**VLSI IMPLEMENTATION OF AES ALGORITHM**

**ABSTRACT**

The main aim of this work is to implement Advanced Encryption Standard (AES) Encryption using Verilog. To protect data, like electronics, cryptographic algorithms are used. Each round of encryption associated with delay can be reduced by AES's parallel design. This work proposes a low power and high throughput implementation of AES algorithm using key expansion approach. This minimizes the power consumption and critical path delay using the proposed high-performance architecture. The fundamental goal of the initiative is to increase data flow, although security considerations have become increasingly important over time. The use of encryption and decryption techniques inside VLSI has recently increased since cryptography can convert plaintext to cipher and vice versa. The most recent developments in cryptography technology will be applied to the hardware security module. by simultaneously writing a lot of HDL modules. The main objective is to send and receive data securely without allowing it to be hacked, as well as to improve the performance of a specific parameter. It is interesting to note that any encryption algorithm works in a digital environment, and all the blocks in the system will handle digital data with security. Certain modulations are made in the algorithm of AES 256, and it is compared with all the other encryption algorithms to give the desired advanced encryption algorithm as an output of this project.

The main goal of this work is to implement Advanced Encryption Standard (AES) encryption using Verilog. To protect data, such as electronic devices, cryptographic algorithms are used. Each encryption cycle associated with latency can be minimized by the AES parallel design. This work proposes to implement a low-power, high-throughput AES algorithm using the key expansion method. This minimizes power consumption and critical path latency using the recommended high-performance architecture. The primary goal of the initiative is to increase data flow, although security considerations have become increasingly important over time. The use of encryption and decryption techniques inside VLSI has recently increased since cryptography can convert plaintext to cipher and vice versa. The latest developments in cryptographic technology will be applied in the hardware security module. by simultaneously recording a large number of HDL modules. The main purpose is to send and receive data securely without allowing data to be hacked, as well as to improve the performance of a particular parameter. Interestingly, any cryptographic algorithm works in a digital environment, and all blocks in the system handle digital data securely. Some adjustments are made in the AES 256 algorithm and it is compared with all other encryption algorithms to come up with the desired advanced encryption algorithm as the output of this project.