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: Innovation and Originality

Course: ICT Engineering Capstone

Academic Year: 2025-26

Department: Information and Communication Technology

❖ Introduction:

The RSA Algorithm on FPGA project tackles a major issue in today's cybersecurity and embedded systems: the need for fast and secure encryption in devices with limited resources. Even though RSA is a key part of public-key encryption, it uses a complex math operation called modular exponentiation, which is slow and hard for software to handle, especially on low-power devices like IoT and edge systems. This project doesn't introduce a new encryption method, but it offers a fresh way to combine hardware and software to speed up and protect the RSA process, making it practical for real-life use.

❖ Novel Approach:

The project uses a special method by building a full system that combines software on the device side with a hardware part made on an FPGA. This way makes the process smooth and focuses on a real-world example keeping a Wi-Fi password safe.

Some key aspects of novel are:

- An integrated approach that combines software and hardware works like this: a Python script called gen_wifi_keyrom.py is used to get a real message (M) from a computer's Wi-Fi settings. Then, it automatically creates a hardware file named wifi_key_rom.v. This method connects the process of collecting data through software with the actual use of physical hardware, showing how this can be done in a real-world situation.
- Application-Specific Hardware Acceleration: This is a custom-designed, optimized hardware circuit specifically tailored for the sequential pipeline of RSA encryption followed by decryption. This application-specific focus allows for fine-tuning of the Square-and-Multiply algorithm in a way that is not possible in general-purpose processors, leading to predictable, low-latency performance

- The rsa_core.v module is built with a configurable WIDTH parameter. This makes the main cryptographic part easy to use again and adjust for different key sizes, like the small 17-bit key used in examples, all the way up to bigger, standard 2048-bit keys, without needing a full redesign.

❖ Comparison with Existing Solution:

Feature	Software	Hardware	FPGA-Based Solution (This Project)
Performance	High latency due to sequential CPU execution.	Very High. Optimized for a single task.	High. Significantly faster than software, with parallel processing capabilities.
Flexibility	Very High. Easily updated and reconfigured.	None. Fixed function.	High. Can be reconfigured to change algorithms, key sizes.
Cost	Low. Runs on existing hardware.	Very High. Requires custom silicon design and manufacturing.	Medium. Higher than software but significantly lower than an ASIC for prototyping and small-scale production.
Security	Low. Prone to side-channel attacks and malware-based key extraction.	High. Designed with physical security in mind.	High. The hardware-level design provides natural resistance to software-based attacks.

❖ Contribution in ICT Field

This project contribution is a practical demonstration of how hardware acceleration can solve the inherent security and performance challenges of the ICT domain's rapidly expanding Edge Computing and IoT ecosystems.

Advancing Cybersecurity: This project handles the growing need for stronger security in IoT devices. By using RSA in hardware, it builds a Hardware Root of Trust, which helps ensure secure booting and authenticating firmware. It shows that complex public-key algorithms can be safely used in hardware, making them more secure against typical software attacks. It also sets the stage for future work on hardware that can resist side-channel attacks.

Enabling New Use Cases: The fast and low-latency performance of this solution supports applications that need real-time encryption. This could be used in secure communication between vehicles, where quick responses are key for safety, or in low-power sensors that need

to encrypt data before sending it to the cloud. The project offers a clear way for developers to add strong encryption without slowing things down or using too much power.

Bridging Research and Application: This project connects the idea of hardware-based cryptography with a real-world issue Wi-Fi password security. It acts as a useful tool for learning and experimenting with various encryption methods, exploring hardware security, and testing how well cryptographic designs work on actual devices. This helps both researchers and industry professionals gain more knowledge and practical experience.