Implementation of Advanced Encryption Standard Algorithm for Communication Security Using FPGA

Madhuri B. Ghodke [1], Dr. Suresh N. Mali [2]

[1]Student M.*E. (VLSI &Embedded system), Sinhgad Institute of Technology and Science, Narhe, Pune.*
[2]*Principal of Sinhgad Institute of Technology and Science, Narhe, Pune.*

---***---

Abstract - Network security is one of the most important factors in today's world. It protects the information from unwanted access or editing of third party and intentional or accidental interference of third party users. Advanced Encryption Standard (AES), is a cryptographic algorithm that can be used for secured communication, it uses same key that is symmetric key for transmission as well as reception. The AES algorithm is capable of using cryptographic keys of 128, 192, and 256 bits, this paper implements the 128 bit standard on a Field Programmable Gate Array (FPGA).

Key Words: Cryptography, FPGA, AES algorithm.

1.INTRODUCTION

Cryptography provides great significance for secured communication. Use of cryptographic algorithms is done for the purpose of security in various applications like secured ATM, DVD content etc. Secured communication is one of the most important things in present day situation and its need is increasing rapidly[1]. Every individual wants their data to be secured and privacy must be maintained. This requirement can be fulfilled by the use of cryptography. So many systems are required to protect the shared data. The present work focuses on cryptography to secure the data while transmitting in the network [2]. This Advanced Encryption standard specifies the Rijndael algorithm [9].

1.1 Cryptography

Cryptography is a skill of protecting the information by transforming it into an unreadable format. The encrypted data is called as ciphertext. At the receiver end, only those who have a secret key be able to decipher the message into plain text for getting the original data. Sometimes encrypted messages can be broken down by cryptanalysis, which is known as codebreaking. Cryptography can be classified into two types symmetric-key systems and Asymmetric-key systems. In symmetric-key encryption systems sender and receiver of the message make use of the identical key, this unique key is used for encryption as well as decryption of the message.

In the second type which is asymmetric cryptography, a pair of keys is used for encryption as well as decryption of the message to provide security.

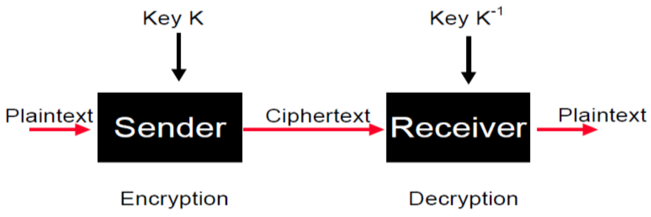


Figure 1: Cryptographic technique.

Encryption is the most effective technique for achieving data security. To read an encrypted message, one must have access to a secret key or password that performs decryption. Decryption is the procedure of converting encrypted data back into the original format, so that it can be understood by the end user.

2.LITERATURE REVIEW

AES algorithm have been standardized and it is considered as very secured as compared to other encryption algorithms[1].

The data which is to be transmitted from sender to the receiver must be encrypted using the encryption algorithm in cryptography. The three encryption techniques i.e. AES, DES, RSA algorithms are compared here.

Table 1: Comparison between AES, DES and RSA

Factors	AES	DES	RSA
Developed	2000	1977	1978
Algorithm	Symmetric Algorithm	Symmetric Algorithm	Asymmetric Algorithm
Encryption & Decryption	Faster	Moderate	Slower
Power Consumption	Low	Low	High
Security	Excellent Secured	Not Secure Enough	Least Secure

1.Advanced Encryption Standard (AES) Algorithm:

Advanced Encryption Standard (AES) algorithm not only for security but also for great speed [1].

2. Data Encryption Standard (DES) Algorithm :

DES provide a standard method for protecting sensitive commercial. In this same key used for encryption and decryption process so it is known as symmetric algorithm.[2]

3. Rivest-Shamir-Adleman (RSA) algorithm :

RSA algorithm is used to encrypt the data to provide security so that only the concerned user can access it [2].

4. AES ALGORITHM

Advance Encryption standard specifies the Rijndael algorithm, this is symmetric block cipher that can process data blocks of 128 bits, using cipher keys with lengths of 128, 192, and 256 bits. The algorithm used with three different key lengths those are AES-128, AES-192 and AES-256. AES algorithm performs encryption and decryption which contains a series of well-defined steps that can be carried out as a procedure. Original information is called as plaintext and the encrypted form is known as cipher text. Cipher text message contains all the information of plaintext data, but it is not in the format readable by a human or computer without proper mechanism for decrypting it.

1.SubBytes Transformation:

This operation provides non-linearity in the cipher text. In this step each byte $a_{i,j}$in the *state* matrix is replaced with a SubByte $S(a_{i,j})$, by making use of Rijndael S-Box (It is a substitution box serves as lookup table).

2. ShiftRows Transformation

In ShiftRows transformation, the bytes from the last three rows in the State are cyclically shifted over different numbers of bytes. The first row, r = 0,which is not shifted.

3. MixColumns Transformation

In MixColumns step, four bytes of each column of the state are united using an invertible linear transformation. The MixColumns function takes four bytes as input and gives four bytes output, where all the four output bytes will be affected by each input byte.

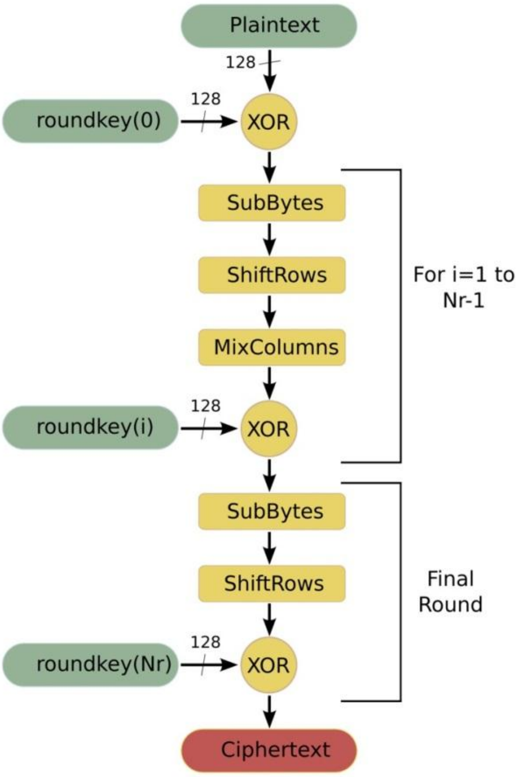


Figure 2: Flowchart of AES algorithm.

4. AddRoundKey Transformation

In AddRoundKey transformation, a simple bitwise XOR operation is performed to add round key to the state.

All the above mentioned steps are repeated for i=1 to Nr-1, where Nr is no. of rounds. In the final step all other steps except AddRoundKey operation are carried out.

5. USE OF FPGA

A field-programmable gate array i.e. FPGA is an integrated circuit designed to be configured by a customer or designer after manufacturing hence it is known as field-programmable. The FPGA configuration is generally specified using HDL that is hardware description language. Same as that used for an application-specific integrated circuit (ASIC). FPGA is study of computation using reconfigurable devices. It consist of large array of configurable logic primitives. Some of the properties of FPGA are its increased capacity, upgradability and high flexibility.

6. EXPERIMENTAL SETUP

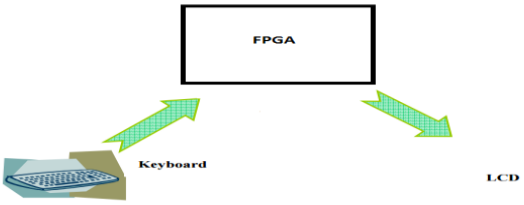


Figure 3: Overall System Diagram

Spartan3e device is used with xc2s250e part . Figure 3 covers the architecture of this implementation of the 128 bit AES, detailed in the FIPS197 that is Federal Information Processing Standard 197. The design was developed and testeded on a Xilinx , FPGA board. Figure 3 shows FPGA, Keyboard, LCD. Two human interface devices (HIDs), a regular PS2 keyboard and a 4x20 line LCD include the inputs and outputs to the system. The inputs to the system are the clock, clk, tested at 50 MHz & 100 MHz, resetn, and the PS2 keyboard inputs, ps2_data and ps2_clk. The ps2_data and ps2_clk are bidirectional ports though the device never sends commands to the keyboard, thus these pins are limited to inputs of the system. For the reset push button on the development board is used.

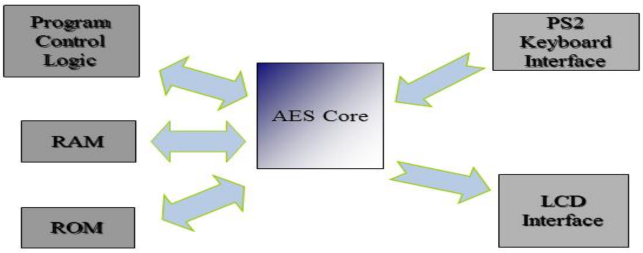
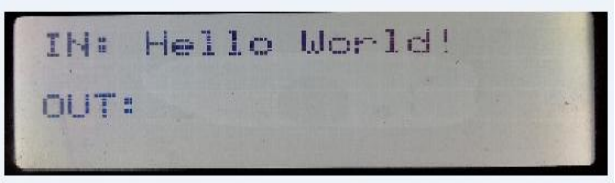


Figure 4: Sub-system block diagram

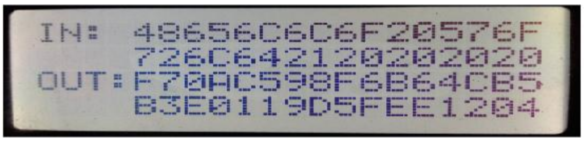
The first sub-system contains the sequence of steps that are performed to execute all three major operations, those are: key expansion, encryption and decryption. The sequential steps are micro-programmed and these steps are output through the opcode bus. F1, F2, and Esc are the keys used. The operation on the signal performed is encryption and decryption routines is instructed by the keys F1 and F2 respectively. The 'Esc' key is used to switch between ASCII input mode and hexadecimal input mode.

7. EXPERIMENTAL RESULTS



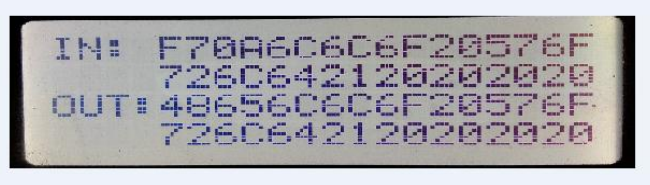
```
IN:  Hello World!
OUT:
```

Figure 5: ASCII input as plain text.



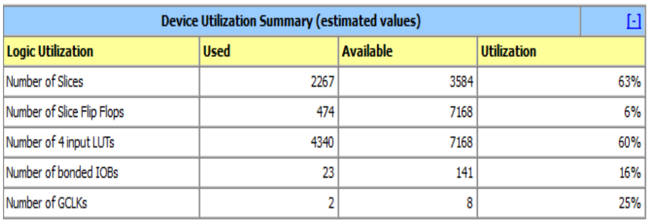
```
IN:  48656C6C6F20576F
     726C642120202020
OUT:F70AC598F6B64CB5
     B3E0119D5FEE1204
```

Figure 6: ASCII to HEX conversion and encrypted data.



```
IN:  F70A6C6C6F20576F
     726C642120202020
OUT:48656C6C6F20576F
     726C642120202020
```

Figure 7: Decryption process.



Device Utilization Summary (estimated values)			[-]
Logic Utilization	Used	Available	Utilization
Number of Slices	2267	3584	63%
Number of Slice Flip Flops	474	7168	6%
Number of 4 input LUTs	4340	7168	60%
Number of bonded IOBs	23	141	16%
Number of GCLKs	2	8	25%

Figure 8: Overall Design Summary

Figure 5 shows that the ASCII input is given which is a plain text. Figure 6 shows that ASCII to hexadecimal convertion is carried out and then various steps of AES algorithm are carried out on the given data for converting it into the cipher text this is encryption. Figure 7 shows decryption is carried out to get the plain text in hexadecimal format. Figure 8 shows the overall design summary, that is persentage of utilization of number of slices ,no. of slice Flip Flops etc.

8. CONCLUSIONS

Network security is important for computer users and organizations , handling of confidential data requires proper security options. The primary goal of AES algorithm on FPGA is to provide significant level of security as well as faster processing time so that it can be used for secured communication of ATM, DVD content as well as for secured storage of confidential corporate documents, government documents etc.

REFERENCES

[1] Atef Ibrahim, "FPGA-based Hardware Implementation of Compact AES Encryption Hardware Core," WSEAS transactions on circuits and systems. ISSN: 2224-266X Volume 14, 2015.

[2] Dr. Prerna Mahajan & Abhishek Sachdeva, "A Study of Encryption Algorithms AES, DES and RSA for Security", Global Journal of Computer Science and Technology Network, Web & Security Volume 13 Issue 15 Version 1.0 Year 2013.

[3] Prakash G L ,Dr. Manish Prateek , Dr. Inder Singh," Data Encryption and Decryption Algorithms using Key Rotations for Data Security in Cloud System", International Journal Of Engineering And Computer Science ISSN:2319-7242 Volume 3 Issue 4 April, 2014 Page No. 5215-5223

[4] Kengo Iokibe, Tetsuo Amano, Kaoru Okamoto, and Yoshitaka Toyota," Equivalent Circuit Modeling of Cryptographic Integrated Circuit for Information Security Design", IEEE transactions on electromagnetic compatibility, 2013.

[5] Dr.R.V.Kshirsagar, M.V.Vyawahare, " FPGA Implementation of High speed VLSI Architectures for AES Algorithm", 2012 IEEE Fifth International Conference on Emerging Trends in Engineering and Technology.

[6] Selva Kumar M., Thamarai P., Arulselvi S.." Network Data Security Using FPGA", International Journal of Scientific Engineering and Technology (ISSN : 2277-1581) Volume 2 Issue 5, pp : 454-457, 2013.

[7] J.Saira Banu, Dr.S.Subha," Loop Parallelization And Pipelining Implementation Of AES Algorithm Using OpenMP And FPGA", IEEE international conference 2013.

[8] Massoud Masoumi and Mohammad Hadi Rezayati," Novel Approach to Protect Advanced Encryption Standard Algorithm Implementation against Differential Electromagnetic and Power Analysis", IEEE Transactions on Information Forensics and Security, 2013.

[9] Announcing the ADVANCED ENCRYPTION STANDARD (AES), Federal Information Processing Standards Publication 197 ,November 26, 2001

[10] Joan Daemen, Vincent Rijmen,AES Proposal: Rijndael. Document version 2, 1999.

[11] C. K. Koc., RSA Hardware Implementation. Technical Report TR 801 , RSA Laboratories, 1996

[12] Pritamkumar N. Khose, Vrushali G. Raut," HARDWARE IMPLEMENTATION OF AES ENCRYPTION AND DECRYPTION FOR LOW AREA & POWER CONSUMPTION", IJRET: International Journal of Research in Engineering and Technology, Volume: 03 Issue: 05 | May-2014.

[13] Pravin B. Ghevari , Jaymala K. Patil, Amit B. Choughule," Efficient Hardware Design and implementation of AES cryptosystem".