Real time Crytography

B . Lakshmi

Abstract - It has been observed from literature, a method of encryption that enhances the security of vital data against Brute force attack . The method is based on dual key encryption in which two different keys encrypt with data simultaneously , one being the regular key and the other being the time of key entry. The encryption process uses conventional encryption methods with some modifications to increase the security but the decryption process is accomplished by checking both the validity of the key and the relative times the keys are entered into the system .This overcomes the fact that the brute force attacks fully depends on the speed of the system used for cryptanalysis as the time interval between two successive key entries also consumes time . Also this paper proposes chemes for dynamically selecting the number of rounds each data set has to get encrypted and this increases the complexity of the cryptanalysis. The system requires the decryption has to be done on a single system and decryption via network require some significant effort . The implementation is done in C language and cryptanalysis is performed to check the level of protection .