section "**INTEGRATION OF CLASSICAL CRYPTIC KEY AND QUANTUM KEY DISTRIBUTION".** The successful communication results in receiving the file sent by the sender as shown in fig. 5.

Fig. 5: Receiver on successful receiving of message

As seen in fig. 5, the message sent by the sender is shown in the text area. This is the result of successful communication among participants and also TC.

5. RESULTS AND DISCUSSIONS

Comparison	**Proposed Quantum key and classical**	**Quantum key Model**	**Classical key Model**
Pre-shared Secret key	Longer Duration	Sampling Pair	Longer Duration
		Instances	
Communication Round	2	5	3
Quantum Channel	Yes	Yes	No
Clock Synchronization	No	No	No
Vulnerable to Passive Attack	No	No	No
Security Proff	Yes	No	No

Table1: Comparison of proposed QKDP and classical to individualized classical and quantum key models

Queries are used to demonstrate the capabilities of adversaries. Thus it demonstrates the attack possibilities made by attackers. The guessing attacks can't be eliminated in existing key distribution protocols. The proposed system is capable of providing secure communication among three parties and also reduce communication cycles when compare with other three party models. Table 1 shows the comparison results.

The results revealed that the proposed QKDP is able to prevent replay attacks, passive attacks and man in the middle attacks. It also eliminates challenge – response paradigm. The communication rounds are reduced. The secret key is pre-shared between TC and participants and random keys are generated and changes in every second thus making it impossible to break the security as it is based on quantum mechanics. This is achieved by combining traditional cryptography and QKD mechanisms.

6. CONCLUSION

In this paper a QKD model is used that involves three parties and the technologies combination with quantum key cryptography and classical cryptography. The proposed model when compared with other such systems is more effective in resisting passive attacks and replay attacks. The proposed design expects to manage keys over a dedicated global network containing key stores linked with classical channels. QKD is the underlying mechanism for key distribution. The proposed system has less number of rounds in communication and thus provides computationally efficient security mechanism. The quantum channel seems to be costly as of now and may not be that costly in future. By combining the quantum key cryptography and also the traditional cryptography the proposed QKDP provides complete security for conversations in a large network.

7. REFERENCES

[1] D. Gottesman and H.-K. Lo, "Proof of Security of Quantum Key Distribution with Two-Way Classical Communications," IEEE Trans. Information Theory, vol. 49, p. 457, 2003.

[2] H.A. Wen, T.F. Lee, and T. Hwang, "A Provably Secure Three-Party Password-Based Authenticated Key Exchange Protocol Using Weil Pairing," IEE Proc. Comm., vol. 152, no. 2, pp. 138-143, 2005.

[3] J. Nam, S. Cho, S. Kim, and D. Won,"Simple and Efficient Group Key Agreement Based on Factoring," Proc. Int'l Conf.Computational Science and Its Applications (ICCSA '04), pp. 45-654, 2004.

[4] B. Neuman and T. Ts'o, "Kerberos: An Authentication Service for Computer Networks," IEEE Comm., vol. 32, no. 9, pp. 33-38, 1994.

[5] W. Stallings, Cryptography and Network Security: Principles and Practice 3/e. Prentice Hall, 2003.

[6] K.-Y. Lam and D. Gollmann, "Freshness Assurance of Authentication Protocols," Proc. European Symp. Research in Computer Security (ESORICS '92), pp. 261-271, 1992.

[7] R. Shirey, Internet Security Glossary, IETF RFC 2828, May 2000.

[8] C.H. Bennett and G. Brassard, "Quantum Cryptography: Public Key Distribution and Coin Tossing," Proc. IEEE Int'l Conf. Computers,Systems, and Signal Processing, pp. 175-179, 1984.

[9] C.H. Bennett, "Quantum Cryptography Using any Two Nonorthogonal States," Physical Rev. Letters, vol. 68, no. 3121, 1992.

[10] A.K. Ekert, "Quantum Cryptography Based on Bell's Theorem," Physical Rev Letters, vol.67, no. 661, 1991.