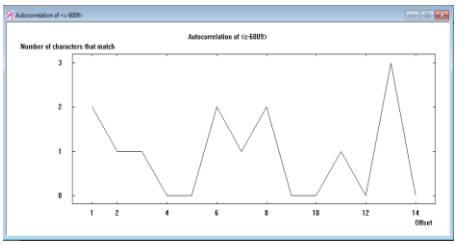

Figure 6.8 Analysis of autocorrelation of RSA technique

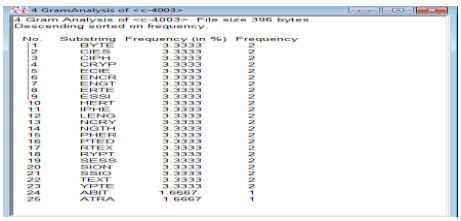

Figure 6.9 Analysis of N-gram of proposed ECC technique

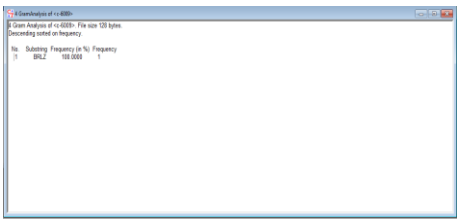

Figure 6.10 Analysis of N-gram of RSA technique

The implementation results show that, the proposed cryptosystem has acquired somehow or apart better results from any existing cryptosystem, the proposed cryptosystem destroys any existing patterns in the input and also it, maximizes entropy. The n-grams, autocorrelation, histograms and floating frequency shows that the proposed cryptosystem is secure against RSA method of the cipher text.

7. CONCLUSION & FUTURE SCOPE

Although the ECC is not evaluated completely, the Proposed technique is very simple and easy to implement. The test results also show that the performance and security provided by the Proposed technique is somehow or apart good and comparable to standard technique. The security provided by the Proposed technique is comparable with other techniques.

The future scope of this proposed technique may be done using Choas technique. In future, some other ECC based approach can be used to generate the session key.

ACKNOWLEDGMENT

The authors are gratefully acknowledged to the ICAST 2017 (International Conference on Advances in Science & Technology) and MCKV Institute of Engineering on Computer Science & Engineering department to give the opportunity of publishing the paper work.

REFERENCES

[1] Khate A. Cryptography and network security, Tata MC Graw.

[2] Anna M.J., Peter S.G. (2002). Authentication key exchange provably secure against the man-in-middle attack, *Journal of Cryptology*, Vol. 2002, No. 2, pp. 139-148.

[3] Antoines J. (2004). Aone round protocol for tripartite Diffie-Hellman, *Journal of Cryptology*, Vol. 17, No. 4, pp. 263-276.

[4] Srjen A., Lenstra K., Verheul E.R. (2001). Selecting cryptographic key size, *Journal of Cryptology*, Vol. 14, No. 4, pp. 255-293.

[5] Chandrasekhar A., et.al. (2007). Some algebraic curves in public key cryptosystems, *International Journal of Ultra Scientists and Physical Sciences*.

[6] Gura N., Shantz S., Eberle H., et al. (2002). An end-to-end systems approach to elliptic curve cryptography, Sun Microsystems Laboratories, from http:// research.sun.com / projects/crypto accessed on 10 May.

[7] Darrel H., Alfred M., Scott V. (2004). A guide to elliptic curve cryptography, Springer.

[8] Rosing M. (1999). Implementation ECC Greenwich, CT: Manning Publications.

[9] Suneetha C., Sravana K.D., Chandrasekhar A. (2011). Secure key transport in symmetric cryptographic protocols using Elliptic curves over finite fields, *International Journal of Computer Applications*, Vol. 36, No. 1.

[10] Chandrasekhar P.K.R., Sebastian M.P. (2010). Elliptic curve based authenticated session key establishment protocol for high security applications in constrained network environment international, *Journal of Network Security & Its Application (IJNSA)*, Vol. 2, No. 3.

[11] Kin C.Y., Amol D.A. (2010). Light-weight mutual authentication and key-exchange protocol based of Elliptic Curve cryptography for energy-constrained devices, *International Journal of Network Security & its Applications*, Vol. 2, No. 2.

[12] Mohsen M., et.al. (2010). Coupled FPGA/ASIC implementation of elliptic curve crypto-processor, *International Journal of Network Security & Its Applications*, Vol. 2, No. 2.

[13] http://ijctonline.com/ojs/index.php/ijct/article/view/426.pdf

[14] Singh A., Gilhorta R. (2011). Data security using private key encryption system based on arithmetic coding, *International Journal of Network Security and Its a (IJNSA)*, Vol. 3, No. 3.

[15] Sravana K.D., Suneetha C.H., Chandrasekhar A. (2012). Encryption of data using elliptic curve over finite field, *IJDSP*, Vol. 3, No. 1.

[16] Padma B.H., Chandravathi D., Prapoorna R.P. (2010). Encoding and decoding of a message int the implementation of elliptic curve cryptography using Koblitz's method, *IJCSE*, Vol. 2, No. 5.

[17] Rajeev S., Geetha G. (2012). Cryptographic hash functions: a review international, *Journal of Computer Science Issues*, Vol. 9, No. 2.