IMPLEMENTATION OF AES AND BLOWFISH ALGORITHM

Chaitali Haldankar[1], Sonia Kuwelkar[2]

[1]Electronics and Telecommunication, GEC, Goa, India
[2]Electronics and Telecommunication, GEC, Goa, India

Abstract

Small embedded devices (including smart cards, RFID, sensor nodes) are now deployed in many applications. They are usually characterized by strong cost constraints. Yet, as they may manipulate sensitive data, they also require cryptographic protection .As a result, many algorithms have been proposed in order to allow strong security at lower cost than standard solution and lack of comparative studies prevent a good understanding for these cryptographic algorithms. Thus in this thesis we study the cryptographic algorithms like AES and Blowfish and compare different parameters and then do further implementation as the implementation of encryption/decryption algorithm is the most essential part of the secure communication. The algorithms are further considered for VLSI implementation. The evaluation is performed in terms of encryption speed, the CPU utilization with time and the battery power consumption. The experimental results specify the efficiency of the algorithms.

Keywords: *Plain text, Cipher text, Encryption, and Decryption*

---***---

1. INTRODUCTION

Cryptography is the science of information and communication security. It entered in mass product markets quite recently and every citizen from developed countries uses it daily. It is used for authentication and encryption(bank card, e-commerce, pay-TV), access control (carlock systems, ski lifts), payment (prepaid telephone cards, e-cash), and may become the fundamental instrument of democracy with the advent of e-voting systems. To master cryptographic tools becomes a requirement for most engineers Cryptographic Algorithms plays a major role in implementation of encrypting the data. As the complexity of algorithm is high the risk of breaking the original plaintext from that of cipher text is less. Greater complexity means greater security.

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 are 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 Fig.1 shows the overview field of cryptography.

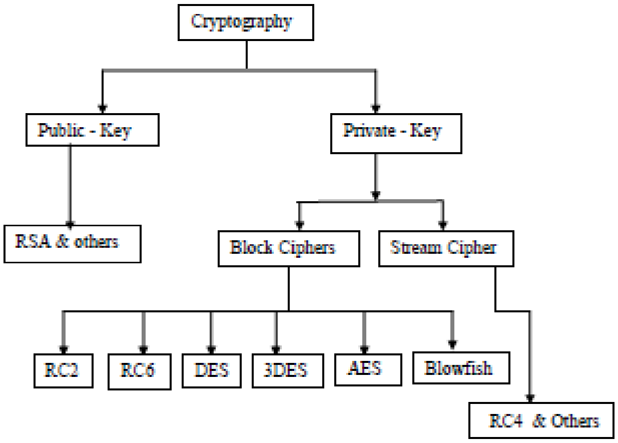

Fig -1: Overview of field of cryptography

1.1 Various Goals

1) Confidentiality
Information in computer is transmitted and has to be a accessed only by the authorized party and not by anyone else.
2) 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.
3) 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.
4) Non Repudiation
Ensure that neither the sender, nor the receiver of message should be able to deny the transmission.

5) Access control
Only the authorized parties are able to access the given information.

1.2 Basic Terms

1) Plain Text
The original message that the person wishes to communicate with the other is defined as Plain Text. For example, Alice is a person wishes to send "Hello Friend how are you" message to the person Bob. Here "Hellow Friend how are you" is a plain text message.
2) Cipher Text
The message that cannot be understood by any one or a meaningless message is what we call as Cipher text. For Example, "Ajd672#@91ukl8*^5%" is a Cipher Text produced for "Hello Friend how are you".
3) Encryption
A process of converting plain text into cipher text is called as Encryption. The process of encryption requires two things- an encryption algorithm and a key. An encryption algorithm means the technique that has been used in encryption. Encryption takes place at the sender side.
4) Decryption
A reverse process of encryption is called as Decryption. It is a process of converting Cipher text into Plain text. The process of decryption requires two things- a decryption algorithm and a key. A decryption algorithm means the technique that has been used in Decryption. Generally the encryption and decryption algorithm are same.
5) Key
A key is a numeric or alpha numeric text or may be a special symbol. The key is used at the time of encryption takes place on the plain text and at the time of decryption takes place on the cipher text. For example, if the Alice uses a key of 3 to encrypt the plain text "President" then cipher text produced will be "Suhylghqw".

2. CRYPTOGRAPHIC ALGORITHMS

There are number of cryptographic algorithms used for encryption data and most of all fall into two generic categories Public key system and secret key system. Symmetric key algorithm is known as secrecy key or shared key algorithm. Because in symmetric key algorithm a shared key does both the encryption and decryption. Only one key is used for doing everything, so the success of algorithm depends on two factors-secrecy of the key and its distribution. Symmetric algorithms are: Data Encryption Standard (DES), Triple DES (3DES), International Data Encryption algorithm (IDEA), Blowfish, Advanced Encryption Standard (AES). Asymmetric key algorithm is also known as public key algorithm. In this algorithm, there are two keys public and private used for encryption and decryption. Public key is used to encrypt the message and private key is used to decrypt the message. Asymmetric algorithms are Diffe-Hellman and RSA Public Key Encryption. Symmetric key technique uses a single key called secret key which uses less mathematics, results in less computation, on the other hand asymmetric key technique uses both public and private keys, results in more processing and consumes more energy. Symmetric key techniques offer better energy efficiency as compared to public key that is why most researches use it for creating MAC in WSN.

2.1 AES

The NIST [1] selected the Rijndael algorithm, which was developed by Joan Daemen and Vincent Rijmen, to replace the dataencryption standard (DES) algorithm [2] as the new advanced encryption standard (AES) algorithm [3].

AES is based on a design principle known as a substitution-permutation network. AES has 128-bit block size and a key size of 128,192 or 256 bits [1].AES operates on a 44 column-major order matrix of bytes, termed the state. Most AES calculations are done in a special finite field. The AES cipher is specified as a number of repetitions of transformation rounds that convert the input plaintext into the final output of cipher text. The number of cycles of repetition are as follows:
a. 10 cycles of repetition for 128 bit keys.
b. 12 cycles of repetition for 192 bit keys.
c. 14 cycles of repetition for 256 bit keys.

Each round of encryption process requires the following four types of operations: SubBytes , ShiftRows , MixColumns, XorRoundkey. Decryption is the reverse process of encryption and using inverse functions: InvSubBytes, InvShiftRows, InvMixColumns[4].

A simpler way to view the AES function order is:
16
1. Scramble each byte (SubBytes).
2. Scramble each row (ShiftRows).
3. Scramble each column (MixColumns).
4. Encrypt (AddRoundKey).

2.2 Blowfish

Blowfish is a 64-bit symmetric block cipher with variable length key. The algorithm operates with two parts: a key expansion part and a data encryption part. The role of key expansion part is to converts a key of at most 448 bits into several sub key arrays totalling 4168 bytes. The data encryption occurs via a 16-round Feistel network . It is only suitable for application where the key does not change often, like communications link or an automatic file encryption. It is significantly faster than most encryption algorithms when implemented on 32-bit microprocessors with large data caches .The nature of encryption algorithms is that, once any significant amount of security analysis is done, it is very undesirable to change the algorithm for performance reasons, thereby invalidating the results of the analysis. Thus, it is imperative to consider both security and performance together during the design phase. While it is impossible to take all future computer architectures into consideration, an understanding of general optimization guidelines, combined with exploratory software implementation on existing architectures to calibrate performance, should help achieve higher speed in future encryption algorithms.

2.2.1 Subkeys

Blowfish uses a large number of subkeys. These keys must be precomputed before any data encryption or decryption.

The P-array consists of 18 32-bit subkeys: P1, P2,..., P18.

There are four 32-bit S-boxes with 256 entries each:
S1,0, S1,1,..., S1,255;
S2,0, S2,1,..,, S2,255;
S3,0, S3,1,..., S3,255;
S4,0, S4,1,..,, S4,255.

2.2.2 Pseudo Code of Blowfish Algorithm

```
    begin itemize
Blowfish has 16 rounds.
The input is a 64-bit data element, x.
Divide x into two 32-bit halves: xL, xR.
Then, for i = 1 to 16:
        xL = xL XOR Pi
        xR = F(xL) XOR xR
Swap xL and xR
```

After the sixteenth round, swap xL and xR again to undo the last swap.

Then, xR = xR XOR P17 and xL = xL XOR P18.

Finally, recombine xL and xR to get the ciphertext.

Decryption is exactly the same as encryption, except that P1, P2,..., P18 are used in the reverse order. Implementations of Blowfish that require the fastest speeds should unroll the loop and ensure that all subkeys are stored in cache.

3. COMPARISON OF ALGORITHMS

Table -1: Comparison of algorithms

Algorithm	Block Size	Rounds	Key
AES	128,192,256 Bits	10,12,14 Rounds	128 Bits
BLOWFISH	32-448 Bits	16 Rounds	64 Bits

4. SIMULATION RESULTS

The calculation for Encryption and Decryption speed of each algorithm for different packet sizes is done. Their implementation has tried to optimize the maximum performance for the algorithm. The throughput for encryption as well as decryption is calculated one by one. Encryption time is used to calculate the throughput of an encryption scheme The performance metrics are analyzed in matlab by
(a) Encryption/decryption time.
(b) CPU process time

Table -2: Comparison of algorithms with respect to time in seconds

algorithm	Encryption/decryption For 64 bits	CPU Time
AES	1.261816	1.54440990
BLOWFISH	0.850568721	0.07800050

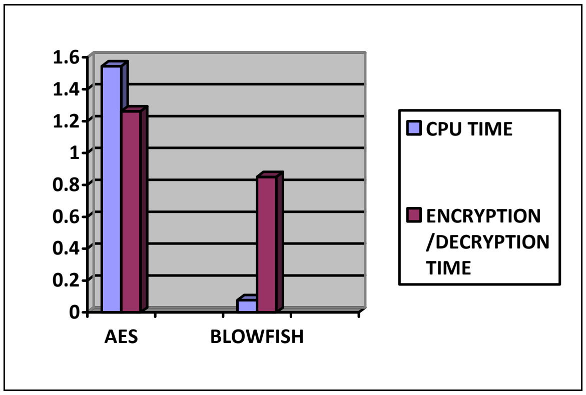

Chart -1: Comparison of AES and Blowfish

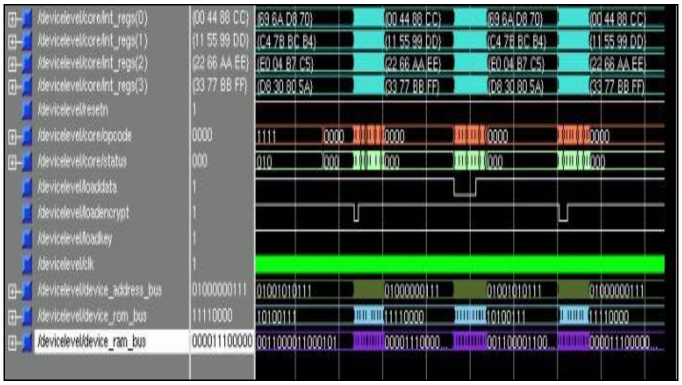
/devicelevel/core/int_regs(0) (00 44 88 CC)
/devicelevel/core/int_regs(1) (11 55 99 DD)
/devicelevel/core/int_regs(2) (22 66 AA EE)
/devicelevel/core/int_regs(3) (33 77 BB FF)
/devicelevel/resetn 1
/devicelevel/core/opcode 0000
/devicelevel/core/status 000
/devicelevel/loaddata 1
/devicelevel/loadencrypt 1
/devicelevel/loadkey 1
/devicelevel/clk 1
/devicelevel/device_address_bus 01000000111
/devicelevel/device_rom_bus 11110000
/devicelevel/device_ram_bus 000011100000
(69 6A D8 70)
(C4 7B BC B4)
(E0 04 B7 C5)
(D8 30 80 5A)
1111
010
01001010111
10100111
0011000011000101

Fig -1: Simulation results of AES-128 bits using Modelsim

Figure 3 shows the simulation results using ModelSim for AES-128 bit by considering the following inputs.
Plain Text – 00112233445566778899aabbccddeeff
Key Input – 000102030405060708090a0b0c0d0e0f
The following Encrypted output obtained is as shown.
Cipher Key –13111d7fe3944a17f307a78b4d2b30c5
Cipher Text –69c4e0d86a7b0430d8cdb78070b4c55a

5. CONCLUSIONS

The above results show the superiority of Blowfish algorithm with AES in terms of the throughput, processing time. More the throughput, more the speed of the algorithm & less will be the power consumption. Finally we can conclude that Blowfish is the best of all. In future we can perform Hardware Implementation to compare different parameters

REFERENCES

[1]. Jawahar Thakur, Nagesh Kumar,"DES,AES and Blowfish: Symmetric Key Cryptography Algorithms Simulation Based Performance Analysis," in International Journal of Emerging Technology and Advanced Engineering (ISSN 2250-2459, Volume 1, Issue 2, December 2011), pp.6-12

[2]. E. Thambiraj,G. Ramesh,Dr. R. Umarani , "A survey on Various Most Common Encryption Technique " International Journal of Advanced Research in Computer Science and Software Engineering , Volume 2, Issue 7, July 2012,pp226-233 I.S.

[3]. S.Pavithra, Mrs. E. Ramadevi "STUDY AND PERFORMANCE ANALYSIS OF CRYPTOGRAPHY ALGORITHMS " International Journal of Advanced Research in Computer Engineering & Technology Volume 1, Issue 5, July 2012 14, pp.82-86 K. Elissa, "Title of paper if known," unpublished.

[4]. J.Daemenand V.rijmen,"AES submission document on Rijndael", version 2, September 1999Role,