ABSTRACT

This dissertation addresses the issues pertaining to the development of a modified Advanced Encryption Standard (AES) algorithm for a block cipher. The present AES algorithm uses a static S-box and Brute-force attack that needs to evaluate only $2^{128}$ keys. The one more threat facing by AES algorithm is the Extended Sparse Linearization attack, which is based on the framing a number of algebraic equations between the input and the output values of each stage/block. Since the S-box is static now, breaking of the algorithm may be possible in future. But in the modified AES algorithm the S-box is a dynamic one and is also a key dependent one. Since $2^{1648}$ AES S-boxes are possible XSL attack becomes very difficult. More over an AES box also contains MIX COLUMN operation which is again static now. This MIX COLUMN is modified as a dynamic one such that there are a large number of possible combinations for the MIX COLUMN matrix and has been made again a key dependent. By introducing these operations no extra memory is needed and the time required is negligible.

While generating dynamic S-box it is found that some of the S-boxes giving maximum Avalanche Criteria. This important characteristic of S-boxes has also been addressed in detail.

Using the dynamic S-box generation principle, a new key dependent stream cipher has been designed. This new stream cipher passes all the tests given by National Institute of Standards and Technology (NIST). The new stream cipher algorithm and the test results are also detailed.

One more important aspect of the computer security is the Integrity of the data. In this dissertation the new HASH function generation based on the dynamic S-box have been discussed and the results have been found satisfactory.