Department of Electronics

EL-401 Final Year Design Project

Proposal for the Final Year Design Project

Title	**Implementing AES Encryption and Decryption on a RISC-V Processor**

Domain 1 **Embedded Systems**	Domain 2 **Network Security**	Domain 3 **Data Security**	Domain 4 **Processor Design**	Domain 5 **Cryptography**

1. Nature of Project

☒ New Project OR ☐ Extension of Existing Project	☐ Industrial Collaboration	☐ Funded
☒ Other Department Collaboration (If yes) Department Name: **Telecommunication**	☐ Other Academic Institution Collaboration (If yes) Institution Name_____	

2. Brief Outline

This project aims to develop a high-performance implementation of the Advanced Encryption Standard (AES) algorithm for encryption and decryption on the RISC-V architecture. The goal is to create a fast, efficient, and secure AES implementation on RISC-V architecture build on FPGA.

AES stands for Advanced Encryption Standard and is developed in 2001 before AES the (Data Encryption Standard) DES was used which is bit-Oriented and has a key size of 56 bits and include 16 round but comparing the security factor AES is far more secure the DES.The following Numbers shows the time taken to get the plain text from an encrypted text using Brutal Force Attack.

56 bit KEY DES Algorithm

Using 56 bit the total combination of key is

$$2^{56} \approx 72{,}000{,}000{,}000{,}000{,}000$$

Using a computer capable of 1 million key per second it will require approximately 60 days. **[1]**

128 bit KEY AES Algorithm

Using 128 bit the total combination of key is

2^{128}

Using a computer capable of 1 million key per second it will require approximately 1 Billion Year to generate all possible keys. **[2]**

192/256 bit KEY AES Algorithm

Using 192/256 bit the total combination of key is

2^{192} **or** 2^{256}

It will require almost an infinite time to access or generate all the possible keys. **[2]**

AES is far more secure then DES that's why its application and usage widely expanded across the sector where secure Data transmission is needed. Such as

- Wireless security
- Data Storage
- Secure Banking
- Industrial data security
- Communication Pathway
- Iot Devices data Transmission

As RISC-V adoption grows in various sectors, including IoT devices, embedded systems, and data centers, there's an increasing need for robust security solutions optimized for this architecture. While AES implementations exist for other architectures, there's a gap in highly optimized versions for RISC-V. This project addresses that gap by providing a tailored AES solution for RISC-V platforms.

Current AES implementations may not fully leverage the RISC-V architecture's capabilities, resulting in sub optimal performance for encryption and decryption operations. This can lead to increased power consumption, reduced throughput, and potential bottlenecks in data processing for RISC-V based system

3. Objectives

The project's main contribution is developing a fast AES algorithm implementation that processes data efficiently on RISC-V architecture. The main objectives of the Project are:

1. Design and implement a high-performance AES accelerator
2. Minimize clock cycles required for encryption and decryption
3. Reduce memory footprint and power consumption
4. Ensure Secure and Efficient data transmission in real world.

By achieving these goals, the project will provide a crucial security component for RISC-V based systems, enabling faster and more efficient data protection across a wide range of applications.

4. Scope

The project covers the implementation of AES on a RISC-V processor, including optimization for performance and security, testing in secure communication scenarios, and validation against common cryptographic attacks.

The whole FYDP session over the next 2 semesters will comprise of A functional AES encryption and decryption module on a RISC-V processor.Report on the implementation, testing, and performance of the project, documentation for the AES module.

Throughout this project, the following chronology is established:

- ◆Completion of design phase
- ◆Integration of AES algorithm and and design on a FPGA
- ◆Completion and certification of testing phase.

The constraints and limitations involves project completion within the due date, budget restrictions and availability of lab resources.

The future applications for AES encryption module include but are not limited to SMS encryption for mobile communication on Android message Application[3] only, A Secure Web-Based Android Chat Application[4], AES is one of the two common methods used in IoT devices[5].

There are some scope exclusions like implementation of other encryption standards like DES and implementation on non-RISC-V architectures.

5. Proposed Methodology

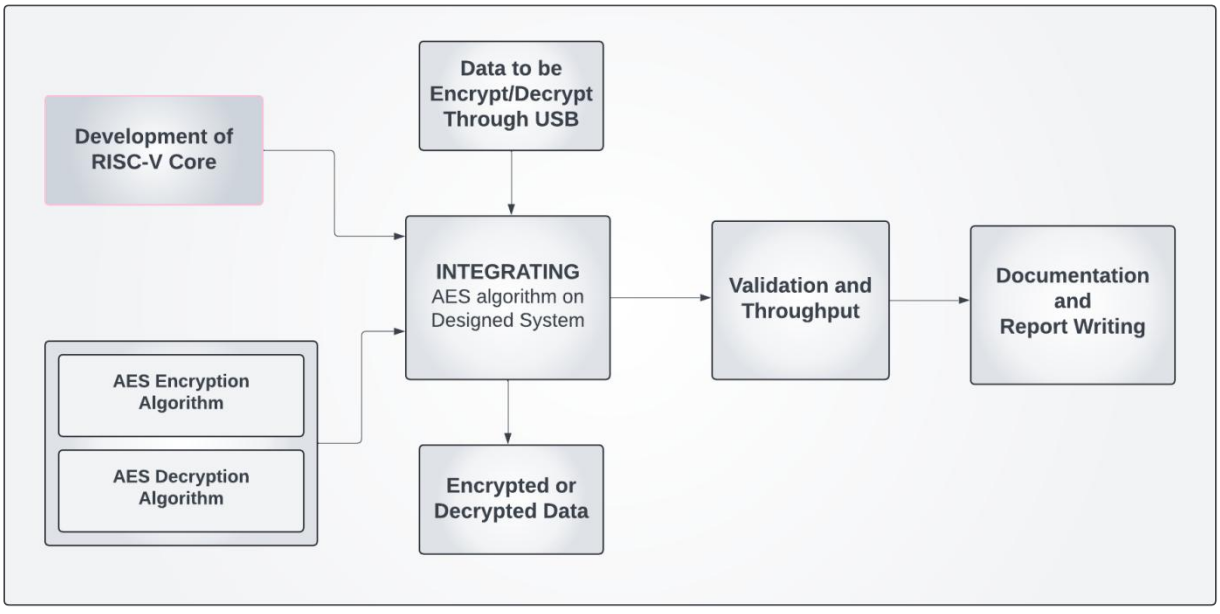

Figure 1. Proposed Methodology

1) **Development of RISC-V core**

Designing a RISC-V core on Quartus Prime for implementing the AES algorithm using Verilog or System Verilog. Connect a memory design to our processor to store the program data and the data to be encrypted or decrypted Peripheral devices for the data input and output we would use a USB to give data input to encrypt and store the encrypt data in USB as well as shown in Figure 1.

2) **Algorithm Implementation on RISC-V**

AES Encryption Module on RISC-V:

- Implement the AES algorithm tailored to the RISC-V instruction set.
- Include key expansion, substitution, permutation, and mixing operations.

AES Decryption Module on RISC-V:

- Implement the reverse AES process to decrypt cipher text back to plain text, ensuring accuracy with the decryption key.

Four different stages are used, one of permutation and three of substitution: [6]
As shown in Figure 2.

1. **Substitute bytes:** Uses an S-box to perform a byte-by-byte substitution of the block.
2. **Shift Rows:** A simple permutation.
3. **Mix-columns:** A substitution that makes use of arithmetic over GF(28).
4. **Add Round Key:** A simple bit wise XOR of the current block with a portion of the expanded key

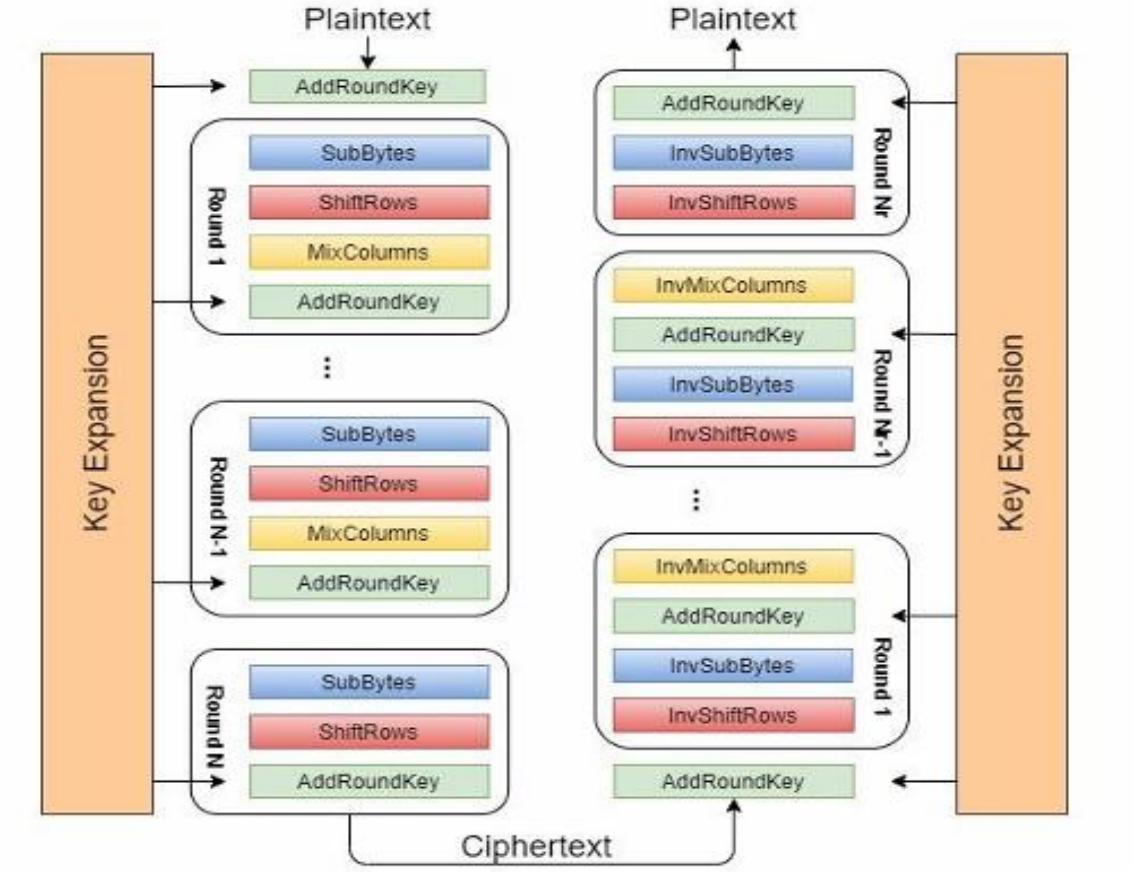

Figure 2 Basic AES encryption and decryption process. [7]

3) **Integration**

- Integrate AES Encryption and Decryption Module within the RISC-V core Designed System as shown in Figure 1.
- Test encryption and decryption using various data sets on the RISC-V processor to verify correctness and performance.

4) **Validation and Throughput**

- Measuring the throughput by providing different data length input and measuring the time taken by the system to encrypt it.
- Validate the system in real-world scenarios, such as secure data transmission or storage, to ensure robustness.

6. Resources Involved

Hardware:

FPGA board to develop a design including RISC-V core, memory modules, programming tools, and peripherals.

Software:

Quartus or Vivado, Modelsim , Questasim, RISC-V tool chain, simulation tools, and security testing software.

7. Description of Industrial Support (If any)

No industrial support is involved in this project.

8. SDGs (If Applicable)

☐ No Poverty	☐ Zero Hunger
☐ Good Health and Well-Being	☐Quality Education
☐ Gender Equality	☐ Clean water and Sanitation
☐ Affordable and Clean Energy	☒ Decent Work and Economic growth
☒ Industry, Innovations and Infrastructure	☐ Reduced Inequalities
☐ Sustainable Cities and Communities	☐ Responsible Consumption and Production
☐ Climate action	☐ Life Below Water
☐ Life on Land	☒ Peace, Justice and Strong Institutions
☐ Partnerships	

9. Gantt Chart

Year	2024 to 2025									
Months	AUG	SEP	OCT	NOV	DEC	JAN	FEB	MAR	APR	MAY
Requirement Analysis & Literature Review	x	x	x	x	x	x	x			
RISC-V core Development		x	x	x						
AES Algorithm			x	x	-	x				
Integration					-	x	x	x		
Validation & Throughput					-		x	x	x	
Documentation & Report			x	x	-	x	x	x	x	x

10. Details of Project Team

i. Students

No.	Name	Seat No.	Signature (s)
1	Muhammad Tariq Waseem	El - 21056	
2	Mirza Musab Baig	El - 21057	
3	Rameez Nawaz	El - 21061	
4	Anas Uddin	El - 21067	

ii. Supervisors / Advisors

	Name	Designation & Department	Address & Contact	Signature(s)
Supervisor	**Hafsa Amanullah**	Lecturer of Electronics Department	hafsa@cloud.neduet.edu.pk +92 301 2430439	
Co-Supervisor (If any)	**Faheem-ul-Haq**	Assistant Professor of Telecommunications	Mfahim@cloud.neduet.edu.pk +92 315 0224430	
Industrial Advisor (If any)	-	-	-	

For Office Use Only		
Project Serial No.: _____ Dated: _____	Signature Convener Steering Committee	Signature FYP Coordinator

☐ Proposal Approved	☐ Not Approved	☐ Returned for Clarification / Modification
Comments: (if any)		

_____

(Signature of Chairperson)

Date: _____

REFERENCES

[1] "Brute Force: Cracking the Data Encryption Standard," RSA Conference, [Online]. Available: https://www.rsaconference.com/library/blog/brute-force-cracking-the-data-encryption-standard.

[2] T. B. and H. Wu, "Improving the Biclique Cryptanalysis of AES," in Information Security and Privacy, Cham, Switzerland, Springer, 2015, pp. 39-56. https://doi.org/10.1007/978-3-319-19962-7_3

[3] S. Ariffi, R. Mahmod, R. Rahmat and N. A. Idris, "SMS Encryption Using 3D-AES Block Cipher on Android Message Application," *2013 International Conference on Advanced Computer Science Applications and Technologies*, Kuching, Malaysia, 2013, pp. 310-314, doi: 10.1109/ACSAT.2013.68.

[4] V. Singh, S. Janarthanan, U. K. Roshan and N. Vaid, "A Secure Web-Based Android Chat Application Using The AES Encryption Algorithm," *2023 5th International Conference on Advances in Computing, Communication Control and Networking (ICAC3N)*, Greater Noida, India, 2023, pp. 1329-1332, doi: 10.1109/ICAC3N60023.2023.10541852.

[5] M. Orsini, J.-L. Danger, and S. Guilley, "Extending a RISC-V core with an AES hardware accelerator to meet IoT constraints," in Proc. 2021 Design, Automation & Test in Europe Conference & Exhibition (DATE), 2021, pp. 1-6. doi: 10.23919/DATE51398.2021.9474226.

[6] W. Stallings, "Chapter 5: Advanced Encryption Standard," in Cryptography and Network Security Principles and Practice (6th Edition), Pearson, 2017.

[7] "Implementation of a 32-Bit RISC-V Processor with Cryptography Accelerators on FPGA and ASIC," [Online]. Available: Implementation_of_a_32-Bit_RISC-V_Processor_with_Cryptography_Accelerators_on_FPGA_and_ASIC.pdf.