Design and Implementation of Asymmetric Cryptography Using AES Algorithm

Madhuri B. Shinde

Student, Electronics & Telecommunication Department, Matoshri College of Engineering and Research Centre, Nashik, Maharashtra, India

ABSTRACT

Advanced Encryption Standard (AES) has accretion favor through its altitudinous security with low adequate expense. The delinquency for prismatic security martial in multitudinous operations has AES algorithm. In this paper, AES encryption software suited for tool in which low expenses are desired. Large data encryption and decryption appears to be achievable in real time processing. The novel approach permits us to perform various attacks on the system developed by using asymmetric cryptography. The conclusion of findings is accomplished by cryptography.

Keyword: -*AES, Cryptography, VLSI Design*

---

1. INTRODUCTION

The benefit of asymmetric Cryptography: i) only the private key kept secret. ii) In the large network, the number of keys necessarily may be smaller than in the symmetric key script.

Confidentdispatch is the primary demand of every board. Now-a-days, the security has become the major phase of life. It can be achieved by different strategies analogous to passcode, cryptography and biometrics.

In the existing system, there is a huge work did on DES, RSA but the processing speed of both the algorithm is large. Also the key size is small so, the algorithm cannot break and encode the large data. Both the algorithms is cracked, so automatically security is less.

In the proposed system, the security problem is overcome .This system prevents the attacks. Encryption and decryption is done using 128 bits key size. Reliability is much strong.

Cryptography is the science of using arithmetic to encrypt and decrypt data. Cryptography permits you to bought perceptive facts or convey it across insecure networks so that it barrel not be peruse by anyone apart from the voluntary recipient. Cryptography divided into three type's symmetric, contemporary cryptography and asymmetric cryptography. In symmetric cryptography; the coequal key is given for both encryption and decryption. This approach is similar in dealing with each message but less secure since the key must be communicated to and knows at both sender and receiver. In Asymmetric cryptography or public key cryptography, a pair of key is accustomed to encrypt and decipher a dispatch so that it appears fence. Initially a network user receives a public and esoteric arch

dyad from a certificate connoisseur. Any disparate user who wants to send an encrypt dispatch can get the knowing recipients public key from, a public directory. They use this key to encrypt the message and they transfer it to the recipient. When the recipient picks up dispatch they decipher it with their nonpublic key, which no one else should have access to. In the modern cryptography a combination of both public-key and traditional symmetric cryptography is used in modern cryptographic systems [2]. A lot of effort has been made by the research community to permit cryptographic martial on expedient-force RFID. The consummate conspicuous martial are strong attest using, for example, symmetric primitives like the AES [3], [4] or asymmetric primitives like elliptic curve cryptography (ECC) [5], [6].

2. SYSTEM MODELLING AND DESIGN

2.1 Plaintext

This is the readable communication or data that is fed into the algorithm as input. For this work, the size of data is 8 bits.

2.2 AddRoundKey

Transfiguration in the Cipher and Inverse Cipher in which a Round Key is append to the State using an XOR assignment. The length of a Round Key coordinate the size of the State (i.e. for N_b= 4, the Round Key length equals 128 bits/16 bytes).The 128 bits of state are bitwise XORed with the 128 bits of the round key.

2.3 Sub Bytes

Transformation in the Cipher that proceeding the State using a nonlinear byte substitution board (S box) that works on per of the State bytes self-dependent. This stage (known as Substitute Bytes) is simply a table lookup using a 16×16 matrix of byte values known as s-box. This matrix consists of all the workable combinations of an 8 bit sequence (28 = 16 × 16 = 256). The Inverse substitute byte conversion (known as InvSubBytes) makes use of an inverse s-box.

This S-box, which is invertible, is constructed by composing two transformations:

- Take the multiplicative inverse in the finite field GF (2^8), the element {00} is chart to itself.
- Apply the following affine transformation (over GF (2)). [1]

$$b'_i = b_i \oplus b_{(i+4) \bmod 8} \oplus b_{(i+5) \bmod 8} \oplus b_{(i+6) \bmod 8} \oplus b_{(i+7) \bmod 8} \oplus c_i \qquad 1$$

2.4 Shift Rows

Changeover in the Cipher that proceeding the State by cyclically shifting the last three rows of the State by different offsets.This is a simple permutation an nothing more.

It works as follow:

• The first row of state is not vary.

• The second row is shifted 1 bytes to the left in a circular form.

• The third row is shifted 2 bytes to the left in a circular form.

• The fourth row is transposed three bytes to the left in a circular form [1].

2.5 Mix Column

This stage (known as Mix Column) is mainly a substitution but it create use of arithmetic of GF (2^8). Each column is operated on peculiar. Each byte of a column is chart into a new value that is a function of all four bytes in the column [1].

$\propto (X)$ = {03}X^3+ {01}X^2+ {01} X+ {02}

2

$s'(x)$= $a(x)$ $\otimes s(x)$

3

2.6 InvMixColumns () Transformation

InvMixColumns () is the inverse of the MixColumns () transformation. InvMixColumns () operates on the State column-by-column, delectation apiece column as a four-term polynomial. The columns are esteem as polynomials over GF (2^8) and procreate modulo x^4 +1with a inexpugnable polynomial a^{-1} (x).

a^{-1} (x) = {0b}x^3+ {0d} x^2+{09}x +{0e}

4

2.7 InvSubBytes () Transformation

InvSubBytes () is the inverse of the byte substitution transformation, in which the inverse S- box is applied to each byte of the State.

2.8 InvShiftRows () Transformation

InvShiftRows () is the inverse of the Shift Rows () transformation. The bytes in the last three rows of the State are cyclically shifted over different numbers of bytes (offsets).

2.9 Key Expansion

Key management can be handled through manual and automatic processes .the frequency of use of a cryptographic key can have a direct correlation to how often the key should change .The AES algorithm has the cipher key, K and performs a key expansion routine to generate a key schedule expansion generates a total of $N_b(N_r + 1)$ words: the algorithm requires an initial set of N_b state and each of the N_r rounds need N_b words of key data.

- The key length should be variable size for the highly secure communication.
- For the secure communication, the key kept secret.
- Keys should not be in clear text in outside the cryptographic device.

3. EXPERIMENTAL RESULT

3.1 Encryption and Decryption

In the program the data or information containing the letters is first converted into their equivalent numbers then they are transformed to their equivalent binary numbers in array to provide more safety. For example if our information is HELLO then it is converted to 010 010 000 100 010 101 001 100 010 011 000 100 1111.

To achieve more security this sequence is Xored with other sequence which act as key. For the above example let us take SPRING as a key, the equivalent binary number of this100 011 011 101 100 010 010 100 011 011 010 010 after Xoring the result comes out to be:

HELLO 010 010 000 100 010 101 001 100 010 011 000 100 1111
SPRING 100 011 011 101 100 010 010 100 011 011 010 010 0000
X-ored 110 001 011 001 110 111 011 000 001 000 010 110 1111

Then this X-ored sequence is transmitted so that, if anyone hacks this sequence then he/she would not able to understand the data. At the receiver section this sequence is Xored with the same key, this will give the original information. This process is known as decryption.The fig 6.1 to 6.3 shows the encryption decryption output with various input. Fig 6.4 shows the key generation output. Fig 6.5 and 6.6 shows the round and inverse round output respectively. Fig 6.7 shows the attack prevention method.

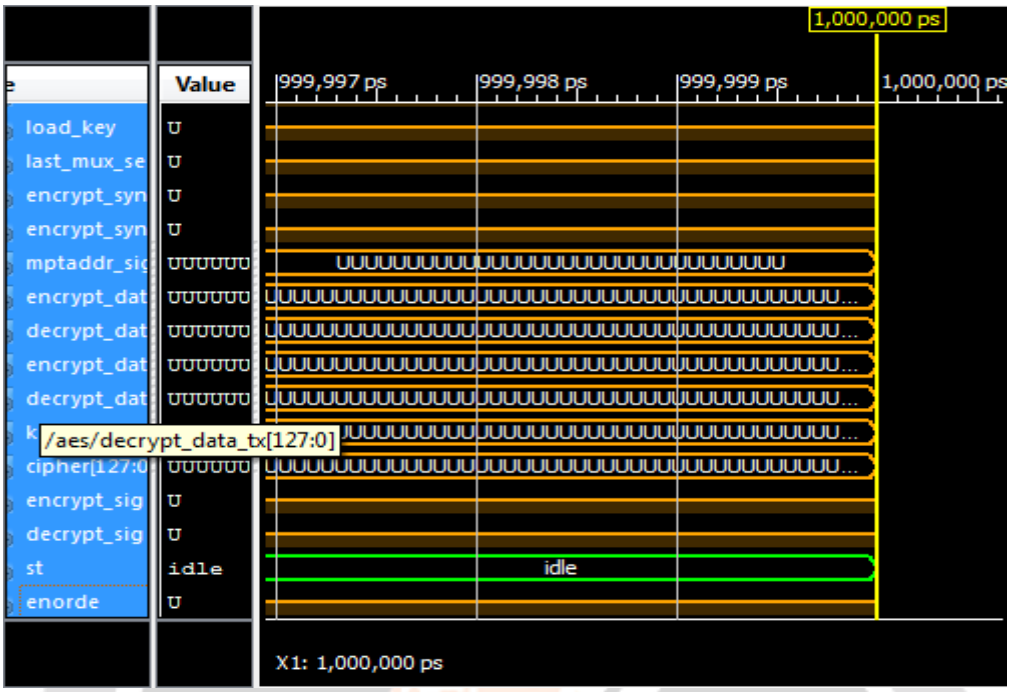

Fig -1: Encryption Decryption with First Message.

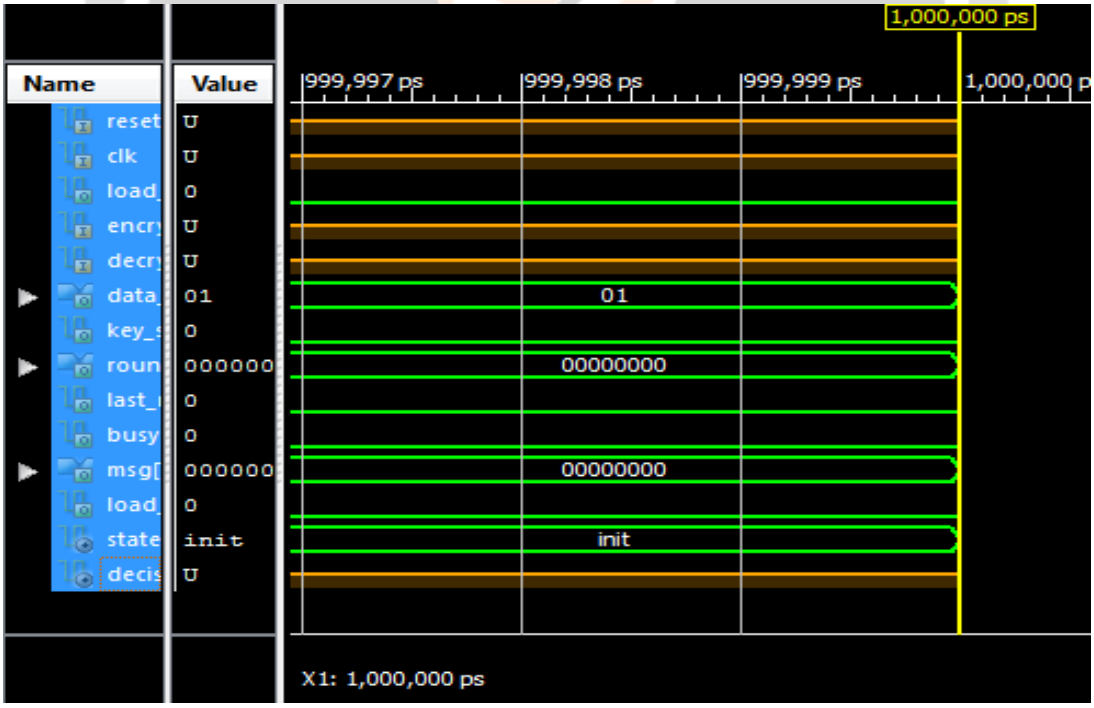

Fig -2: Encryption Decryption with Second Message

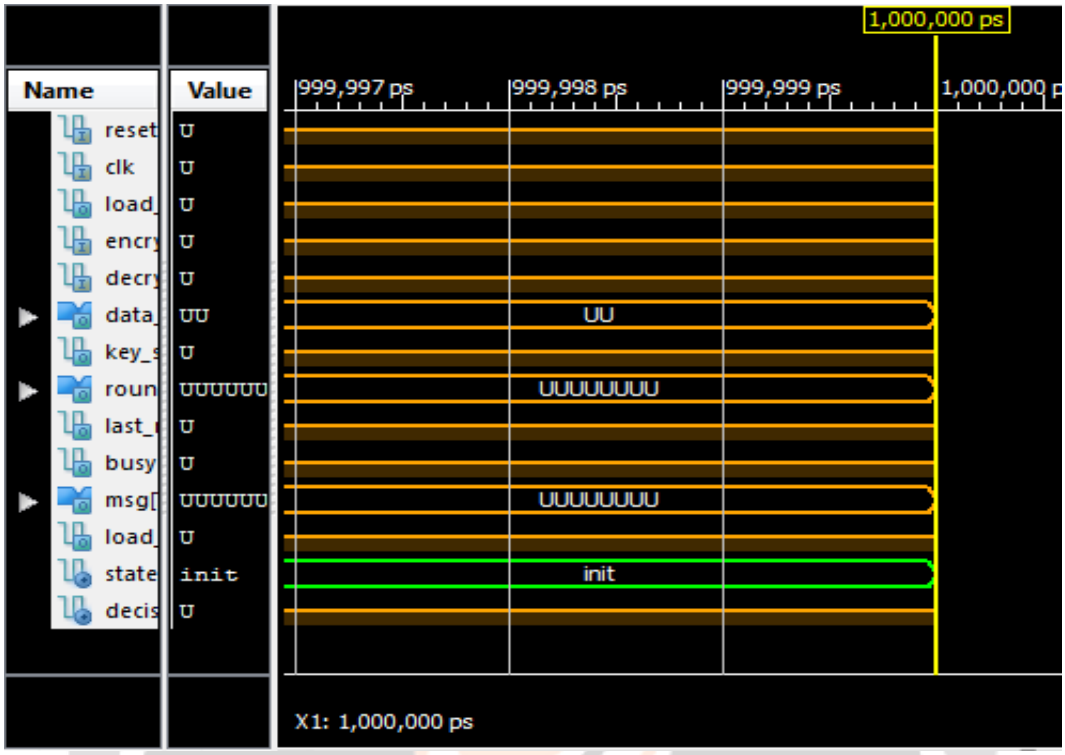

Fig -3: Encryption Decryption with Third Message

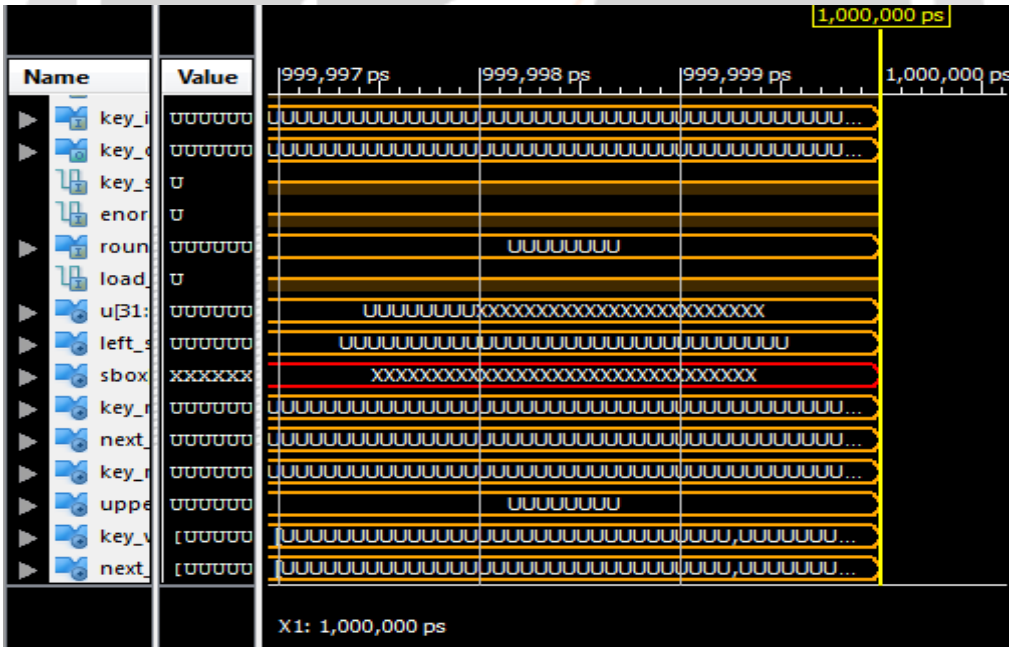

Fig -4: Key Generation Output.

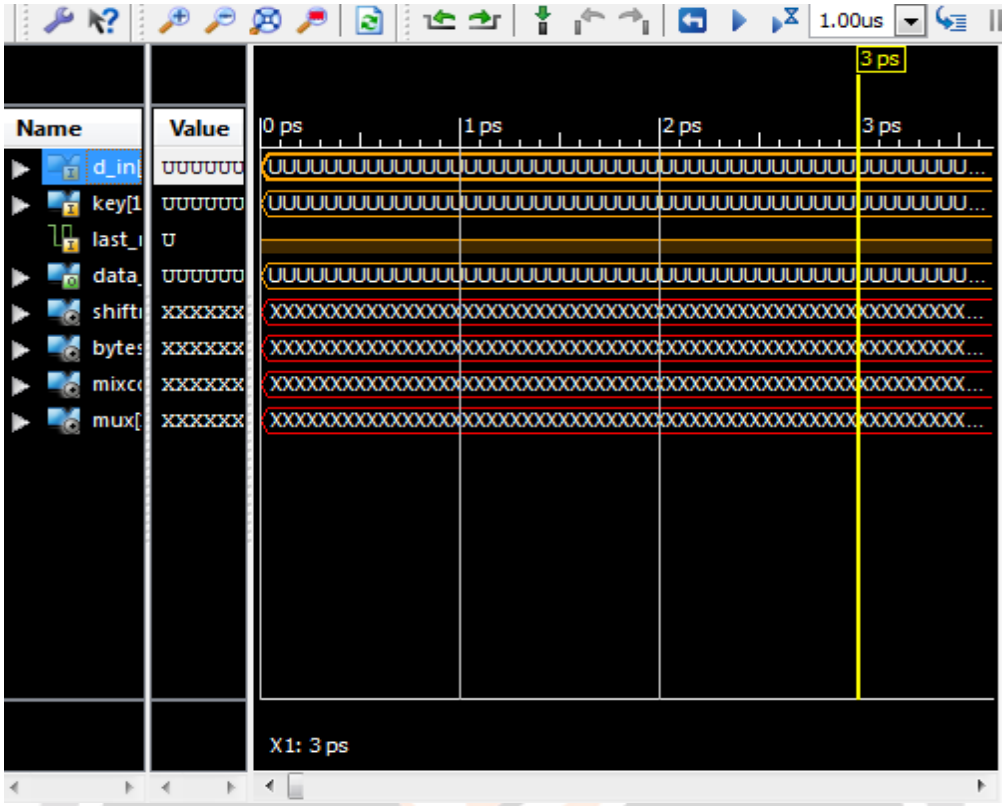

Fig -5: Round Output

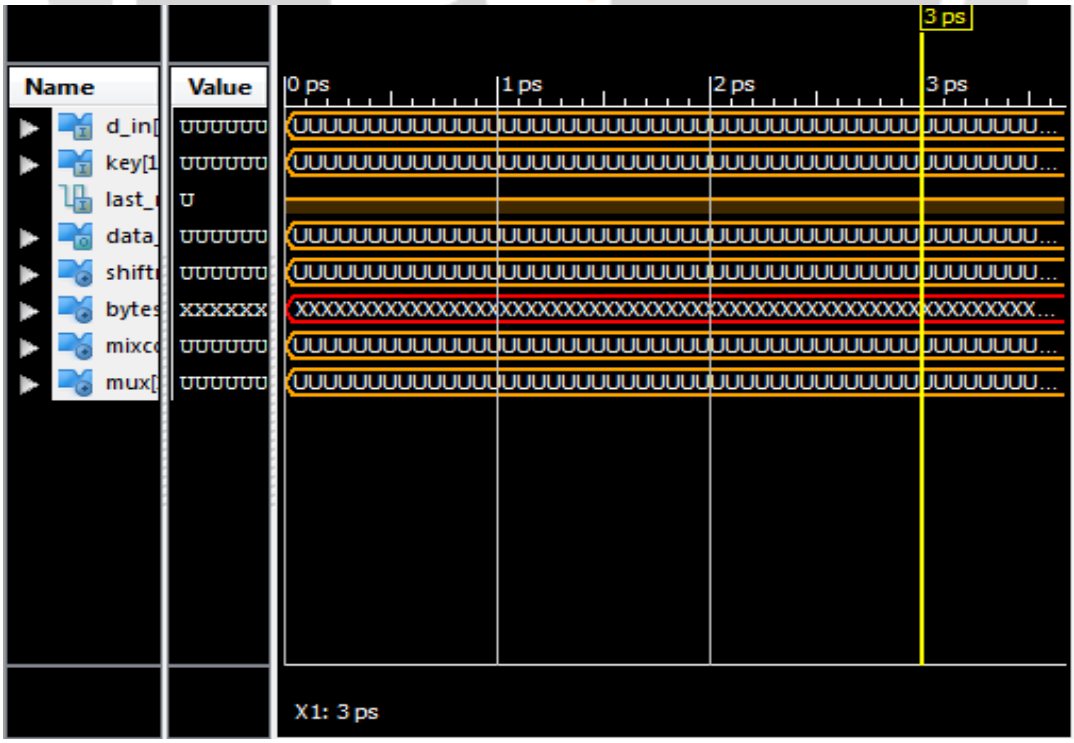

Fig- 6: Inverse Round Output

3.2 Prevention of Attacks

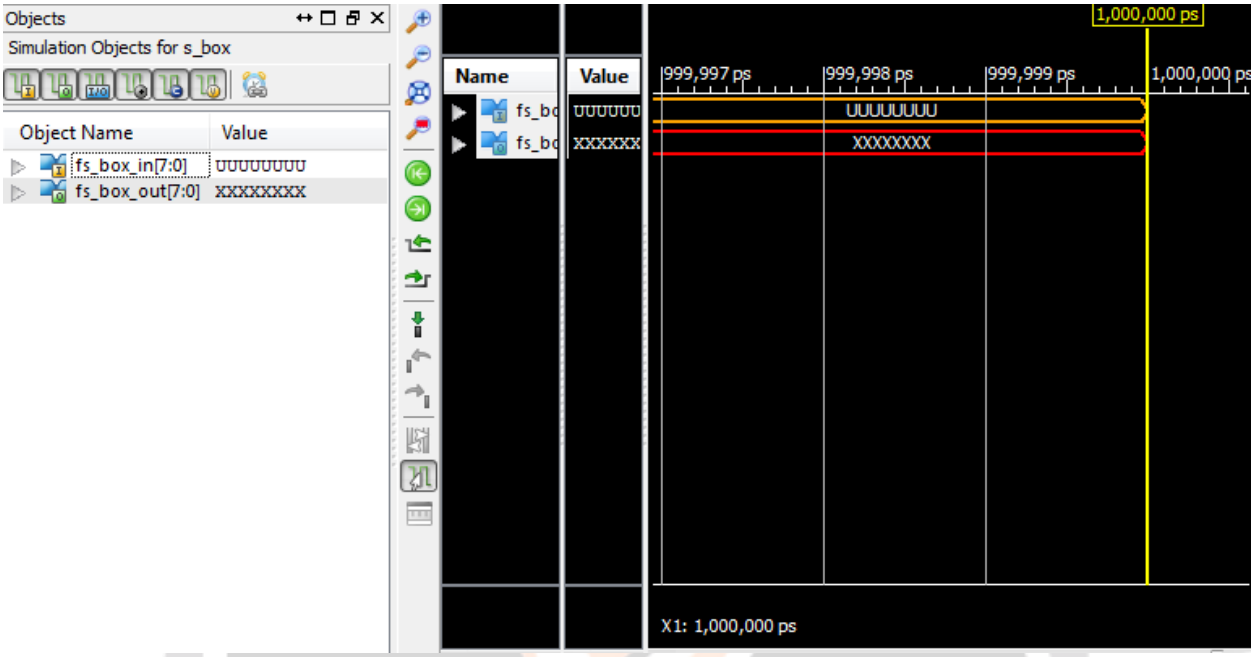

Fig -7: Prevention of Attacks.

4. CONCLUSIONS

This system provide the better security. As compared to other algorithm its processing speed is less. This system prevent the attacks. Asymmetric cryptography also gives the better security compared to symmetric algorithm. AES gains more popularity due to its high security and low acceptable cost.

REFERENCES

[1] National Institute of Standards and Technology. (2001, Nov.). FIPS-197: Advanced Encryption Standard, Gaithersburg, MD [Online]. Available: http://www.itl.nist.gov/fipspubs//

[2] Andrew S. Tanenbaum: "Computer Networks" by Prentice Hall.

[3] M. Feldhofer, S. Dominikus, and J. Wolkerstorfer, "Strong authentication for RFID systems using the AES algorithm," in Proc. CHES, vol. 3156. Aug. 2004, pp. 357–370.

[4] P. Hamalainen, T. Alho, M. Hannikainen, and T. D. Hamalainen, "Design and Implementation of Low-Area and Low-Power AES Encryption Hardware Core," in Proc. 9th Euromicro Conf. Digit. Syst. Design, Sep. 2006, pp. 577–583.

[5] L. Batina, J. Guajardo, T. Kerins, N. Mentens, P. Tuyls, and I. Verbauwhede, "Public-Key Cryptography for RFID-Tags," in Proc. RFID sec, 2006, pp. 1–16.

[6] Manisha Madhwani, Kavyashree C. V, Dr. Jossy P. George, "Cryptography on Android Message Application Using Look-Up Table and Dynamic Key" IOSR Journal of comp. Engg. Vol 6, issue, pp. 54-59, 2012.