IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
Vol. 06, Issue 06 (June. 2016), ||V1|| PP 01-07

Comparative Study Of AES, Blowfish, CAST-128 And DES Encryption Algorithm

Youssouf Mahamat koukou, Siti Hajar Othman,
Maheyzah MD Siraj. Herve Nkiama
I. *Faculty of Computing, University Technology Malaysia*

Abstract *This paper provides a fair comparison between four most common symmetric key cryptography algorithms: AES, DES, CAST 128 and Blowfish. The comparison takes into consideration the behavior and the performance of the algorithm when different data load are used as the main concern here, is to study the performance of the algorithms under different settings. The comparison is made on the basis of these parameters: speed, block size, and key size. This paper aims to compare the Avalanche Effect and integrity checking using ECB and CBC mode of the different algorithms: Blowfish, Cast-128, DES and AES for one bit change in key and one bit changed in the cipher text. Crypto tool will be used for implementing the performance analysis for all algorithms mentioned above. After analysis has been conducted we found that AES gives the best security. The experiment shown that in both modes DES gives strong avalanche affect and AES and Cast 128 gives strong change in term of integrity checking compared with others algorithms using ECB and CBC mode.*

Keywords: *Comparison, Avalanche Effect, Integrity Check, Symmetric Encryption Algorithm*

I. INTRODUCTION

Cryptography is the practice and study of hiding information. Prior to the modern age, cryptography was almost synonymous with encryption i.e. the conversion of information from a readable state to nonsense. In order to avoid unwanted person being able to read the information, senders retain the ability to encrypt the information. Its main goal is to keep the data secure from unauthorized access [1]. Symmetric encryption techniques are almost 1000 times faster that asymmetric techniques as they require less computational processing power. For secure communication over public network data can be protected by the method of encryption. Encryption converts that data using an encryption algorithm using the key in scrambled form. In Symmetric keys encryption or secret key encryption, only one key is used to encrypt and decrypt data. In Asymmetric keys, two keys are used private and public keys. Avalanche Effect is changing one bit in the plain text or one bit change in the key should produce a modification in many bits of the cipher text. Therefore, this paper will do the comparison of four most common symmetric key cryptography algorithms of block cipher: AES, DES, CAST 128 and Blowfish using cryptography tool by implementing avalanche effect and integrity checking. Hence security of modified algorithm is at least as strong as the original algorithm. We will try to theoretically prove this fact. Also we will study the speed, security, flexibility and limitation of all algorithms listed above.

II. DESCRIPTIONS

2.1. AES

AES (Advanced Encryption Standard) also known as Rijndael, is the new encryption standard recommended by NIST to replace DES in 2001. AES algorithm can support any combination of data (128 bits) and key length of 128, 192, and 256 bits. The algorithm is referred to as AES-128, AES-192, or AES-256, depending on the key length. During encryption-decryption process, AES system goes through 10 rounds for I28-bit keys, 12 rounds for I92-bit keys, and 14 rounds for 256-bit keys in order to deliver final cipher-text or to retrieve the original plain-text [7]. AES allows a 128 bit data length that can be divided into four basic operational blocks. These blocks are treated as array of bytes and organized as a matrix of the order of 4×4 that is called the state. For both encryption and decryption, the cipher begins with an Add Round Key stage.

2.2. Blowfish

Blowfish is a keyed symmetric block cipher designed in 1993 by Bruce Schneider. Schneider designed Blowfish as a general-purpose algorithm, intended as an alternative to the aging DES. Blowfish has a 64-bit block size and a variable key length from 32 bits up to 448 bits. 18 sub-keys are derived from a single initial key. It requires total 521 iterations to generate all required sub keys. It is a 16-round Feistel cipher and uses large key-dependent S-boxes. In structure it resembles CAST-128 [2], which uses fixed S-boxes. Blowfish performs well for applications in which keys does not change often.

2.3. CAST-128

CAST-128 was created in 1996 by Carlisle Adams and Stafford Tavares. It is a 12 or 16-round Feistel network with a 64-bit block size and a key size of between 40 to 128 bits (but only in 8-bit increments). The full 16 rounds are used when the key size is longer than 80 bits. Components include large 8×32-bit S-boxes based on bent functions, key-dependent rotations, modular addition and subtraction, and XOR operations. There are three alternating types of round function, but they are similar in structure and differ only in the choice of the exact operation (addition, subtraction or XOR) at various points. Although Entrust holds a patent on the CAST [8] design procedure, CAST-128 is available worldwide on a royalty-free basis for commercial and non-commercial uses.

2.4. DES

DES (Data Encryption Standard) is symmetric key algorithm based on the backbone concept of Feistel Structure. The DES is a block cipher that uses a 64 bit plain text with 16 rounds and a Key Length of 56-bit, originally the key is of 64 bits (same as the block size), but in every byte 1 bit in has been selected as a 'parity' bit, and is not used for encryption mechanism. The 56 bit is permuted into 16 sub- keys each of 48- bit length. It also contains 8 S- boxes and same algorithm is used in reversed for decryption [5].

2.5. Blowfish, DES, CAST and AES Encryption Algorithm comparisons

Blowfish is a 16-round Feistel cipher and uses large key-dependent S-boxes. It is similar in structure to CAST-128, which uses fixed S-boxes. It is significantly faster than DES. Blowfish is unpatented, license-free, and available free for all uses. CAST is named for its developers, Carlisle Adams and Stafford Tavares. CAST is similar to DES and uses a 128- or 256-bit key structure. It is less secure than DES, but is faster than DES and blowfish. Table 1 shows their characteristics.

Table 1. Algorithms Characteristics

Factors	Cast 128	DES	Blowfish	AES
Key length	128-bits	56 bits	448 bits	128 bits
Cypher Type	Symmetric Block Cipher	Symmetric Block Cipher	Symmetric Block Cipher	Symmetric Block Cipher
Block Size	64 bits	64 bits	64 bits	128 bits
Developped	1996	IBM in 1975	1993	2000
Speed	Fast	Slow	Fast	Fast
Security	Less Secure	Not Secure Enough	Secure Enough	Excellent Security
number of rounds	12	16	16	10
No. of S-boxes.	4	8	4	1
Structure	Feistel Network	Feistel Network	Feistel Network	substitution-permutation Network

In the Table 1 above, a speed level comparison of the four symmetric algorithms has been done and based on the analysis we found that Cast 128, blowfish, AES has the fastest speed compared with DES. The encryption performance of the four algorithms is stronger and faster in contrast DES which has the lowest speed level compared with others. Because of the largest key size the four major algorithms mentioned above has been given a fastest and strongest speed level compared with DES.

III. EXPERIMENTS

2.6. Avalanche Effect Experiment Result

Based on the Table 2 using ECB mode the experimental result shows that DES gives strong avalanche affect compared with others algorithms listed above. This experimental result evaluated to compare how many bits change in cipher text once one bit change in the key. Hence, the analysis gives a clear explanation that DES has a strong avalanche affect based on evaluation criteria.

Table 2. Avalanche effect in ECB mode

Algorithm	Bit Position	Bits Change in ECB Mode	Percentage Change in Cipher text
AES	6th	67 bits	52.34%
Blowfish	6th	59 bits	46.09%
CAST-128	6th	63 bits	49. 21%
DES	6th	68 bits	53.12%

Based on the observation of the Table 3 using CBC mode the experimental result shows that DES gives significant avalanche affect compare with others algorithms listed above. This experimental result evaluated to compare how many bits change in cipher once one bit change in the key. Hence, the analysis gives a clear explanation that DES has a strong avalanche affect based on evaluation criteria. The evaluation is done by comparing the initial cipher text with modified cipher text then we multiplied the two ciphers texts using XOR, once we found the result after that we used to convert the cipher text into binary in order to count how many bits has been changed after one bit change in key.

Table 3. Avalanche effect in CBC mode

Algorithm	Bit Position	Bits Change in CBC Mode	Percentage Change in Cipher text
AES	6th	58 bits	45.31%
Blowfish	6th	63 bits	49.21%
CAST-128	6th	48 bits	37.50%
DES	6th	72 bits	56.25%

The summary of avalanche affect in both ECB and CBC mode lead to conclude that one bit changed in key has been given strong avalanche affect in DES compared with Cast128, Blowfish and AES. We used to change the bit in position 6th in each algorithm then we counted how many bits have been changed after one bit change in the key. We used to change the bit in position 6th in ECB and CBC both and we found that DES has given a strong Avalanche effect compared with others based on the experiment result. The Figure 1 and 2 illustrate the result of the avalanche effect in both ECB and CBC mode. When a single change in one bit of the key is made, it produces a change in many bits of the cipher text. If there is a change in number of bits in the cipher text whenever there is a change in one bit of the key or cipher text, this is called Avalanche effect.

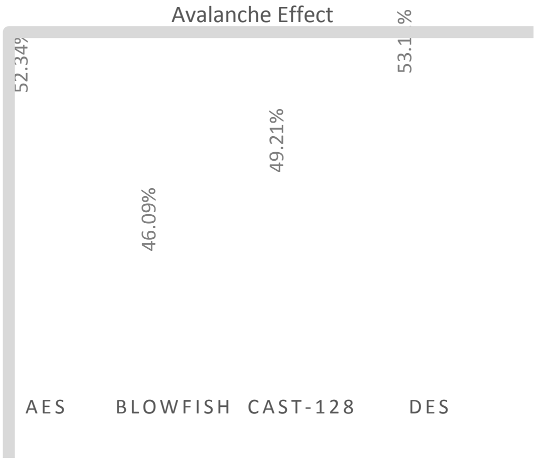

Figure 1. Avalanche effect in ECB mode

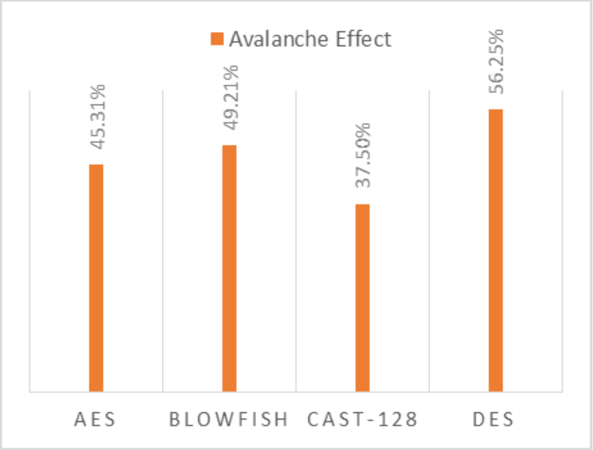

Figure 2. Avalanche effect in CBC mode

A desirable feature of any encryption algorithm is that a small change in either the cipher text or the key should produce a significant change in the cipher text. So, in order to say that any cryptographic algorithm is secure, it should exhibit strong avalanche effect, and this is the reason why we have considered Avalanche effect for comparing security of our modified change of bit in the key with the original cipher text. After analysis of avalanche affect for the four algorithms we found that DES produces strong avalanche effect compared with others algorithms moreover, AES also gives better avalanche but less than DES and greater than blowfish. Hence, CAST-128 gives avalanche effect but less than DES, AES and Blowfish. Furthermore, all four algorithms give avalanche for different percentage. We have demonstrated that change in one bit in the key produces strong avalanche effect. The above graph means that DES has a strong avalanche effect compared with others algorithms mentioned above.

2.7. Integrity Checking Experimental Result

Table 4. Integrity Checking in ECB mode

Algorithm	Bit Position	Bits Change in ECB Mode	Percentage Change in Plain text
AES	6th	77 bits	60.15%
Blowfish	6th	63 bits	49.21%
CAST-128	6th	69 bits	53.90%
DES	6th	61 bits	47.67%

Based on the Table 4, we found that integrity checking in ECB mode gives strongest integrity in AES which comes at first position with higher percentages but in contrast, cast128 gives higher integrity checking in CBC mode. In ECB mode AES has higher integrity compared with Blowfish, Cast 128 and DES but in CBC mode, the Cast 128 became the first to maintain the higher integrity compared with AES, Blowfish and DES.

Table 5. Integrity Checking in CBC mode

Algorithm	Bit Position	Bits Change in CBC Mode	Percentage Change in Plain text
AES	6th	72 bits	56.25%
Blowfish	6th	56 bits	43.75%
CAST-128	6th	73 bits	57.03%
DES	6th	71 bits	55.46%

The experimental result of integrity checking for the Table 5 shows that CAST-128 gives strong integrity compared with blowfish, AES and DES. In CBC mode integrity check gives higher percentage for the Cast 128 but in ECB mode AES has the higher compared Cast 128 and blowfish. We went through all four algorithms to change the bit position number 6th in order to verify which algorithm gives higher integrity therefore; the result shows that AES has higher integrity in ECB mode in other hand CAST-28 gives strong integrity in CBC mode.

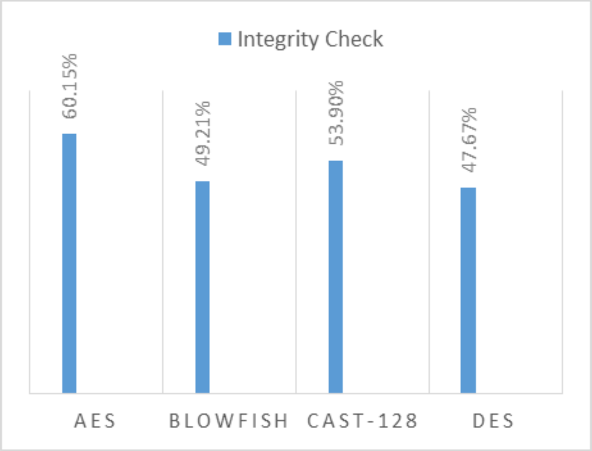

Figure 3. Integrity checking in ECB mode

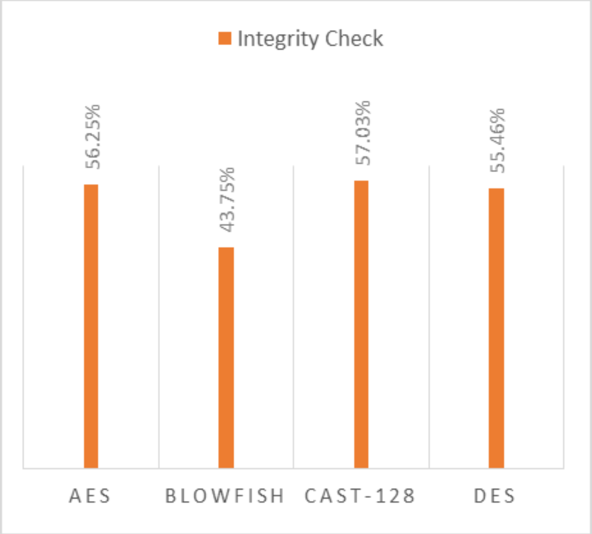

Figure 4. Integrity checking in CBC mode

According to the Figure 3 and 4, we found that changing one bit in the cipher text will give major change in the plain text. Hence, based on the above graph of integrity checking AES gives more strong integrity because the percentage of the modification is higher than others algorithms but Cast 128 also gives strong integrity in CBC mode compared with AES, blowfish and DES. Moreover, blowfish also gives higher effect of change in the plain text after change one bit in the cipher text but the percentage gives less compared with CAST-128, AES and DES. Furthermore, based on the statistic of above graph AES gives a significant effect of integrity in ECB mode but less than cast 128 in CBC mode greater therefore, both AES and CAST-128 have the higher integrity compared with Blowfish and DES. The analysis of the integrity checking shows that CAST-128 and AES have greater effect on integrity in both modes which are ECB and CBC.

IV. SECURITY LEVEL ANALYSIS

According to the security level for the four algorithms, the security level shows that AES is excellent compared with others but Blowfish also gives higher level security, however not higher than AES but stronger than CAST-128 and DES. We learned from the comparison that CAST-128 has a greater level of security compared with DES because basically DES is less secure enough and it does not provide good security level and AES also provides excellent level of security based on comparative study. Analysis of security level lead to conclude that AES, CAST-128, Blowfish are more secure not including DES because it does not preserve the security measures.

AES: AES provides a very high security level because of using variable length key i.e. 128 bits. Different types of attack tried to crack AES like Square attack, Key attack, differential attack and improved square attack but none of them is possible to crack this algorithm. So, AES is a highly secured encryption technique. AES can also protect data against future attack (collision attack).
Blowfish: Blowfish has a high security level because it uses variable length key of 448 bits. Blowfish is a secure algorithm against differential key attacks, because each bit of the master key involves multiple round key which is independent.
DES: Security is the main drawback of DES. DES does not provide strong security because of its key length 0f 56 bits. DES can easily crack by brute force attack [6]. Initially DES was accepted as the standard algorithm with strong security but after sometimes Brute force attack cracked DES. So, DES is not a secure encryptions algorithm.
CAST-128: by increasing security level CAST uses variable key length operation, its security level is great and CAST-128 protects information from linear and differential attacks.

V. LIMITATION

Blowfish: Blowfish is a very secure algorithm but Initial 4 rounds of blowfish are observed unprotected from 2^{nd} -order differential attack.
AES: No any such kind of weakness has been observed in AES. Some initial rounds of AES are observed unprotected i.e. initial round can break by square method.
CAST128: by means of a known plain text attack Key of CAST 128 can be known by linear cryptanalysis. It can be broken by 2^17 chosen plaintexts along with one related-key query in offline work of 2^48.
DES: because of short key length brute force attack can crack easily by implementing brute force attack. Hence, Weak key is the major problem of DES. It doesn't protect data against linear and differential attacks. DES didn't design for software so it runs slowly. The Table 6, illustrates a flexibility comparison between the four algorithms.

Table 6. Flexibility comparison

Algorithms	Flexibility	Modification	Remarks
AES	Yes	128	Its structure was flexible to the multiples of 64
BLOWFISH	Yes	448	Key length in blowfish should be multiples of 32.
CAST-128	Yes	128	CAST-128 has a flexible structure so it modified to 128 and 256 bits to increase its security level
AES	Yes	128	Its structure was flexible to the multiples of 64

VI. CONCLUSION

The results of the tests and analysis conducted in this paper lead to conclusion that the security of Blowfish Algorithm is good as compared to Cast-128 Algorithm. Hence, after analyzing the most popular symmetric algorithms AES was found the most secure, faster and better among the entire existing algorithm with no serious weaknesses, there are some flaws in symmetric algorithms such as weak keys, insecure transmission of secret key. In this paper a detailed analysis of symmetric block encryption algorithms is presented on basis of different parameters. The main objective was to analyze the performance of the most popular symmetric key algorithms in terms of avalanche effect, integrity checking, Flexibility, Reliability, Robustness, Scalability, Security, and to highlight the major weakness of the mentioned algorithms, making each algorithm's strength and limitation transparent for application. During this analysis it was observed that AES was the best among all in terms of Security, Flexibility, and Encryption performance. The experiment was done using ECB and CBC mode in order to check the avalanche effect and integrity check after we have done to implement the two modes we found that DES gives strong avalanche effect and in term of integrity check we found that AES gives strong integrity in ECB mode in contrast the Cast 128 gives strong integrity in CBC mode.

REFERENCES

[1] Alanazi Hamdan.O., Zaidan B.B., Zaidan A.A., Jalab Hamid.A., Shabbir .M and Al- Nabhani.Y, “New Comparative Study Between DES, 3DES and AES within Nine Factors” Journal of Computing, Volume 2, Issue 3, March2010, ISSN 2151-9617, pp.152-157 .

[2] B. Schneider, “Applied Cryptography: Protocols, Algorithms, and Source Code in C”, 2nd ed., John Wiley & Sons, 1995.

[3] W. Stallings, “Cryptography and Network Security: Principles and Practices”, 2nd ed., Prentice Hall, 1999.

[4] C.M. Adams, “Constructing symmetric ciphers using the CAST design procedure”, Designs, Codes, and Cryptography, Vol. 12, No. 3, November 1997, pp. 71–104

[5] Anoop MS, ―Public key Cryptography (Applications Algorithm and Mathematical Explanations).

[6] Ham, K., Chien, Y. R., Kiesler, K., ―An Extended Cryptographic Key Generation Scheme for Multilevel Data Security‖, Fifth Annual Computer Security Applications Conference, Tucson, AZ, USA 1989.

[7] Mr. Gurjeevan Singh, Mr. AshwaniSingla and Mr. K S Sandha, "Cryptography Algorithm Comparison for Security Enhancement in Wireless Intrusion Detection System", International Journal of Multidisciplinary Research, Vol.1 Issue 4, pp. 143-151, August 2011.

[8] B. Schneier, "Applied Cryptography", John Wiley & Sons Inc., 1999