Design of Advanced Encryption Standard Using VHDL

[1]Chaudhari R. Priyanka, [2]Pinky Brahmbhatt
[1]P.G. Student, [2]Associate Professor
[1]Electronics and Communication Department
[1]L.D. College of Engineering, Ahmedabad, India

Abstract: Security is very important parameter of today's era. Today most concerned thing about communication includes looks into on security concern. At present most recognized cryptographic algorithm for encryption is Advance Encryption Standard. Advanced encryption standard is most important algorithm of cryptographic. AES is symmetric key algorithm which is used to encrypt (cipher text) and decrypt (plain text) the data. Previously Data Encryption Standard (DES) is used but it's proved inadequate because of smaller key length. An AES takes an input block size of 128 bit. AES has three size of cryptographic key 128,196 and 256 bit. Basically, AES uses substitution and permutation operation. AES can be implemented by both software simulation and hardware simulation but as compared to software simulation hardware simulation has more merits like low area consumption and less time requirement. A huge amount of hardware required for implementation of Advanced Encryption standard because if it's complex nature. The huge amount of hardware requirement makes AES very complex and burdensome. In this paper we implemented FPGA based AES algorithm. Xilinx _ISE 14.7 software is being used for simulating and to synthetize the VHDL code. Xilinx's SPARTEN 6 FPGA is used for implementation. One application is developed for transferring the data from PC to FPGA.

***Index Terms*—AES, Encryption, Decryption, FPGA, Visual Basic, VHDL ,Different Key Length.**

I. INTRODUCTION

In this era of technology data is considered as very important thing. Security is must because millions of devices are sharing their files daily such as financial and legal files, medical support, and bank related services via web, telephone talk, and transactions. Important files can be accessed by intruder very easily if data is not encrypted. Cryptographic is one of the secure algorithm. Cryptographic is Greek origin word which means "secret-writing". Cryptography was synonyms with encryption it convert original data or secure message in completely non sense form. Cryptography is secure way for transferring the information without theft or change. Cryptography is used for both side to encrypt the information and to decrypt the information. The encryption's task is to change our main information or plain text (data) into a cipher text (non-sense text). The decryption process is convert cipher text (non-sense text) into a plain text or original information. There are two types of cryptographic algorithm secret key (symmetric) and public key (asymmetric) algorithm. Secret key (symmetric) algorithm are algorithm for cryptography that used same cryptographic key for encryption and decryption. Key is also called private key. Advantage of symmetric key algorithm that it executes and it's less complex; they are used for bulk data transmission. Private Key (Asymmetric key) algorithm is known as public key algorithm, uses public and private key to encrypt and decrypt the data. One key is shared with everyone, and other key is kept secret. Asymmetric key is complex in nature as compared to symmetric key. So mainly symmetric key algorithm is used for to transmit the secure information. There are numerous types of secret key (symmetric) key algorithm: DES. AES, triple DES, RSA.

Data Encryption Standard is used to secure communication in earlier 90's. DES is symmetric key algorithm that use 56 bit key. DES has 64 bit plain text. It will convert 64 bit plain text into a 64 bit chipper text with the help of 56 bit symmetric key. But as said the time requirement to decrypt the encryption algorithm is proportional to the length of the bit key used for the safe conversion. To show that DES was inadequate and less secure a challenges were sponsored to see how long it would take to decrypt a message. In 1997 challengers took 87 days to decrypt the message using brute force attack. In 1998 challengers took less than one month to decrypt the DES. In 1999 challengers took 22 hours and 15 minutes. So they proved DES was inadequate. Even triple DES was inadequate and slower because of using DES encryption three times it was proved in adequate.

In 2001 National Institute of Standard and Technology introduced AES which is public (symmetric) key algorithm to overcome the Data Encryption Standard failure. AES is also known as RIJNDAEL algorithm. Till now no one can break RIJNDAEL algorithm. So AES algorithm is most important algorithm for secure communication.

The further paper is organized as follow: Section II gives application of cryptographic. Section III gives introduction of AES algorithm Section IV gives encryption of AES Section V gives decryption of AES Section VI gives simulation results. Finally section VII gives Conclusion.

II. APPLICATION

1. Automatic Teller Machines (ATM)
2. Smart Cards
3. WhatsApp
4. HTTP Source

5. Bluetooth Transfer
6. Digital Signature

III. INTRODUCTION OF AES

In 2001 National Institute of Standard and Technology introduced Advanced Encryption Standard developed by Joan Daemen of Proton World International and VicentFijmen of Ketholieke University Leauen Advance Encryption Standard is Symmetric block chipper that uses Substitution and Permutation. AES use for both side Encryption and Decryption. Encryption convert original data into a completely non-sense form that called chipper text. Decryption covert chipper text into an original data. AES is more efficient cryptographic algorithm compared to Des but its most positive advantage is that it can use various key length. AES allow to select a 128,192, 256 bit key length, making it exponentially stronger. AES has different number of rounds depends on size of the key. AES has 10, 12 and 14 rounds which are dependent to size of the key. In this paper we have used 128-bit key for 128-bit data.

Table 1
AES ROUND INFORMATION

	Key size	Block size	Rounds
Aes 128 bit	**4 bit**	**4 block**	**10 rounds**
Aes 192 bit	**6 bit**	**4 block**	**12 rounds**
Aes 256 bit	**8 bit**	**4 block**	**14 rounds**

Table 2
Comparison between AES and DES [1]

BASIS FOR COMPARISON	DES (DATA ENCRYPTION STANDARD)	AES (ADVANCED ENCRYPTION STANDARD)
Basic	In DES the data block is divided into two halves.	In AES the entire data block is processed as a single matrix.
Principle	DES work on Feistel Cipher structure.	AES works on Substitution and Permutation Principle.
Plaintext	Plaintext is of 64 bits	Plaintext can be of 128,192, or 256 bits
Key size	DES in comparison to AES has smaller key size.	AES has larger key size as compared to DES.
Rounds	16 rounds	10 rounds for 128-bit algo 12 rounds for 192-bit algo 14 rounds for 256-bit algo
Rounds Names	Expansion Permutation, Xor, S-box, P-box, Xor and Swap.	Subbytes, Shiftrows, Mix columns, Addroundkeys.
Security	DES has a smaller key which is less secure.	AES has large secret key comparatively hence, more secure.
Speed	DES is comparatively slower.	AES is faster.

IV AES ENCRYPTION

Encryption transforms original information or plain text into a completely non-sense form called chipper text. Value of the rounds in Encryption process is depends on key length of the AES. AES has three different key lengths 128,192,256 bit key. AES algorithm operates on 128 bit block data and similarly 10 rounds for algorithm. Encryption process has four round block sub-byte transformation, Mix column transformation, Shift row, and Key expansion.An additional Add Round Key transformation is added at the beginning of the round and no Mix Columns transformation are added in the last round. The first step of the round is to convert 128 bit into 4 x 4 state matrix.

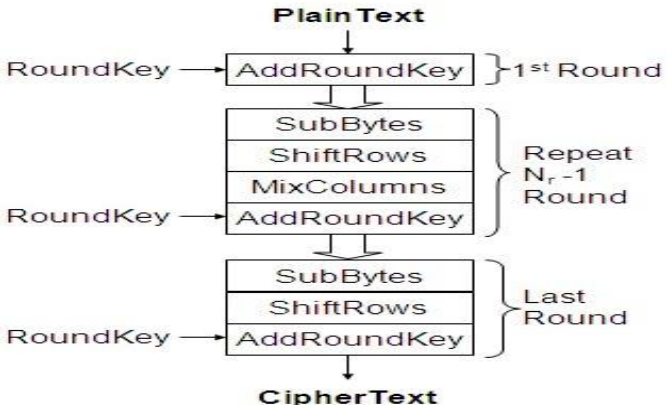


Figure 1 Block of Encryption

1. Sub Byte Conversion:

Sub Byte conversion is Non-linear transformation. In sub byte transformation each byte in substitute matrix is replaced by another byte using S-box. Using S-box first hexadecimal number correspond to row poisoning and second hexadecimal number correspond to column poisoning is replaced.

	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	63	7c	77	7b	f2	6b	6f	c5	30	1	67	2b	fe	d7	ab	76
1	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
3	4	c7	23	c3	18	96	5	9a	7	12	80	e2	eb	27	b2	75
4	9	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
5	53	d1	0	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
6	d0	ef	aa	fb	43	4d	33	85	45	f9	2	7f	50	3c	9f	a8
7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
8	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
a	e0	32	3a	0a	49	6	24	5c	c2	d3	ac	62	91	95	e4	79
b	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	8
c	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
d	70	3e	b5	66	48	3	f6	8e	61	35	57	b9	86	c1	1d	9e
e	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
f	8c	a1	89	0d	bf	e6	42	68	41	99	2d	of	b0	54	bb	16

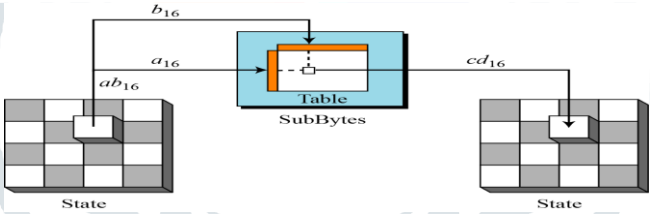


Figure 2: Sub byte transformation

2. Shift Row Conversion:

In Shift row conversion every row of the matrix is shifted by left. Rows are shifted left by 1 byte respectively, the first row of the matrix is does not change, second row is shifted by1 byte to the left, third row is shifted by 2 byte to the left and fourth row is shifted by 3 byte to the left.

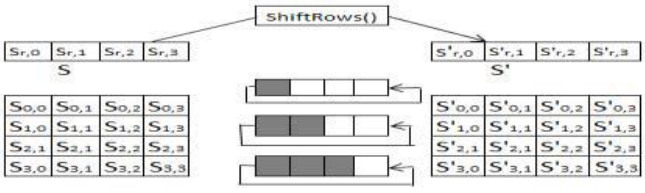


Figure 3: Shift Row transformation

3. Mix Column Conversion:

In mix column conversion each byte in column is replaced by another byte using Galois field (2^8).

$$\begin{bmatrix} S'_{0,c} \\ S'_{1,c} \\ S'_{2,c} \\ S'_{3,c} \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 01 \end{bmatrix} \begin{bmatrix} S_{0,c} \\ S_{1,c} \\ S_{2,c} \\ S_{3,c} \end{bmatrix} \dots for 0 \le c \le Nb$$

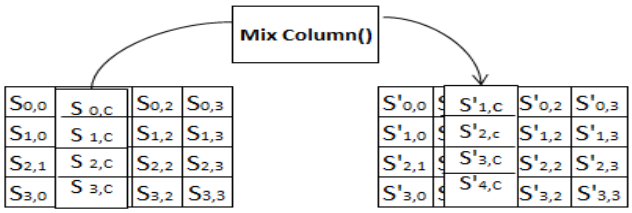


Figure 4: Mix column transformation

4. Add round key:

In add round key operation output of the mix column conversion is EX-OR with input key. The EX-OR operation is done bit by bit. Total 10 round key is obtain from this operation.

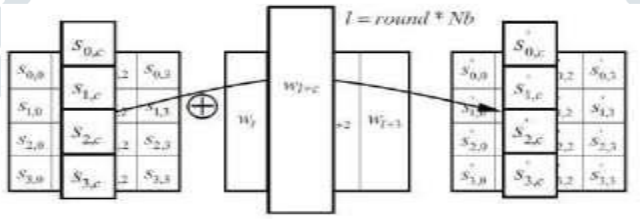


Figure 5: round key generation

5. Key Expansion:

From the first master key word total 10 key word matrix will be obtained.

Method:

- For the word column in any key matrix which is not a multiple of 4 it will take simply XOR (Wi-1) and (Wi-4).But for word column in any key matrix which is a multiple of 4 is filled in a special way.

Let us take one matrix which contain 128 bit data.Here W4 is a multiple of 4 we follow following procedure:

32	88	31	e0
43	5a	31	37
f6	30	98	07
A8	8d	a2	34

Step 1:

Rotate by one byte column that is just previous to it. In case of previous column is W3 so rotate it one byte.it can get following O/P.

37
07
34
e0

Step 2:

Now apply the S-box to all four bytes of above O/P.

9a
c5
18
e1

Step 3

Now it will XOR the above O/P by a round constant RCON according to a predefined value for each round as follows:

Values of RCON in hexadecimal

$$Rcon = \begin{bmatrix} 01 & 02 & 04 & 08 & 10 & 20 & 40 & 80 & 1b & 36 \\ 00 & 00 & 00 & 00 & 00 & 00 & 00 & 00 & 00 & 00 \\ 00 & 00 & 00 & 00 & 00 & 00 & 00 & 00 & 00 & 00 \\ 00 & 00 & 00 & 00 & 00 & 00 & 00 & 00 & 00 & 00 \end{bmatrix}$$

As seen into a table for round-1 RCON value is 01.

$$\begin{bmatrix} 9a \\ c5 \\ 18 \\ e1 \end{bmatrix} + \begin{bmatrix} 01 \\ 00 \\ 00 \\ 00 \end{bmatrix} = \begin{bmatrix} 94 \\ c5 \\ 18 \\ e1 \end{bmatrix}$$

Step 4:

Finally XOR the value of above step with fourth previous column to i.e. Wi-4 i.e. W4-4 i.e. W0 which is,

$$\begin{bmatrix} 32 \\ 43 \\ f6 \\ a8 \end{bmatrix} + \begin{bmatrix} 94 \\ c5 \\ 18 \\ e1 \end{bmatrix} = \begin{bmatrix} a6 \\ 86 \\ e6 \\ 59 \end{bmatrix}$$

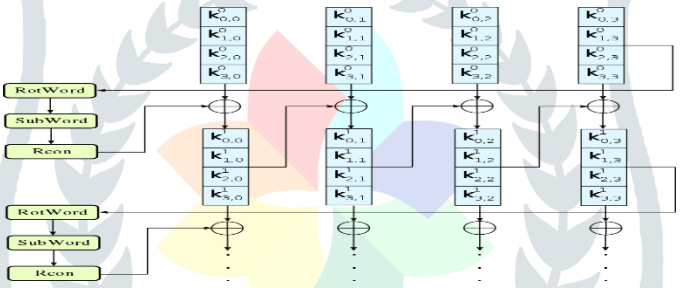


Figure 6: Key expansion

V. AES DECRYPTION

AES Decryption is inverse process of encryption. Decryption transforms chipper text or encrypted text into an original or plain text. The key length is same for decryption process. The decryption process has four rounds inv shift row, inv sub byte transformation, inv min column transformation and inv key expansion.

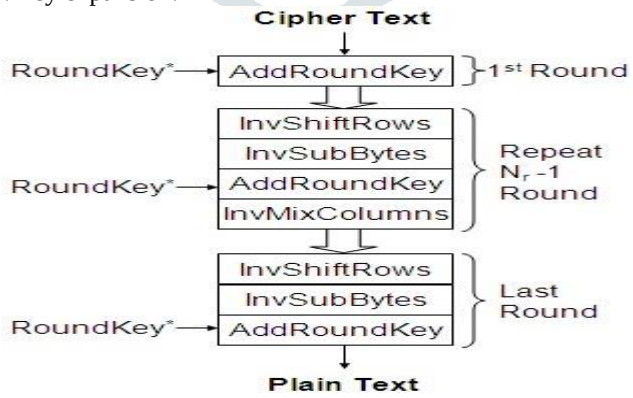


Figure 7: Block of Decryption

1. **Add round key:**

   EX-OR is done between chipper text and round key.

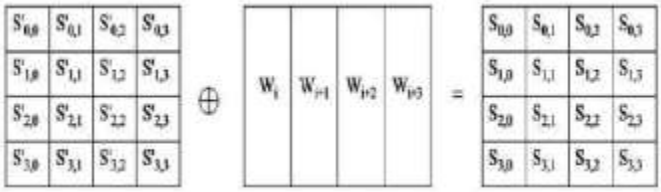


Figure 8: Add round key

2. Inverse sub byte transformation:

In Inverse sub byte every byte of the matrix is replaced by another byte using inverse S-box look up table.

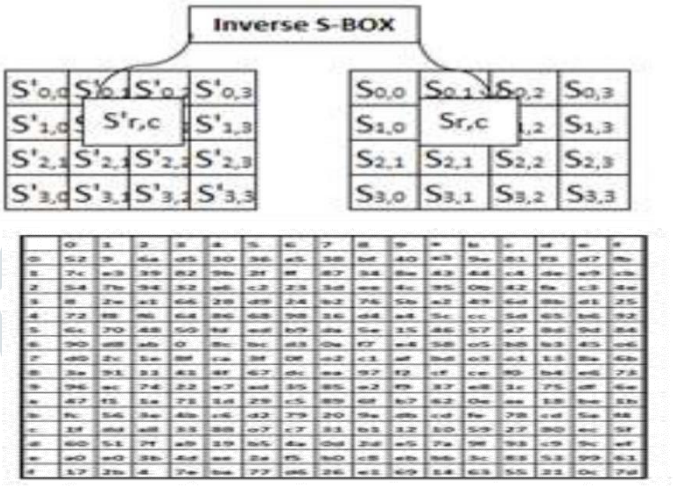


Figure 9: sub byte inverse conversion

3. Inverse shift row transformation:

In inverse Shift row transformation every row of the matrix is cyclically shifted by right. Rows are shifted right by 1 byte respectively, The first row of the matrix is does not change, second row is shifted by 1 byte to the right, third row is shifted by 2 byte to the right and fourth row is shifted by 3 byte to the right.

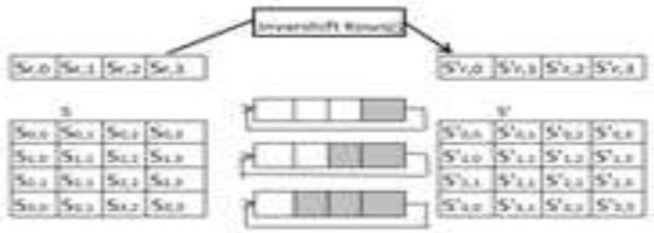


Figure 10: shift row inverse conversion

4. Mix column inverse conversion :

In mix column inverse conversion every byte of the column matrix is replaced by another byte using Galois field (2^8).

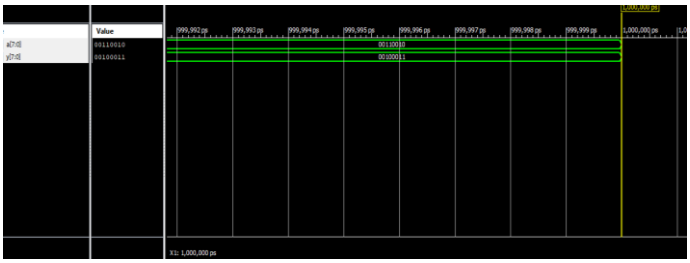
$$\begin{bmatrix} S'_{0,c} \\ S'_{1,c} \\ S'_{2,c} \\ S'_{3,c} \end{bmatrix} = \begin{bmatrix} 0e & 0b & 0d & 09 \\ 09 & 0e & 0b & 0d \\ 0d & 09 & 0e & 0b \\ 0b & 0d & 09 & 0e \end{bmatrix} \begin{bmatrix} S_{0,c} \\ S_{1,c} \\ S_{2,c} \\ S_{3,c} \end{bmatrix} \quad \ldots for\, 0 \le c \le Nb$$

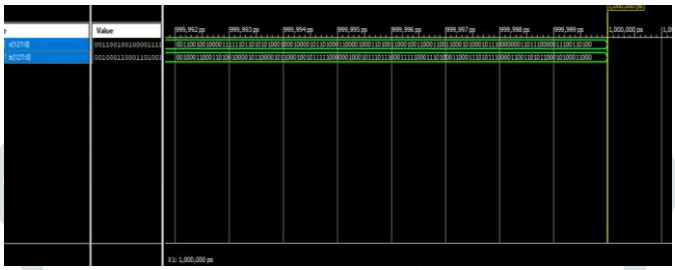
Figure 11: Inverse mix column transformation

VI. Simulation Result

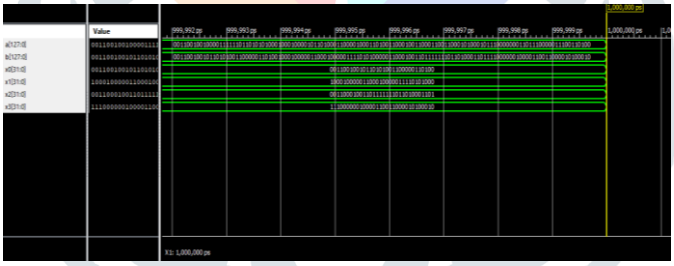
The purpose of our paper to design Advanced Encryption Algorithm using VHDL to improve performance. The Xilinx 14.7 environment was used for written the code.After coding behavioural Simulation was done using Xilinx ISM.

1. **S-box and Sub byte transformation**

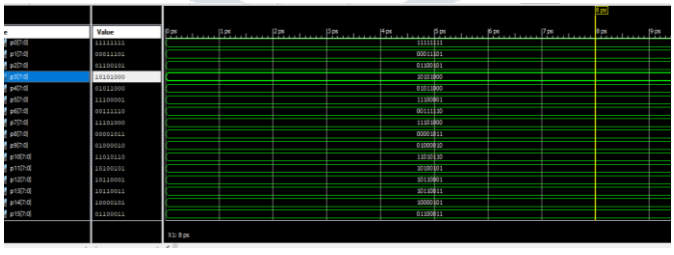




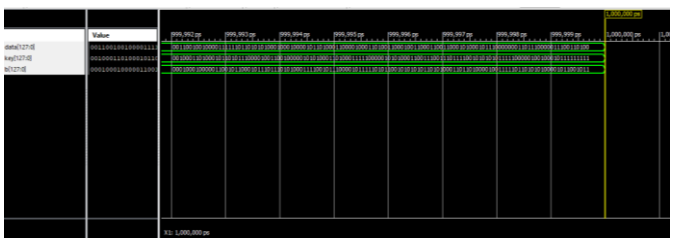
2. **Shift row transformation:**



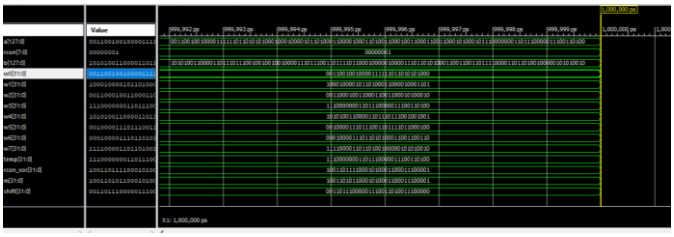
3. **Mix column transformation:**



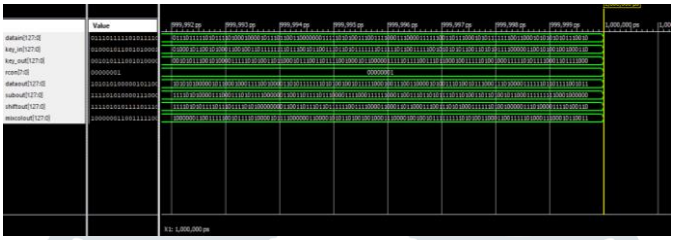
4. **Add round key:**



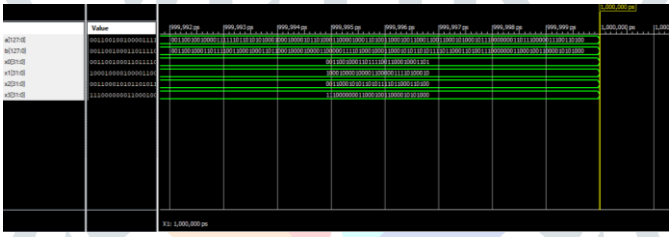
5. **Key expansion:**



6. **Round 1:**



7. **Inverse shift row:**



VII. Conclusion

In this research work we have shown the simulation results of Encryption of Advance Encryption Standard and some part of decryption of Advance Encryption Standard. We will be doing the full implementation of AES algorithm.However more research has to be done to apply fully function code and to implement on VHDL board.AES provide less area consumption and gives better result compare to other algorithm. AES is best option for telecommunication security. In recent years popularity of AES is increased. For simulation and implementation purpose XILINX 14.7 and SPARTEN 6 board is useful. AES is useful for long term security planning. AES will be secure more than 25 years.

REFERENCE

[1] Amit Kumar, Manoj Kumar, P. Balramudu “Implementation ofAES algorithm using VHDL”IEEE 2017 International ConferenceOnComputing Methodologies and Communication (ICCMC).
[2]A.P. ANUSHA NAIDU, B. Prof (Mrs.) POORVI K. JOSHI “FPGA Implementation of Fully Pipelined Advanced Encryption Standard”IEEE ICCSP 2015 conference.
[3]Dr.R.V.Kshirsagar, M.V.Vyawahare”FPGA ImplementationOf High speed VLSI Architectures for AES Algorithm”2012 Fifth International Conference on Emerging Trends in Engineering And Technology.
[4]Hoang Trang and Nguyen Van Loi, "An efficient FPGA Implementation of the Advanced Encryption Standard (AES) algorithm “, IEEE Transactions, vol. 20 pp. 978-1-4673-0309-5, 2012.
[5]Daemen J., and Rijmen V, "The Design of Rijndael: AES-the Advanced Encryption Standard", Springer -Verlag, 2002.
[6]Yang Jun Ding Jun Li Na GuoYixiong “FPGA-based design and Implementation of reduced AES algorithm,” IEEE D