Chapter 7

Conclusion and Future Work

7.1 Conclusion

The data security is an important and challenging task for the users. Since the inception of the cipher system, new algorithms are developed for data confidentiality and integrity. The important aspect of any cryptosystem is its simplicity, memory requirement, time of execution and strength against the attacks. In block ciphers the substitution box plays an important role in providing the strength against any attack. In AES algorithm static S-box is used and its construction is based on the Affine transformation. Construction of key dependent dynamic S-box using the Affine transformation is a big challenge and successfully implemented the same in the thesis. Different S-boxes are generated by using different keys and tested. The Avalanche property of each S-box has been tested. Classification of S-boxes giving maximum Avalanche criteria, based on the irreducible polynomials are achieved.
The key dependent dynamic S-box has been used to construct New AES algorithm, New Stream cipher and New hash function algorithm. In all these implementations it is found that the memory requirement and time of execution are almost same as that of original algorithms. All these new algorithms make cryptanalysis much more difficult.

7.2 Future Work

The future work on the dynamic S-box is to test for the Strict Avalanche Criteria, i.e. to test for the S-boxes that give all the difference vector value of 128. As though algebraic attacks are difficult and Brute-force attack requires more time, some more investigations are required against other possible attacks if any.