5. Conclusions:

In this paper we have proposed a new method suitable for securing plaintext message in resource constrained Ad Hoc environments such as MANET and WSN. In this method we have used Elliptic curve analog of Massey Omura method for encryption and decryption of plaintext. The plaintext message is mapped over the points of Elliptic curve by using non-singular square matrix multiplication. In our method regularity in resultant ciphertext is avoided due to non-singular matrix multiplication. It hides the frequency pattern in the plaintext and it becomes very difficult for an attacker to launch letter frequency count attack. This makes the decryption process difficult for the attacker and hence enhancing the security of our cryptographic method. It can be concluded that our method is simple, fast and efficient and guarantees the security of messages in resource constrained environment.

References:

[1] Alfred J. Menezes; Paul C. van Oorschot and Scott A. Vanstone (1996). Handbook of Applied Cryptography, CRC Press.

[2] Arita S. (2000), Weil descent of elliptic curves over finite fields of characteristic three, Advances in Cryptology-Asiacrypt 2000, Lecture Notes in Computer Science, Vol.1976, Springer-Verlag, 248-259.

[3] Certicom (2000). Standards for Efficient Cryptography, SEC 2: Recommended Elliptic Curve Domain Parameters, Version 1.0, September, Available at http://www.secg.org/download/aid-386/sec2_final.pdf

[4] Katz Jonathan; YehudaLindel, (2014). Introduction to Modern Cryptography, Second Edition, November 6, by Chapman and Hall/CRC ISBN 9781466570269.

[5] King Brian (2009). Mapping an Arbitrary Message to an Elliptic Curve when Defined over GF(2n), International Journal of Network Security, Vol.8, No.2, pp.169-176.

[6] Koblitz N. (1987). Elliptic Curve Cryptosystems, "Mathematics of Computation, Vol. 48, No. 177, pp. 203-209.

[7] Levent Ertauland; Nitu J. Chavan (2007). Elliptic Curve Cryptography based Threshold Cryptography (ECC-TC) Implementation for MANETs. IJCSNS International Journal of Computer Science and Network Security, VOL.7 No.4, April.

[8] Lange H. and W. Ruppert (1987). Addition laws on elliptic curves in arbitrary characteristics, Journal of Algebra, Vol.107(1), pp.106-116.

[9] Bhatia Rajendra (1997), Matrix Analysis, Graduate text in Mathematics, Springer.

[10] Miller.V. S. (1986). Use of Elliptic Curves in Cryptography, Advances in Cryptology CRYPTO85, pp. 417-426.

[11] Stinson Douglas R. (2005). Cryptography: Theory and Practice, Third Edition, Chapman and Hall/CRC ISBN 9781584885085

[12] Singh L. Dolendro; K. Manglem Singh (2015). Implementation of Text Encryption using Elliptic curve cryptography. Science Direct, Eleventh International Multi Conference on Information Processing-2015(IMCIP-2015).