PROJECT REPORT

VLSI IMPLEMENTATION IN HARDWARE SECURITYMODULE BASED ON AES ENCRYPTION METHOD

20ECPJ801- PROJECT PHASE - II

Submitted by

AKASH A (412520106007)

JAIGANESH P (412520106053)

MAHIZHAN M (412520106085)

in partial fulfillment for award of the degreeof

BACHELOR OF ENGINEERING

IN

ELECTRONICS AND COMMUNICATION ENGINEERING

SRI SAI RAM ENGINEERING COLLEGE

(An Autonomous Institution; Affiliated to Anna University, Chennai - 600 025)

ANNA UNIVERSITY :: CHENNAI 600 025

APRIL 2024

SRI SAIRAM ENGINEERING COLLEGE

(An Autonomous Institution; Affiliated to Anna University, Chennai -600 025)

BONAFIDE CERTIFICATE

Certified that this project report on **"VLSI IMPLEMENTATION IN HARDWARE SECURITY MODULE BASED ON AES ENCRYPTION METHOD"** is the bonafide work of **"AKASH A (412520106007), JAIGANESH P (412520106053) and MAHIZHAN M (412520106085)"** who carried out the **20ECPJ801- PROJECT PHASE - II** Work under my supervision.

SIGNATURE

Dr J Raja

HEAD OF THE DEPARTMENT

Department of Electronics and Communication Engineering,
Sri Sairam Engineering College, (Autonomous) Chennai - 600 044

SIGNATURE

Mr. K Srinivasan

SUPERVISOR

Associate Professor, Department of Electronics and Communication Engineering,
Sri Sairam Engineering College, (Autonomous) Chennai - 600 044

Submitted for VIVA-VOCE EXAMINATION held on:

INTERNAL EXAMINER

EXTERNAL EXAMINER

ACKNOWLEDGEMENT

We express our deep sense of gratitude to our beloved Founder Chairman **Shri. MJF. Ln. LEO MUTHU** for his blessings which made our project a great success.

Our heartfelt thanks to our CEO **Dr. SAI PRAKASH LEO MUTHU** and beloved Principal **Dr. K. PORKUMARAN,** for their help and for the advice they shared upon us.

We express our indebtedness and sincere thanks to **Dr. J. Raja, Professor and Head of the Department,** Department of Electronics and Communication Engineering, for his assistance throughout the course of our project.

We also thank our project Coordinator **Ms. S. SARANYA, Assistant Professor**, Department of Electronics and Communication Engineering for his unceasing ideas which helped us to take the right decision to attain our goals.

We express our indebtedness and sincere thanks to our Project guide **Mr.K. SRINIVASAN, Associate Professor,** Department of Electronics and Communication Engineering, for his assistance throughout the course of our project.

We also express our sincere gratitude to all the Teaching and non- teaching faculty members of our Department of Electronics and Communication Engineering who contributed directly or indirectly to our project.

ABSTRACT

As ecommerce and internet applications have grown in popularity, cryptography has become increasingly vital for data security and integrity. However, it is often overlooked in many circumstances due to the additional memory and other needs required for implementation. The primary goal of this project is to use Verilog to develop Advanced Encryption Standard (AES) encryption methods. Cryptographic algorithms are used to safeguard data, such as electronics. AES parallel design can decrease the latency associated with each encryption round. This paper presents a low-power, high-throughput version of the AES algorithm based on the key expansion technique. Using the suggested high-performance design, we reduce power consumption and critical path latency. Although security concerns have grown in importance over time, the initiative's primary purpose is to maximize data flow. The employment of encryption and decryption techniques inside VLSI has lately risen since cryptography can transform plaintext to cipher and vice versa. The most current advances in cryptography technology will be utilized in the hardware security module by simultaneously developing a large number of HDL modules. The primary goal is to send and receive data securely while preventing data from being hacked, as well as to increase the performance of a certain parameter. It is worth noting that any encryption technique operates in a digital environment, and all blocks in the system will handle digital data securely.

JUSTIFICATION FOR SDG & SAP

SDG No: 9

: Industry, Innovation and Infrastructure

SAP No: SAP090C

9 Support domestic technology development, research and innovation in developing countries, including by ensuring a conducive policy environment for, inter alia, industrial diversification and value addition to commodities.

TABLE OF CONTENTS

List of Figures

CHAPTER-1
INTRODUCTION

1.1 OBJECTIVE:

Security is becoming a crucial component of contemporary warfare Cyberattacks account for the majority of attacks. Cyberattack against Systems, Aircraft, Drones, and other Military Equipment, etc.

The initiative's main objective is to increase data flow, but as time goes on, security issues have taken on more significance. Since cryptography can transform plaintext into cypher and vice versa, its use inside VLSI has lately increased. A large number of HDL modules will be simultaneously written in order to implement the most recent advancements in cryptography technology in the hardware security module. The major goal is to send and receive data securely without allowing data to be hacked, as well as to boost the efficiency of a certain parameter. Verilog code was used as the technique in this system. Analog and digital platforms are offered by Xilinx to support the design of both analogue and digital circuits. Interesting fact: Any encryption algorithm will function.

1.2 Motivation:

The primary goal of the project is to increase system security. To that end, we would use our adaptation of AES encryption to strengthen the hardware security module's security in an environment centered around network-centric warfare. Additionally, to strengthen the security of defense technologies from cyber-attacks.

1.3 Relevance of the project:

Security is becoming a crucial component of contemporary warfare. Cyberattacks account for the majority of attacks. Cyberattack against Systems, Aircraft, Drones, and other Military Equipment, etc. These seriously harm a nation's collateral. In order to achieve our goal of improving system security, we would use our adaptation of AES encryption to strengthen the security of the hardware security module, which is an HSM (Hardware Security Module) chip implanted in the system controller.

CHAPTER-2

LITERATURE SURVEY

S.NO	TITLE	AUTHOR	PUBLISHED IN	INFERENCE
1	Journal of Electrical Systems and Information Technology 2 (2015) 178–183	Power efficient and high performance VLSI architecture for AES algorithm K. Kalaiselvi a,∗, H. Mangalam	**2022**	Advanced encryption standard (AES) algorithm has been widely deployed in cryptographic applications. This work proposes a low power and high throughput implementation of AES algorithm using key expansion approach
2	VLSI implementarion of AES Algorithm	Surabh Kumar	**2022**	This paper presents In the past cryptography means only encryption and decryption using secret keys, nowadays it is defined in different mechanisms like asymmetric-key encipherment and

				symmetric-key encipherment
3	VLSI Implementation of Cryptographic Algorithms & Techniques	Favin Fernandes, Gauravi Dungarwal, Aishwariya Gaikwad, Ishan Kareliya, Swati Shilaskar	**2021**	Through the years, the flow of Data and its transmission have increased tremendously and so has the security issues to it. Cryptography in recent years with the advancement of VLSI has led to its implementation of Encryption and Decryption techniques, where the process of translating and converting plaintext into cypher text and vice versa is made possible

CHAPTER-3

EXISTING AND PROPOSED SYSTEM

3.1 EXISTING SYSTEM:

Through the years, the flow of Data and its transmission have increased tremendously and so has the security issues to it. Cryptography in recent years with the advancement of VLSI has led to its implementation of Encryption and Decryption techniques, where the process of translating and converting plaintext into cypher text and vice versa is made possible. In this paper, the review of various aspects of VLSI's implementation of encryption and decryption are covered. Ultimately, with this review, the basic understanding of different VLSI techniques of Encryption and Decryption can be studied and implemented. This is the existing system of the project.

3.2 PROPOSED SYSTEM:

Verilog coding is the method used in this system. We would examine the most recent version of AES encryption first, modify it to reach the algorithm's optimum efficiency, and then implement it in a Hardware Security Module. After that We would implement into a Controller for further study of the Security of the Controller System. This is our proposed methodology of our Project.

CHAPTER-4

REQUIREMENT SPECIFICATION

4.1 Hardware requirements:

4.1.1 Hardware security module:

A hardware security module (HSM) is a physical computing device that protects and manages digital keys, as well as encrypting and decrypting digital signatures, strong authentication, and other cryptographic operations. These modules have historically been in the form of a plug-in card or an external device that connects directly to a computer or network server. A hardware security module consists of one or more secure crypto processor chips.

HSMs may have features that give tamper proof, such as visual symptoms of tampering or logging and alerting, tamper resistance, which makes tampering difficult without rendering the HSM useless, or tamper responsiveness, such as deleting keys when tampering is detected. Each module has one or more secure crypto processor chips to avoid tampering and bus probing, or a combination of chips in a module that is secured by the tamper evident, tamper resistant, or tamper responsive packaging.

Figure 4.1

Uses of HSM:

Any application that makes use of digital keys can benefit from using a hardware security module. Typically, the keys would be of great value, which means that if they were compromised, the owner would suffer a large loss.

The functions of an HSM are:

- Generates safe cryptographic keys on-board.
- Onboard safe cryptographic key storage for top-level and sensitive keys, also known as master keys.
- key management.
- Use cryptographic and sensitive data for decryption and digital signature tasks.
- Offloading application servers for full asymmetric and symmetric cryptography.

HSMs are also used to handle transparent data encryption keys for databases and storage media such as disks or tapes. HSMs secure these materials, including cryptographic keys, logically and physically from disclosure, unauthorized use, and possible adversaries. HSMs may perform both symmetric and asymmetric (public-key) cryptography. For certain applications, such as certificate authorities and digital signature, the cryptographic material is asymmetric key pairs (and certificates) from public-key cryptography. In other applications, such as data encryption or financial payment systems, cryptographic material is mostly composed of symmetric keys.

Figure 4.2

4.1.2 FPGA:

Field Programmable Gate Arrays (FPGAs) are semiconductor devices that consist of a matrix of customizable logic blocks (CLBs) coupled via programmable interconnects. FPGAs may be reprogrammed to meet specific application or functionality needs after they have been manufactured. This characteristic separates FPGAs from Application Specific Integrated Circuits (ASICs), which are custom-built for specific design needs. Although one-time programmable (OTP) FPGAs are available, the most common variants are SRAM-based and may be reprogrammed as the design changes.

Applications:

- Aerospace & Defense: Radiation-tolerant FPGAs and intellectual property for image processing, waveform production, and SDR reconfiguration.
- FPGA-based ASIC prototyping allows for faster and more accurate SoC system modeling and verification of embedded software.

• Broadcast & AV - Design platforms and solutions for high-end professional broadcast systems allow for faster adaptation to new needs and longer product lifespans.

- Our cost-effective technologies enable full-featured consumer applications such convergence phones, digital flat panel displays, information appliances, home networking, and residential set top boxes.Data Center - Designed for high-bandwidth, low-latency service, networking, and Storage applications to bring higher value into cloud deployments.
- We offer high-performance computing and data storage solutions for NAS, SAN, and storage systems.Industrial - Xilinx FPGAs and targeted design platforms for Industrial, Scientificand Medical (ISM) enable higher degrees of flexibility, faster time-to-market, andlower overall non-securing engineering costs (NRE) for a wide image of applications such as industrial imaging and surveillance, industrial automation,and medical imaging equipment.
- The Vivado FPGA and Spaítan® FPGA families can address processing, display, and I/O interface requirements for medical applications, including diagnostics, monitoring, and treatment..

- Xilinx provides solutions for security applications, including as access control, surveillance, and safety systems. Video & Image Processing - Xilinx FPGAs and targeted design platforms enable higher degrees of flexibility, faster time-to-market, and lower overall non-securing engineering costs (NRE) for a wide range of video and imaging applications.

- Wireless Communications - RF, base band, connection, transport, and networking solutions for wireless devices that support standards such as WCDMA, HSDPA, WiMAX, and more.

Figure 4.3

4.2 Software Requirements:

4.2.1 VIVADO:

Vivado is a comprehensive design suite created by AMD for developing and implementing designs on Adaptive SoCs and FPGAs. It offers a variety of tools and features to streamline the entire design flow, from design entry to implementation and verification.

Capabilities:

- Design Input: Vivado supports various design entry formats, including Verilog, VHDL, System Verilog, and IP Integrator.
- Synthesis: Converts HDL code into a netlist that represents the logic gates and interconnections of your design.
- Place and Route: Maps the synthesized netlist onto the FPGA fabric, optimizing placement and routing for performance and timing closure.
- Verification/Simulation: Provides tools for simulating and verifying your design at various levels of abstraction, ensuring its functionality before implementation.
- System-on-Chip (SoC) Design: Offers advanced features for designing and implementing complex SoC systems, including IP integration, power analysis, and floor planning.
- High-Level Synthesis (HLS): Enables C/C++ code to be converted into hardware for faster prototyping and design exploration.
- Timing Closure: Provides a comprehensive set of tools for analyzing and optimizing timing performance, ensuring your design meets timing constraints.
- Methodology Support: Supports various design methodologies, including Agile, Waterfall, and IP-centric design.

Benefits:

- Improved Productivity: Streamlines the design flow with a unified interface and advanced automation features, leading to faster design cycles.
- Enhanced Performance: Optimizes designs for performance and timing closure, enabling efficient implementation on FPGAs.
- Reduced Design Errors: Comprehensive verification tools help identify and eliminate errors early in the design process.
- Increased Flexibility: Supports various design entry formats and methodologies, offering flexibility for different design styles.
- IP-Centric Design: Enables efficient integration and reuse of intellectual property (IP) cores, accelerating design creation.

Figure 4.4

CHAPTER-5

ALGORITHM

5.1 Advanced Encryption Standard:

. The Advanced Encryption Standard (AES) is a symmetric block cipher used by the United States government to safeguard confidential information.

AES is used in software and hardware across the world to encrypt critical data. It is critical to government computer security, cybersecurity, and electronic data protection.

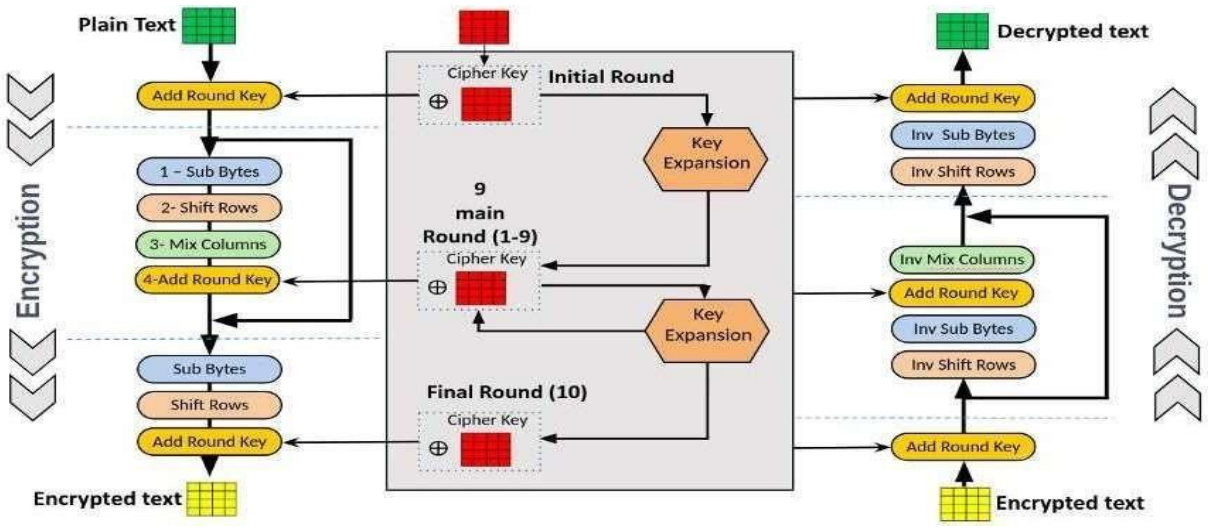


Figure 5.1

Working of AES:

AES includes three block ciphers:

- AES-128 employs a 128-bit key to encrypt and decode a block of messages.AES-192 uses a 192-bit key length to encrypt and decrypt a block ofmessages.
- AES-256 encrypts and decrypts blocks of messages using a 256-bit key length. Each cipher encrypts and decrypts data in blocks of 128 bits using cryptographic keys of 128, 192 and 256 bits, respectively.

Symmetric, often known as secret key, ciphers employ the same key for both encryption and decryption. The sender and receiver must both know and use the same secret key.

The government categorizes material into three categories: confidential, secret, and top secret. All key lengths can be used to secure the Confidential and Secret levels. Keylengths of 192 or 256 bits are required for top-secret information.

There are 10 rounds for 128-bit keys, 12 for 192-bit keys, and 14 for 256-bit keys. A round is made up of many processing steps that involve substitution, transposition, and mixing of the input plaintext to produce the final ciphertext.

The AES encryption technique undergoes several rounds of encryption. It may even go through 9, 11, or 13 rounds like this.

Each round involves the same steps below.

- Divide the data into blocks.
- Key expansion.

- Add the round key.
- Substitute/replacement of the bytes.
- Shift the rows.
- Mix the columns.
- Add a round key again.
- Do it all over again.

Following the final round, the algorithm will go through one more round. The algorithm will do steps 1 through 7, with the exception of step 6.

It modifies the sixth step since it would be ineffective at this time. Remember, it has previously gone through this procedure several times.

As a result, repeating step 6 is unnecessary. The amount of processing power required to mix the columns again is just not worth it because the data will not be considerably altered.

The AES encryption technique offers a number of modifications that may be applied to data stored in an array. The initial stage of the cipher is to place the data in an array, following which the cipher modifications are repeated throughout several encryption cycles.

The first transformation in the AES encryption cipher is data substitution using a substitution table. The second transformation rearranges data rows. The third step combines columns. The final transformation is applied to each column, using a different component of the encryption key. Longer keys require several rounds to accomplish.

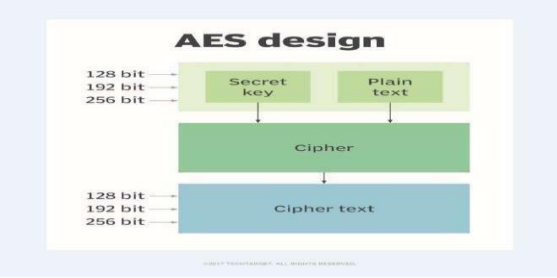


Figure 5.2

Features of AES:

NIST stipulated that the new AES algorithm must be a block cipher capable of processing 128-bit blocks with keys sized at 128, 192, and 256 bits. Other factors for being picked as the next AES algorithm were as follows:

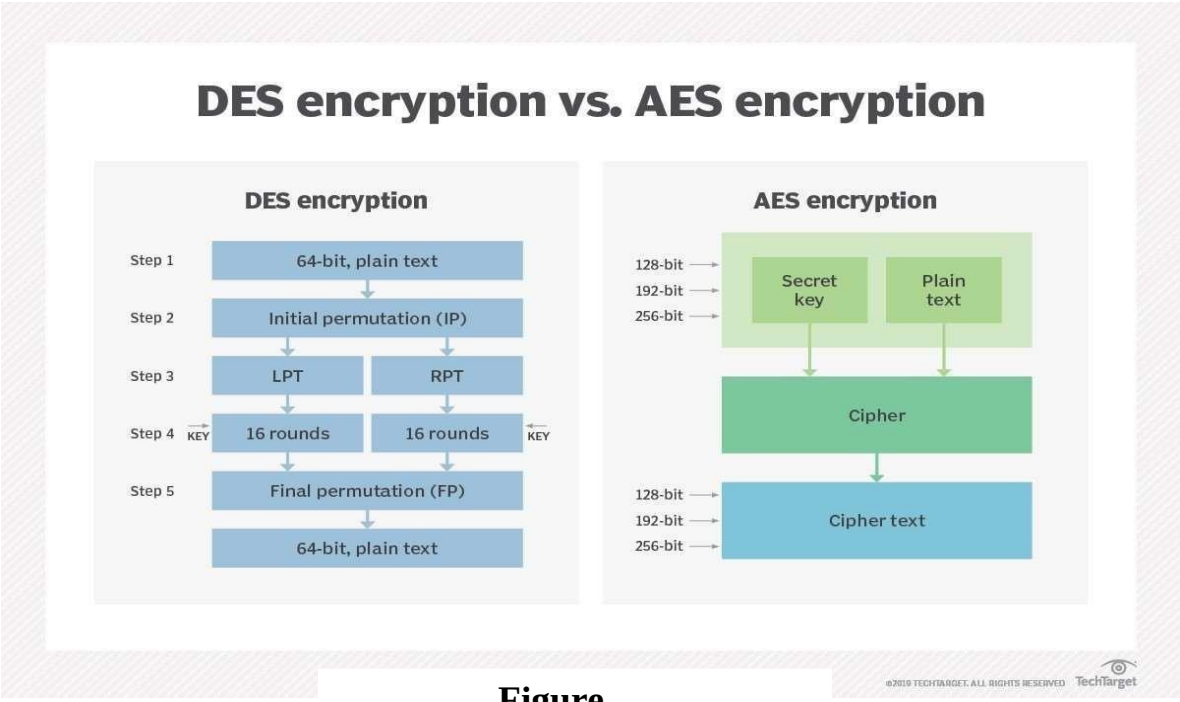
- Security: Competing algorithms were to be rated on their capacity to withstand attacks when compared to other ciphers. Security was to be the most crucial issue in the competition.
- Cost: The potential algorithms were to be evaluated in terms of computational and memory efficiency before being provided on a worldwide, nonexclusive, and royalty-free basis.
- Consider the algorithm's flexibility, applicability for hardware or software, and general simplicity while implementing it.

Difference between AES encryption and DES encryption:

For years, DES was the foundation of government encryption, until 1999, when researchers used a distributed computer system to break the algorithm's 56-bit key. In 2000, the US government decided to employ AES to secure confidential information. DES is still employed in some cases for backward compatibility.

Both protocols use symmetric block ciphers, although AES is mathematically more efficient. The main benefit of AES lies in its key length

options. The time required to crack an encryption technique is directly proportional to the length of the key used to protect the transmission (128-bit, 192-bit, or 256-bit keys). As a result, AES is orders of magnitude more powerful than DES' 56-bit keys. AES encryption is also more quicker, making it excellent for applications, firmware, and devices that need low latency or high throughput.



Figure

AES 256 Encryption:

We know that encryption methods jumble the information they protect, resulting in a random mess.

I mean, the fundamental concept of all encryption is that each unit of data is replaced with a new one based on the security key.

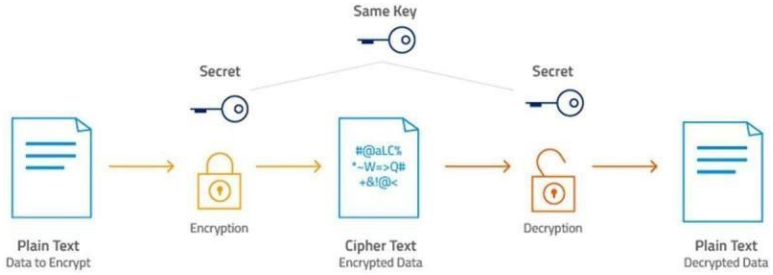


Figure 5.4

There are several rounds in this encryption process,

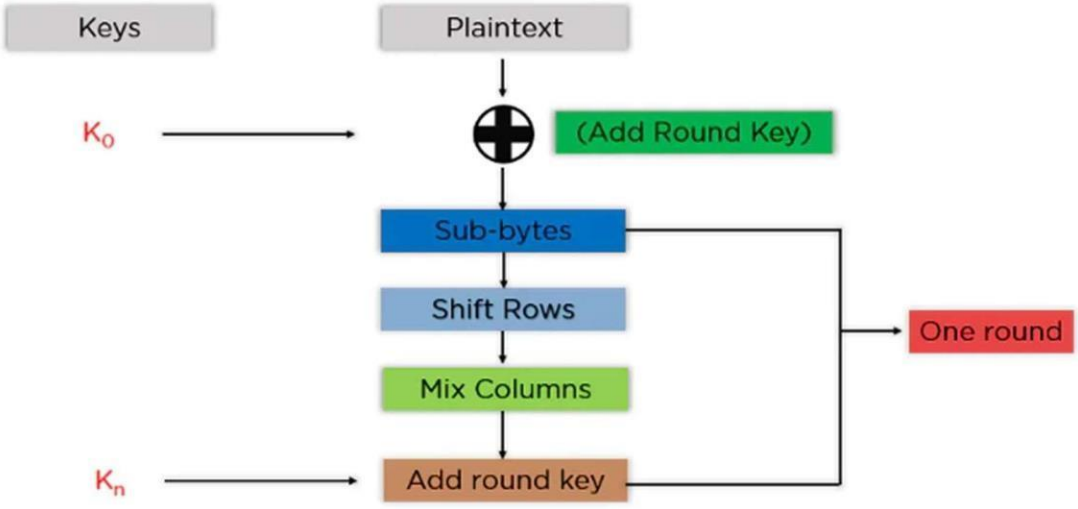


Figure 5.5

Add Round Key: You use an XOR function to combine the block data contained in the state array with the first key created. It passes the resulting state array as input to the following phase.

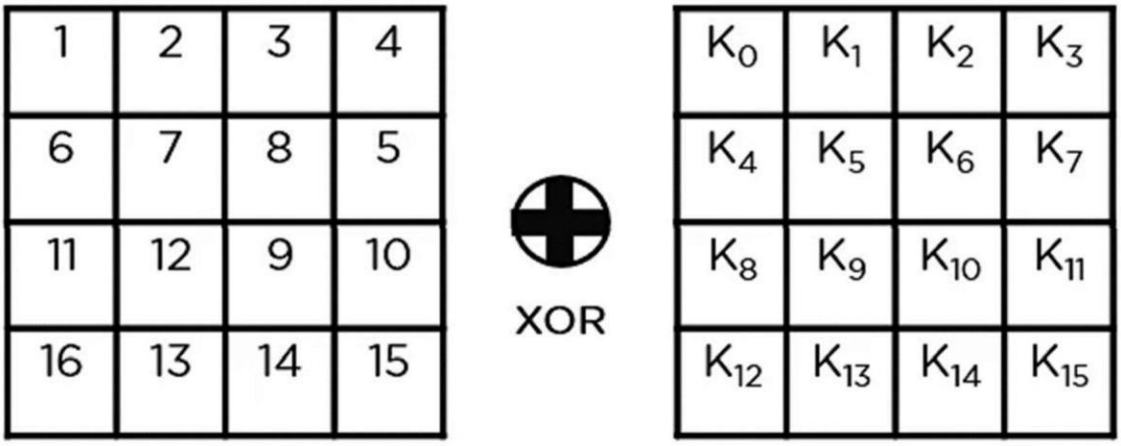


Figure 5.6

Sub-Bytes: In this stage, each byte from the state array is converted to hexadecimal and divided into two equal halves. These components are the rows and columns, mapped using a substitution box (S-Box) to produce new values for the final state array.

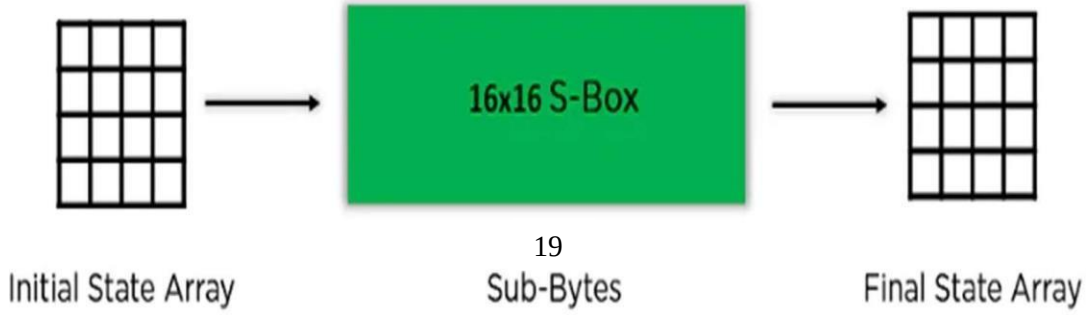


Figure 5.7

Shift Rows: It swaps row items. It skips the first row. It moves the components in the second row one place to the left. It also moves the items in the third row two places to the left, and the last row three positions to the left.

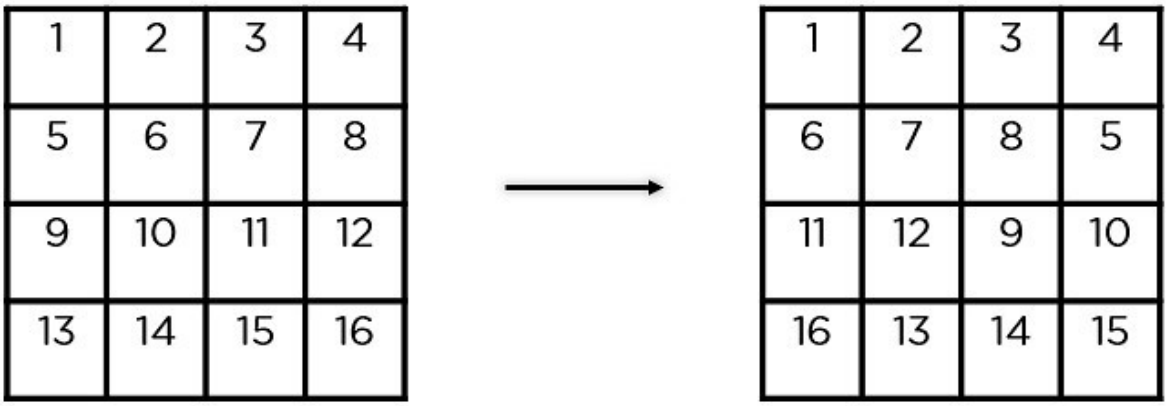


Figure 5.8

Mix Columns: It multiplies a constant matrix by each column in the state array to generate a new column for the next state array. Once all of the columns are multiplied by the same constant matrix, you'll have your state array for the following step. This particular stage is not to be completed in the final round.

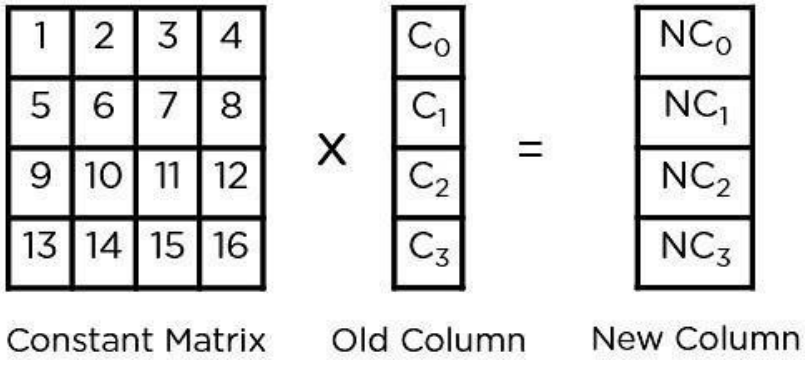


Figure 5.9

Add Round Key: The round's key is XOR'd with the state array produced in the previous phase. If this is the final round, the resulting state array becomes the ciphertext for the specified block; otherwise, it serves as the new state array input for the following round.

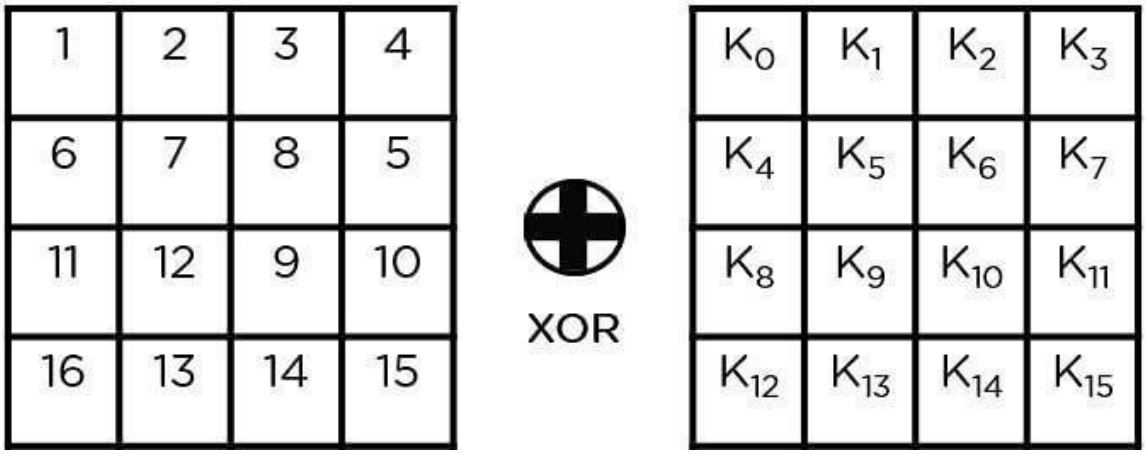


Figure 5.10

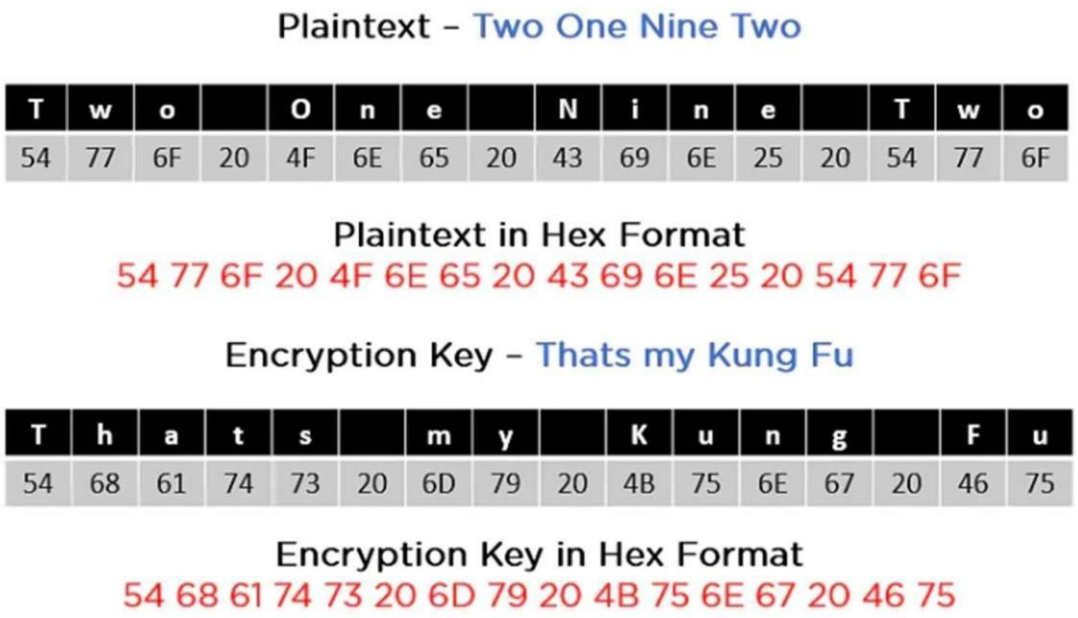


Figure 5.11

As seen in the graphic above, plaintext and encryption convert keys to hexadecimal format before beginning operations. As a result, you may create keys for the next ten rounds, as seen below.

You must repeat the processes outlined above, successively extracting the state array and sending it on as input to the following round. The steps are as follows.
Add a circular key.

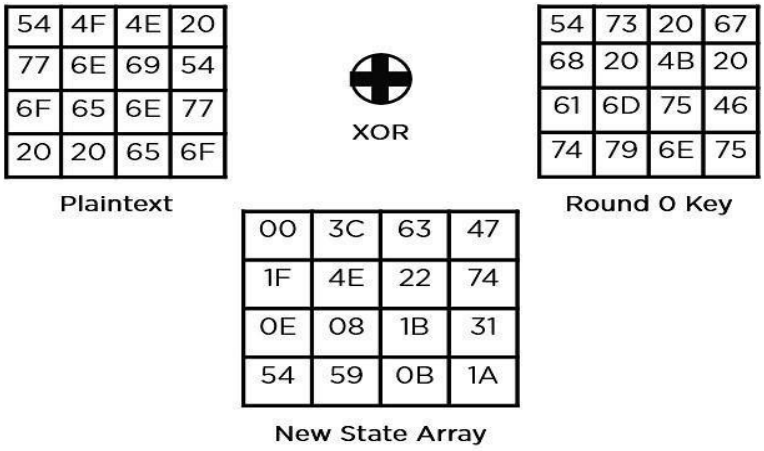


Figure 5.12

Sub-Bytes: It passes the elements through a 16x16 S-Box to get a completely new state array

63	EB	9F	A0
C0	2F	93	92
AB	30	AF	C7
20	CB	2B	A2

New State Array

Figure 5.13

Shift rows,

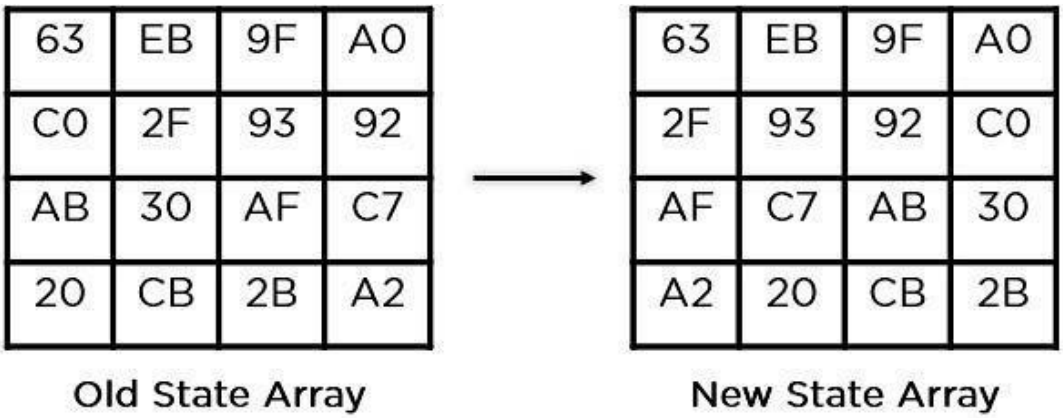


Figure 5.14

Mix columns,

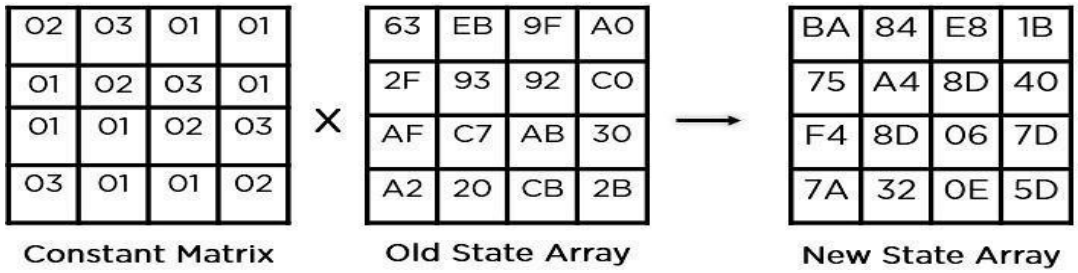


Figure 5.15

Add round key,

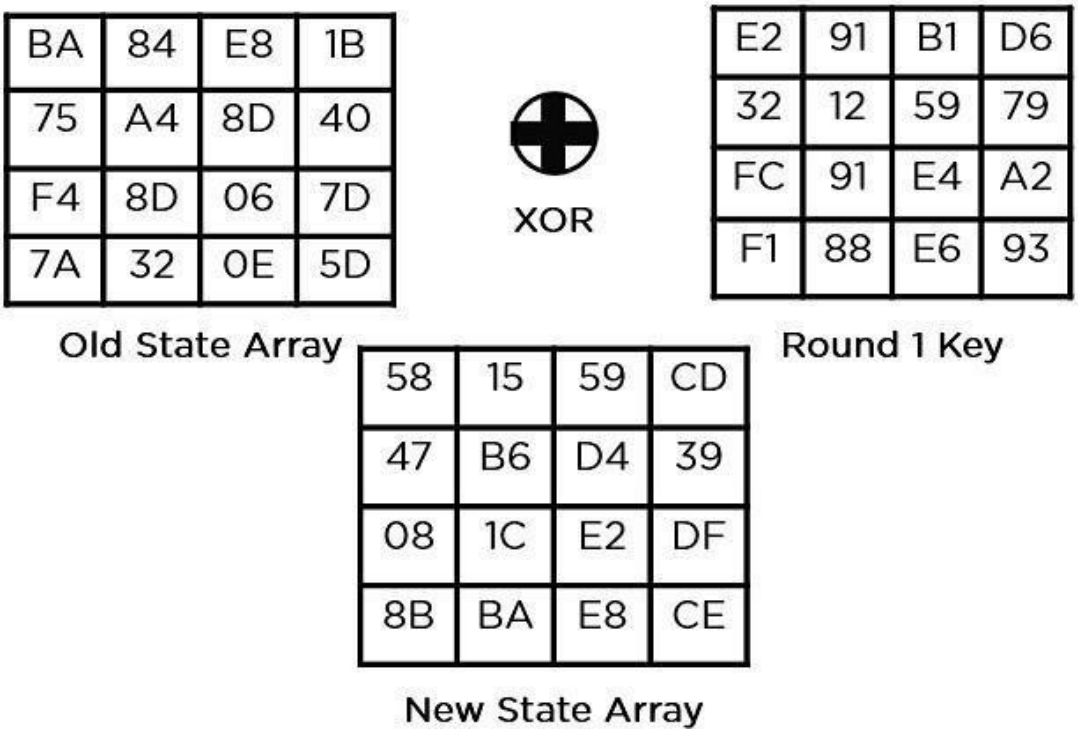


Figure 5.16

This state array now contains the final ciphertext for this particular round. This becomes the input for the following round. Depending on the key length, continue the procedures above until round 10, at which point you will obtain the final ciphertext.

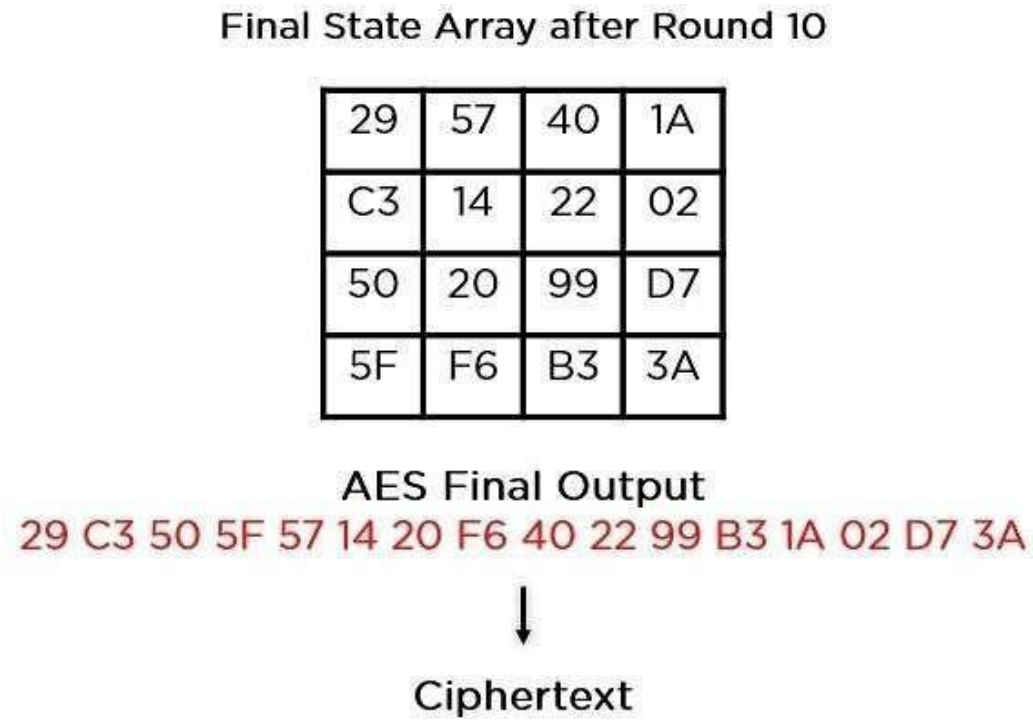


Figure 5.17

Application of AES:

- Wireless networks use the Advanced Encryption Standard to authenticate routers and clients. Wi-Fi networks employ firmware software and comprehensive security systems based on this method, which are now widely used.

- AES encryption ensures secure website server authentication from both client and server end. With both symmetric and asymmetric encryption in use, this technique aids SSL/TLS encryption protocols in ensuring the highest level of security and privacy when browsing.

- AES is commonly used for transferring encrypted data between partners, in addition to business purposes. Encrypted material might include chat conversations, family photos, and legal papers.

- Processor Security: Many processor manufacturers provide hardware-level encryption, such as AES encryption, to strengthen security and minimize meltdown failures, among other low-profile concerns.Processor Security: Many processor manufacturers provide hardware-level encryption, such as AES encryption, to strengthen security and minimize meltdown failures, among other low-profile concerns.

CHAPTER – 6
POWER AND LUT ANALYSIS

POWER ANALYSIS

our project's success in reducing power consumption compared to existing standards is a testament to our commitment to innovation, efficiency, and sustainability. By embracing advanced technologies, implementing optimized design methodologies, and prioritizing power efficiency throughout the development process, we have achieved remarkable reductions in energy consumption with far-reaching implications for cost savings, environmental preservation, and market competitiveness. As we continue to push the boundaries of power efficiency in our projects, we remain steadfast in our commitment to driving positive change and shaping a more sustainable future.

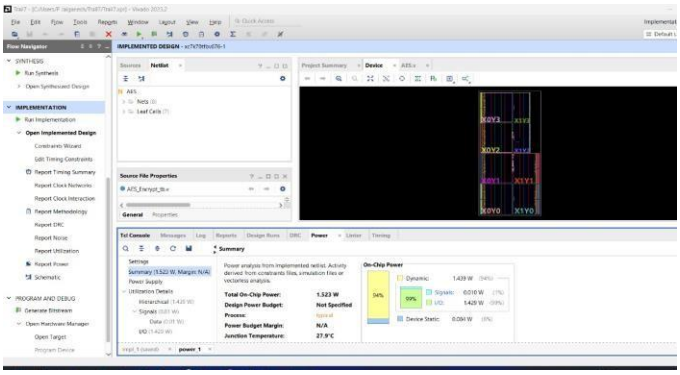


Figure 6.1

LUT ANALYSIS

The strategic integration of LUT optimization techniques within our project represents a pivotal milestone in our pursuit of efficiency and performance excellence. By harnessing the power of LUTs, we have unlocked new realms of computational efficiency, performance enhancement, and scalability, propelling our project towards unprecedented levels of success. As we continue to innovate and refine our approach, we remain committed to leveraging cutting-edge technologies to drive positive change and deliver value to stakeholders.

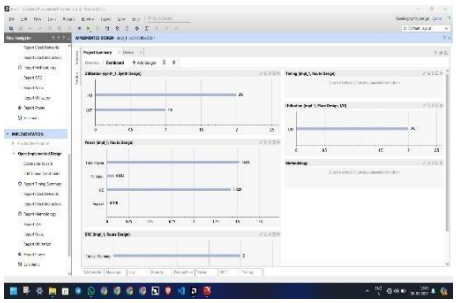


Figure 6.2

CHAPTER – 7

EXPERIMENTS OUTPUTS

Encryption:

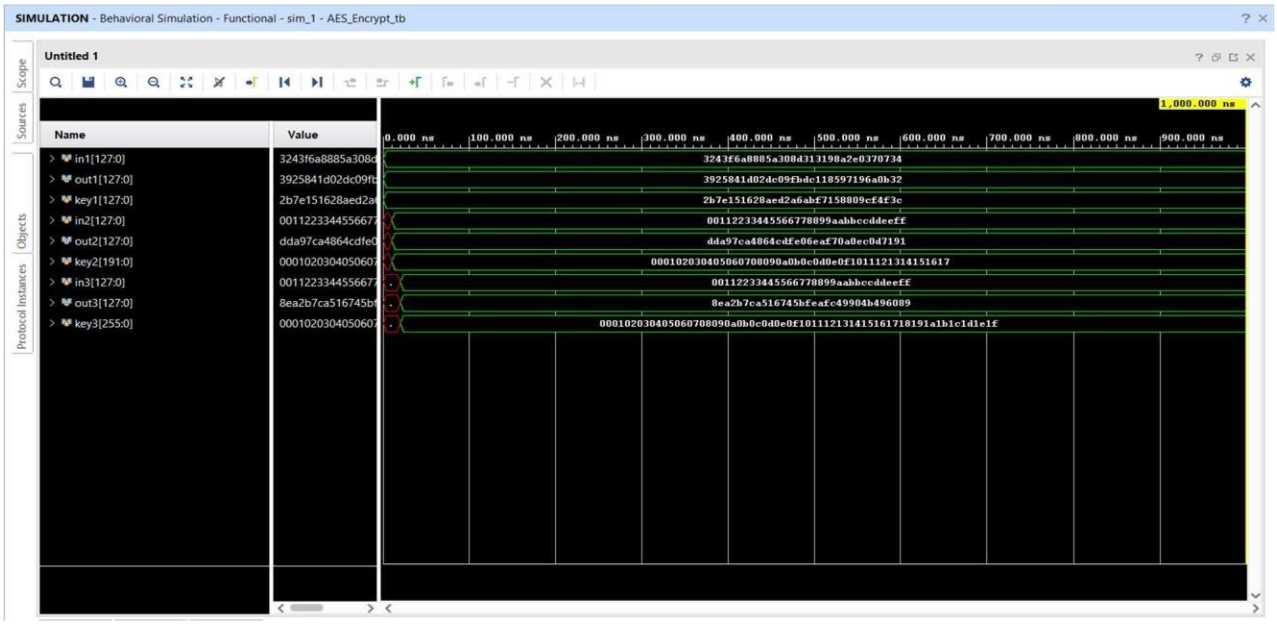


Figure 7.1

Decryption:

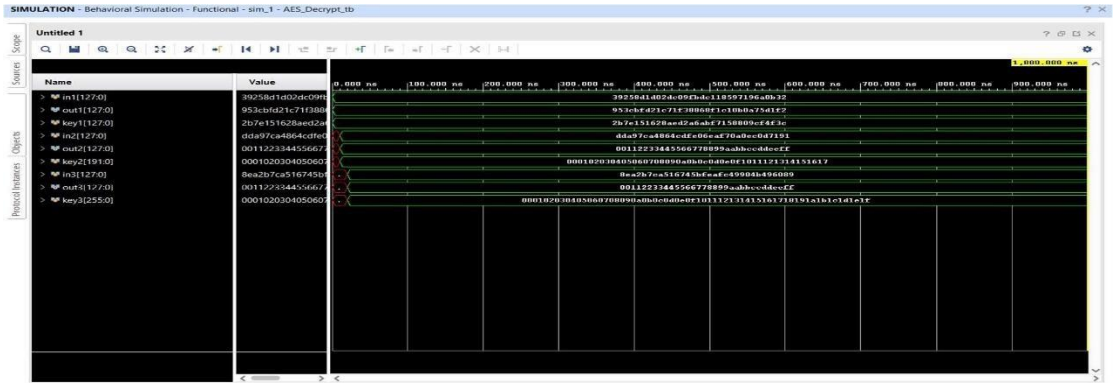


Figure 7.2

CHAPTER – 8

CONCLUSION AND FUTURE SCOPE

Conclusion:

This leads us to the conclusion that this project might have research on the definition of cryptography, the AES encryption algorithm, and Xilinx software. From this study, we would modify the AES Encryption algorithm in the best way possible and implement it in the FPGA kit.

Future scope:

We intended to enhance this project by using an FPGA kit to implement the optimal algorithm in the circuit. Embed this in a controller so that we could check the controller's security and create a commercial product. the DRDO will receive this for integration into their weapon.

APPENDICES A

PROOF FOR PUBLICATION

Gmail Jaiganesh P <bk24072002@gmail.com>

Paper accepted for presentation- congratulations - IC3IoT2024
3 messages

Microsoft CMT <email@msr-cmt.org> Wed, Mar 20, 2024 at 3:56 AM
Reply-To: Sumathi Krishnaswamy <sumathik.ece@sairam.edu.in>
To: Jaiganesh P <bk24072002@gmail.com>

Dear Author,

Congratulations!! Your paper 290 - A VLSI Perspective on Encryption Algorithm Analysis has been accepted with major revision for presentation in the 2024 INTERNATIONAL CONFERENCE ON COMMUNICATION,COMPUTING & INTERNET OF THINGS
Reviewers comments:
The algorithms (AES/DES/RSA) are already available. So much of FPGA implementations were carried out already. This work did not mention the issues of the previous works and did not propose any new ideas to rectify those issues. No simulation results were given. Any FPGA implementation work using HDLs should include the name of the target FPGA (including its family details), but the authors did not mention clearly. The authors claim the reduction in power consumption and critical path delays but no analysis was given in the paper. The number of LUT analysis for existing and proposed FPGA implementations are missing. The authors should rewrite the paper thoroughly after including all these details. Implementation photographs can be included.

You are now welcome to submit the camera-ready paper incorporating reviewer comments in the Microsoft CMT portal and register your paper for the conference using the link below:
Physical presentation is mandatory for Indian authors to proceed with publication

The following is the registration link:
https://forms.gle/TPxGmkxjFDWPf6cDA

Deadline for Registration: 28 March 2024
Deadline for Camera-ready submission: 28 March 2024

Instructions for eCopyright form:

1. Login to your Microsoft CMT Portal
2. Navigate and select "Submit IEEE Copyright Form" in the actions section (Right-mid side of your screen)
3. Click "here" in 'Click here to redirect to the IEEE Copyright Web Site' which will be shown on your screen. This will redirect you to IEEE copyright website
4. Follow the instructions given by the website, and finally enter your name as a digital signature.
5. Upon doing all the above procedures, you could download a filled IEEE eCopyright form.
6. Then, upload the downloaded eCopyright form in your Microsoft CMT portal in the "Submit IEEE Copyright Form" tab.

Instructions for Camera-ready submission:

1. Please strictly follow the IEEE conference paper template which you can download from https://www.ieee.org/conferences/publishing/templates.html (Both A4 & US letter is accepted)
2. Please adhere to the IEEE guidelines and keep the number of pages of your submission with a minimum of 4 pages and a maximum of 6 pages including reference.
3. Process your camera-ready submission by logging in IEEE PDF eXpress site https://ieee-pdf-express.org/account/Login and use the conference ID '60841X'. Please create an account if you don't have one and follow the same instructions.
4. Once logged in, upload your submission file and once it is processed and approved, download the final processed file (which will be renamed in random numbers).
5. Upload the final processed file as your paper ID(Example: 1.pdf , where 1 is the paper ID) which is the camera-ready file in the microsoft CMT portal.

Please make sure your paper's similarity index is less than 15% during camera-ready submission.
Plagiarism report services are provided upon mailing your paper id attached with the paper to ieeeic3iot2024@sairam.edu.in, report will be mailed back to you in 24-48 hours.
If your paper's similarity index is already less than 15% please proceed with the camera-ready paper.

Kindly follow the guidelines strictly,

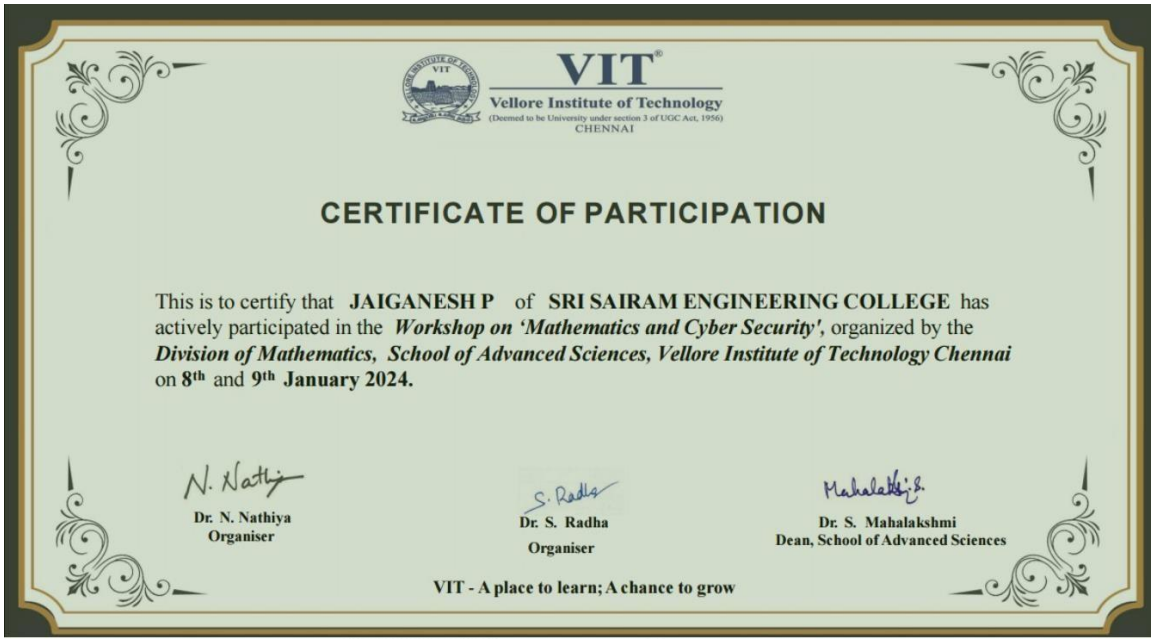
APPENDICES B

ACHIEVEMENTS

INNOVATHON 1.0 FINALISTS

SOLVEATHON 1.0 WINNER

COURSES



REFERENCES

1. Kumar, Pramod, T. V. Narendra, and N. A. Vinay. "Short Hand Recognition using Canny Edge Detector." International Journal 7, no. 5 (2017).
2. Kumar, Mamatha MS Pramod, and M.Mamatha. "FPGAImplementation Of Low Area Single Precision Floating Point Multiplier."International Journal of Science Technology and Engineering, Vol.2, no. 2 (2016): 560-566.
3. M.Natheera Banu, FPGA Based Hardware Implementation of Encryption Algorithm, International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 8958, Volume-3, Issue-4, April 2014.
4. Deguang Le, Jinyi Chang, Xingdou Gou, Ankang Zhang ,Conglan Lu , Parallel AES Algorithm for Fast Data Encryption on GPU, IEEE journal on AES 2010.
5. K. Xinmiao Zhang, High speed VLSI architectures for the AES algorithm, IEEE transactions on VLSI systems, Tech. Rep., sep2004.
6. National Institute of Standards and Technology, Advanced Encryption Standard, Federal Information Processing Standards 197, November 2001.
7. M.Pitchaiah, Philemon Daniel, Praveen, Implementation of Advanced Encryption Standard Algorithm, International Journal of Scientific Engineering Research.