Name: Harshvardhan Soni
Enrollment No: 92200133028
Department of Information and Communication Technology
Subject: Capstone Project – 01CT0715

Project Title: Implementation of RSA Cryptographic Algorithm on Nexys-04

Component: System Design and Architecture

Course: ICT Engineering Capstone

Academic Year: 2025-2026

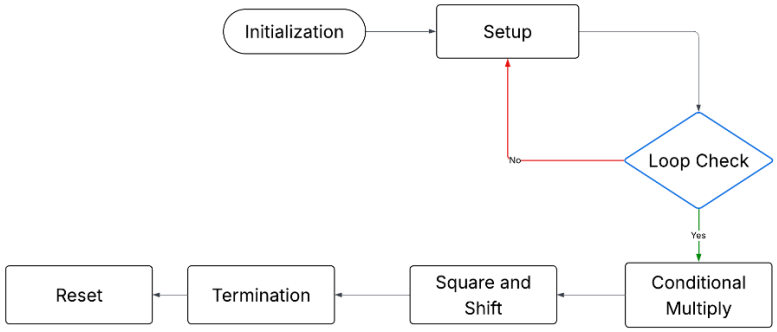
Department: Information and Communication Technology

❖ Introduction:

Hardware acceleration for modular exponentiation is shown through an 8-digit seven-segment display visualization. The message (M) originates from a pre-programmed Wi-Fi key, goes through two specialized RSA Core components, and the plain text, cipher text, and decrypted message are shown. This design focuses on breaking things into smaller parts that can be changed easily, making it fast and safe for use in devices needed for protecting secrets. This project implements the core operations of the RSA Cryptography algorithm (Encryption M^e (mod n) and Decryption C^d (mod n) using Verilog HDL on a Field-Programmable Gate Array (FPGA).

❖ Modular Design:

The system uses separate Verilog modules for distinct tasks. This design improves ease of upkeep and reuse, especially for crucial encryption parts. The highest. A module acts as the main controller, linking the data origin, processing components, and result presentation system.



❖ Technology Stack:

Hardware Description Languages (HDLs) and FPGA tools form the specialized technology stack that supports the project's needs of high performance, customization, and direct access to hardware resources.

Component	Technology
Hardware Platform	Xilinx Artix-7 FPGA (Implied by Nexys-4 DDR)
Design Language (RTL)	
Core Algorithm	Square-and-Multiply Modular Exponentiation
Input Generation	Python Script (gen_wifi_keyrom.py)
Synthesis Tools	Xilinx Vivado Suite (Implied)

❖ Scalability Plan:

The current system uses a small 17-bit key size (WIDTH=17) for demonstration. To meet real-world cryptographic requirements (e.g., 2048-bit keys), the system requires scaling the core design and addressing the resulting performance bottlenecks.

- Key Size
- Throughput (Performance)
- Resource Efficiency
- Algorithm Security

❖ Conclusion:

By using the rsa_core.v module and its rectangular-and-multiply approach, the device handles encryption and decryption as a synchronized process managed by top.v. Using Verilog HDL and the FPGA platform, this setup provides a base for creating high-performance, custom cryptographic functions. The scalability plan focuses on moving to standard key sizes by focusing on digit-serial math and pipelining, which shows the design is suitable for real-world applications in low-latency embedded security and edge computing.