CHAPTER 5

CONCLUSION AND RECOMMENDATION

5.1 Conclusion:

The RC4 stream cipher is an important encryption algorithm that can be used to protect the information on the common channel as its implementation is simpler and its cryptographic function is faster than Different algorithms like DES .

The simplicity and speed of operation of RC4 make it one of the most widely used stream cipher in most software and hardware. But there are many weakness in RC4 algorithm so that are many research done to enhanced security issues of algorithm.

In this research we enhanced RC4 algorithm by using two state table to improve the security of algorithm.

The result of enhanced algorithm is analyzed using MATLAB by calculate the MSE and PSNR value. also we use the crypTool and diehard testing tool to test the result randomness .

The experimental results show that the new algorithm is given good result compared to the standard RC4.

5.2 Recommendation:

In future research the enhancement of RC4 algorithm can be done in key generation process. also recommended to use compression with cryptography.

There are many classical encryption algorithm that can make combination between classical and modern algorithms.

The increase the security of the hardware that is used RC4 algorithm is one of recommended solution.