AES Keys and Round Functions for Data Security

Preetinder Singh
RIMT MAEC, Mandi Gobindgarh,
Punjab, India

Ajay kumar
Beant college of engineering and technology
Gurdaspur , Punjab, India

ABSTRACT
Security is a basic requirement of an organization in the world to keep their information secure from their competitors. AES is the most recent algorithm which includes encryption with the help of reliable keys. It is used to protect the data including banking, financial, and government information. In this paper we analyzed various parameters of encryption techniques/algorithm. We encrypt the plain text by using different key size 128,192 and 256. On the basis of encryption time, other parameters can be determined e.g. processing time, round time, throughput etc. It is investigated that if clock frequency increases the throughput also varies.

Keywords
Encryption, Decryption, Processing time, Round time, Advanced Encryption Standard (AES).

1. INTRODUCTION
Various techniques and algorithms were developed by research organizations in order to achieve secure data transmission. These techniques include multiple passwords, encryption algorithms, biometrics, etc. Basic aim is to protect the data from hacker during transmission. Multiple passwords suffer from low entropy; much software is available in the market which is capable enough to break the model in few minutes. It has been observed that biometrics produces harmful effects on the body of user. In case of retina scanning rays are used this directly enters into the user's eyes. So, one does not want security of data at the cost of his health. Also, it is very hard to adjust the false acceptance ratio (FAR) and false rejection ratio (FRR) of a model. The strength of encryption algorithm depends upon its key management. Basically, key is a secret parameter (alphabet or number) known to both sender and recipient. It is used to define the type of cryptography; that means if same key is used to encrypt and decrypt the data then it is known as private key cryptography. On the other hand if different keys are used for both the process then it is known as public key cryptography as shown in Figure 1. Modern key cryptography becomes popular because it utilizes the concept of symmetrical and asymmetrical key cryptography. The key expansion is used to provide better security but increases the processing time. Encryption process depends on permutations and substitutions which results in cipher-text. It is of two types: transposition and substitution ciphers.

The order of plain-text rearranges in case of transposition cipher but the bits of plaintext are replaced by other bits systematically in substitution ciphers. Substitution boxes are used to replace the values of input matrix. At present various algorithms/ techniques are available in the markets such as Data Encryption standard (DES), Triple Data Encryption standard (TDES), Blowfish, International data encryption Algorithm (IDEA), AES, etc.

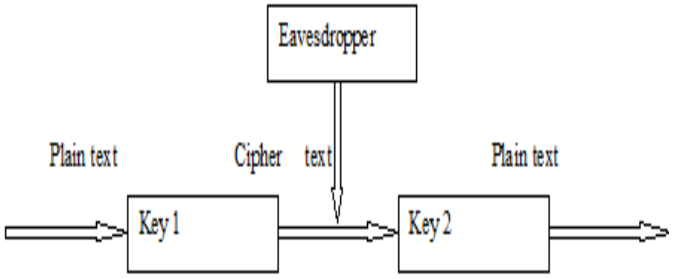

Figure 1: Encryption/Decryption process

2. LITERATURE REVIEW
Irma B. Fernandez [1] provided the technique for voice security over the packet switched channels and ISDN communication. The primary objective of the work was to develop and implement methodologies for successful data encryption schemes which can be embedded into the ISDN Customer Premises Equipment (CPE), which would make the public ISDN network look like a private network to the security conscious user. Hassina. G et. al, [3] proposed the development of rapid prototype and also discussed the applications of security algorithms along with the designing of rapid prototype through Rapid prototype of a fast data encryption standard with integrity processing for cryptographic applications. Bruce Schneier et. al [4] proposed an algorithm based upon permutations and substitutions. The algorithm supports fixed key size approach to secure the data. Specification for Advanced encryption standard [5] provides the whole mechanism for encryption algorithm for which Rijmen provided the concept of AES. It specifies the Rijndael algorithm a symmetric block cipher that can process data blocks of 128 bits, using cipher keys. However, lengths of Rijndael, which are required to handle additional block sizes and key lengths, are not adopted in this standard. Guido Bertoni et al [6] represented a growing market segment in which security is becoming an essential requirement. However, a proper software implementation of AES was of fundamental importance in order to achieve significant performance. The implementations presented in the literature differ in terms of the amount of look-up tables used for pre-computing the functions of the encryption decryption phase. This raises some questions regarding which AES implementation. Chih-Hsu Yen et al [7] proposed the idea to prevent the AES from suffering from differential fault attacks. This technique of error detection can be adopted to detect the errors during encryption or decryption. Because errors occur within a function, it was not easy to predict the output. Md. Nazrul Islam et al [8] presented the Effect of Security Increment to Symmetric Data Encryption through AES Methodology. The selective application of technological and related procedural safeguards was an important responsibility of every organization in providing adequate security to its electronic data systems. The algorithm uniquely defines the

mathematical steps required to transform data into a cryptographic cipher and also to transform the cipher back to the original form. DES use 64 bits block size as well as 64 bits key size that were vulnerable to brute force attack.

A choice of a particular algorithm depends upon the requirement of the encryption time, processing time, round time. TDES provides a large key to encrypt the data in order to achieve more secure model. It has been observed that increase in the key length leads to more processing time, thus hacker have more number of options to destroy the model. TDES has 192-bit key (but only uses 168 of them). TDES is three times slower than DES but it provides a billion times more secure algorithm. Advanced Encryption Standard (AES) was proposed by National institute of standards technology provides Rijndael named after two Belgium inventers Rijmen and Daemon. AES of 128 bit key provides equivalent security terms of 3072-bit RSA key. It is a round cipher having different key lengths 128,192 & 256. This algorithm overcomes the drawbacks of DES and TDES such as key size and processing time. The block size IDEA is 64 bits and key size is 128 bits and consists of eight rounds. Blowfish was developed by Bruce Schneier and was in running to become new AES [9-14].

In all these literatures the processing time is quite large. Moreover these literatures are silent about their ability to transmit data over radio frequency.

In present work, we have developed the program based upon Rijndael encryption algorithm because of its ability to transmit data over radio frequency and due to its minimum processing time. We have used this algorithm to find the encryption time, processing time, round time and throughput for different key sizes. The results obtained have been compared with various algorithms. From the analysis it has been found that as the clock frequency is increased, the processing time to encrypt the data is reduced.

3. AES ALGORITHM

AES Algorithm consists of two parts: Computational flow of AES includes various steps to complete its operation. The steps are briefly described given below and are shown in Figure 2. Four basic steps are involved in operations of AES computation flow: Add Round Key, Sub Bytes, Shift Rows and Mix Columns. The Add Round Key means plaintext is updated with the result of XOR operation of each individual Byte of round key and element of plaintext. The Substitute Byte is a non-linear byte substitution, it uses substitution table (S-Box) which is constructed by composing two transformations, first, polynomial m(x) ('11B') is ported, followed by an affine transformation. In Shift Rows the rows of the plaintext block are cyclically shifted to generate another matrix. The Mix Columns means transformation of four elements of each column of the plaintext by a polynomial multiplication. This multiplication is simple multiplication. This routine is final step for encryption process. Numbers of rounds are possible to encrypt the data. This varies from 10, 12, and 14 for different key sizes of 128,192,256 bits respectively.

Behind the scenes, the encryption routine takes the key array and uses it to generate a "key schedule" shown in Figure3.4.Expand this key stream by (4r+4) i.e. 32 bit words where r represents rounds {10, 12, 14}, Nk number of key segments {4, 6, 8}.It generates ith (32) bit word by XORing the (i - Nk)th word either with (i-1)th word or conditionally generated (i-1) word.

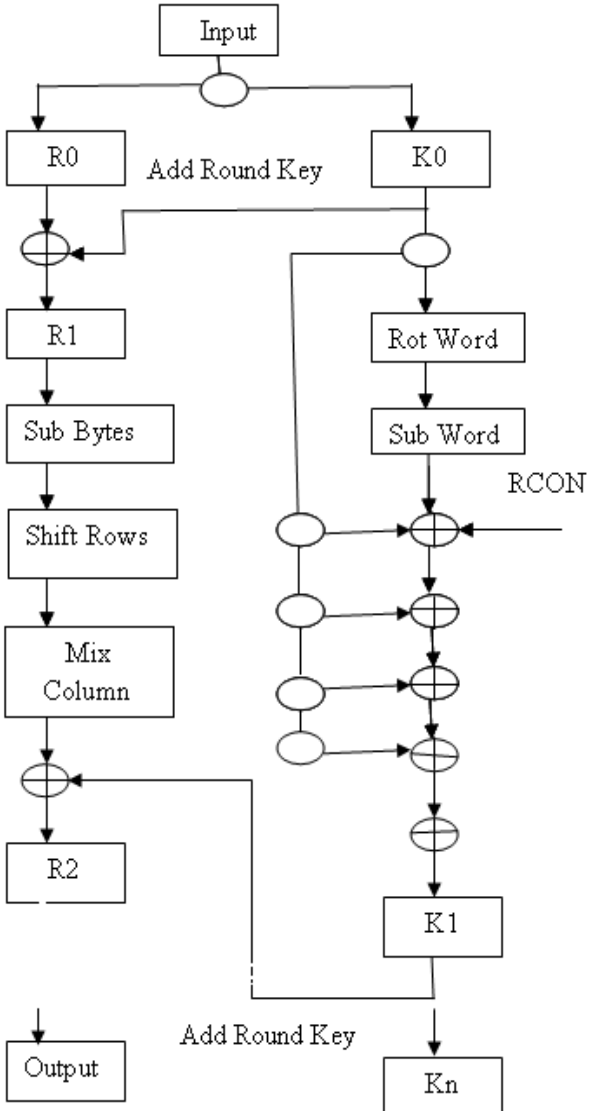

Figure 2 AES flow chart

$Nk \leq i \leq (4r+3)$

Rcon [i /Nk] = $[02^{i/Nk}, 00, 00,00]$

Rcon represents the round contants. The round functions are generated from original key value (0x00 through 0x17). The variable Nk represents the size of the seed key in 32-bit words. The point is that there are now many keys to use instead of just one. These new keys are called the round keys to distinguish them from the original seed key. The main loop of the AES encryption algorithm performs four different operations on the state matrix, which are named as Sub Bytes, Shift Rows, Mix Columns, and Add Round Key in the specification. The Add Round Key operation is the same as the preliminary Add Round Key except that each time Add Round Key is called; the next four rows of the key schedule are used. The Sub Bytes routine is a substitution operation that takes each byte in the State matrix and substitutes a new byte determined by the S-box table. Shift Rows is a permutation operation that rotates bytes in the state matrix to the left. Row 0 of State is rotated 0 positions to the left, row 1 is rotated 1 position left, row 2 is rotated 2 positions left and row 3 is rotated 3 positions left. The addition and

multiplication are special mathematical field operations, not the usual addition and multiplication on integers.

1.3 Theory

Processing time can be calculated by fly technique and are as follows:

$$T(\text{processing}) = K + V/F \quad (1)$$

$$V = N \times P + \text{offset} \quad (2)$$

K1: Constant part of the execution Time.

V: Variable part of the execution time.

F: System clock frequency.

N: Number of programmed bytes

P: Multiplication factor

Offset: Additive value

As per INFINEON [14] the values of factors K, P, offset are

K1= 4.48

P= 0.06

Offset = 0.27

Clock frequency = 16 MHz

$$\text{Round Time} = T(pr) \times (\text{Number of rounds} + 1) \quad (3)$$

We observe the processing time of different key sizes and observed that processing time of 256 bit key is more as compared to 192 and 128 bit streams at each frequency level. Figure 3 shows the encryption time for different key lengths, and is observed that encryption through higher order key requires more time as compared to low order key. Encryption time of AES depends upon of key length. Different algorithms take different times to manage the different keys but in AES case encryption and decryption is independent of key length.

4. RESULTS AND DISCUSSIONS

The 192 bit key requires 22 clock cycles to encrypt the data but 256 bit key requires 25 clock cycles to encrypt the data in the case of Pentium. TDES is the combination of three DES algorithms and provides the better security as compared to DES but with the cost of speed. So if we use a variable key size to encrypt the data it requires less time to set up the key parameters. Variable key provides the flexibility to users to choose their own key.

The processing time and encryption times for different key lengths for the developed program are tabulated in Tables 3 and 4 respectively for clock frequencies 16 MHz and 32MHz respectively. Throughput can be calculated by quoted values which are calculated for different keys.

Table 3 Timing table specifying Encryption, Processing and Round times at 16 MHz.

S. No	Key Size (bits)	Encryption time (ms)	Processing (ms)	Clock (MHz)	Round time (ms)	Throughput (Mbps)
1	128	0.60	4.496	16	49.4582	186.63
2	192	0.85	4.5043	16	58.5559	236.31
3	256	1.02	4.5124	16	67.686	273.06

Table 4 Timing table specifies Encryption, Processing and Round times at 32 MHz.

S.No	Key Size (bits)	Processing time (ms)	Clock (MHz)	Round time (ms)	Throughput (Mbps)
1	128	4.5072	32	49.5792	372.3636
2	192	4.5109	32	58.6417	472.6154
3	256	4.9728	32	67.2	546.1313

Figure 3 and 4 shows the comparison of processing times of 16 MHz and 32 MHz clock at diffrent key sizes (128,192, 256 bit). This shows that by using 32 MHz clock the processing time to encrypt the data raises by little bit as compared to 16 bit processor.So at 32 MHz clock the comparitive efficiency increases. The processing time and round time are functions of each other which is shown in Figures 3 and figure 4.

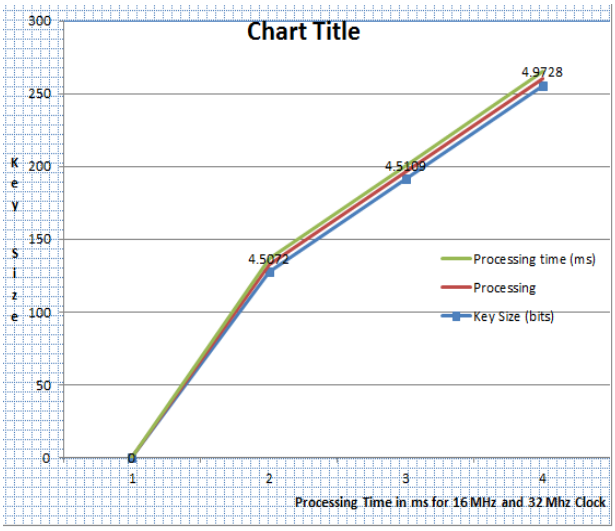

Figure 3: Key Size Vs processing time (ms) at different clock frequencies

As from the above results we observe that processing time of 256 bit key is more as compared to 192 and 128 bit streams. The 16 MHz clock is used than these are more time consuming then a 32 MHz clock as shown in Figure 4. The round time is the time to calculate the data during its processing it is more in the case of 32 Mhz than 16 MHz in respective key sizes.The encryption time for ddiffrent key sizes is shown in figure 6.

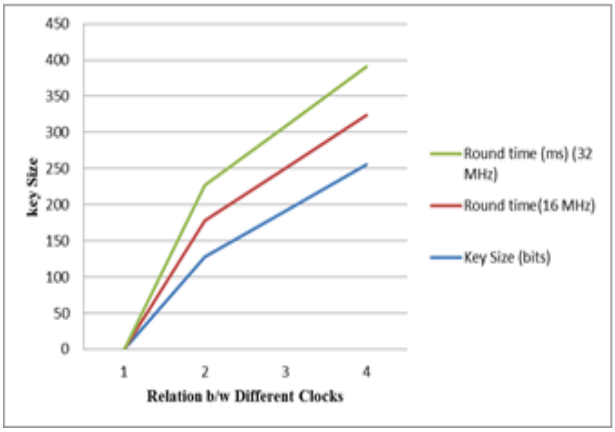

Figure 4: Comparison between Round Time of different Key sizes at 16 MHz and 32 MHz Clock Frequencies

Comparison of throughput at 16 MHz and 32 Mhz clock frequencies in fogure 5 shows that throughput of 32 MHz clock is more as compared to 16 MHz clock for diffrent key patterns which means ability to deliever the information accurately and efficiently. The main advantage of high throughput is that we can use the same algorithm in optical networks.

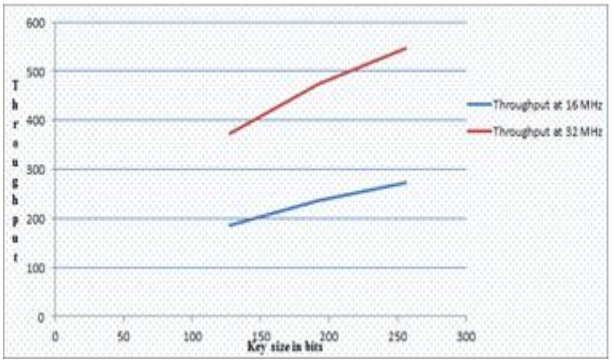

Figure 5 : Comparison of Throughput versus key size at 16 MHz and 32 MHz Clock Frequencies

Figure 6 shows time to encrypt the data at different key levels by using Rijndael algorithm (AES). As from the above calculations we found that the main advantage of this algorithm is that if we use a short stream containing bits for encryption of data than it takes less time as compared to the 128 bit long stream to encrypt the data. So encryption time is variable depends upon key length and data streams. For 32 MHz clock the processing time and time duration to complete the number of rounds is less comparatively so it is time efficient mechanism.

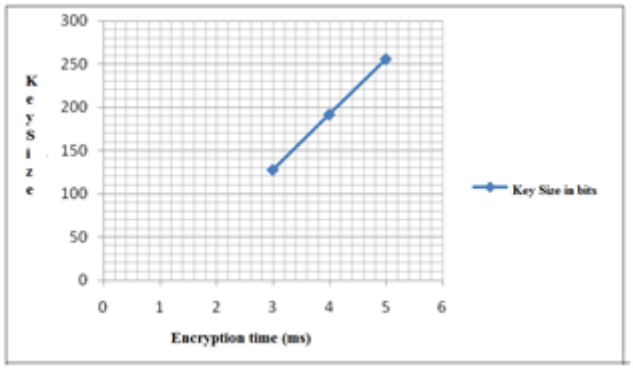

Figure 6: Encryption Time versus Key

5. CONCLUSION

This network can be used for providing enhanced security for optical glass fibre networks so it can be used at optoelectronic networks. In this paper we concluded that Rijndael algorithm is time efficient for short stream containing bits for encryption of data. This Algorithm provides flexibility to user to choose different key sizes. Throughput increases with increase in frequency level but the processing time is reduced at high frequency level. The round time is the function of processing time so with frequency it also reduces. Rijndael provides a security equivalent to RSA of 3072 bit key and also overcome the drawbacks of DES and TDES. It is also concluded that if the throughput is increased then the same algorithm can be implemented on optical networks.

6. REFERENCES

[1] Irma B. Fernandez, M. S. E. E. Wunnava V. Subbarao, "Encryption based Security for ISDN Communication Technique & Application" IEEE transactions, pp.70-73, 1994.

[2] Hassina Guendouz & Samir Bouaziz, "Rapid prototype of a Fast Data Encryption Standard with Integrity Processing for Cryptographic Applications" IEEE, pp.VI-434-437, 1994.

[3] Bruce Schneier and Mudge, "Cryptanalysis of Microsoft's PPTP Authentication Extensions (MS-CHAPv2)", CQRE '99, Springer-Verlag, pp. 192-203, 1999.

[4] Federal Information Processing Standards, "Specification for advanced encryption standard" Publication 197, pp.1-47, 2001.

[5] Guido Bertoni; Aril Bircan; Luca Breveglieri; Pasqualina Fragneto; Marco Macchetti. Vittorio Zaccaria; "Performances of the Advanced Encryption Standard in embedded Systems with Cache Memory" IEEE transactions, 2003.

[6] Chih-Hsu Yen and Bing-Fei Wu, "Simple Error Detection Methods for Hardware Implementation of Advanced Encryption Standard", IEEE transactions on computers, vol.55, no. 6, pp.720-731, June 2006.

[7] Md. Nazrul Islam, Md. Monir Hossain Mia, Muhammad F. I. Chowdhury, M.A. Matin, "Effect of Security Increment to Symmetric Data Encryption through AES Methodology", IEEE Ninth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing, pp 291-294, 2008.

[8] J. Daemen and V. Rijmen, AES Proposal, "Rijndael, AES Algorithm", Dr. Brian Gladman, v3.1, 3rd March 2001.

[9] Jingmei Liu1, Baodian Wei2, Xiangguo Cheng1, Xinmei Wang1, "An AES S-box to Increase Complexity and Cryptographic Analysis",IEEE, Proceeding of 19th International Conference on Advanced Information Networking and Applications, pp. 1-5,2005.

[10] Saleh Abdel-hafeez, Ahmed Sawalmeh, Sameer Bataineh "AES Design using pipelining structure Over GF(2^4)2", IEEE International Conference on Signal Processing and Communications, Dubai, United Arab Emirates, pp.716-719,24-November, 2007.

[11] Zhao Xinjie, WANG Tao, Mi Dong, Zheng Yuanyuan, Lun Zhaoyang "Robust First Two Rounds Access Driven Cache Timing Attack on AES",International Conference on Computer Science and Software Engineering, IEEE transactions, pp. 785-788, 2008.

[12] Ashwini M. Deshpande, Mangesh S. Deshpande, Devendra N. Kayatanavar, "FPGA Implementation of AES Encryption & Decryption", International conference on control automation, communication and energy conservation, pp.1-6,4th-6th June 2009.

[13] Chi-Feng Lu; Yan-Shun Kan; Hsia-Ling Chiang; Chung-Huang Yang; "Fast Implementation of AES Cryptographic Algorithms in Smart Cards" research of NexSmart Technology, Inc. Taipei, Taiwan, R.O.C. IEEE pp: 573-579,2003.

[14] Aamer Nadeem, Dr. M. Younus Javed "A Performance Comparison of Data Encryption Algorithms", International Conference on Information and Communication Technologies, pp. 84-89, 2005.

7. AUTHORS PROFILE

Er. Preetinder Singh, Assistant Professor RIMT MAEC Mandi Gobindgarh Punjab, India. (Associated Research through BCET/ Govt college Gurdaspur,Punjab,India.)

Dr. Ajay Kumar, Associate Professor and Registrar Establishment Beant college of Engineering and technology, Punjab, India.