Security Enhancement in WEP by Implementing Elliptic Curve Cryptography Technique

Jaspreet Singh, Er. Sandeep Singh Kang

Abstract: Wireless Network has been gaining rapid popularity over the years because they provide a significant advantage over the traditional Wired Network. Many wireless networks are based on security scheme Wired Equivalent Privacy (WEP). Despite employing the well-known and believed-secure RC4 cipher, WEP falls short in accomplishing its security goals. In this paper weaknesses and possible attacks on the RC4 stream cipher in WEP have analyzed and we proposes more secure WEP Protocol that offers secure encrypted communication by using Elliptic Curve Cryptography (ECC) Technique. Point Multiplication is the core operation performed in ECC. NAF (Non – Adjacent Form) is the efficient method used for Point Multiplication. We implemented both Standard and Block method for computing NAF of ECC and done the comparative study of these methods by taking several parameters in WEP. The proposed ECC Technique will ensure secure encryption in WEP and will enhance its security.

Keywords: Elliptic Curve Cryptography, ECC in WEP, Security of WEP, Standard NAF in ECC, Block method in ECC.

I. INTRODUCTION

Although WLAN 802.11b protocol provides some security mechanisms, they have some weaknesses and hacker can attack WLAN easily by making use of these weaknesses [3].

WEP is used to improve the security of wireless LAN (WLAN) when WEP is active in wireless LAN, packet is encrypted separately with RC4 stream cipher with keys of 64 to 256 bits [3][4]. However, security experts revealed several weaknesses in the key scheduling algorithm of RC4, showing that RC4 is completely insecure in the common mode of operation which is used in WEP which in turn generate WEP security problems such as Weak encryption, offline dictionary attacks, and key exchange problem [5][6]. The WEP provides encrypted communication using an encryption key between the client station and Access point (AP). All client stations and APs on a network use the same key to encrypt and decrypt data. The secret key shared between all 802.11 devices can be retrieved by attackers which are passively collecting data over the wireless network [9].

Elliptic Curve Cryptography (ECC) fits for an efficient and secure encryption scheme in wireless networks because ECC utilizes smaller key sizes for equivalent security. The key exchange problem is the major flaw of Using symmetric algorithms. Asymmetric encryption algorithms solve the problems by replacing single shared secret key with a pair of mathematically related keys: one public key that can be made publicly available and one secret private key[7]. They require only that the communication entities exchange keying material that is authentic (but not secret). Each entity selects a single key pair (e,d) consisting of public key e and private key d property that it is computationally infeasible to determine the private Key solely from knowledge of the public key [14].

Manuscript received on November, 2012.

Jaspreet Singh, Department of Computer Science and Engineering (MTech Scholar), Chandigarh Engineering College, Landran (Mohali) Punjab, India.

Er. Sandeep Singh Kang (Associate Professor), Department of Computer Science and Engineering, Chandigarh Engineering College, Landran (Mohali) , Punjab, India.

II. WEP

The Wired Equivalent Privacy (WEP) was designed to provide the security of a wired LAN by encryption through use of the RC4 algorithm with two side of a data communication [1]. The WEP encryption algorithm works

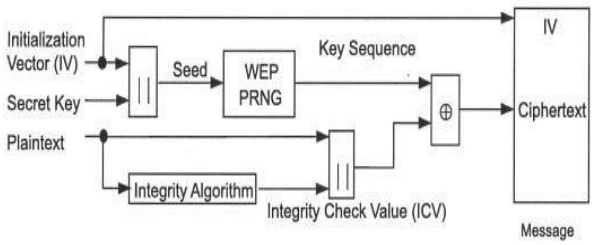

Figure shows the encryption process of WEP.

This process consists of following steps:

1. Calculate ICV using CRC 32 over the plaintext message.
2. Concatenate ICV to Plaintext.
3. Choose a random Initialization Vector (IV) And concatenate with secret key.
4. Input the secret key k+IV into RC4 Algorithm to produce a pseudorandom Key sequence.
5. Perform Encryption Plain Text + ICV by Exclusive OR with pseudorandom key Sequence under RC4 to produce the Cipher text.
6. Send IV to receiver by placing with Cipher text.

The Weaknesses of WEP Algorithm

(1) Invariance Weakness

RC4 is a kind of stream key algorithm widely used. RC4 is composed of key schedule algorithm (KSA) and pseudo-random generation algorithm (PRGA). In KSA process the WEP key is changed to a state array s with hundreds of plus and swap operation. The process of PRGA generates a pseudo-random stream. This stream is used to encrypt the plaintext or decrypt the cipher text. Some researches indicate that the RC4 algorithm is vulnerable in the aspect that every 256 keys or less produce one weak key.

This is called invariance weakness. These weak keys will result in the pseudorandom have the specific and recognizant prefix. The data that are encrypted with these weak keys will become breakable [3] [11] and also The RC4 algorithm is vulnerable to analytic attacks of the state table [11].

(2) IV Weakness

There is another weakness is repeat-used IV, which is called IV weakness. The input key of RC4 is composed of 24bytes IV and 40 bytes WEP key. The IV is used to guarantee that the same plaintext will never generate the same cipher text [3]. Being 24-bit long, there are 2^{24} different IVs .On a busy network, the IV will surely be reused, if the default key has not been changed, the original message can be retrieved relatively easily.

The RC4 algorithm can be broken into two stages: initialization and operation. In the initialization stage the 256-bit state table, **S** is populated, using the key, K as a seed. Once the state table is setup, it continues to be modified in a regular pattern as data is encrypted [10].

III. DICTIONARY ATTACK IN WEP

In this attack, the wireless LAN is subjected to defeat by determining its secret key by repeatedly trying different passwords from a standard set, which in cryptography is known as the dictionary; hence the name Dictionary Attack. This attack targets weakly chosen keys. The capture of as few as two encrypted packets is sufficient for this type of attack. The attack requires a large dictionary that contains the likely list of words that would be the keys used for encryption [12].

In WEP sender S generates a random data packet (Dp) and sends it to receiver R after encrypting it using the secret key Sk. This forms a challenge for the receiver R. R decrypts, calculates Dp +1 and returns it back to S after encryption [13].

However if secret key S_k is a weakly chosen password, and it belongs to a set of words in the dictionary D, then the challenge – response transaction can be attacked . The intruder guesses a key Gk ∈ D and tries to decrypt both messages Dp and Dp + 1 with the guessed key (Gk). Using this key the intruder obtains two values, P and Q respectively. If P = Q + 1, then the attacker has deduced the correct secret key S_k = Gk [13].

In our demonstration of the Dictionary attack in WEP, the key which are being generated by the RC4 (Symmetric Algorithm) are being hacked by the implementation of dictionary attack. So the key generated by RC4 which is used for the encryption of packets in WEP are not secure while as the ECC based on Public key cryptography(we have pair of one private and one public key) the Dictionary attack is unable to hack the keys generated by ECC in WEP. So ECC generated keys for encryption of packets for transmission on network in WEP is more secure.

IV. ELLIPTIC CURVE CRYPTOGRAPHY

Elliptic Curve Cryptography (ECC) is a public key cryptography.ECC uses the arithmetical operation as the core operation for high level security function such as Encryption. ECC devices require less storage, less power, less memory, and less bandwidth than other systems [7]. ECC has a very unique mathematical structure that enables the process of taking any two points on a specific curve, of adding the two points and getting as a result another point on the same curve. This special feature is advantageous for cryptography due to the inherent difficulty of determining which original two points were used to get the new point [13].The mathematical operations of ECC is defined over the elliptic curve $y^2 = x^3 + ax + b$. Each value of the 'a' and 'b' gives a different elliptic curve [14].

The public key is a point in the curve and the private key is a random number. The public key is obtained by multiplying the private key with the generator point G in the curve[14]. Scalar multiplication is the central operation of elliptic curve cryptosystem. It involves the computation of kP where k is the secret key (scalar) and P a point on the elliptic curve. For any k, the calculation of kP is broken down into a series of additions and doublings. The speed of scalar multiplication plays an important role in the efficiency of whole system [15].

POINT MULTIPLICATION

In point multiplication a point P on the elliptic curve is multiplied with a scalar k using elliptic curve equation to obtain another point Q on the same elliptic curve i.e. KP=Q [15].

Point multiplication is achieved by two basic elliptic curve operations

- Point addition, adding two points J and K to obtain another point L i.e., L = J + K. [15]
- Point doubling, adding a point J to itself to obtain another point L i.e. L = 2J. [15]

Example : Let P be a point on an elliptic curve. Let k be a scalar that is multiplied with the point P to obtain another point Q on the curve. i.e. to find Q = kP.

If k = 23 then kP = 23.P = 2(2(2(2P) + P) + P) + P. [15]

Thus point multiplication uses point addition and point doubling repeatedly to find the result. The above methods is called double and add method for point multiplication. There are other efficient methods for point multiplication such as NAF (Non – Adjacent Form) [15].

NAF Method

Another method for scalar multiplication was proposed by Booth, called signed binary method. The property of this representation is that, of any two consecutive digits, at most one is non-zero. Before discussing this method we first discuss about nonadjacent form (NAF) that is the basis of this method [16]. An improved method for computing kP can be obtained from the following facts:

Every integer *k* has a unique representation of the Form

$$k = \sum_{j=0}^{l-1} k_j 2^j,$$

Where each kj € {-1, 0, 1}such that no two consecutive digit are nonzero [8][16].

Algorithm 1: Standard Method for computing NAF of an integer

Input: Positive integer *k*
Output: NAF (*k*)

1. i □ 0
2. While $k \geq 1$ do
2.1 If *k* is odd then: *k*i □ 2 - (*k* mod 4),

k □ *k* - *k*i
2.2 Else: *k*i □ 0
2.3 *k* □ *k*/2, i□ i +1
3. Return (*k*i-1, *k*i-2,….., *k*1, *k*0). [16]

Algorithm 2: NAF Method for Point Multiplication

Input: NAF of a Positive integer *k* and P
Output: kP

1. R □ P
2. For i= n −2 to 0 do
2.1 R□ □ 2R
2.2 if ki = 1 then R □ R+P
2.3 if ki = −1 then R □ R-P
2.4 i □ i −1
3. Return R. [16]

Block Method for computing NAF

Procedure for converting the scalar k into signed binary representation is as follows:

a) The first step is to partition the input into blocks of binary of equal size.
b) If there is an odd block at the end, sufficient padding bit will be appended to the left of this block to make all blocks equal in size.
c) Then get the index for each block of binary to extract the NAF value for each block from look up table.
d) Perform the combine part for the blocks to get Final result in NAF

In the Block method, look up table is used to store NAF values for the blocks. Block size used r=8bits and NAF values are stored using 9bytes.Look up table contains 256 values of NAF for the present case with 8bits block size as 2^8=256. [16]

Algorithm 3:Block method for computing NAF of an Integer [16]
Input: A positive Integer k
Output: NAF (k)
Step1:

1.1 Define input size to be m bits

1.2 Divide the input into n blocks of binary with each block having equal that is r bit size

n=m/r

1.2 Choose the least significant (rightmost) block as lower block and all other blocks towards left are upper blocks.

Step2:

Obtain NAF for each block from look up table

Step3:

3.1 Do the combine of blocks that already in NAF starting from right to left.
3.2 Perform the boundary addition with MSB of lower block and LSB of upper block.
3.3 Get the final combine result in NAF
Step 4:
Return (km, km-1,….., k1,k0)NAF
Point multiplication operation for Block method can be performed with algorithm 2. [16]

NAF Value	
0	000000000
1	000000001
2	000000010
3	00000010-1
4	000000100
5	000000101
6	0000010-10
7	00000100-1
8	000001000
.	
.	
148	010010100
149	010010101
150	01010-10-10
151	01010-100-1
.	
.	
255	10000000-1

Look up Table containing NAF values

Example : Let k=6211
The binary representation of 6211 is (1100001000011)2
There are two blocks of 8bits as
Block 1=01000011
Block 2=00011000
Above blocks after making to NAF are
Block 1=0100010-1
Block 2=0010-1000
Now combining the blocks:
0010-1000
0100010-1
= 0010-10000100010-1
$=2^{13}+2^{11} * -1+2^{6}+2^{2}+1*^{-1}$
=8192-2048+64+4-1
=6211

COMPARISON GRAPHS OF ECC Methods (Standard NAF and Block Method) In Wired Equivalent Privacy (WEP).

1. (1.1) Comparison graph between ECC Block/lookup Method and Standard NAF Method in WEP at key size of 128 bit by taking (**End to End delay)** parameter**:**
End-to-end delay refers to the time taken for a packet to be transmitted across a network from source to destination.

As the less is the end to end delay the better is the performance. So at key size of 128 bit clearly the Block Method of ECC gives the better performance than Standard NAF method of ECC in WEP.

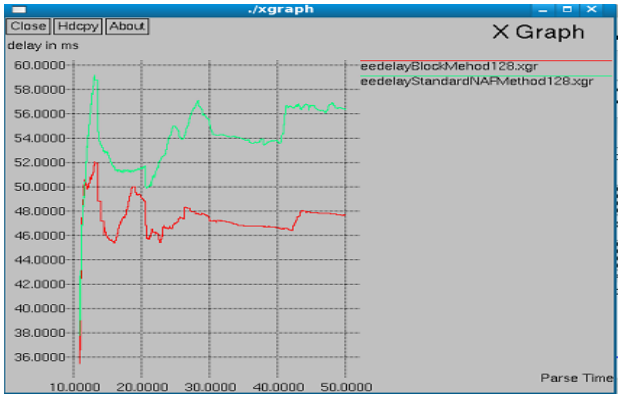

Figure 1.1

(1.2) The below graph is at key size of 256 bit by taking end to end delay parameter**:**

As the less is the end to end delay the better is the performance. So at key size of 256 bit clearly the Block Method of ECC gives the better performance than Standard NAF method of ECC.

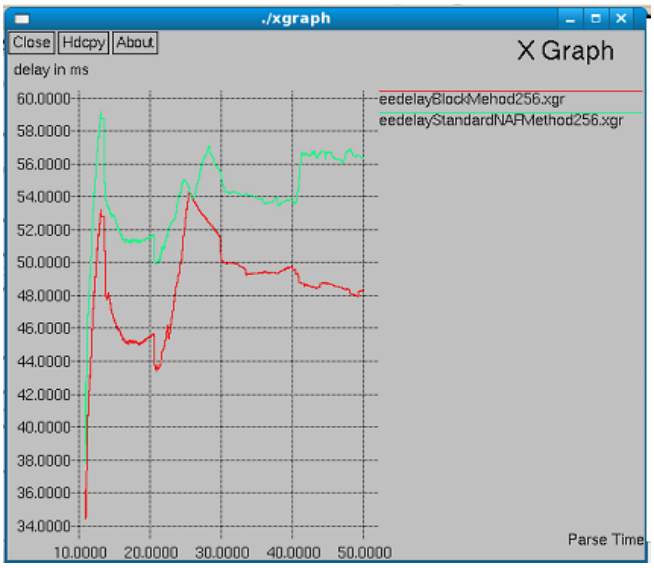

Figure 1.2

2. (2.1) Comparison graph between ECC Block/lookup Method and Standard NAF Method in WEP at key size of 128 bit by taking (**Packet Delivery fraction**) parameter**:**

Packet Delivery Fraction (PDF): It represents the ratio of the data packets received at destination and the delivered packets.

As the more is the packet delivery fraction the better is the performance. So at key size of 128 bit clearly the Block Method of ECC gives the better performance than Standard NAF method of ECC in WEP.

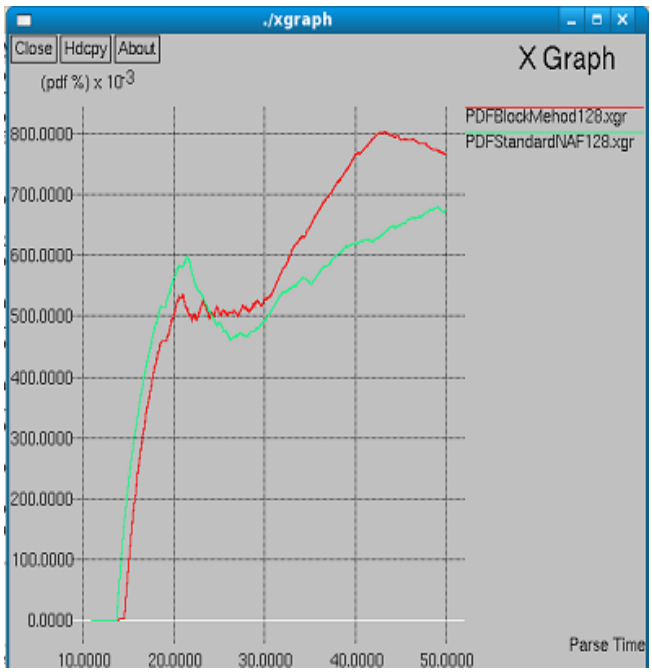

Figure2.1

(2.2) As the more is the packet delivery fraction the better is the performance. So at key size of 256 bit clearly the Block Method of ECC gives the better performance than Standard NAF method of ECC in Wired Equivalent Privacy (WEP).

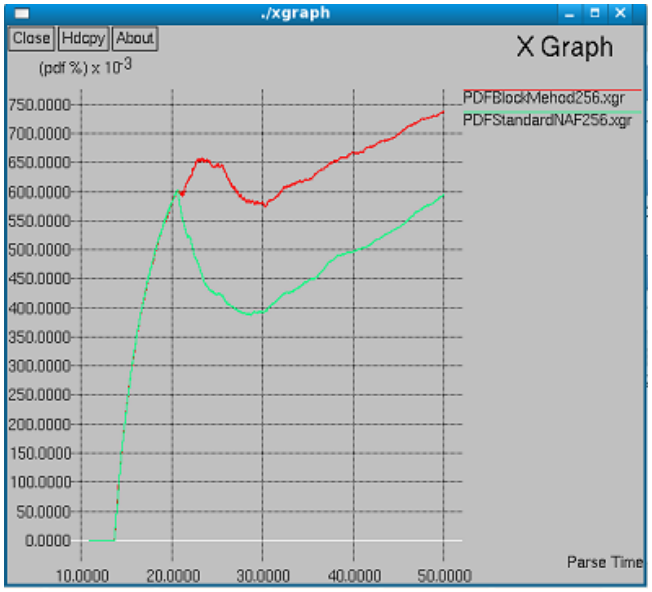

Figure 2.2

As the more is the packet delivery fraction the better is the performance. So at key size of 256 bit clearly the Block Method of ECC gives the better performance than Standard NAF method of ECC in Wired Equivalent Privacy (WEP).

3. (3.1) Comparison graph between ECC Block Method and Standard NAF Method in WEP at key size of 128 bit by taking (**Throughput)** parameter**:**

Throughput: refers to average rate of successful message delivery over a communication channel.

As the more is the throughput the better is the performance. So at key size of 128 bit clearly the Block Method of ECC gives the better performance than Standard NAF method of ECC in (WEP).

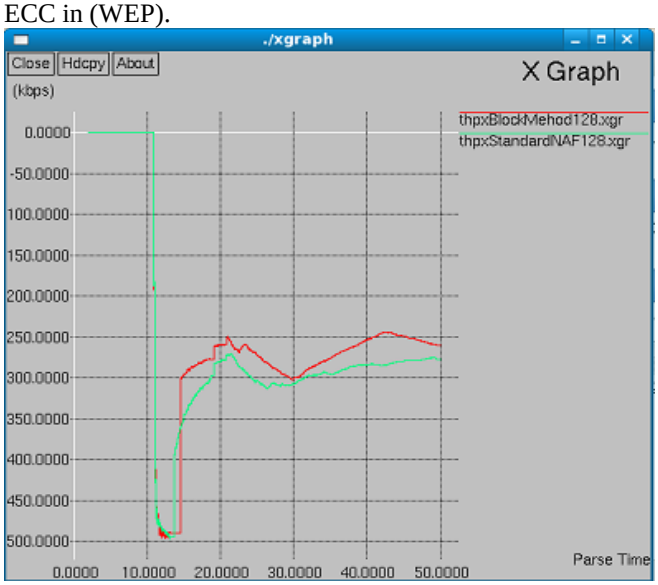

Figure 3.1

(3.2) As the more is the throughput the better is the performance. So at key size of 256 bit clearly the Block Method of ECC gives the better performance than Standard NAF method of ECC in Wired Equivalent Privacy (WEP).

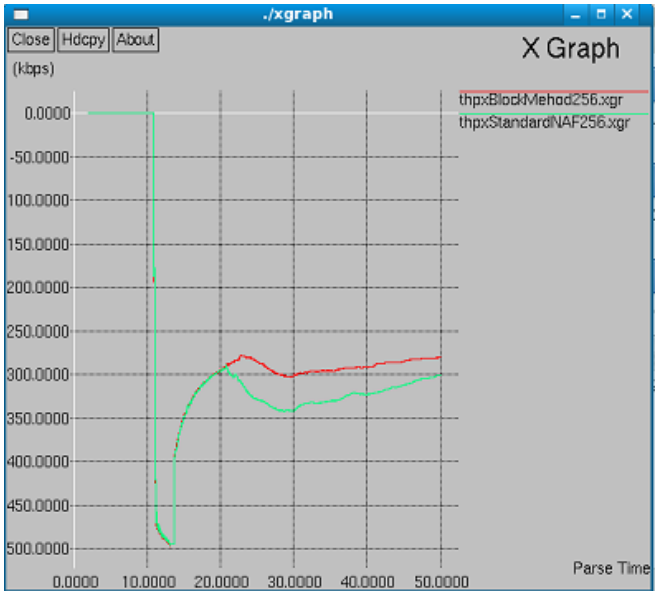

Figure 3.2

V. CONCLUSION

So when we replaced the RC4 Algorithm with the ECC Algorithm in WEP the keys generated by ECC methods are more secure because we test it by implementing the Dictionary Attack (to hack the keys generated by ECC method). The Dictionary attack is unable to hack the keys because Public-key algorithms have the property that different keys are used for encryption and decryption and that the decryption key cannot be derived from the encryption key and further when we implemented both Standard and Block method of ECC at the key sizes of 128 bit and 256 bit by taking the parameters End to End Delay, PDF and Throughput in WEP the Output which we analyzed is that as the Block method computes NAF faster than the Standard NAF hence it shows greater performance on all above mentioned three parameters than the Standard NAF in WEP. So from our research ECC provides more secure encryption in WEP and Block Method shows better performance on all parameters which we have successfully tested therefore use of ECC for encryption in WEP makes it more secure.

REFERENCES

1. ARASH HABIBI LASHKARI, MIR MOHAMMAD SEYED DANESH, "A Survey on Wireless Security protocols (WEP, WPAWPA2/802.11i)", IEEE 2009 .
2. Rajni Pamnani, Pramila Chawan , "Building a secured wireless LAN", International Journal of Recent Trends in Engineering, Vol 2, No. 4, November 2009.
3. Peisong Ye and Guangxue Yue, "Security Research on WEP of WLAN", Proceedings of the Second International Symposium on Networking and Network Security (ISNNS '10) Jinggangshan, P. R. China, 2-4, April. 2010.
4. Emilio J.M. Arruda Filho, Paulo N. L. Fonseca Jr Mairio J. S. Leitdo and Paulo S. F. de Barros , "Security versus Bandwidth: The Support of Mechanisms WEP e WPA in 802.11g Network" , IEEE 2007.
5. Vincent Guyot ,"Using WEP in Ad-Hoc Networks", IEEE 2007.
6. Shadi R. Masadeh and Nidal Turab, "A Formal Evaluation of the Security Schemes for Wireless Networks", Research Journal of Applied Sciences, engineering and Technology 3(9): 910-913, September 2011.
7. C. SAJEEV and G. JAI ARUL JOSE , "Elliptic Curve Cryptography Enabled Security for Wireless Communication , International Journal on Computer Science and Engineering Vol. 02, No. 06, 2010.
8. Md. Rafiqul Islam, Md. Sajjadul Hasan, Ikhtear Sharif and Muhammad Asaduzzaman, "A New Point Multiplication Method for Elliptic Curve Cryptography Using Modified Base Representation" International Journal of The Computer, the Internet and Management Vol.16. N.o.2 (May-August, 2008).
9. Olufade, F. W. Onifade, Adenike, O. Osofisan and Chukwuzitere, U. OBODO, "A Dual Layered Encryption Algorithm For WIreless Equivalent Privacy (WEP) Algorithm", IJCSNS, VOL.8 No.5, May 2008.
10. Allam Mousa and Ahmad Hamad ,"Evaluation of the RC4 Algorithm for Data Encryption", International journal of computer and Application,Vol 3, No 2, June 2006.
11. Lazar Stosic, Milena Bogdanovic," RC4 stream cipher and possible attacks on WEP, (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 3, No. 3, 2012.
12. Vinay Bhatia, Dushyant Gupta AND SINHA H.P, "Analysis OF Dictionary Attack On Wireless LAN FOR Different Nodes" , Journal of Information Systems and Communication ,ISSN: 0976-8742 & E-ISSN: 0976-8750, Volume 3, Issue 1, 2012.
13. Vinay Bhatia, Dushyant Gupta AND SINHA H.P. "Throughput and Vulnerability Analysis of an IEEE 802.11b Wireless LAN", IJCA (0975 – 8887) Volume 52– No.3, August 2012.
14. Marisa W. Paryasto, Kuspriyanto, Sarwono Sutikno and Arif Sasongko , "Issues in Elliptic Curve Cryptography Implementation", Internetworking Indonesia Journal , Vol 1 / No 1 2009.
15. Elliptic Curve Cryptography – An Implementation Tutorial by Anoop MS.