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 main objective of this project is to employ Verilog to create Advanced Encryption Standard (AES) encryption algorithms. Cryptographic algorithms are used to safeguard data, such as electronics. AES parallel design can decrease the latency associated with each encryption round. This study proposes a low-power, high-throughput variant of the AES algorithm using the key expansion approach. 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 important to note that any encryption approach works in a digital environment, and all blocks in the system will handle digital data safely.

JUSTIFICATION FOR SDG & SAP

SDG No: 9

: Industry, Innovation and Infrastructure

SAP No: SAP090C

This is implementing effective strategies to promote research and development initiatives is crucial for the sustainable growth of emerging economies.

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	JESIT-15	K. Kalaiselvi, H. Mangalam	**2022**	The implementation of this algorithm has shown, that with the increasing demand for secure data transmission, processes like key expansion are crucial. By incorporating this technique into the AES algorithm, significant advancements in both power efficiency and data processing speed can be achieved
2	VLSI implementarion of AES Algorithm	Surabh Kumar	**2022**	This paper offers Historically, cryptography was limited to the use of secret keys for encryption and decryption; currently, it encompasses a variety of operations, such symmetric-key and asymmetric-key encipherment.

3	VLSI Implementation of Cryptographic Algorithms & Techniques	Favin Fernandes, Gauravi Dungarwal, Aishwariya Gaikwad, Ishan Kareliya, Swati Shilaskar	**2021**	The movement and flow of information has risen dramatically over time, as have the security risks connected to it. Recent advances in VLSI technology have allowed the usage of encryption and decryption techniques in cryptography, permitting the encoding and conversion of plaintext into cipher text and vice versa.

CHAPTER-3

EXISTING AND PROPOSED SYSTEM

3.1 EXISTING SYSTEM:

The volume of data and its transmission has expanded dramatically over the years, as have the security challenges that accompany it. Cryptography has advanced in recent years, with the advent of Encryption and Decryption procedures, which allow for the translation and conversion of plaintext into cypher text and vice versa. This study reviews many elements of VLSI's encryption and decryption implementations. Finally, using this overview, a fundamental grasp of several VLSI approaches for encryption and decryption may be examined and used. This is the current 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:

Strong authentication, digital signature encryption and decryption, digital key management, and other cryptographic functions are all performed by hardware security modules (HSMs), which are actual computer devices. Historically, a computer or network server may be directly connected to these modules via an external device or as a plug-in card. With one or more safe crypto processor chips, a hardware security module is assembled.

Tamper-proof features on HSMs include visible indicators of tampering, logging, and alerts; tamper resistance, which makes tampering challenging but does not render the HSM unusable; and tamper responsiveness, which removes keys upon detection of tampering. A combination of chips in a module that is protected by the tamper evident, tamper resistant, or tamper responsive packaging, or one or more secure crypto processor chips to prevent tampering and bus probing, are included in each module.

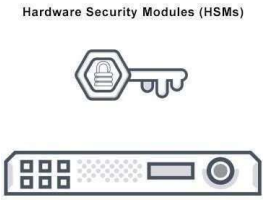


Figure 4.1

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.
- Master keys, or top-level and sensitive cryptographic keys, are stored safely onboard.
- Key personnel.
- For jobs involving digital signatures and decryption, use sensitive data and cryptography.
- Application servers that are offloaded for complete symmetric and asymmetric cryptography.

Transparent data encryption keys for databases and storage devices like disks and tapes are also managed by HSMs. Logically and physically, HSMs protect these resources—including cryptographic keys—from prying eyes, unsanctioned access, and potential enemies. Both symmetric and asymmetric (public-key) cryptography may be carried out using HSMs. Asymmetric key pairs and certificates from public-key cryptography are the cryptographic material used in some applications, such as certificate authorities and digital signatures. For other uses, including financial payment systems or data encryption, symmetric keys make up the majority of cryptographic material.

Figure 4.2

4.1.2 FPGA:

A matrix of programmable logic blocks (CLBs) connected by programmable interconnects makes up Field Programmable Gate Arrays (FPGAs), which are semiconductor devices. After being created, FPGAs may be reprogrammed to satisfy certain application or feature requirements. This feature sets FPGAs apart from Application Specific Integrated Circuits (ASICs), which are specially made to meet certain design requirements. While there are FPGAs that can be programmed once, commonly available variations are SRAM-based and may be programmed again when the design evolves.

Applications:

- Defense & Aerospace: Intellectual property and radiation-tolerant FPGAs for waveform generation, image processing, and SDR reconfiguration.
- Embedded software verification and SoC system modeling may be completed more quickly and accurately using FPGA-based ASIC prototyping.

- Broadcast & AV - High-end professional broadcast systems' design platforms and solutions enable quicker response to changing requirements and longer product lifetimes.

- Full-featured consumer applications including digital flat panel displays, information appliances, home networking, convergence phones, and residential set-top boxes are made possible by our affordable technology. The purpose of a data center is to enhance cloud deployments by providing high-bandwidth, low-latency service, networking, and storage applications.

- For NAS, SAN, and storage systems, we provide high-performance computing and data storage solutions. Industrial: Higher degrees of flexibility, quicker time-to-market, and lower total non-securing engineering costs (NRE) are made possible by Xilinx FPGAs and targeted design platforms for Industrial, Scientific, and Medical (ISM) applications. These applications include industrial automation, medical imaging equipment, and industrial imaging and surveillance. The processing, display, and I/O interface needs for medical applications, such as diagnosis, monitoring, and therapy, may be met by the Vivado FPGA and Spartan FPGA families.

• Xilinx offers solutions for safety systems, surveillance, and access control, among other security-related applications. Video & Image Processing: A variety of video and imaging applications can benefit from more flexibility, a quicker time to market, and cheaper total non-securing engineering expenses (NRE) thanks to Xilinx FPGAs and tailored design platforms.

- Wireless Communications: This category includes base band, RF, networking, connectivity, and transport solutions for wireless devices that comply with WiMAX, HSDPA, and other standards.

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:

. Secret data is protected by the US military using a identical block cipher called the Advanced Encryption Standard (AES).

Encrypting important data is a global usage of AES in hardware and software. Cybersecurity, electronic data protection, and military computer security all depend on it.

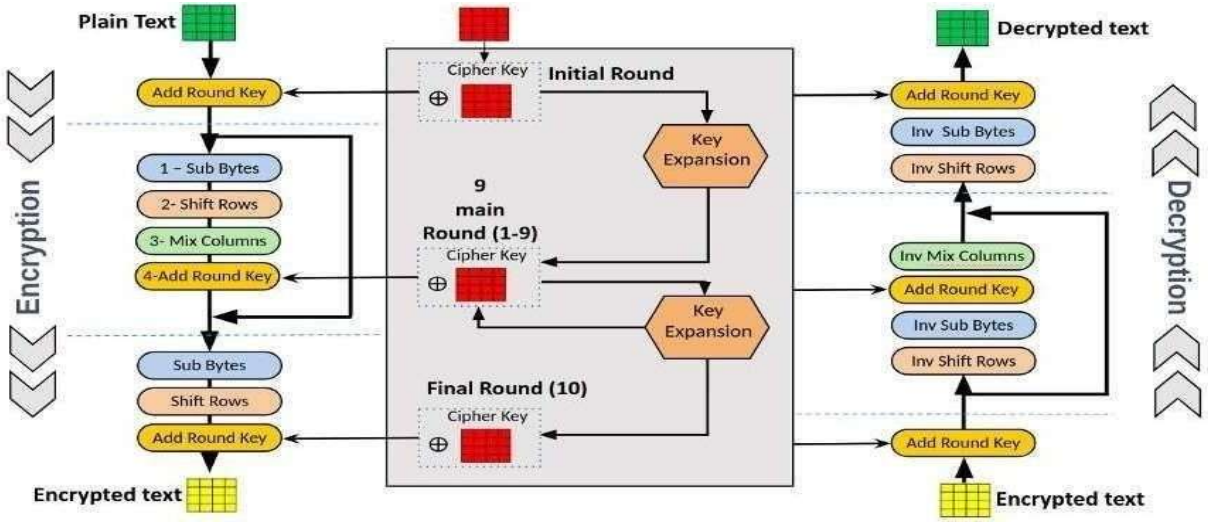


Figure 5.1

Working of AES:

AES includes three block ciphers:

- AES 128 bit encrypts and decrypts a block of messages using a 128 bit key. A block of messages is encrypted and decrypted using a 192 bit key length using AES 192.
- Using a 256 bit key length, AES 256 encrypts and decrypts message blocks. With cryptographic keys measuring 128, 192, and 256 bits, respectively, each cipher encrypts and decrypts data in blocks of 128 bits.

The same key is used by symmetric ciphers, sometimes referred to as secret key ciphers, for both encryption and decryption. The secret key must be known and used by both the sender and the recipient.

Rounds for 128 bit keys are 10, 192 bit keys are 12, and 256 bit keys are 14. To create the final ciphertext, a round's worth of processing stages include mixing, trans positioning, and substituting the input plaintext.

Multiple encryption rounds are used to the AES encryption method. It may even go in this manner through 9, 11, or 13 rounds.

The instructions following are the same for every round.

- Split the information into chunks.
- Expansion of the key.

- Include the spherical key.
- The bytes are changed or substituted.
- Rearrange the rows.
- Stir the columns together.
- Reapply a circular key.
- Re-do everything.

The algorithm will go through one more round after the last one. With the exception of step 6, the algorithm will complete steps 1 through 7.

Since the sixth step would not work at this time, it is modified. Recall that it has already gone through this process several times.

Consequently, there's no need to repeat step 6. The data won't be much changed; therefore, it just isn't worth the processing effort needed to mix the columns once again.

Data stored in an array may be modified in a number of ways using the AES encryption algorithm. The data is first placed in an array as part of the cipher's first stage. Afterward, many encryption cycles are completed by repeating the cipher's alterations.

Using a substitution table, data substitution is the initial alteration in the AES encryption algorithm. The data rows are rearranged in the second transformation. Columns are combined in the third phase. Using a separate part of the encryption key for each column, the last transformation is applied. Longer keys take more rounds to complete.

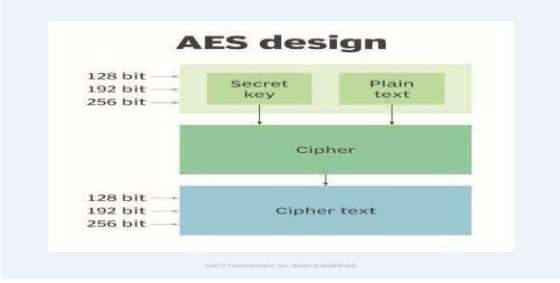


Figure 5.2

Features of AES:

NIST mandated that the newly developed AES algorithm should be a block cipher that can handle 128 bit blocks using keys that have sizes of 128, 192, and 256 bits. The following criteria were also considered when choosing the next AES algorithm:

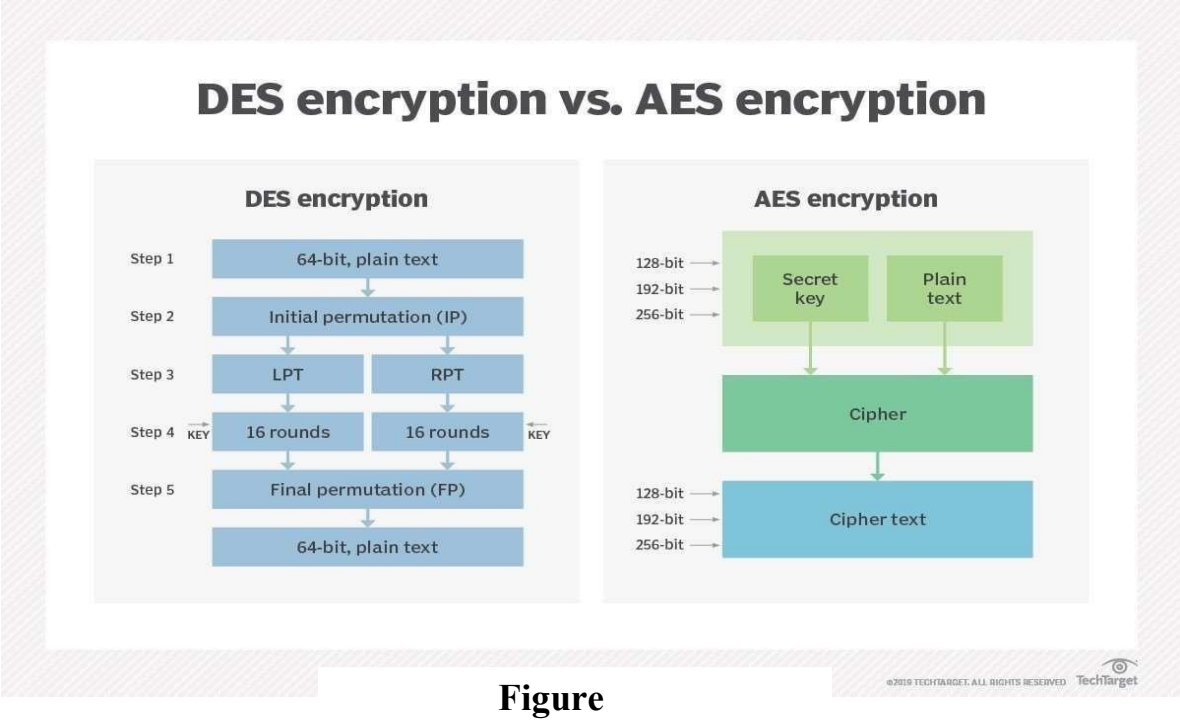
- Security: In comparison to other ciphers, competing algorithms were to be scored according to how well they could survive assaults. The competition's most important concern was going to be security.
- Cost: The prospective algorithms were to be made available internationally, nonexclusively, and royalty-free after being assessed for computational and memory efficiency.
- When putting the method into practice, take into account its overall simplicity, adaptability to different hardware and software, and flexibility.

Difference between AES encryption and DES encryption:

Up until 1999, when researchers employed a distributed computer system to crack the algorithm's 56-bit key, DES served as the cornerstone of government encryption. The US government made the decision to use AES in 2000 to protect sensitive data. In certain situations, DES is still used for backward compatibility.

Symmetric block ciphers are used by both protocols, while AES is theoretically more effective. AES's primary advantage is its key length.

An encryption technique's breaking time is closely correlated with the size of the key (128-bit, 192-bit, or 256-bit keys) used to secure the message. Consequently, AES's 56-bit keys are orders of magnitude weaker than DES's. Because AES encryption is faster, it is a great choice for firmware, programs, and devices that require high throughput or low latency.



Figure

AES 256 Encryption:

We are aware that encryption techniques mix up the data they are meant to secure, creating an unpredictable confusion.

All encryption is based on the basic idea that every data unit is replaced with a new one according to the security key.

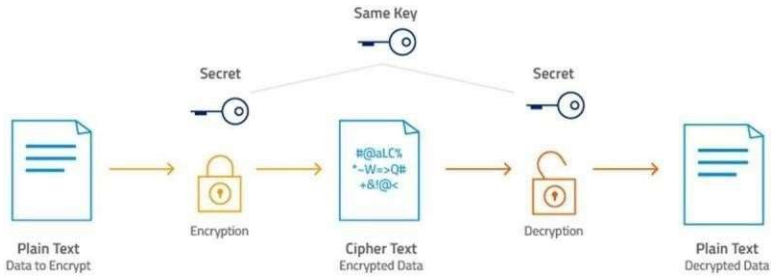


Figure 5.4

This encryption procedure consists of many rounds.

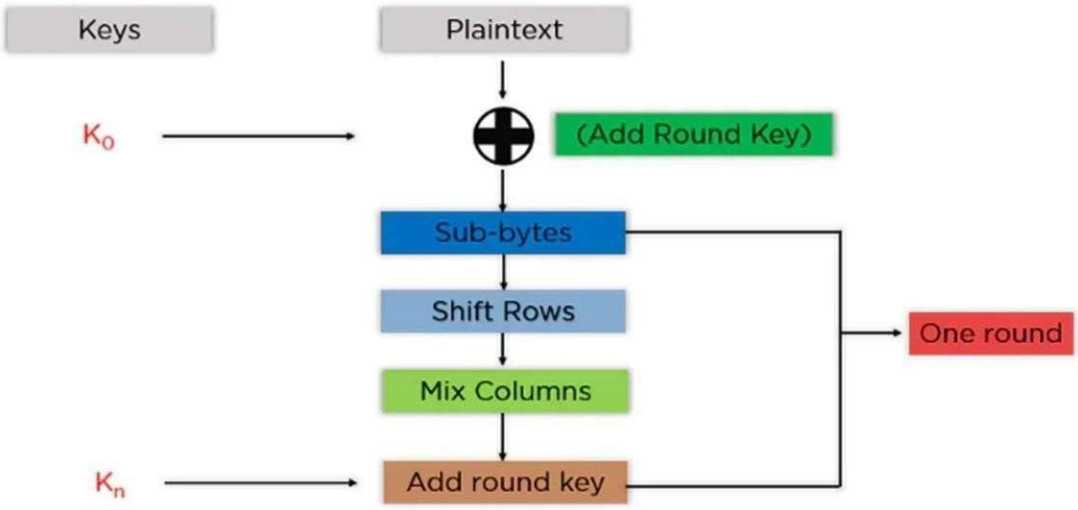


Figure 5.5

Add Round Key: The block data in the state array is combined with the first key generated using an XOR algorithm. The resultant state array is passed as an input to the phase that comes next.

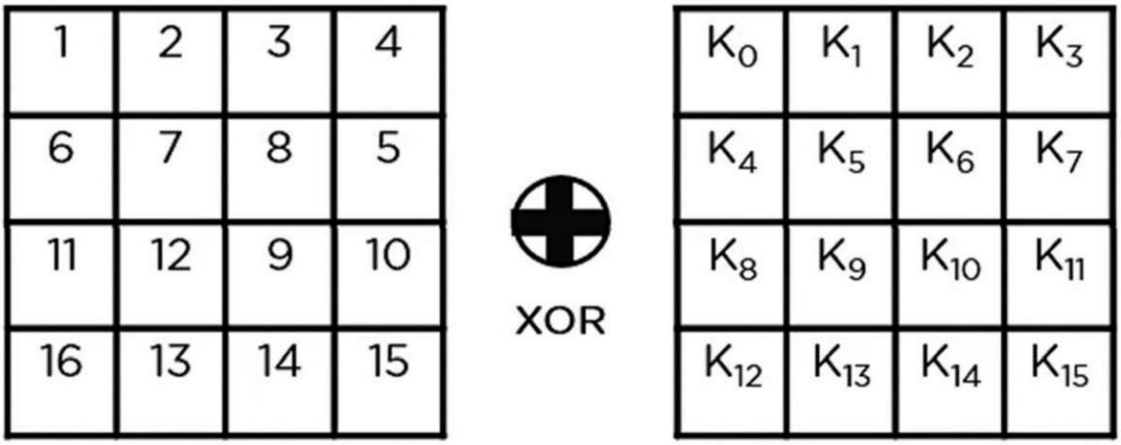


Figure 5.6

Sub-Bytes: Each byte from the state array is now split into two equal halves and converted to hexadecimal. These are the rows and columns that are mapped to the final state array in order to generate new values using a substitution box (S-Box).

19

Figure 5.7

Shift Rows: Row items are switched. It avoids the initial row. It shifts the parts in the second row to the left by one position. Additionally, it shifts the items in the last row three positions to the left and the third row's contents two places to the left.

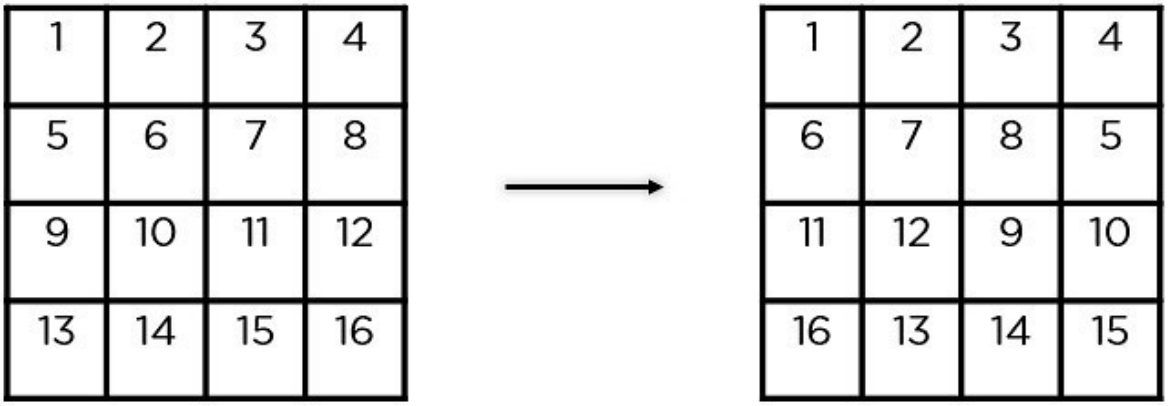


Figure 5.8

Mix Columns: To create a new column for the following state array, it multiplies a constant matrix by each column in the state array. You'll have your state array for the next step after multiplying each column by the same constant matrix. In the last round, this specific step is not to be finished.

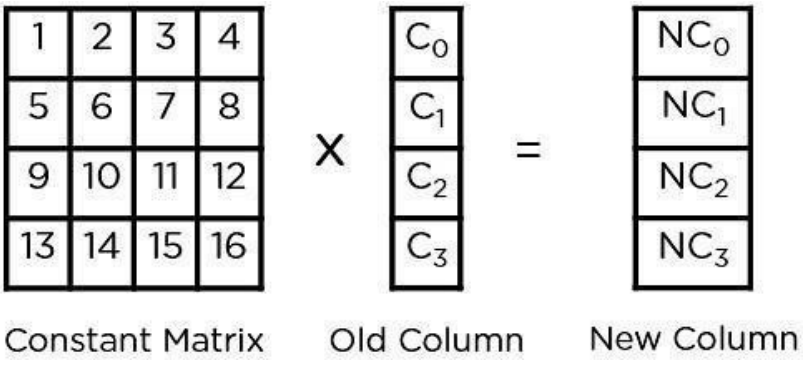


Figure 5.9

Add Round Key: The state array created in the preceding phase is XORed with the round's key. The resultant state array becomes the ciphertext for the designated block if this is the last round; if not, it becomes the new state array input for the next round.

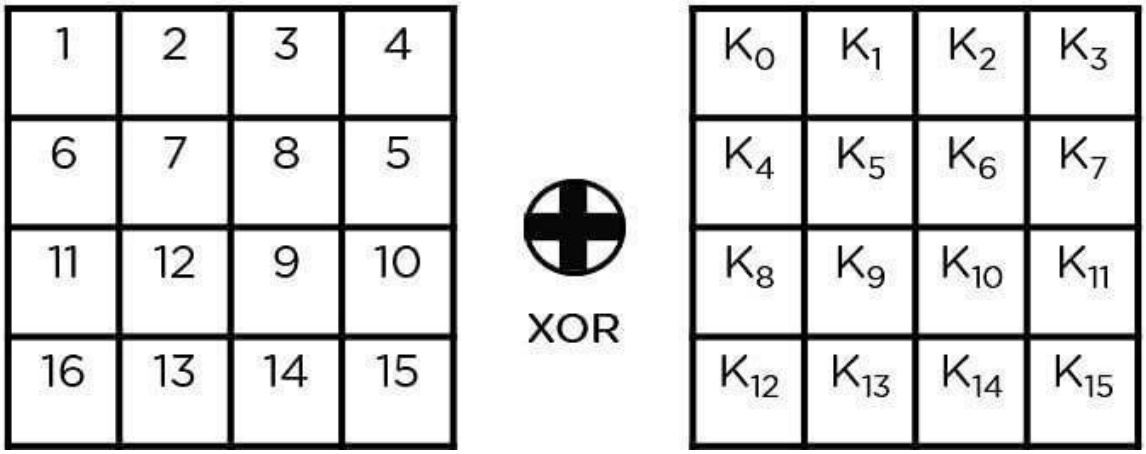


Figure 5.10

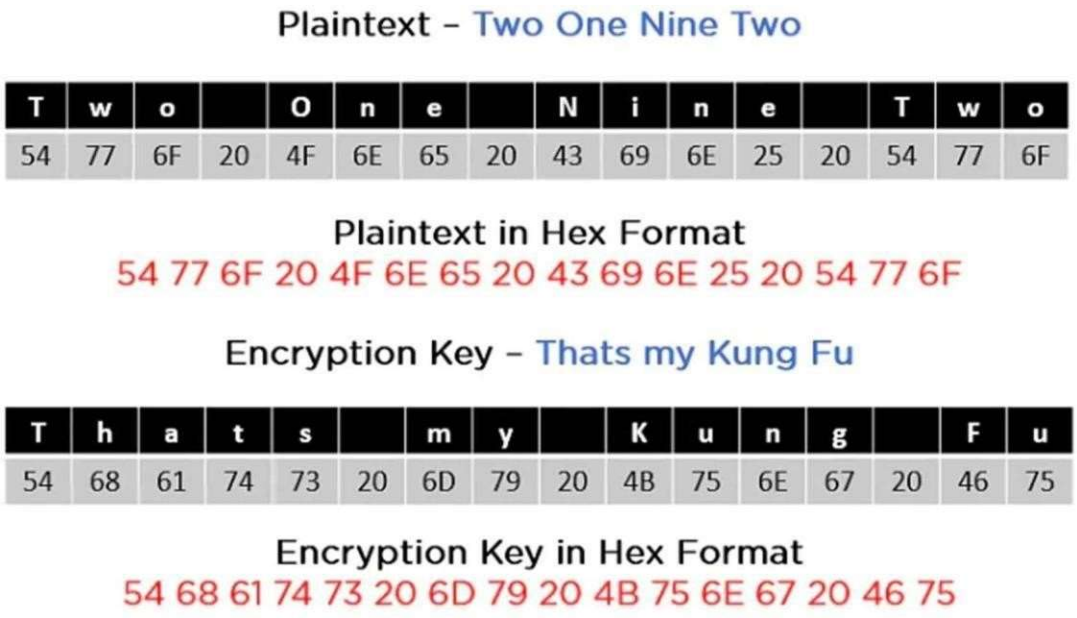


Figure 5.11

Plaintext and encryption first convert keys to hexadecimal format before starting operations, as seen in the above image. You may thus make keys for the following 10 rounds, as indicated below.

The above-described procedures must be repeated in order to extract the state array and send it on as input to the subsequent round. Here are the steps to follow.
Put a circular key there.

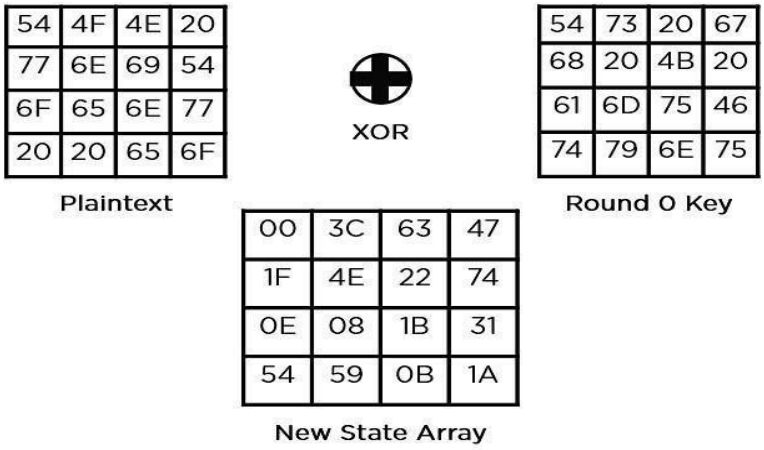


Figure 5.12

Sub-Bytes: To obtain a whole new state array, the elements are passed through a 16x16 S-Box.

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

New State Array

Figure 5.13

Shift rows,

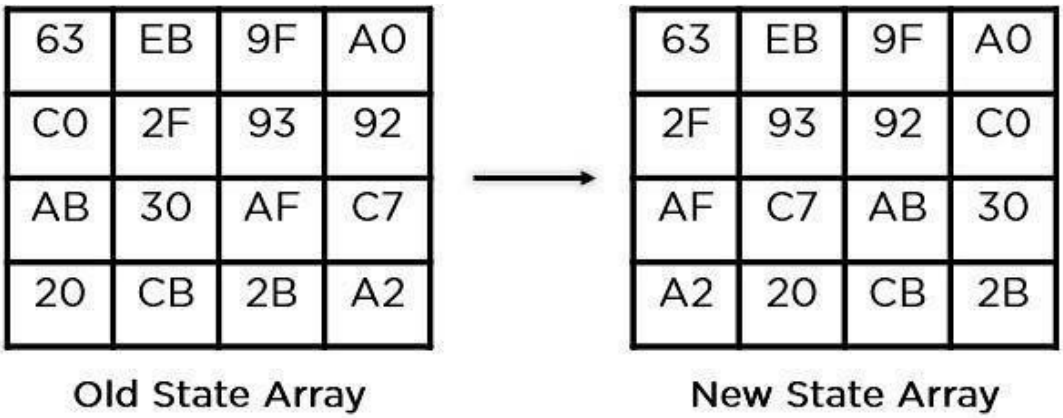


Figure 5.14

Mix columns,

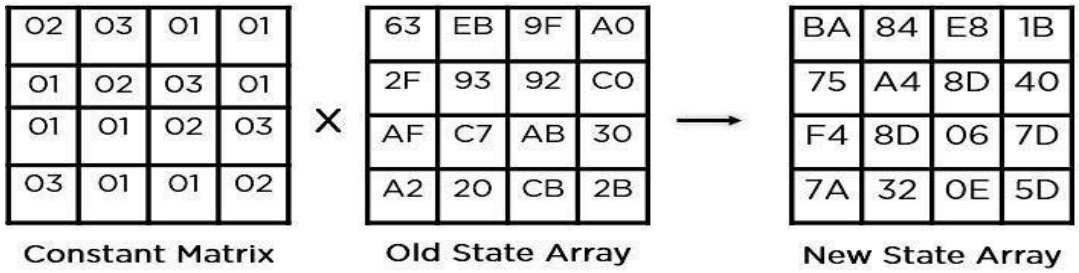


Figure 5.15

Add round key,

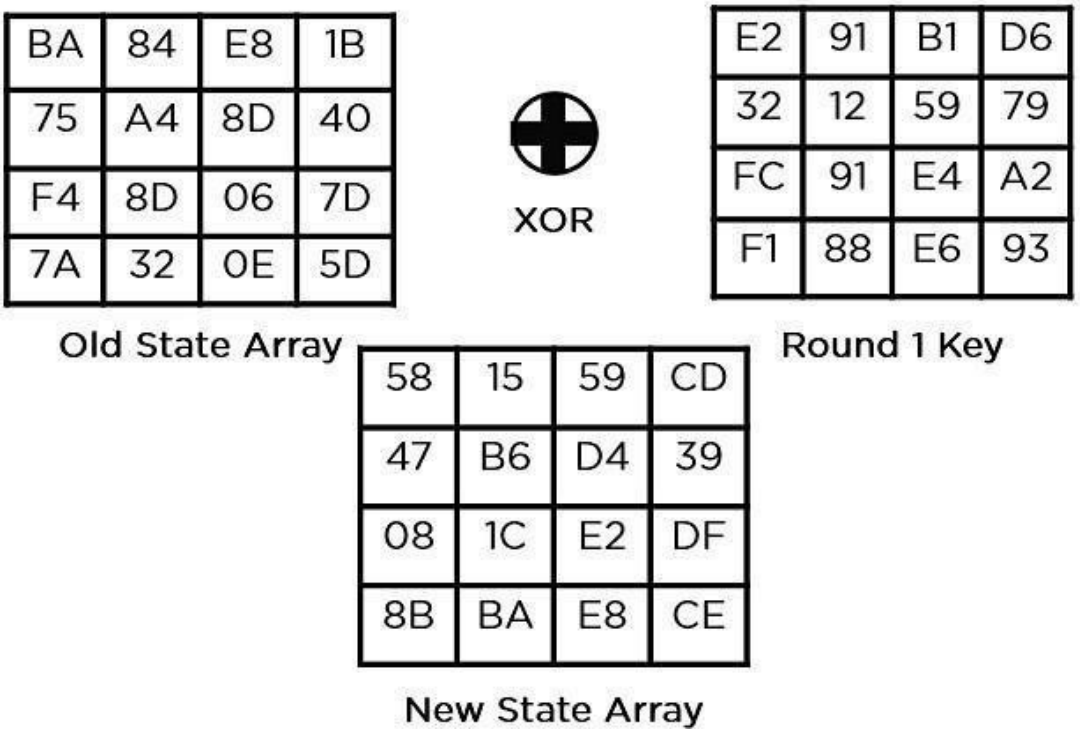


Figure 5.16

The final ciphertext for this round is now contained in this state array. This is used as the input in the subsequent cycle. Follow the aforementioned steps until round 10, at which time you will receive the final ciphertext, depending on the length of the key.

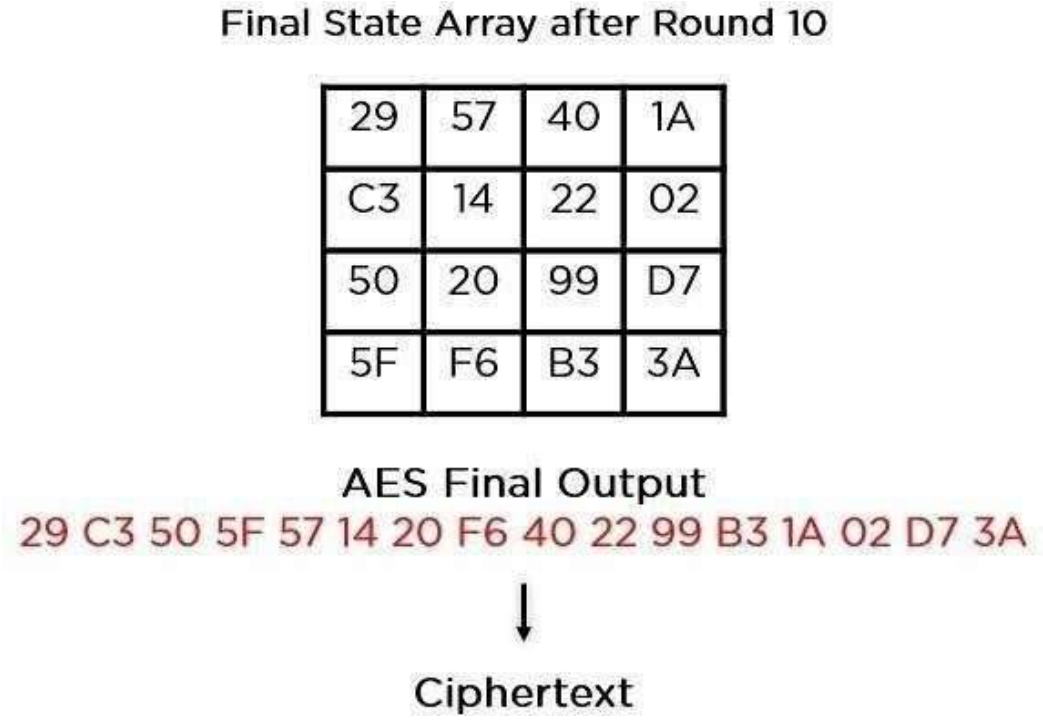


Figure 5.17

Application of AES:

- Advanced Encryption Standard is used by wireless networks for client and router authentication. Firmware software and all-encompassing security measures built on this technique are utilized by Wi-Fi networks and are currently in widespread usage.

- Secure website server authentication is guaranteed by AES encryption on both the client and server ends. This method helps SSL/TLS encryption methods to guarantee the best level of security and privacy when surfing by utilizing both symmetric and asymmetric encryption.

- AES is frequently used for business as well as encrypted data transfers between partners. Legal documents, family photographs, and chat discussions can all contain encrypted content.

- Processor Security: Among other low-profile issues, a lot of processor makers offer hardware-level encryption, including AES encryption, to bolster security and reduce meltdown failures. Processor Security: Among other low-profile issues, a lot of processor makers offer hardware-level encryption, including AES encryption, to bolster security and reduce meltdown failures.

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.

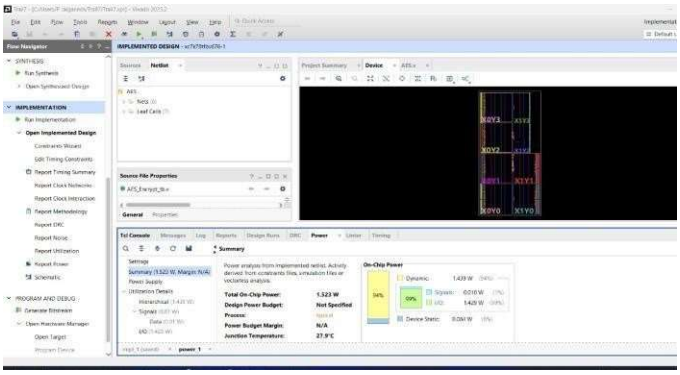


Figure 6.1

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.

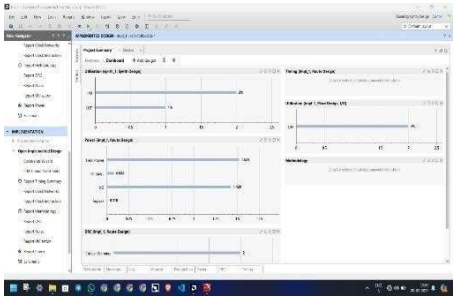


Figure 6.2

CHAPTER – 7

EXPERIMENTS OUTPUTS

Encryption:

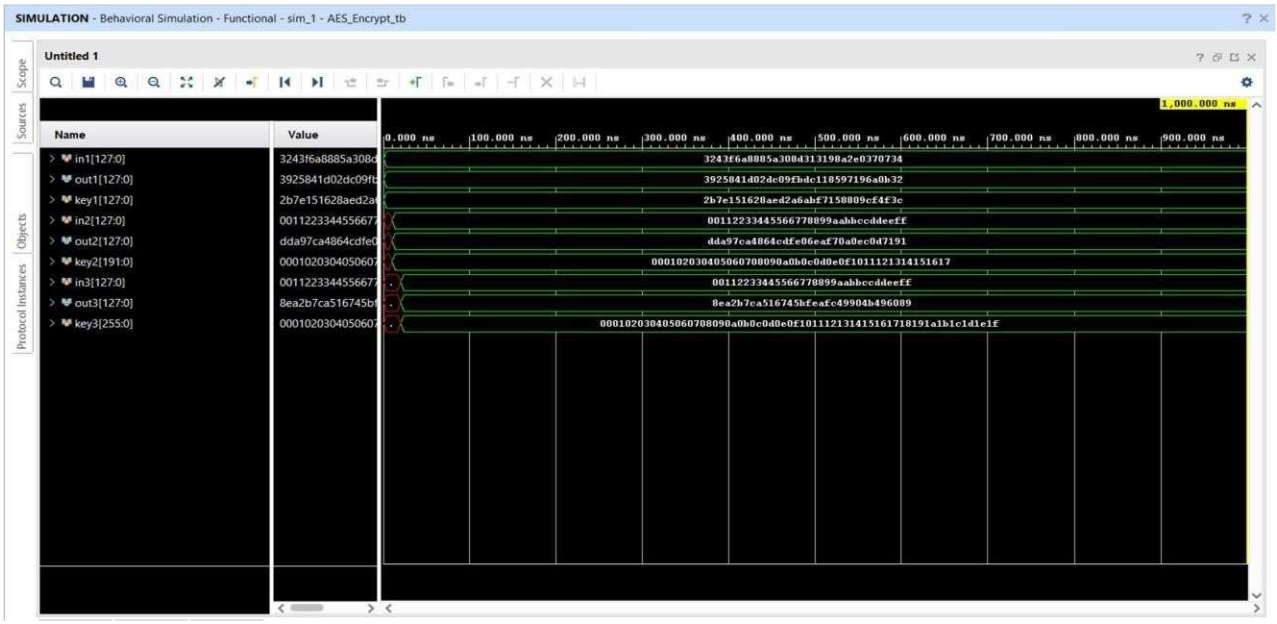


Figure 7.1

Decryption:

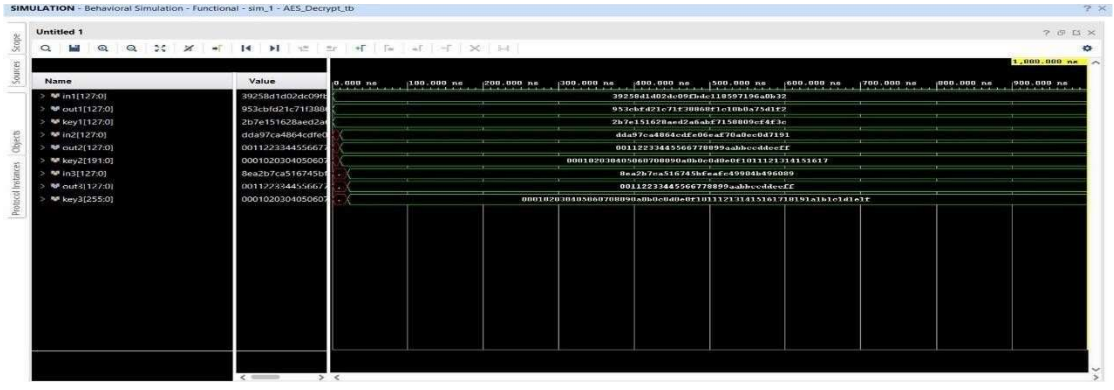


Figure 7.2

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

ACHIEVEMENTS

INNOVATHON 1.0 FINALISTS

SOLVEATHON 1.0 WINNER

Sairam Innovation Eco-system

Sairam SDG SOLVEATHON 1.0
Student Project Team of Innovators and Live in Lab Group

CERTIFICATE OF APPRECIATION

Sri SAIRAM ENGINEERING COLLEGE INSTITUTE OF TECHNOLOGY
Autonomous Institutions
West Tambaram, Chennai - 44

This is to certify that Mr. /Ms. JAI GANESH

of SEC / ECE has won 1st prize for

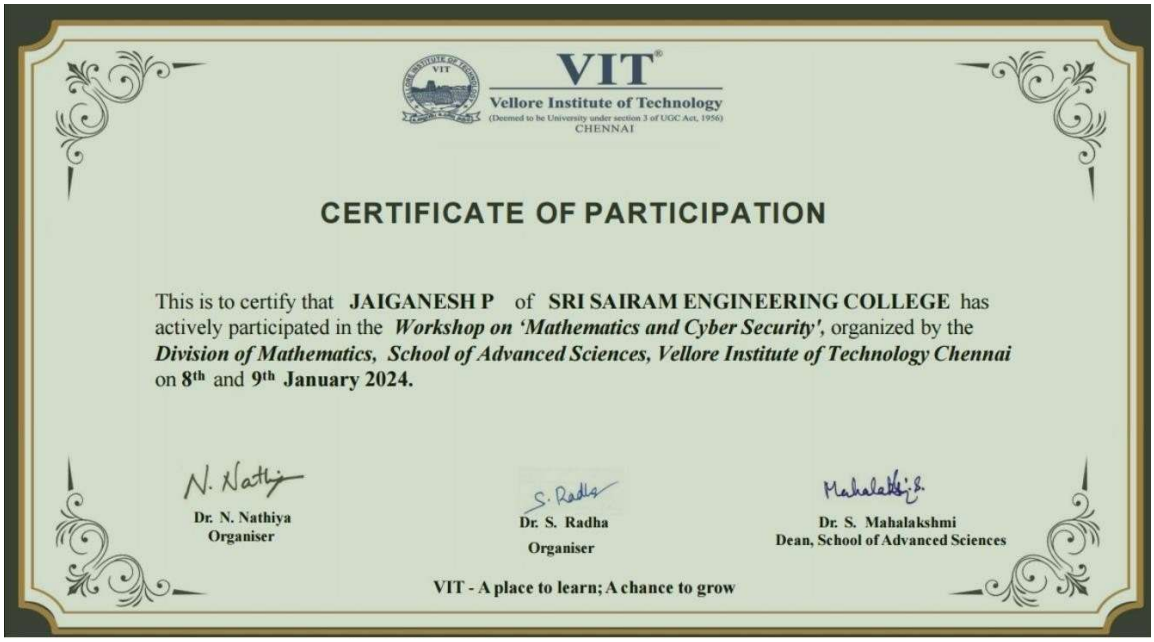
the project titled WIRELESS CHARGING OF ELECTRONICS DEVICES WCE under SDG Goal number 11

in Sairam SDG SOLVEATHON 1.0 - An event to convert student innovative ideas into product on 20th April 2022 & 21st April 2022

Dr. C. R. Rene Robin, Dean (Innovation)
Dr. K. Palanikumar, Principal
Dr. K. Porkumaran, Principal, Sri Sairam Engineering College
Sai Prakash LeoMuthu, Chairman & CEO, Sairam Institutions

Sairam RAISE EOMS · ARIIA EXCELLENT BAND · nirf · SUSTAINABLE DEVELOPMENT GOALS · Sairam

COURSES



VIT
Vellore Institute of Technology
(Deemed to be University under section 3 of UGC Act, 1956)
CHENNAI

CERTIFICATE OF PARTICIPATION

This is to certify that **JAIGANESH P** of **SRI SAIRAM ENGINEERING COLLEGE** has actively participated in the ***Workshop on 'Mathematics and Cyber Security'***, organized by the ***Division of Mathematics, School of Advanced Sciences, Vellore Institute of Technology Chennai*** on **8th** and **9th January 2024.**

Dr. N. Nathiya
Organiser

Dr. S. Radha
Organiser

Dr. S. Mahalakshmi
Dean, School of Advanced Sciences

VIT - A place to learn; A chance to grow

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.