International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 06 Issue: 03 | March - 2022 ISSN: 2582-3930

Research Paper on A Detailed Evaluation on Advance Encryption Standard Algorithm

POOJA BALAN MORE

Student, Dept. of B.Sc. I.T, Model College, Dombivli, Mumbai, Maharashtra, India

***Abstract*—**Encryption is that the peace officer that forestalls a Wild West-type situation from ever happening. It offers businesses complete assurance that their information are going to be protected, and nobody will it higher than AES encoding**.-**Cryptography is the study of mathematical techniques related to aspects of information security such as confidentiality, data integrity, entity authentication and data origin authentication. In data and telecommunications, cryptography is necessary when communicating over any unreliable medium, which includes any network particularly the internet. In this paper, a 128 bit AES encryption and Decryption by using Rijndael algorithm (Advanced Encryption Standard algorithm) is been made into a synthesizable using Verilog code which can be easily implemented on to FPGA. The algorithm is composed of three main parts: cipher, inverse cipher and Key Expansion. Cipher converts data to an unintelligible form called plaintext. Key Expansion generates a Key schedule that is used in cipher and inverse cipher procedure. Cipher and inverse cipher are composed of special number of rounds. For the AES algorithm, the number of rounds to be performed during the execution of the algorithm uses a round function that is composed of four different byte-oriented transformations: Sub Bytes, Shift Rows, Mix columns and Add Round Key.

Keywords-**Advanced Encryption Standard, Cryptography, Decryption, Encryption**

1.INTRODUCTION

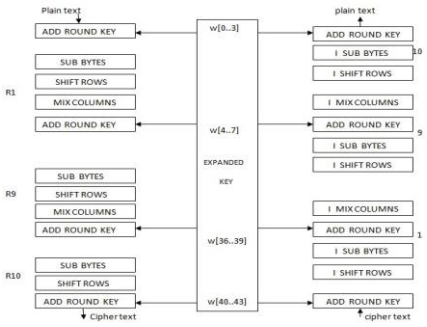
THE Cryptography plays an important role in the security of data transmission This paper addresses efficient hardware implementation of the AES (Advanced Encryption Standard) algorithm and describes the design and performance testing of Rijndael algorithm.A strong focus is placed on high throughput implementations, which are required to support security for current and future high bandwidth applications . This implementation will be useful in wireless security like military communication and mobile telephony where there is a gayer emphasis on the speed of communication This standard specifies the Rijndael algorithm, a symmetric block cipher that can process data blocks of 128 bits, using cipher keys with lengths of 128,192, and 256 bits. Throughout the remainder of this standard, the algorithm specified herein will be referred to as ―the AES algorithm.‖ The algorithm may be used with the three different key lengths indicated above, and therefore these different ―flavors‖ may be referred to as ―AES-128‖, ―AES192‖, and ―AES-256‖.

2.What is AES algorithm?

AES is brief for Advanced secret writing customary and may be aUnited States secret writing customary outlined in

Federal information science customary (FIPS) 192. AES is that the most up-to-date of the four current algorithms approved for federal United States within the u. s.. AES may be a regular secret writing rule process information in block of 128 bits. AES is regular since constant secret's used for secret writing and also the reverse transformation, coding [2]. the sole secret necessary to stay for security is that the key. AES might designed to use totally different key-lengths, the quality defines three lengths and also the ensuing algorithms square measure named AES-128, AES-192 and AES-256 severally to point the length in bits of the key. The older customary, DES or encoding customary. DES is upto 56bits solely [4]. to beat the disadvantages of des rule, the new customary is AES rule. This customary expressly defines the allowed values for the key length (Nk), block size (Nb), and range of rounds (Nr).

B.AES algorithm specification:For the AES algorithmic rule, the length of the input block, the output block and also the State is 128 bits. This is often delineated by Nb = four, that reflects the quantity of 32-bit words (number of columns) within the State.



Fog 1 General structure of AES algorithm

An implementation of the AES algorithmic rule shall support a minimum of one among the 3 key lengths: 128, 192, or 256 bits (i.e., Nk = 4, 6, or 8, respectively). Implementations could optionally support 2 or 3 key lengths, which can promote the ability of algorithmic rule implementations. For the AES algorithmic rule, the length of the Cipher Key, K, is 128, 192 or 256 bits. The key length is diagrammatical by Nk = four, 6, or 8which reflects the quantity of 32-bit words (number of columns) within the Cipher Key. For the AES algorithmic rule, the quantity of rounds to be performed throughout the execution of the algorithmic rule is Nk = six, and Nr = fourteen once Nk = eight. The sole Key-Block-Round mixtures that adapt to the current normal area unit given in Table

Bit pattern	**Key length (NK words)**	**Block size (Nbwords)**	**No of Rounds (Nr words)**
AES-128	4	4	10
AES-192	6	4	12
AES-256	8	4	14

Table 1. Key-Block-Round Combinations.

The following characteristics make AES encryption extremely software and hardware friendly:

- Immune to all known attacks
- Speed and compatibility of source code on various computing platforms
- Simplicity of design

AES secret writing is that the gold normal of secret writing. Period. You see it with electronic communication apps like WhatsApp, organizations coping with sensitive information like independent agency, school giants like Microsoft and diverse tiny businesses round the world

2.Encryption

In coding mode, the initial secret's other to the input price at the terribly starting, that is named Associate in Nursing initial spherical. This can be followed by nine iterations of a traditional spherical and ends with a rather changed final spherical, joined will see in Figure two. Throughout one traditional around the following operations ar performed within the following order: Sub Bytes, Shift Rows, combine Columns, and Add spherical key. The ultimate spherical could be a traditional spherical while not the combo Columns stag

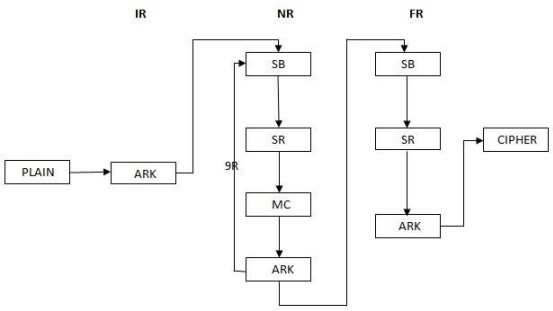


Fig 2 A general structure of encryption

Steps in AES coding

• Sub Bytes—a non-linear substitution step wherever every computer memory unit is replaced with another consistent with a operation table.

• Shift Rows—a transposition step wherever every row of the state is shifted cyclically a particular range of steps.

• Mix Columns—a compounding operation that operates on the columns of the state, combining the four bytes in every column

• Add spherical Key—each computer memory unit of the state is combined with the spherical key; every spherical secret is derived from the cipher key employing a key schedule

3.History of AES algorithms

- **The 1970's-Birth of DES .**

The U.S. National Bureau of Standards (NBS) required a surreptitious formula to code sensitive government info. Their search light-emitting diode them to a regular key algorithm: encryption customary (DES). Over succeeding few decades, DES was the indisputable champion within the world of cryptography.

- **The 1997-The fall of DES.**

The nineties saw an increase in improved computing power, because of that the 56-bit key rule became susceptible to brute-force attacks. The National Institute of Standards and Technology (NIST) proclaimed a public competition to search out a DES replacement.

- **The 1999 DES broken**

The Electronic Frontier Foundation designed a DES cracker that with success brute-forced the formula in mere twenty two hours and quarter-hour (less than on a daily basis

- **2001-AES win**

NIST proclaimed AES because the winner of the competition. The new algorithmic rule worked on an identical symmetric-key block cipher as DES, however far more advanced.

- **2002 – AES in action.** The U.S. central formally adopted AES-192 and AES-256 to secure classified data on the advice of federal agency. The algorithmic rule was approved by the United States intelligence agency also, and shortly once, the remainder of the technology community started taking notice.
- **Present** – **The gold commonplace.** AES encoding has fully replaced DES worldwide because the default bilateral encoding cipher used for public and business functions.

How does AES encryption work?

AES encoding is thought for speed and security.Speed comes from the very fact that AES could be a symmetric-key cipher associate degreed needs less process power as compared to an uneven one.

Security is that the direct results of a complicated block cipher algorithmic rule. Information is encrypted on a per-block basis, that is measured in bits. As an example, 128 bits of plain text can manufacture 128 bits of ciphertext.

The cipher involves substitution and permutation, which means substitution inputs with specific outputs so shuffling those outputs, aka rounds. These rounds compose the distinction between the varied key lengths. AES uses ten rounds for 128-bit keys, twelve rounds for 192-bit keys and fourteen rounds for 256-bit keys.

Key growth is allotted before every spherical. The initial key's accustomed derive a series of 'new spherical keys' to confirm an equivalent keys aren't employed in every spherical.

Each spherical of AES involves:

- Byte Substitution
- Shift Rows
- Mix Column
- Add roundl Key

Byte Substitution:

The sixteen input bytes (128-bit) ar substituted supported a preset table. The result's a matrix of 4 rows and 4 columns wherever the information is altered in a very non-linear thanks to add confusion.

73	df	id	ks
hb	hq	h2	tg
9f	st	7f	14
S5	2h	30	h9

The algorithm looks up the table where the value of each character is equated with another character. You get a matrix with new values but the same data.

jb	n3	kf	n2
9f	jj	1h	js
74	wh	0d	18
hs	17	d6	px

Shift row:The algorithmic program appearance up the table wherever the worth of every character is equated with another character. You get a matrix with new values however constant knowledge.The data is enraptured from its original position to make diffusion

jb	n3	kf	n2
jj	1h	js	9f
0d	18	74	wh
px	hs	17	d6

Mix columns

Each spherical key's combined with the plaintext mistreatment the additive XOR algorithmic program to any diffuse the information. The result's another new matrix consisting of sixteen new bytes.

1s	j4	2n	ma
83	28	ke	9f
9w	xm	31	m4
5b	a9	ci	ps

Add round Key

The result from the mixed column is further to the primary spherical key. After this, it goes back to the computer memory unit substitution step and therefore the entire method (round) starts once more. That means, if you're mistreatment 256-bit

key coding, you may bear this spherical fourteen times.

,yjb	n3	kf	n2
9f	jj	1h	js
74	wh	0d	18
hs	17	d6	18

Once the information has skillful this grotesque method, your plaintext can start off trying like 'we238adjkjloncvty' (for example) as a results of totally different mathematical operations being applied to that once more and once more.

Decryption

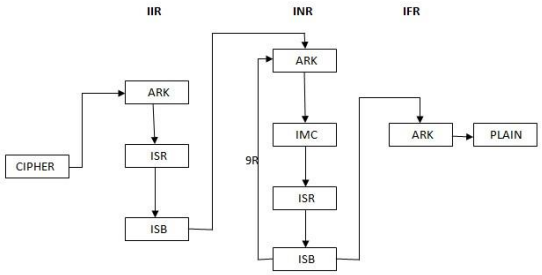


fig 3 A general structure of Decryption

Although identical key's used for each coding and cryptography, the algorithms ought to be one by one enforced. The cryptography method is comparable to the coding method however in reverse order.

Here's the sequence for AES decryption:

Add spherical Key

Mix Columns

Shift Rows

Byte Substitution

How to secure 256 AES?

If AES is that the gold normal, 256-bit encoding is its kid. With the longest rounds, the 256-bit key provides the strongest level of encoding.

It is close to potential} to crack it though brute force is applied – attempting each combination of numbers possible till the proper key's found. The longer the key size, the additional tries area unit required.

A hacker attempting to crack a two56-bit key would want 2 to the ability of 256 tries to search out the proper key. Though hackers use Tianhe-2 (MilkyWay-2), the quickest mainframe computer within the world, it'll take them some million lifetimes to crack a 256-bit AES encoding.

The bottom line is, entities that face threats from all directions, like the U.S. Military or your workplace 365 that stores business-critical info, want AES 256-bit protection

Securing your data with AES algorithm

To ensure your SaaS information is safe, check if your backup marketer uses AES 256 cryptography. If not, likelihood is they're mistreatment service accounts, which implies your information is in danger.

AES APPLICATIONS

AES secret writing and decoding has several applications. It's utilized in cases wherever information is simply too sensitive that solely the approved folks ar imagined to recognize and to not the remainder. The subsequent ar the assorted applications

- **Secure Communication**
  - Smart Cards – RFID.
  - ATM networks.
  - Image secret writing

- **Secure Storage**
  - Confidential work Documents
  - Government Documents
  - FBI Files
  - Personal Storage Devices
  - Person info Protection

4.Conculsion:

In this paper we describe the brief evaluation of AES Algorithm, the AES algorithmic program computes quicker than RSA in execution and implementation. RSA algorithmic program is reliable for key exchange management however it's not extremely economical in terms of performance and worth.

There are unit several unknowns concerning future computing platforms and therefore the big selection of environments during which the AES are going to be enforced. However, once thought of along, Rijndael's combination of security, performance, efficiency, implementability, and suppleness create it associate degree applicable choice for the AES to be used within the technology of nowadays and within the future.

5.ACKNOWLEDGEMENT:

It gives me great pleasure to present my Research paper on " A detailed evaluation on AES algorithm". I would like to express my sincere thanks to all the teachers who helped us throughout. I would like to acknowledge the help and guidance

provided by our professors in all places during the presentation of this research paper.

We are also grateful to, Head of Department. This acknowledgement will remain incomplete if we do not mention a sense of gratitude towards our esteemed Principal who provided us with the necessary guidance, encouragement and all the facility available to work on this project.

6.REFERENCE:

[1] A. Lee, NIST Special Publication 800-21, *Guideline for Implementing Cryptography in the Federal Government*, National Institute of Standards and Technology, November 1999.

[2] J. Daemen and V. Rijmen, *The block cipher Rijndael*, Smart Card research and Applications, LNCS 1820, SpringerVerlag, pp. 288-296.

[3] J. Nechvatal, et. al., *Report on the Development of the Advanced Encryption Standard (AES)*, National Institute of Standards and Technology, October 2, 2000.

[4] —Specification for the Advanced Encryption Standard (AES),|| Federal Information Processing Standards Publication 197, Nov. 2001

[5] A. Menezes, P. van Oorschot, and S. Vanstone, *Handbook of Applied Cryptography*, CRC Press, New York, 1997, p. 81-83.

[6] C.-P. Su, T.-F. Lin, C.-T. Huang, and C.-W. Wu, —A highthroughput low-cost AES processor,|| *IEEE Commun.*
Mag., vol. 41, no. 12, pp.86–91, Dec. 2003.

[7] C.-P. Su, C.-L. Horng, C.-T. Huang, and C.-W. Wu, —A configurable AES processor for enhanced security,|| in *Proc. ASP-DAC*, Shanghai, China, Jan. 2005, pp. 361–366.

[8] Rachh, R.R.; Anami, B.S.; Ananda Mohan, P.V. —Efficient implementations of S-box and inverse S-box for AES algorithm,|| in TENCON 2009 - 2009 IEEE Region 10 Conference , Nov. 2009, pp. 1–6.

[9] Kaur, Swinder; Vig, Renu , || Efficient Implementation of AES Algorithm in FPGA Device|| in Conference on
Computational Intelligence and Multimedia Applications,
Nov 2007,pp. 179-187