ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 10, October 2013

Comparative Implementation of Cryptographic Algorithms on ARM Platform

Ms. Pallavi H.Dixit [1], Dr.Uttam L. Bombale [2], Mr. Vinayak B.Patil [3]

M-Tech (Electronics) Student, Department of Technology, Shivaji University, Kolhapur, Maharashtra, India [1]

Professor, Department of Technology, Shivaji University, Kolhapur, Maharashtra, India [2]

M-Tech (Electronics) Student, Department of Technology, Shivaji University, Kolhapur, Maharashtra, India [3]

Abstract: This paper present the comparison between two cryptographic algorithm AES and Blowfish algorithm on the basis of ARM implementatiom.LPC 2148 from NXP Philips family kit is used for implementation. In Embedded system security blowfish is suitable. For comparison, we considered points like memory size, encryption cycle, and decryption cycle for both algorithms on ARM7 etc. For small embedded system like mobile, smart card etc Blowfish is best algorithm for security.

Keywords: Encryption, Decryption, AES, Blowfish

I. INTRODUCTION

CRYPTOGRAPHY algorithms are divided into Symmetric and Asymmetric key cryptography [1]. Symmetric key encryption use only key to encrypt and decrypt data. Key plays an important role in encryption and decryption. If a weak key is used in the algorithm then easily data can be decrypted. The size of the key determines the strength of Symmetric key encryption. Symmetric algorithms are of two types: block ciphers and stream ciphers. The block ciphers are operating on data in groups or blocks. .Examples is of Data Encryption Standard (DES), Advanced Encryption Standard (AES) and Blowfish. Stream ciphers are operating on a single bit at a time. RC4 is stream cipher algorithm. In Asymmetric key encryption, two keys are used; private keys and public keys. Public key is used for encryption and private key is used for decryption (e.g Digital Signatures). Public key is known to the public and private key is known only to the user Plain Text is the original message that we wish to communicate with the others is defined as Plain Text.

In cryptography the actual data that has to be send to the other is referred as Plain Text. For example, Alice is a person. Wishes to send "Congratulation" message to the person Duke. Here "Congratulation" is a plain text message. Cipher Text is the message which has been converted by the encryption algorithm is called cipher text. In cryptography the original message is transformed into non readable message. Encryption is a process of converting plain text into cipher text is called as Encryption. Cryptography uses the encryption algorithm and a key to send confidential data through an insecure channel. Decryption is a reverse process of encryption is called decryption. It is a process of converting cipher text into plain Text. Decryption requires decryption algorithm and a key. Cryptography provides a number of security goals to ensure the privacy of data, non alteration of data cryptography it is widely used today due to the great security advantages of it. Here are the various goals of cryptography.

Confidentiality: Information in computer is transmitted and has to be accessed only by the authorized party and not by anyone else.

Authentication: The information received by any system has to check the identity of the sender that whether the Information is arriving from a authorized person or a false identity.

Integrity: Only the authorized party is allowed to modify the transmitted information. No one in between the sender and receiver are allowed to alter the given message.

Our PDAs store personal e-mail and contact lists; GPS receivers and, soon, cell phones keep logs of our movements; and our automobiles record our driving habits. On top of that, users demand products that can be reprogrammed during normal use, enabling them to eliminate bugs and add new features as firmware upgrades become available.

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 10, October 2013

II. RELATED WORK:

In paper [5] "Superiority of Blowfish Algorithm" in this paper comparison takes place on java. Comparison between four most common and used symmetric key algorithms: DES, 3DES, AES and Blowfish. A comparison has been made on the basis of these parameters: rounds block size, key size, and encryption / decryption time, CPU process time in the form of throughput and power consumption. These results show that blowfish is better than other algorithm.

In paper [7] comparison takes place in symmetric cryptographic algorithm by taking software and hardware support.

In paper [6] they said that AES is faster and more efficient than other encryption algorithms. When the transmission of data is considered there is insignificant difference in performance of different symmetric key schemes. Under the scenario of data transfer it would be better to use AES scheme in case the encrypted data is stored at the other end and decrypted multiple times.

Paper [2] Discussed for different popular secret key algorithms such as DES, 3DES, AES, and Blowfish. They were implemented, and their performance was compared by encrypting input files of varying sizes and contents.

In paper [4] consider the performance of encryption algorithm for text files .AES, DES and RSA algorithm has been evaluated from the parameters like Computation time, Memory usage, Output bytes. Comparing these three algorithms they found RSA takes more time for computation process. The memory usage of each algorithm is considered as memory byte level. RSA takes more memory than AES and DES. Finally, the output byte is calculated by the size of output byte of each algorithm. The level of output byte is equal for AES and DES, but RSA algorithm produces low level of output byte.

III. PROPOSED WORK

This paper presents comparison between AES and BLOWFISH algorithms on cryptography. Here we used 32 bit ARM LPC 2148 platform to implement these algorithm. Comparison taken place on various points like key length, block size, encryption time and decryption time, simplicity, security. Proposed block diagram as shown in figure 1.

We considered two algorithms separately. Text and key given to ARM kit by PC serially. We create simple GUI on PC using visual basic 6. Code is written in embedded c for both algorithms. Keil 4.0 compiler used to run programs. Then the encrypted text displayed on LCD.

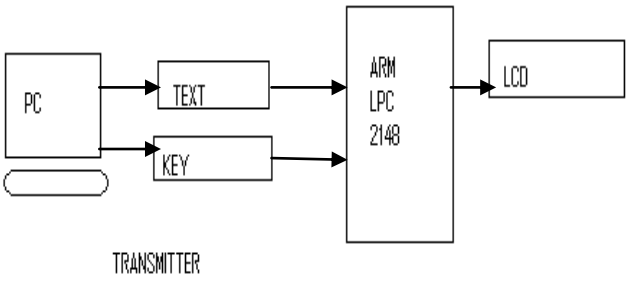


Fig 1. Block Diagram

A. *Need of ARM implementation:*

A software implementation of a cryptography scheme provides the benefits of flexibility, speed of implementation, and lower cost over time.

More importantly, the NXP ARM microcontrollers feature. In Application Programming (IAP) and the popular LPC2300 and LPC2400 series also feature Ethernet, USB and CANIAP allows customers to periodically change the security algorithm in the field whether or not the product has been comprised.

Competitive hardware encryption cannot be updated without replacing the microcontroller, which is costly and complicated [8].

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 10, October 2013

B. *ARM kit description:*

The LPC2148 microcontrollers are based on a 32/16 bit ARM7TDMI-S CPU with real-time emulation and embedded trace support, that combines the microcontroller with embedded high speed flash memory ranging from 32 kB to 512 kB. A 128-bit wide memory interface and a unique accelerator architecture enable 32-bit code execution at the maximum clock rate. For critical code size applications, the alternative 16-bit Thumb mode reduces code by more than 30 % with minimal performance penalty. Due to their tiny size and low power consumption, LPC2148 are ideal for applications where miniaturization is a key requirement, such as access control and point-of-sale. A blend of serial communications interfaces ranging from a USB 2.0 Full Speed device, multiple UARTs, SPI, SSP to I2Cs, and on-chip SRAM of 8 kB up to 40 kB, make these devices very well suited for communication gateways and protocol converters, soft modems, voice recognition and low end imaging, providing both large buffer size and high processing power. Various 32-bit timers, single or dual 10-bit ADC(s), 10-bit DAC, PWM channels and 45 fast GPIO lines with up to nine edge or level sensitive external interrupt pins make these microcontrollers particularly suitable for industrial control and medical systems

C. *Algorithm description*

1. AES

(Advanced Encryption Standard), also known as the Rijndael (pronounced as Rain Doll) algorithm, is a symmetric block cipher that can encrypt data blocks of 128 bits using symmetric keys 128, 192, or 256. AES was introduced to replace the DES. Brute force attack is the only effective attack known against this algorithm. The 128 bit data block is divided into 16 bytes, which are represented by a 4X4 matrix of bytes. The entries are denotes by,

S0,0, S0,1, S0,2, S0,3,
S1,0, S1,1, S1,2, S1,3,
S2 0, S2,1, S2,2, S2,3,
S3,0 , S3,1, S3,2, S3,3

The matrix represents a state *S*. All the four transformations map an input state to an output state. The AddRoundKey involves only one bit-wise XOR operation between the state *S* and the round key. The shiftRows cyclically shifts k bytes to the left on kth row of the state matrix, k=0~3. The position changes to,

s0.0 s0,1 s0,2 s0,3
s1.1 s1,2 s1,3 s1,0
s2.2 s2,3 s2,0 s2,1
s3.3 s3,0 s3,1 s3,2

The MixColumn uses each column of the state matrix as a polynomial over GF(28)and multiples them modulo x+1 with a polynomial a(x) ={03}x +{01}x + {01}x + {02}.

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 10, October 2013

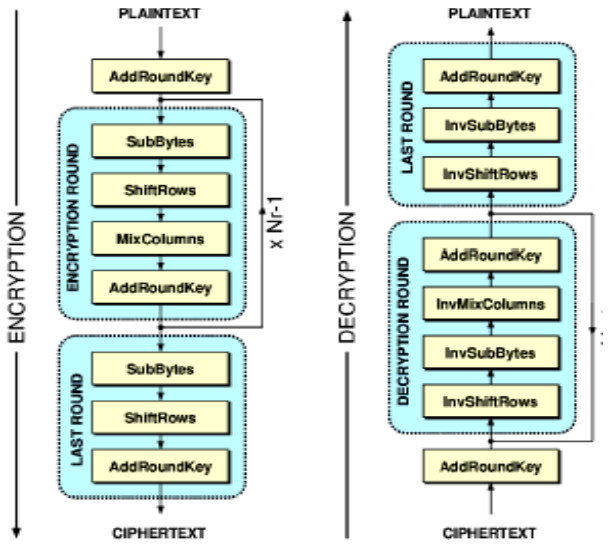


Fig 2. Operation of AES algorithm

2. BLOWFISH:

Blowfish is a symmetric block cipher that can be effectively used for encryption and safeguarding of data. It takes a variable-length key, from 32 bits to 448 bits, making it ideal for securing data. *Blowfish* was designed in 1993 by **Bruce Schneier** as a fast, free alternative to existing encryption algorithms. *Blowfish* is unpatented and license-free, and is available free for all uses. *Blowfish Algorithm* is a **Feistel Network**, iterating a simple encryption function 16 times. The block size is 64 bits, and the key can be any length up to 448 bits. Although there is a complex initialization phase required before any encryption can take place, the actual encryption of data is very efficient on large microprocessors. *Blowfish* is a variable-length key block cipher. It is suitable for applications where the key does not change often, like a communications link or an automatic file encryptor. A graphical representation of the Blowfish algorithm appears in Figure 3. In this description, a 64-bit plaintext message is first divided into 32 bits. The "left" 32 bits are XORed with the first element of a P-array to create a value

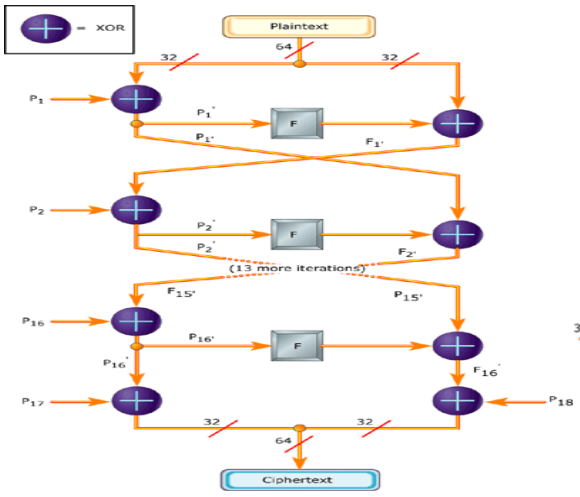


Fig 3. Operation of Blowfish algorithm

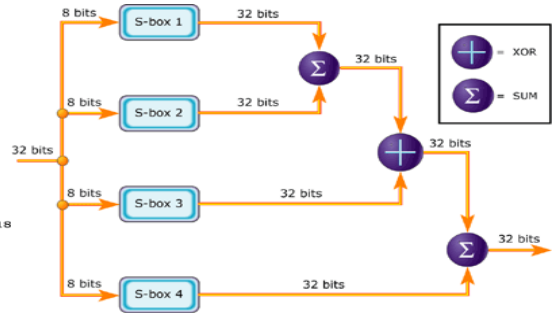


Fig 4. Operation of function F

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 10, October 2013

we'll call P', run through a transformation function called F, then XORed with the "right" 32 bits of the message to produce a new value I'll call F'. F' then replaces the "left" half of the message and P' replaces the "right" half, and the process is repeated 15 more times with successive members of the P-array. The resulting P' and F' are then XORed with the last two entries in the P-array (entries 17 and 18), and recombined to produce the 64-bit ciphertext.

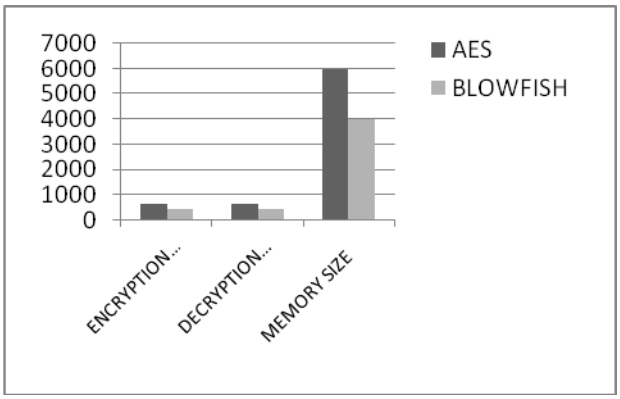
IV. EXPERIMENTAL RESULT

Fig 5. ARM LPC 2148 Kit With LCD

A. *Practical analysis*

ALGORITHM	AES	BLOWFISH
BLOCK SIZE IN BIT	128	64
KEY SIZE IN BIT	64	64 TO 448
MEMORY SIZE IN BYTE	5966	4011
ENCRYPTION TIME(cycle)	639	440
DECRYPTION TIME(cycle)	638	443

B. Graphical presentation:



From graph and table, it is clear that AES algorithm and BLOWFISH implementation on ARM LPC2148 are possible. Both are working smoothly on 32 bit platform separately. When we measure encryption time, decryption time it is observed that ARS require more cycles than BLOWFISH.

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 10, October 2013

V. CONCLUSION

From results, it is shown that, blowfish algorithm requires less time to perform, so in that case blowfish is good. As the algorithm steps consider AES is more complex algorithm than BLOWFISH, it is good for security and key size is fixed for AES as blowfish have variable key size. Memory requirement is less in BLOWFISH. For small embedded system like mobile, smart card etc Blowfish is best algorithm for security.

REFERENCES

[1] IEEE paper on "performance analysis of symmetric key cryptography algorithms: des, aes and blowfish" by o p verma 2011.
[2] IEEE paper on "a study of des and blowfish encryption algorithm" by tingyuan nie , teng zhang
[3] IEEE paper on "high speed soc design for blowfish cryptographic algorithm" by cody, brian ; kulicke & soffa industries, usa ; madigan, justin ; macdonald, spencer ; hsu, k.w.
[4] IEEE paper on "aes encryption algorithm based on the high performance computing of gpu" by fei shao, zinan chang, yi zhang.
[5] "Superiority of Blowfish Algorithm" by Pratap on Volume 2, Issue 9, September 2012 ISSN: 2277 128X International Journal of Advanced Research in Computer Science and Software Engineering
[6] Shashi Mehrotra Seth, Rajan Mishra on " Comparative Analysis Of Encryption Algorithms For Data communication " in IJCST Vol. 2, Issue 2, June 2011 I ,pp. 292-294
[7] Nagesh Kumar, Jawahar Thakur, Arvind Kalia on "PERFORMANCE ANALYSIS OF SYMMETRIC KEY CRYPTOGRAPHY ALGORITHMS:DES , AES and BLOWFISH " in An International Journal of Engineering Sciences ISSN: 2229-6913 Issue Sept 2011, Vol. 4 ,pp.28-37.
[8] Pratap et al., International Journal of Advenced Research in Computer Science and Software Engineering 2(9), September - 2012, pp. 196-201 © 2012, IJARCSSE All Rights Reserved Page | 201
[9] Ruangchaijatupon, P. Krishnamurthy, ,,"Encryption and Power Consumption in Wireless LANs-N,"The Third IEEE Workshop on Wireless LANs -September 27-28, 2001- Newton, Massachusetts.
[10] Fast Software AES Encryption Dag Arne Osvik1, Joppe W. Bos1, Deian Stefan2, and David Canright3
[11] Intel Strong ARM SA-1110 Microprocessor. Developer's Manual 278240-003, Intel Corporation, Jun 2000.
[12] Arm Ltd. website. http://www.arm.com.
[13] Intel Ltd. website. http://www.intel.com.
[14] A survey of Rijndael implementations. http://www.tcs.hut.fi/_helger/aes/rijndael.html.

BIOGRAPHY

Ms. Pallavi Hemant Dixit did her B.E (E&TC) from Shivaji University, Kolhapur in the year 2008. She is pursuing her M-TECH (Electronics) from Department of Technology, Shivaji University, Kolhapur. She has a total of 04 years of experience in teaching. She has presented 2 papers in National Conferences. She has attended number of workshops on various subjects.

Prof. Dr. U.L Bombale Has received PhD from Dhirubhai Ambani Institute of Information & Communication Technology, (DA-IICT) Gandhinagar, Gujarat, India, under the guidance of Dr. Sanjeev gupta. M.E in Electronics & Telecommunication in 1994 from COE, Pune, and currently he is working as a Professor in Dept. of Technology, Shivaji university, Kolhapur (India).

Mr. Vinayak Bajirao Patil did his B.E (Electronics) from Shivaji University, Kolhapur in the year 2010. He is pursuing her M-TECH (Electronics) from Department of Technology, Shivaji University, Kolhapur. He has a total 02 years of experience in teaching. He has presented 1 paper in National Conference. He has attended number of workshops on various subjects