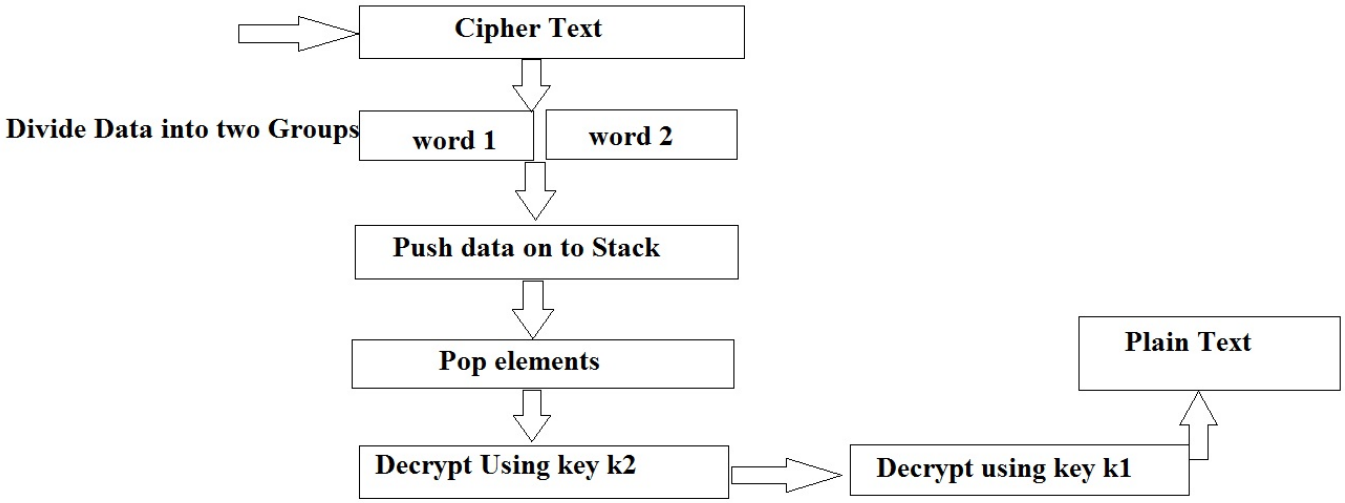
6. Block Diagram of Proposed Work

6.1Block Diagram of Proposed Encryption Algorithm



BLOCK DIAGRAM OF PROPOSED ENCRYPTION ALGORITHM

6.2 Block Diagram of Proposed Decryption Algorithm



Block diagram for Proposed Decryption Algorithm

7. Example

7.1 Encryption

1) let the plain text to be Encrypted is**" SAMALKHA GROUP OF INSTITUTIONS".**
2) Arrange the plaintext across rows in a rectangular format ,using **key K1= 4 3 2 1(**Columnar Transposition),as shown in figure

LET PLAIN TEXT BE"
SAMALKHA GROUP OF INSTITUTIONS"

KEY	4	3	2	1
	S	A	M	A
	L	K	H	A
	G	R	O	U
	P	O	F	I
	N	S	T	I
	T	U	T	I
	O	N	S	

READ THE TEXT AS COLOUMNS IN ORDER TO
GET CIPHER TEXT AS="AAUIIIMHOFTTSAKROSUNSLGPNTO"
CT1="AAUIIIMHOFTTSAKROSUNSLGPNTO"

A	A	U	I	I	I	M	N	O	F	T	T	S	A	K	R	O	S	U	N	S	L	G	P	N	T	O
1	1	21	9	9	9	13	8	15	6	20	20	19	1	11	8	15	19	21	14	19	12	7	16	14	20	15
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	1
2	3	24	13	14	15	20	16	24	16	31	32	32	15	26	34	32	37	40	34	40	34	30	40	39	46	16
2	3	24	13	14	15	20	16	24	16	- 26	- 26	- 26	15	26	- 26	- 26	- 26	- 26	- 26	- 26	- 26	- 26	- 26	- 26	- 26	16
2	3	24	13	14	15	20	16	24	16	5	6	6	15	26	8	6	11	14	8	14	8	4	14	13	20	16
B	C	X	M	N	O	T	P	X	P	E	F	F	O	Z	H	F	K	N	H	N	H	D	N	M	T	P

CIPHER TEXT 1
ONE TIME PAD KEY
TOTAL SUM
SUBTRACT 26 IF SUM>26
TOTAL SUM
CIPHER TEXT 2

ONE TIME PAD ENCRYPTION WE GET CIPHER TEXT 2="BCXMNOTPXPEFFOZHFKNHNHDNMTP"

CT2="BCXMNOTPXPEFFOZHFKNHNHDNMTP

B	X	N	T	X	E	F	Z	F	N	N	D	M	P	
	C	M	O	P	P	F	O	H	K	H	H	N	T	

READ AS ROWS WE GET CIPHER TEXT CT3="BXNTXEFZFNNDMPCMOPPFOHKHHNT"

RAIL FENCE TECHNIQUE ON CT2

3) Now read columns in order, we get cipher text(CT1).”**AAUIIIMHOFTTSAKROSUNSLGPNTO**”
4) Using One time pad cipher(Substitution Technique),Encrypt CT1 by **Key K2** we get New cipher text, let it be labeled as **CT2**=”**BCXMNOTPXPEFFOZHFKNHNHDNMTP**”. As shown in figure
5) Now perform rail fence technique on CT2,as shown in figure, we get again New cipher text, labeled as **CT3=”BXNTXEFZFNNDMPCMOPPFOHKHHNT” As shown in figure**
6) Now divide cipher text CT3,into two equal Halves,as Word1 and Word 2,as shown below

B X N T X E F Z F N N D M P

C M O P P F O H K H H N T

READ AS ROWS WE GET CIPHER TEXT CT3="BXNTXEFZFNNDMPCMOPPFOHKHHNT"

RAIL FENCE TECHNIQUE ON CT2

DIVIDE CT3 INTO TWO PARTS (WORDS) AS= "BXNTXEFZFNNDMP" "CMOPPFOHKHHNT"

WORD 1 WORD 2

REPRESENTS THE CHARACTER THAT WE ADDED TO BALANCE THE WORDS

7)To add more complexity,put these different words into two stacks,by using PUSH Operations.As shown

STACK 1
P
M
D
N
N
F
Z
F
E
X
T
N
X
B

STACK 2
1(*)
T
N
H
H
K
H
O
F
P
P
O
M
C

8)Now **POP** elements from both stacks
Stack1:**PMDNNFZFEXTNXB**
Stack2:**1TNHHKHOFPPOMC,**let this be CT4.

9)Final cipher text is Stack1+Stack2,that is CT= **"PMDNNFZFEXTNXB1TNHHKHOFPPOMC"**

7.2 Decryption

1) Write cipher text **CT="PMDNNFZFEXTNXB1TNHHKHOFPPOMC"**

2) Divide it into two halves as=" **PMDNNFZFEXTNXB"**and **"1TNHHKHOFPPOMC,"as shown**

FINAL CIPHER TEXT CT4="PMDNNFZFEXTNXB1TNHHKHOFPPOMC"

DIVIDE CT4 INTO TWO WORDS="PMDNNFZFEXTNXB" "1TNHHKHOFPPOMC

WORD 1 WORD 2

PUSH THESE TWO WORDS ON TWO SEPARATE STACKS,AND POP ONE ELEMENT FROM STACK 1 AND SECOND ELEMENT FROM STACK 2 AT A TIME WE GET CT3="BCXMNOTPXPEFFOZHFKNHNHDNWTP"

3) Push these two words on different stacks, as shown in figure

STACK1
B
X
N
T
X
E
F
Z
F
N
N
D
M
P

STACK 2
C
M
O
P
P
F
O
H
K
H
H
N
T
1(*)

4) **POP** one element from Stack 1 and Second element from Stack 2,we get pair of two words, example first pair **BC,XM,NO,TP,XP,EF,,FO,ZH,FK,NH,NH,DN,MT,P 1**
Therefore
CT3=“”BCXMNOTPXPEFFOZHFKNHNHDNMTP”

5) Now with **Key K2** decrypt CT3 using one time pad cipher, TechniqueWe get
CT1=”AAUIIIMHOFTTSAKROSUNSLGPNTO” as shown below

A	A	U	I	I	I	M	N	O	F	T	T	S	A	K	R	O	S	U	N	S	L	G	P	N	T	O
1	1	21	9	9	9	13	8	15	6	20	20	19	1	11	8	15	19	21	14	19	12	7	16	14	20	15
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	1
2	3	24	13	14	15	20	16	24	16	31	32	32	15	26	34	32	37	40	34	40	34	30	40	39	46	16
2	3	24	13	14	15	20	16	24	16	- 26	- 26	- 26	15	26	- 26	- 26	- 26	- 26	- 26	- 26	- 26	- 26	- 26	- 26	- 26	16
2	3	24	13	14	15	20	16	24	16	5	6	6	15	26	8	6	11	14	8	14	8	4	14	13	20	16
B	C	X	M	N	O	T	P	X	P	E	F	F	O	Z	H	F	K	N	H	N	H	D	N	M	T	P

CIPHER TEXT 1
ONE TIME PAD KEY
TOTAL SUM
SUBTRACT 26 IF SUM>26
TOTAL SUM
CIPHER TEXT 2

DECRYPTION OF CT2,BY ONE TIME PAD CIPHER WE GET CT1="AAUIIIMNOFTTSAKROSUNSLGPNTO"

6) Now using Key **K1=4 3 2 1** ,arrange CT1 in rectangular format columns.(Columnar decryption),
CT1=” **AAUIIIMHOFTTSAKROSUNSLGPNTO**”

KEY	4	3	2	1
	S	A	M	A
	L	K	H	A
	G	R	O	U
	P	O	F	I
	N	S	T	I
	T	U	T	I
	O	N	S	

7) Now Read as row by row we get original plain text.
PT=SAMALKHA GROUP OF INSTITUTIONS

8. Advantages of Proposed Algorithm

This One Time Pad in which security is enhanced using Columnar Transposition Technique ,with Rail Fence has various advantages over simple One Time Pad technique-

1) Diverse cipher text
If we scrutinize at the Algorithm we can notice at every Stage we are getting diverse cipher text, thus more trouble to cryptanalyst.
2) Brute force attack on it is impossible
3) There is no chance to cryptanalyze overcomes the limitation of simple One Time Pad.

9. Disadvantage of Proposed Algorithm

1) It makes use of two keys .
2) Use of Simple Coloumnar Transposition technique makes it a complex method.
3) difficult to implement.

10. Conclusion

In this paper I have presented how to improve security of One Time Pad Cipher to make it more secure and strong by Its implementation with Rail fence and columnar transposition cipher. As we know One Time Pad is already a strongest Substitution technique and used for high security data. It is a substitution technique in which only letter replaced by any other letter. Transposition techniques are mainly used with other technique to improve the level of security. Only use of Substitution technique replaces the letter by any other letter and only use of Transposition technique changes the place of letters but use of both techniques concurrently progress the level of security and provide more secure data. The above proposed method is the combination of both techniques and provides much more secure data than only use of single Substitution technique.as one time pad it self is Substitution cipher.

10.1 Acknowledgment

Author's would like to give sincere gratitude especially to Mrs Nautan sani,(Astt Prof) for his guidance and support to pursue this work.

References

[1] Jawad ahmad dar,*"Humanizing the Security of Rail Fence Cipher Using Double Transposition and Substitution Techniques*, International *Journal of Science and Research (IJSR) ISSN (Online): 2319-7064, Volume 3 Issue 9, September 2014*
[2] Atul Kahate (2009), *Cryptography and Network Security*, second edition, McGraw-Hill
[3] William Stalling *"Network Security Essentials(Applications and Standards)*",Pearson Education,2004
[4] practicalcryptography.com/ciphers/rail-fence-cipher/
[5] Charles P.Pfleeger "Security in Computing", 4th edition, Pearson Education
[6] Neal R. Wagner "*The Laws of Cryptography: Perfect Cryptography: The One-Time Pad* "

Author Profile

Jawad Ahmad Dar is currently in final year M TECH Computer science and Engineering from **Kurukshetra University, Kurukshetra**. He did B.TECH in Computer Science and Engineering from **Islamic University of Science and Technology Kashmir in 2013 (2009 Batch).** He has 5 International Publications. His interested areas of research are, Neural Networks, Mobile computing, Network security, and Design and Analysis Algorithms, Advanced Optimization and Simulation Techniques.

Sandeep Sharma is also currently in final year M TECH Computer science and Engineering from **Kurukshetra University, Kurukshetra**. He did B.TECH from Delhi Institute of Technology and Management, affiliated to **Maharshi Dayanand University, Rohtak** in Information technology. My areas of interest are wireless communication, wireless networking, cryptography, network security.