Design of Advanced Encryption Standard Using Verilog HDL

Thipparthi Pooja
Dept. ECE
Institute of Aeronautical Engineering Hyderabad,
Telangana, India poojareddy0698@gmail.com

T. Spandana
Dept. ECE
Institute of Aeronautical Engineering Hyderabad,
Telangana, India spandana.thupalli@gmail.com

Chelle Radhika
Dept. ECE
Institute of Aeronautical Engineering Hyderabad,
Telangana, India radhikachelle@gmail.com

Dandu Maniteja
Dept. ECE
Institute of Aeronautical Engineering Hyderabad,
Telangana, India maniteadandu6@gmail.com

***Abstract*—Cryptography focuses on ensuring the security and integrity of data. Initially, various algorithms were developed for encoding and decoding, but many proved inadequate for protecting large and sensitive datasets. This led to the creation of AES, a robust standard for data encryption and decryption. Originally designed to safeguard highly confidential information, AES has since been adopted widely in networking applications to secure data. It primarily aims to protect sensitive information and is also utilized in network backends to bolster security. AES operates with 16-byte blocks and supports key sizes ranging from 128 to 256 bits. The choice of Verilog over standard VHDL is due to its reduced operational time and lower propagation delays in data encoding and decoding compared to other hardware description languages. Before AES, DES served as the encryption standard, but its limitation of a fixed 56-bit key size posed significant security risks. AES addresses this issue by allowing variable key sizes for enhanced flexibility.**

***Index Terms*—Advanced Encryption Standard, Input text, Cipher text, Verilog.**

I. Introduction

Data security is the prevention of misuse and unwanted access to the data. It is regarded as one of the basic com- ponents of information protection in almost every profession of data science. It is for this reason that digital security has gained such a tremendous demand, and AES remains the most commonly used encryption method [6].

AES is one of the most widely used standards for encryption which helps in securing data transmission over networks. To synthesize an AES-based circuit in Verilog HDL [3], a design of a digital system performing encryption/decryption has to be produced first. These are the fundamentals of AES, and its sub-components need to be explained. Each one of these steps is a fundamental part of both encryption as well as decryption operations. You will be able to express these components and

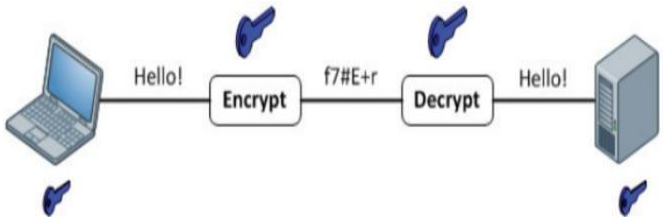


Fig. 1. Symmetric Encryption

their relationships in Verilog language in order to ensure secure encryption. Processing that would allow the capability to add the simplex AES encryption into a hardware encryption device that can be embedded with other devices like microprocessors or communications systems is available with the usage of Verilog HDL [5]. Compared to some software based and hardware accelerated methods, efficiency and speed increase significantly in terms of encryption.

In summary, the design of the figurative ”fortress” encryp- tion algorithms in the advanced hardware description language Verilog is implied by the Advanced Encryption Standard and is expressed in Hardware Description Language. The use of Verilog HDL allows one to design an encryption module that could consider interactions and operations be- tween various components of the AES system. The hardware module that is applied for encryption and decryption can be further described with the help of the behavioral and structural modeling elements of the Verilog HDL, and this particular module is functioning well. For proper secure encryption, together with the Verilog HDL, AES core procedures consist of AddRoundKey, MixColumns, SubBytes, and ShiftRows. The SubBytes operation simply uses a look-up table to perform byte substitution in the input data as a preprocessing step in preparation for its impending encoding. The two broad

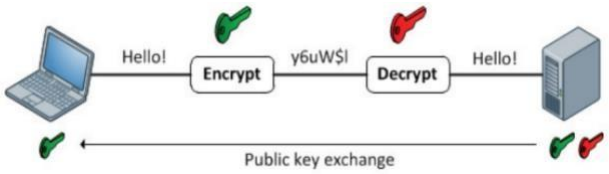


Fig. 2. Asymmetric Encryption

categories of cryptography are as follows:

1. Symmetric key encryption, whereby exactly the same key performs encryption for the message and decryption for the message.

2. Asymmetric Key Encryption In this type of encryption, two keys are used to secure information through both encryp- tion and decryption processes. The key is public as well as private.

Reorder Rows. Because the MixColumn operation also performs multiplication on the data columns of the matrix, this further muddles the waters. Plus, it further enhances security by XORing the data with the round key using the AddRoundKey operation [8]. Using Verilog HDL for the AES algorithm implementation leads to the generation of a hardware module that can be included within the devices such as microprocessors or communication hardware. Because its room software applies data encryption much faster and more efficiently than it is, this pure hardware acceleration is very helpful.

By using the coding of Verilog HDL, the encryption stan- dard is implemented in robust and efficient hardware within the architecture of AES. Most digital systems are protected by this implementation.

II. DATA ENCRYPTION STANDARD

The DES is an encryption technique that uses a symmetric key algorithm with 56 bits for the key to encrypt and decrypt the data. Once more, the DES breaks the data input for this process into blocks of 64 bits each, with encryption taking place through numerous iterations of both permutation and substitution. In this scenario, a round key scheduling determines the key sub-blocks for each round using the initial 56-bit key. A round consists of an initial permutation, an S- box replacement, another permutation, and finally a critical mixing step [15]. These operations are performed in a round, with the same subkeys but in an order different from that for the encryption step, to decrypt. While DES was important historically, its small key size and ease with which brute force attacks can be committed makes it a rather ineffective encryption system for security considerations today. Given that the scenario is so, one needs to recall that DES is no longer useful and that the most advanced encryption technique now in use simply due to its high level of security is Advanced Encryption Standard (AES). Knowing the

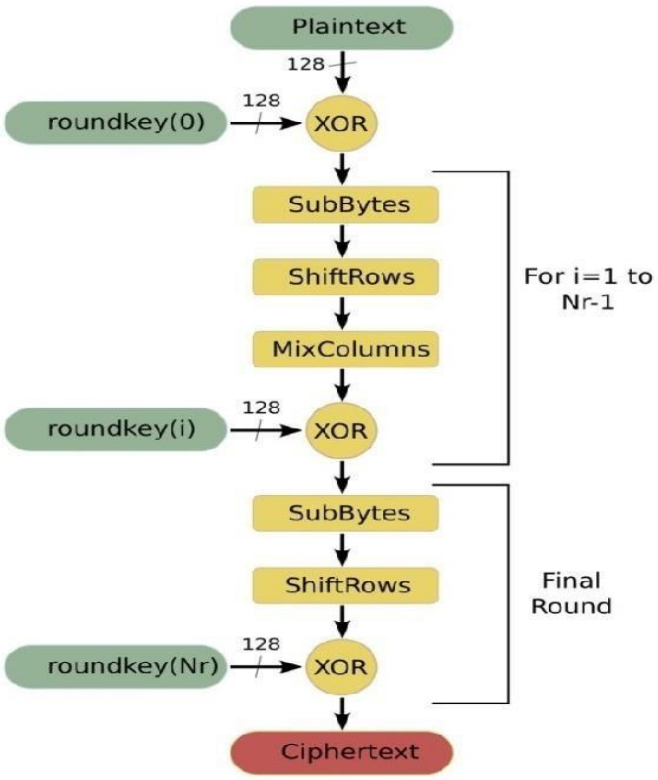


Fig. 3. AES Algorithm

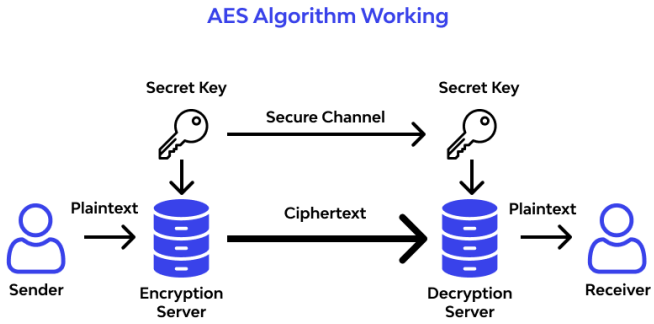


Fig. 4. Advanced Encryption Standard

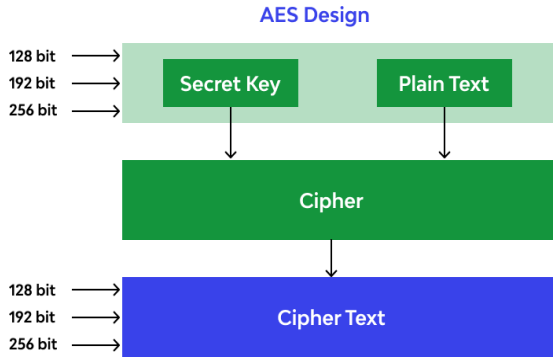


Fig. 5. AES Design

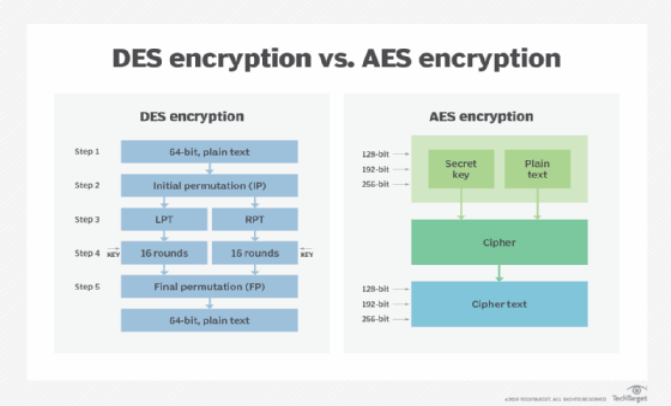


Fig. 6. DES VS AES

Data Encryption Standard (DES) symmetric-key algorithm is composed of sixteen complicated operations through an expansion, substitution, and permutation process in order to transform the input plaintext into ciphertext. It's a block cipher that processes data in 64-bit blocks using 56-bit key. Initially, this system was highly used; however, with its growth in computationally powered capability, it came under much criticism due to its short length of keys and vulnerability to brute-force attacks[6]. Imperfections in DES were overcome with Triple DES, an extension that raises the bar for data security by executing the encryption and decryption process three times utilizing a pair or trio of independent DES keys.

III. DES VS AES

Although DES and AES are the two symmetric encryption algorithms, the security and efficiency levels of these two algorithms differ immensely. As it was developed in the 1970s, DES has been one of the most commonly used encryption methods since its development time. It converts plaintext into ciphertext by using 16 substitutive and permutative cycles and a 56-bit key to encrypt data into 64-bit blocks. The DES algorithm was developed in the belief that there would never be a way to crack their code, but since computers were getting faster and speed technology advanced, brute force attacks were made which exposed the weakness of this technique. In response to the complexity of rising danger levels, one of the first solutions developed was Triple-DES, or 3DES. Since its key is a rather short 56 bits in size, Triple-DES encrypts and decrypts using a different 56-bit key assigned to an identical operation each time. Although better secured than traditional DES-based systems, users began to phase out 3DES because urned out to be ultimately too slow and inefficient.

According to ESTL, the Australian government installed AES, developed in 2001 to replace DES systems which eventually became obsolete since the enciphering was too easy. Unlike DES, AES is a better and faster algorithm developed by Rijndael and moreover selected by the National Institute of Standards and Technology (NIST)[14]. Furthermore, as its specifications support key lengths of 128, 192 and 256 bits, it is far better placed to resist any brute force attacks [12].

parameter	DES	AES
Key length	56 bits	128 bits
Block length	64 bits	128 bits
Rounds	16	10

Fig. 7. Table-1

The number of encryption rounds for AES is dependent on the size of the key; for 128 bit keys it is 10, for 192-bit keys it is 12 and for 256 bit keys it is 14. Block size for AES is 128 bits [7]. Owing to these factors, as well as its high speed and ability to defeat all modern threats, AES has become the encryption system of choice in many applications such as file encryption, VPNs and wireless security.

This is not to say that DES and AES are both encryption systems that can be used exactly the same way; they actually carry quite a lot of difference when it comes to the issue of efficiency and security[10]. Data Encyption Standard, for instance, DES is characterized by usage of 56 ks and the 64 data blocks. However, today's computing capacity allows attacks carried against any known encryption

systems making many including DES quite risky for users.

Advanced Encryption Standard (AES) is in a different league as it is a more efficient and secure encryption standard. In discussing, AES vs DES one can use keys bearing sizes of 128, 192 or 256 bits making it even more attack resistant. AES works with 128 data blocks and more advanced encryption technique like several rounds of mixing up the key, subtitutions and permutations.

IV. LITERATURE OVERVIEW

In the field of cryptography, the design and implementation of the Advanced Encryption Standard (AES) in the Verilog hardware description language has received great interest in the academic and industrial research because of the growing

AES Bits	Key Length (Nk)	Block length (Nb)	No of Rounds (Nr)
128bit	4	4	10
192bit	6	4	12
256bit	8	4	14

Fig. 8. Table-2

necessity for secure and efficient cryptographic hardware. As there is a rise in the already existing high demand of secure and efficient cryptographic hardware, design and implemen- tation of Advanced Encryption Standard (AES) using Verilog Hardware Description Language (HDL) has attracted a lot of attention in academic and industrial research. It is common knowledge that when an application requires high-speed en- cryption with low power consumption and high security, then hardware implementation of advanced encoding standards is a must, as blockades are mostly done in software. This is because of the wide range of usage of the algorithm, and its capable robust applications. Thanks to the power of the widely-known hardware description language Verilog HDL, it is possible to characterize the ASE algorithms at the hard- ware level, thereby optimizing the resource and performance. Several studies [8] have addressed some of the primary AES hardware design optimization approaches such as fundamental expansion, SubBytes transformations, and MixColumns op- erations. For higher performance, more emphasis is put on additional pipelining and parallelism.

Additionally, research often explores the balance among speed, area, and power, modifying AES designs for specific applications including secure communication protocols[1], embedded systems, and IoT devices. In the software imple- mentation of AES, the literature on Verilog suggests that certain accelerators improve the performance-to-security ratio of the encryption systems, making them faster than software systems and more resistant to side channel attacks[3].

V. DATA SECURITY IN AES

The use of strong encryption and advanced cryptologic mechanization protects the data in AES encryption. [6] Stronger algorithms and dependable encryption methods offer protection for data in AES. Advanced Encryption Standard, also known as AES, manages to secure the information from brute force attacks by employing key elements such as key sizes of 128, 192 or 256 bits. AES encodes the data more securely by using distinct rounds of enciphering that incor- porates substitution, transposition and key mixing techniques. AES prohibits a simple linking of input data and output data by using S-box substitution which applies non-linear transformations on the input data and expands the encryption process. AES enhances the security by incorporating aspects of diffusion and confusion that makes intermingling of encrypted data and plaintext orderly arranged making it difficult to

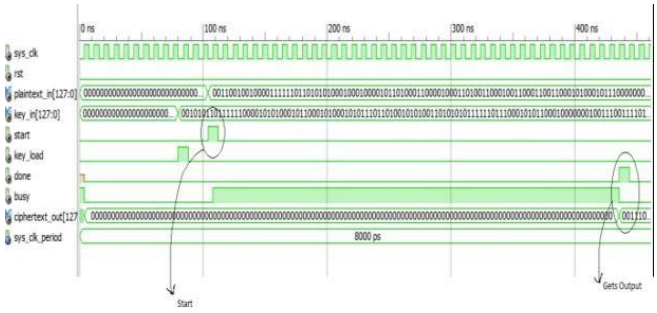


Fig. 9. Timing Diagram of AES encryption

separate the two. Based on the given, even more, complication is added to the encoder as masterpieces of expansion of keys are provided for each enciphering cycle instead of a single key used in a classical encryption. All these measures enhance the data security enabling system of AES and secure transfer of data in a variety of systems well above average [9]. It is important to mention that since AES employs symmetric encryption similar key is required for both encrypting and decrypting the data. This helps maintain high levels of security measures but makes the process easier for the authorized individuals.

In addition, AES has been and continues to be thoroughly tested by cryptographers and practitioners form every corner of the earth who have shown how reliable and resistant it is to different cryptographic

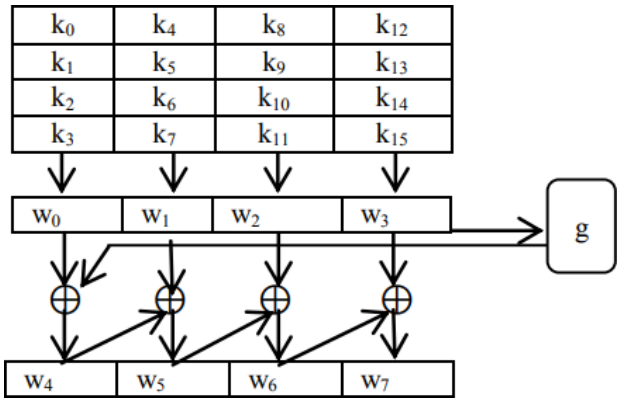
attacks. Its wide application in the finance, trade, and state sectors is a good indicator of its reli- ability and efficiency in the field of safety of information[11]. This is one of the best encryption method available in the market today due to its security without compromising on speed. It is due to these advantages that it can be applied in many places, from the encryption of voice calls over the internet to the storage of private information in devices[16].As a useful encryption standard for assuring confidentiality as well as data integrity and authenticity in a sophisticated digital world, AES has embraced these modern approaches to encryption along with extraordinary safety features.

VI. Advanced Encryption Standard Algorithm

The Advanced Encryption Standard (AES) algorithm be- longs to the universal algorithm family and is widely used in symmetric encryption. It has adopted several key sizes which are 128, 192 and 256 bits respectively, while it operates on fixed block sizes of 128 bits[10]. Capable of longer key lengths, AES consists of several core components includ- ing SubBytes, ShiftRows, MixColumns, and AddRoundKey transformations. These transformations are applied in multiple rounds, based on the chosen key length.

The enciphering procedure can be characterized as a series of rounds each of which alters the input plaintext in its unique way by means of substitution and permutation processes, thereby making the input more complex. In order to ensure that differentkeys are applied in each of the encryption rounds, the

Fig. 10. AES block diagram



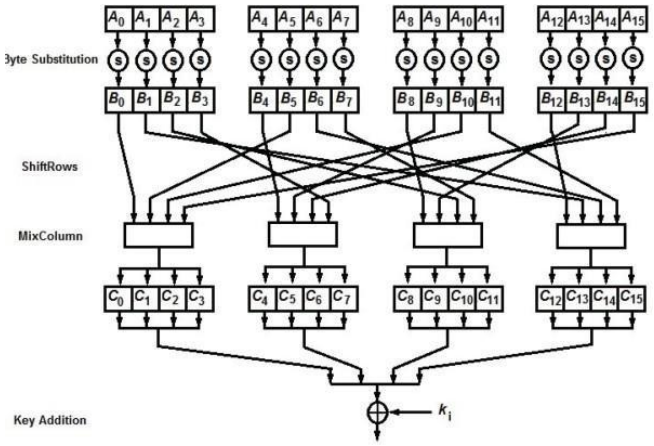


Fig. 11. Key Expansion Algorithm

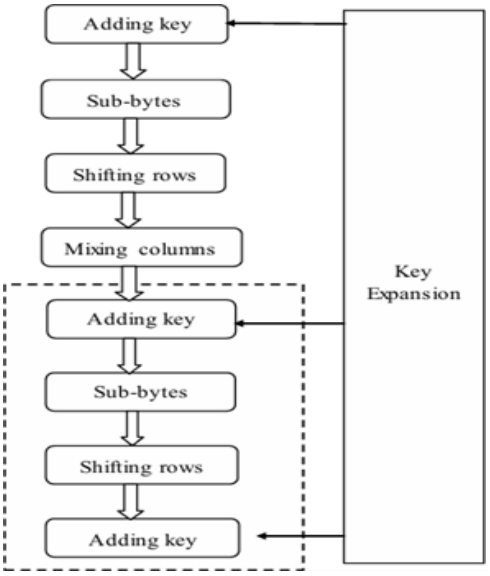


Fig. 12. AES Round Function

key expansion methods grow round keys based on the original encryption key. These factors combined further contribute to the overall strength and security of the AES cryptosystem.

In AES, decryption is exactly the reverse of encryption. Once the ciphertext is provided, the sequence of operations is carried out in reverse along with the use of round keys in reverse order to get back the original plain text. Acquiring the right key makes it easier for authorized users to decrypt the information without a hassle, which is a big advantage due to the symmetric aspect of AES [5].

1. Key Expansion: To develop a set of round keys from the earlier stated encryption key is an aspect added by the AES algorithm. These round keys are employed in each additional encryption round to boost security and level of difficulty.

Initial Round: AddRoundKey: The primary level of ciphering is incorporated by taking the plain text and performing XOR operation with the first round key generated. 3. Rounds: With the exception of the very last one, every AES round consists of four fundamental operations.

- SubBytes: During this operation, each byte existing in the state matrix is substituted with a different byte by looking up in a fixed substitution table called S – box.

- ShiftRows: This operation translates the rows of the state matrix to the left. There are four rows, row 1 remains in the same place, row 2 moves to 1 position, row 3 to 2 positions, and row 4 shifts to three positions left.

- MixColumns: Due to a mathematical function that mixes the columns of the state matrix, there is a diffusion of the data.

- AddRoundKey: In this operation the cipher key in state matrix is modified by XORing each byte of the state matrix with a round-specific expanded key.

4. Final Round: - In order to facilitate decoding, the final round does not make use of the MixColumns transformation.

5. Result: - The so-called state matrix, which is the artwork state after the last round, is the transformed image of the initial clear text, referred to as ciphertext.

It is known as Advanced Encryption Standard (AES) which is a symmetric encryption algorithm developed by NIST and adopted back in the year 2001 and widely used because of its rapidness, safety, and versatility in many functions including encrypting data over wireless networks, VPNs and file systems. AES data is split into blocks of 128 bits and can operate on three different key sizes of 128 bits, 192 bits or 256 bits based on the level of security required[11]. Key Expansion: AES starts with a primary key and goes through a procedure to obtain a total collection of round keys which the number of the later depends on the size of the encryption key.

1.Rounds: The algorithm performs a number of repetitive cycles known as rounds of encryption; the respective rounds for keys of128 bits, 192 bits, and

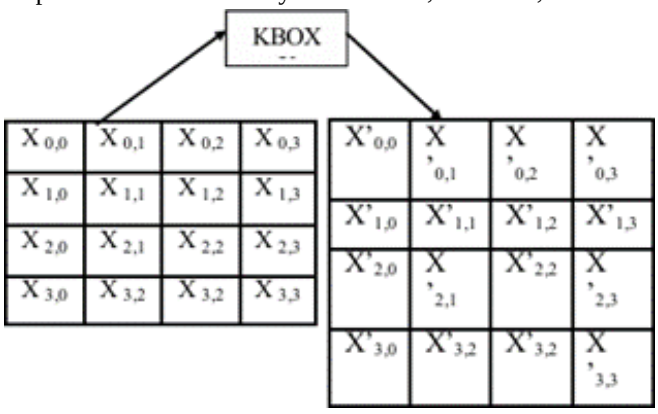


Fig. 13. Sub Bytes

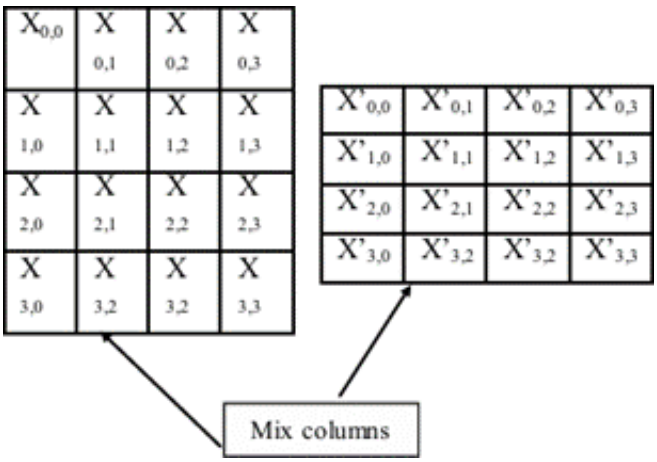


Fig. 15. Mix columns

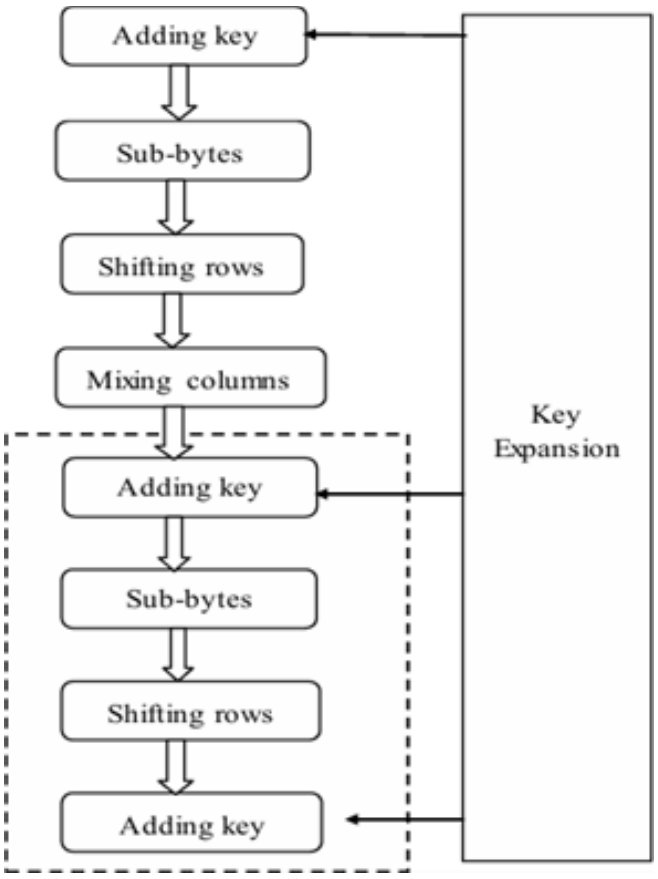


Fig. 14. Shift rows

SubBytes: Each byte of the state is replaced with a related byte from the Substitution box (S-box) that adds non-linearity to the cipher.

3. ShiftRows: Transfer the rows of the state over a number of places in a circular manner to enhance diffusion, that is dispersion (in both the rounds and the columns).

4. MixColumns: Mix the information contained in every column for better diffusion (except for the final round). 5.Ad- dRoundKey: XOR the state with a round key to key K derived from the original key. This is the layer which requires most of the security features.

Final Round: This final round as compared to the other rounds is special because there is no MixColumns step. How- ever, the algorithm could not have transformed data completely into ciphertext that cannot be cracked.

AES Properties: There must be two processes, encoding and decoding, in symmetric encryption. The same key must be used for both processes. Block Cipher: In AES, the data often gets encrypted by block format with a fixed block size of 128 bits. Security: Due to the large number of keys employed and the highly complex procedure of transformations, AES has been designed in such a way so as to be vulnerable to all types of cryptanalysis and even to the malicious intent- including brute force techniques of attacks.

In fact, decryption in AES is carried out using the same steps as in encryption, but a little differently in that the round keys are applied in the reverse order in order to convert ciphertext to plaintext [18]. The decryption functions are ex- actly opposite to the SubBytes, ShiftRows, and AddRoundKey functions, apart from the addition of In MixColumns.

The above-mentioned order of operations when applied to AES encryption guarantees high security and confidentiality of the protected information.

VII. DESIGN AND IMPLEMENTATION

The Advanced Encryption Standard allows for 128, 192, or 256 bits. That is where the comparisons of encryption strength start. Its block size is 128 bits, which d

=128'h86C8705F870950F8944288B67A09D89A clock=1
key=128'h4598989823706D97204B896E89206475

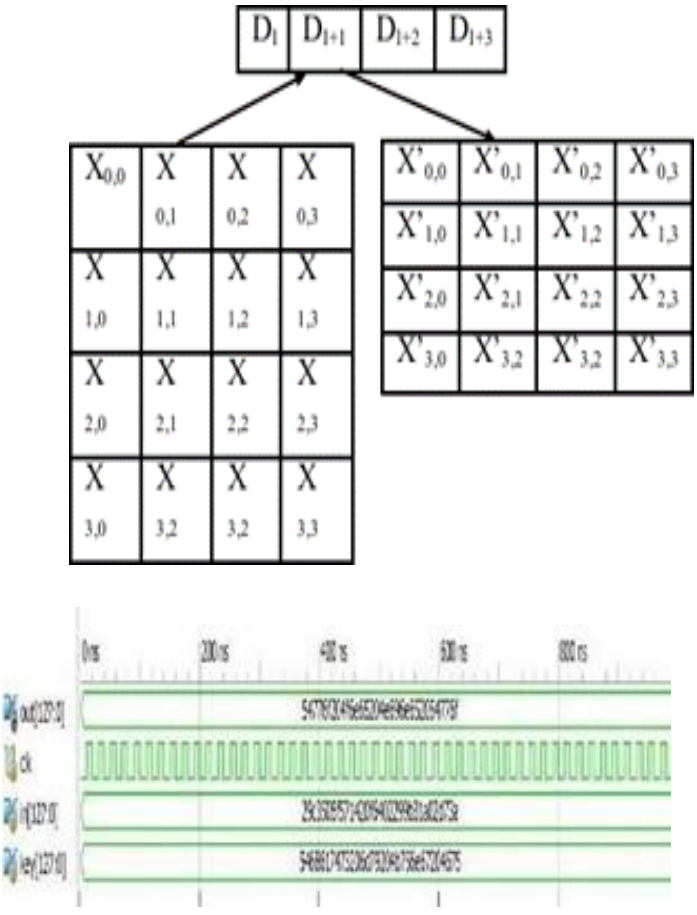
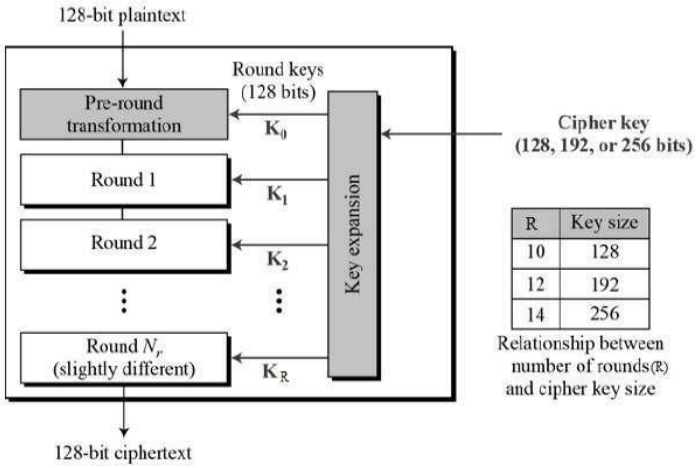


Fig. 16. Adding rounding Key

Ten rounds are used for 128-bit keys, twelve rounds for 192-

Output:

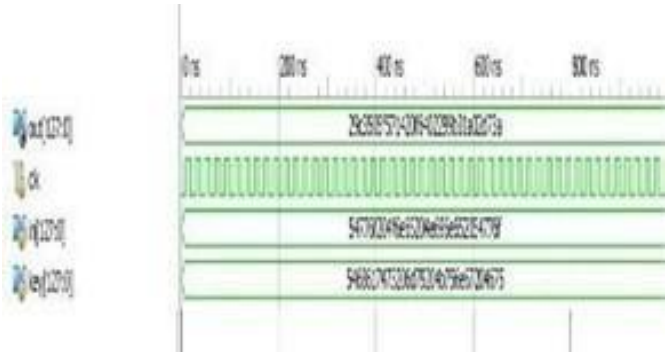
Fig 17:encryption output



bit keys, and fourteen rounds for 256-bit keys[5]. Some of the steps include Sub- Bytes substitution, ShiftRows shifting, MixColumns mixing, AddRoundKey XOR operations, and a type of implementation of getting round keys through key expansion [10].

VIII. Results and Observations

A. Simulation result of encryption: Input:
in=128'h67544F402F6E20567E969E025667745F
clock=1
key=128'h4598989823706D97204B896E89206475



Output:
plain
txt=128'h7653459081456c898f876245676d0d0aPlaintx
t=128'h7653459081456c898f876245676d0da

Fig 18 : AES

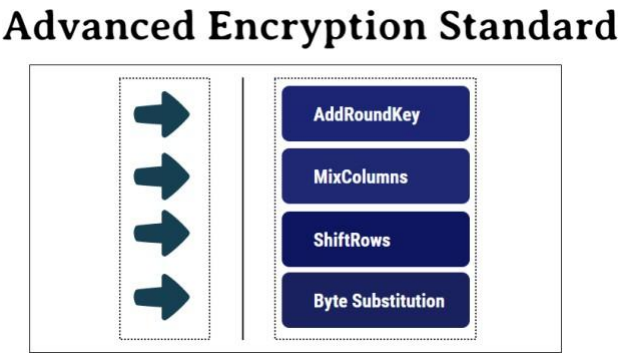
IX. Conclusion

The Advanced Encryption Standard is a method of encoding for sensitive data that is reliable, effective, and widely used. The primary reason for this is the variation in the various applications of data today or its designed of fixed data block with flexible key length and many rounds. Systematic use of this design has been proved to be quite useful in the process of encoding and decoding any message, therefore cryptography based on this approach has found a lot of application in the contemporary world.

In the future, it is expected that more research and de- velopment will be conducted on AES to improve its design and performance under new digital threats, like quantum computers. As quantum computing reaches its gains, new approaches to cryptography including alterations to AES may be sought in order to safeguard information from changing technologies.

Additionally, in various computing environments, the effi- ciency of AES implementations can also be improved through the use of hardware acceleration, optimization, and the appli- cation of parallel processing techniques. All things considered; AES is a core basic encryption standard that has means to be enhanced and altered for the changing landscape of cybersecurity threats.

Fig19:AES



References

[1] Jamal, K., Chari, K. M., Srihari, P. (2019). Test pattern generation using thermometer code counter in TPC technique for BIST implementation. Microprocessors and Microsystems, 71, 102890.

[2] Hady Mohamed Soliman, Baher Magdy and Mohamed A. Abd E1 Ghany, "Efficient implementation of the AES algorithm for security applications", IEEE 2016.

[3] J. Daemen and V. Rijmen, The block cipher Rijndael, Smart Card Research and Applications, LNCS 1820, Springer- Verlag, pp. 288-296.

[4] Jamal, K., Srihari, P., Kanakasri, G. (2016). Test Vector Generation using Genetic Algorithm for Fault Tolerant Systems. International Journal of Control Theory and Applications (IJCTA), 9(12), 5591-5598.

[5] Kumar, A., Gupta, R. (2016). Design and implementation of AES algorithm in Verilog. International Journal of Engineering Research and Technology, 5(4), 217-220.

[6] J. Orlin Grabbe, "The DES algorithm illustrated".

[7] Zabina Kouser, Manish Singhal, and Amit M.Joshi, "FPGA imple- mentation of Advanced encryption standard algorithm", IEEE Interna- tional Conference on Recent Advances and Innovations in Engineering, (ICRAIE-2016).

[8] Jamal, K., Srihari, P., Chari, K. M., Sabitha, B. (2018). Low power test pattern generation using test-per-scan technique for BIST implementa- tion. ARPN Journal of Engineering and Applied Sciences, 13(8).

[9] Mohini Mohurle and Vishal V. Panchbhai, "Review on the realization of AES encryption and decryption with power and area optimization",1st IEEE Conference on Power Electronics, Intelligent Control and Energy system (ICPEICES-2016).

[10] Yehya A. Nasser, Mohammad A. Bazzoun, Samih Abdul Nabi, "AES algorithm implementation for a simple low- cost portable 8-bit micro- controller", IEEE 2016.

[11] Hrushikesh S. Deshpande, Kailash J. Karande, Altaaf O. Mulani, "Efficient implementation of AES algorithm on FPGA", International conference on communication and signal processing, 2014.

[12] Jamal, K., Srihari, P. (2015, January). Analysis of test sequence generators for built-in self-test implementation. In 2015 International Conference on Advanced Computing and Communication Systems (pp. 1 4). IEEE.

[13] Ayushi, "A symmetric key cryptographic algorithm", International jour- nal of computer applications (0975- 8887), Volume 1-no.15,2010.

[14] "AES 128- A C implementation for encryption