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: Project Definition and Scope

Course: Capstone Project – 01CT0715

Academic Year: 2025-26

Department: Information and Communication Technology

Date: 25-09-25

❖ Introduction:

In today's world, where spoofing and databases are the common problems in cyber security, we have to ensure that the communication is done securely. Software encryption can be flexible, but if we implement hardware-based cryptography, it offers speed, tamper resistance, and protection against physical attacks. It's like locking your secret in your wallet instead of in a drawer. It can be said that we can lock our secret in our pocket rather than in an open publication, so for that, we have to implement RSA, which is the most trusted public encryption method, which is perfect for real-time security. Fanaa, we have use in a Wi-Fi password, which is right now weak, using outdated protocols and poor configuration, which can be tracked and which can be decrypted easily. The attackers or the hackers can exploit the gap and use this project to crack it for unauthorized access, while the solution boosts security and integration and is wide and can be used for development also.

❖ Problem Statement:

So if we use the software based RSA implementation it can be site channel attack and like Power analysis and timing attack and the private keys are also leak easily also let the physical security and the speed needed to protect and secure Wi-Fi password exchange is in the real time so the difference between Software and hardware is that software offers puffer's flexibility but it can also be vulnerable and the physical observation is that based on a text hardware RSA specially and Key provide better isolation it also faster and it is not easy to temper which making it for ideal for secure systems there is some limitations in software or essay that it is slow resource AVI and it has very constraint but for example 2 seconds in software while hardware and reduce this into micro second it's important for education of

Purpose can feel the gap between theory and practice and helping the students to grapes real world security challenge there is a clear need option of modular and educational tool which can be used as a hardware based description.

❖ Objectives:

The objective of two implement this project is the a symmetric RSA encryption decryption Algorithm which run in core very long HDL which is capable of processing 16 bit message is messages with configurable key sizes and achieving function verification we have developed this using automated Wi-Fi password extraction and system using python scripting and windows netsh commands right now it is having accuracy of 95% of password brazing and 64 bit data packaging of cryptography processing we have created a real time visualization demonstration also using eight 7 segment display on Nexus 4 DDR FPGA which display plain text cyphertext and decrypted result with user control switching and having the response type response time of less than 100 millisecond we can valid functionality through comprehensive testing including mathematical verification hardware implementation and achieving the 100% encryption decrease in accuracy for the well-defined bit constraint the project also support the architecture of key of 8 bit to 32 bit which having the analysis and performance making for research and application purpose.

❖ Relevance to ICT Domain:

It is relevant to the cyber security domain because hardware security modules represent the fastest-growing segment in cyber security, and the FPGA-based implementation that we have done in this project is the perfect solution for the modern mitigation and complaint requirements. The current FPGA market in cyber security applications is about 2.4 million dollars; by 2025, it will be used to accelerate encryption security and real-time cryptography processing with respect to digital logic design. This project is in line with Industry 4.2 requirements of demonstrating the practical implementation of digital design applications.

❖ Feasibility Analysis:

- **Technical Feasibility:**

  Nexys-4 DDR FPGA board featuring Xilinx Artix-7 XC7A100T FPGA with 15,850 logic slices, 4.9Mb RAM, and 240 DSP slices provides sufficient resources for RSA implementation with <5% utilization. Xilinx Vivado Design Suite 2025.1 WebPACK edition (free license) offers comprehensive RTL synthesis, simulation, and implementation tools specifically optimized for Artix-7 FPGA family with integrated debugging capabilities.

- **Economic Feasibility:**

  Nexys-4 DDR FPGA development board costs approximately $279 (educational pricing $199), representing one-time investment with multi-project reusability for entire academic program duration. All required software tools utilize free licenses including Xilinx Vivado WebPACK,

Python interpreter, and Windows built-in utilities, eliminating ongoing software costs and subscription fees. Estimated 80-100 hours of development time over 8-week period requires only student time investment. Maximum budget of $300 including hardware, miscellaneous components. Educational return on investment exceeds 1000% when considering reusable platform for multiple students, projects, and courses spanning digital design, cybersecurity, and embedded systems curricula.

- **Ethical Considerations:**
  Data Privacy Protection: Wi-Fi password extraction occurs entirely on local system without network transmission, external storage. All cryptographic implementations follow published standards and algorithms without introducing backdoors or vulnerabilities, maintaining educational integrity and promoting proper understanding of security principles.

❖ Market/User Needs Analysis:

For market analysis computer science and electrical engineering students have the hands on experience with hardware cryptography digital logic design and fpga development through practical visual and learning platform cyber security educator research and professional requires cost effective demonstration tools for teaching rsa algorithm hardware security concept it can also be used for side channel attacking mitigation technique for academic and training purpose in universities and college is they can implement this cyber security program for practical laboratory equipments with 78% of institution reporting need for affordable hardware security market is growing at the rate of 8.6 cagr with the help of IEEE security and privacy 2023 cyber security work for shortage exceeds to 3.5 millions professionals globally weekend have this types of rsa algorithm implementation demonstration kit and tools for education purpose and for training platform to use this to demonstrate people and students for practical purpose and exposure.

❖ Literature Review:

In the literature review there are some existing RSA FPGA implementation research papers, which I am uploading here as a drive link.

Link:

https://drive.google.com/drive/folders/178IzQctKePBLFUpsZYVyY21NED3PVU4t?usp=sharing

Also, talking about the Novelty section, it is a project innovation where my first implementation is combined with real-world Wi-Fi password extraction with an interactive FPGA-based RSA demonstration, which is used to bring practical system administration with hardware program education through real-time feedback for education improvements. Unlike existing research focusing on performance optimization, this project emphasizes the learning experience through visual display, which can have the intersection of control over the system. This is the cost-effective design approach that is used in standard FPGA boards and makes the

hardware cryptograph+y accessible for every individual student and faculty member because the current education landscape is dominated by expensive commercial platforms to use like these tools.

❖ Conclusion:

This project is critical which is used to bridge the gap between theoretical and practical knowledge education of cyber security implementation and providing accessible hands-on learning platform that demonstrate RSA algorithm execution in real time with actual password of Wi-Fi this is a complaint of technical achievement. define constraints economic evaluability for education deployment it is ethical to complaint for responsible security research and it is also applicable for future any multiplication.