History Research Journal

ISSN: 0976-5425

Vol-5-Issue-6-November-December-2019

Analytical Study of Security Ciphers Based on Quality of Service Parameters

Dr. Ravi Khurana
Assistant Professor
Dept. of Computer Science and Application
Kanya Maha Viidyalaya, Jalandhar

Amandeep Singh
Assistant Professor
School of Humanities
Lovely Professional University, Phagwara, Punjab, India

Abstract **-** Quality of service is a relevant term in today's computing scenario. Quality is a subjective issue; we need to devise some parameters, based on which quality can be measured. In this paper, we devised metrics on the basis of which we compared cryptographic strengths of ciphers namely SDES (Simplified Data Encryption Standard), DES (Data Encryption Standard), 2DES (Double Data Encryption Standard), BLOWFISH, CAST (Carlisle Adams Stafford Tavares) –128 and found the strongest and weakest cipher. This comparison has been made by using metrics namely Block size, Encryption key length, Complexity of round function F, Confusion & Diffusion, S-boxes, Number of operators involved and Number of Cycles. After analyzing all the ciphers, we have arranged them in tables with respect to each metric. Based on these metrics, the ranking has been done by assigning stars to the ciphers. Maximum number of 5 stars means the best or strongest cipher and minimum number of stars means the weakest cipher. We have found that CAST-128 is the strongest cipher and SDES is the weakest cipher out of the five ciphers studied.

Keywords: Ciphers, Round Function, Confusion & Diffusion, Block Size, S-Boxes, Encryption Key.

I. INTRODUCTION

Security is the prime concern since the evolution of computer networks. Any system cannot completely prevent unauthorized access to transmission media, so a practical way is to protect information is to change it, so that only the authorized receivers can understand the same. This can be achieved by Cryptography. Cryptography is the art and science of maintaining secure messages; it means to scramble the message so badly that even if the enemies cover the message, they will face difficulty in reading the entire message.

A. Network Security Objectives

Network security mainly concerns into following areas, and they are: -

- Confidentiality: - The information cannot be understood by anyone for whom it was unintended.
- Integrity: - The information cannot be altered in storage or transit between sender and intended receiver without the alteration being detected.
- Non-repudiation: -The creator/sender of the information cannot deny at a later stage his or her intentions in the creation or transmission of the information.
- Authentication: - The sender and receiver can confirm each other's identity and the origin/destination of the information.

II. OBJECTIVES

- To identify Parameters for Comparative analysis of five Symmetric Block Ciphers namely SDES (Simplified Data Encryption Standard), DES (Data Encryption Standard), 2DES (Double DES), BLOWFISH, CAST (Carlisle Adams Stafford Tavares) -128.
- To decide Weakest & Strongest cipher based on these parameters.

III. PARAMETERS OF THE STUDY

- Block Size: - Number of bits in the block of data.
- Encryption Key Length: - Number of bits in the Encryption key.
- Complexity of Round Function F: - Computations involved in a round function, complexity of function F is measured by complexities of phases.
- Confusion & Diffusion: - They are basic building blocks for any cryptographic system.
  - Confusion: - It is a property by which relationship between the statistics of the ciphertext and the value of the encryption key is made so complex that is difficult for intruders to judge the plaintext.
  - Diffusion: - It is a property by which relationship between the statistics of the plaintext and ciphertext is made so complex that is difficult for cryptanalyst to deduce the value of the encryption key.

ISSN: 0976-5425

Vol-5-Issue-6-November-December-2019

- S-boxes: - They are the substitution boxes, used to substitute different output bits corresponding to given input bits. They give non-linearity to the cipher.
- Number of Operators involved: - It is the number of operators in the Encryption / Decryption processes of the cipher.
- Number of Cycles (Rounds): – It is number of rounds in Encryption/ Decryption processes of the cipher.

IV. ANALYSIS OF CIPHERS ON THE BASIS OF PARAMETERS

Cryptographic strengths of ciphers are directly proportional to block size, encryption key length, complexity of round function F, S-boxes & confusion and diffusion property i.e.

Cryptographic strength $\propto$ Parameters

- Block Size

Cryptographic strength $\propto$ Block size

As the size of block increases, its cryptographic strength increases.

Now we will discuss key scheduling algorithms of block ciphers.

a) SDES: -

Block Size: 8 bits

Total number of possible plaintext $=2^8$ =256 blocks. Due to small block length, it is vulnerable to cryptanalysis. Known plaintext attack is possible because, due to small block; since total number of possible plaintext blocks is just 256, which is too small to resist cryptanalysis.

b) DES: -

Block Size: 64 bits

Total number of possible plaintext blocks = $2^{64} \sim 1.8 * 10^{19}$ blocks. Due to small block, SDES suffers from cryptanalysis, the solution is given by DES by choosing block of 64 bits, here the total number of plaintext blocks is very large, so it is difficult to have known plaintext attack, DES is more secure than SDES.

c) 2DES: -

Block Size: 64 bits

Total number of possible plaintext blocks = $2^{64} \sim 1.8* 10^{19}$ blocks. Linear Cryptanalysis is possible in DES. Although DES & 2DES have same block size, but 2DES is more secure than DES because of larger key length.

d) BLOWFISH: -

Block Size: 64 bits

Total number of possible plaintext blocks = $2^{64} \sim 1.8* 10^{19}$ blocks. In BLOWFISH Encryption/Decryption algorithm operate on both halves of data.

e) CAST -128: -

Block Size: 64 bits

Total number of possible plaintext blocks = $2^{64} \sim 1.8* 10^{19}$ blocks. Unlike BLOWFISH cipher encryption/decryption algorithm operate on half of data.

TABLE I
BLOCK SIZE ANALYSIS

Cipher	Block Size (in bits)	Block Type	Comment
SDES	8	F	Not Secure
DES	64	F	Less Secure
2DES	64	F	Less Secure
BLOW-FISH	64	F	Highly Secure
CAST-128	64	F	Secure

F:- Fixed ; TNPB:- Total Number Of Possible Blocks

Out of the ciphers given above BLOWFISH is highly secure because it operates on both halves of the block, rest of the ciphers operate only on single half of the block. SDES is not secure because of its small fixed block size.

- *Encryption Key Length*

Cryptographic strength $\propto$ Encryption key length

i.e more the number of bits in the encryption key, secure is the cipher.

Now we will discuss key sizes of block ciphers and also purposes a optimal choice for key length

a) SDES: -

Key Size: 10 bits

Total number of possible keys=2^{10} =1024 keys. Key is not secure against brute force attack by trying different keys plaintext can be easily be recovered from ciphertext, Known plaintext attack is easily possible.

b) DES: -

Key Size : 56 Bits

Total number of possible Keys = 2^{56} ~$7.2*10^{16}$ keys. Since total number of keys are far greater than SDES. Therefore it is more secure than SDES. , Brute Force attack is infeasible because, on average , if half the keys space is searched , a single machine performing one DES encryption per microsecond , would take 1192 yrs, to break the cipher , Also as we know more elements in a set of possible keys, difficult to decrypt the message , hence secure.

c) 2DES:-

Key Size: 112 Bits

The fixed 56- bit key is too short to prevent brute force attack, in today's machines of high computational power. In a parallel machine with 1 million encryption devices, each of which could perform one encryption per microsecond, it would bring average search time down to about 10 hours, DES is also vulnerable to linear and differential cryptanalysis and can be easily broken by these analyses.

So, we have seen that DES is not secure. Thus, there is a need to strengthen DES. We have variant of DES as Double DES which uses a key of 112 bits. This leads to higher security of encryption.

d) BLOWFISH:-

Key Size : 32 to 448 bits

ISSN: 0976-5425

Vol-5-Issue-6-November-December-2019

Total number of possible keys = 7.27 * 10^{134} keys. BLOWFISH cipher has variable key length, which add to its cryptographic strength. How to choose particular key length depend on the security and speed. If we want to attain high security but we can compromise with speed, then we can use key of large length. Due to variable key its security is unchallenged, by setting appropriate length for the key, we can increase the security. To test Single key for brute force attack, 522 times execution of encryption algorithm is required, which is difficult task.

BLOWFISH cipher provides a highly secured and the most robust encryption algorithm, in addition to being the fastest of all. BLOWFISH has a better encryption algorithm and substantially larger key size emerges as the most secure. It is also flexible algorithm

Better choice for key length is 128 bits, only exhaustive search is possible that too require 2^{128} ! encryption trials.

e) CAST –128 :-

Key Size : 40 to 128 bits with increment of 8 bits

Cipher with variable key, it is more secure than DES, Rotations are dependent on Key (which increases its strength). Best implementation is with 128 bits key. No weak key has been detected.

So, based on above simulation we have prepared a following table showing the comparison of ciphers,

TABLE II
KEY LENGTH ANALYSIS

Cipher	Key Length (in bits)	Key Type	Comment
SDES	10	F	Not Secure
DES	56	F	Less Secure
2DES	112	F	Intermediately Secure
BLOWFISH	32 to 448	V	Highly Secure
CAST-128	40 to 128	V	Secure

F:- Fixed ; V:- Variable ; TNPK:- Total Number Of Possible Keys

As in the table, BLOWFISH is highly secure because of variable and largest key length. SDES is not secure because it has fixed and small key length.

- Complexity of Round Function F

Cryptographic strength $\propto$ Complexity of round function F

i.e. More the complexity of F, greater the security.

Round Function F is a basic building block of any cipher, strength of which is lies in S- boxes. The basic objective of F is to create Confusion, diffusion and avalanche effect.

Now we will discuss the function F of various ciphers as shown below

a) SDES: -

Number of occurrences: 2

Input (in bits): 4 (Message), 8 (Subkey)

Output (in bits) : 4

Components:-

I. E/P (Expansion Permutation) Phase
   Input : 4 bits
   Output : 8 bits
II. XOR (Bitwise Exclusive OR) Operator
   Operands : 8 bits (Output of E/P Phase), 8 bits (Subkey).
   Result : 8 bits.
III. Two S-boxes S_0 and S_1 (4* 2 each)
   Input (of each S-box): 4 bits
   Output (of each S-box): 2 bits
IV. P4(Permutation) Phase:-
   Input: 4 bits
   Output: 4 bits

b) DES: -

Number of occurrences: 16

Input (in bits) : 32 (Message) , 48 (Subkey)

Output (in bits): 32

Components:-

I. E/P(Expansion Permutation) Phase
   Input : 32 bits
   Output : 48 bits
II. XOR (Bitwise Exclusive OR) Operator
   Operands : 48 bits (Output of E/P Phase), 48 bits (Subkey).
   Result : 48 bits.
III. 8 S-boxes S_0.. S_8 (6* 4 each)
   Input (of each S-box) : 6 bits
   Output (of each S-box) : 4 bits
   Input (Substitution/Choice Phase) : 48 bits
   Output (Substitution/Choice Phase) : 32 bits
IV. P4(Permutation) Phase :-
   Input : 32 bits
   Output : 32 bits(but with different arrangements)

c) 2DES: -

   Number of occurrences : 32 (2 * 16)
   Input (in bits): 32 (Message), 48 (Subkey)
   Output (in bits) : 32

Since 2DES is just a DES, applied two times. Therefore, description of all the components is same. Also each component is twice in it e.g. Number of Occurrences of E-table in DES are 16: but in it are 32 (2 * 16)

d) BLOWFISH: -

Number of occurrences: 16

Input (in bits) : 32 (Message)

Output (in bits): 32

Components:-

I. + Operator (Addition of words modulo 2^{32})
   Operands : 32 bits (two)
   Result : 32 bits
II. XOR (Bitwise Exclusive OR) Operator
   Operands : 32 bits (two)
   Result : 32 bits.
III. 4 S-boxes S_0 .. S_4 (8* 32 each)
   Input (of each S-box) : 8 bits

ISSN: 0976-5425

Vol-5-Issue-6-November-December-2019

Output (of each S-box) : 32 bits

e) CAST –128:-

Cipher with variable F i.e. round Function F depend on Particular round number. There are basically three categories of rounds to which function F belongs and they are

I. 1,4,7,10,13,16.
II. 2,5,8,11,14
III. 3,6,9,12,15

This dynamic property of F strengthens the cipher against cryptanalytic attack. Function F provides good confusion, diffusion and avalanche effect.

Number of occurrences: 16

Input: Right half of block (of 32- bit); Kr_i (Subkey) of 5 bits)

Output: 32 bits

Components:-

I. Four functions, that are dependent on rounds and they are $f1_i$, $f2_i$, $f3_i$ and $f4_i$

Operands (of $f1_i$) : Subkey (32-bit) and right half of block (32- bit)

Result : 32 bits

Operands (of $f2_i$ $f3_i$ and $f4_i$): Two 32 bit blocks

Result : block of 32 – bit.

II. <<< (Left Circular Rotation Function)

Input : Output of Km_i32 bits , Kr_I (5 bit)

Output : 32 bits.

III. 4 S-boxes S_0 .. S_4 (8* 32 each)

Input (of each S-box) : 8 bits

Output (of each S-box): 32 bits

Following table summarizes shows Function all these above discussed ciphers.

TABLE III
COMPLEXITY OF F-FUNCTION ANALSIS

Cipher	F Type	Complexity of S-boxes	Complexity of F
SDES	F	L	L
DES	F	L	L
2DES	F	L	L
BLOWFISH	F	H	I
CAST-128	V	H	H

F: - Fixed; V: - Variable; L: - Low; I: - Intermediate; H: - High

Ciphers from 1-3 have low complexity because S-boxes have small dimensions (6×4). BLOWFISH has intermediate complexity because of its fixed type. Complexity of F is high in case of CAST-128 because complexity of S-boxes are high(8×32) and F depends on round number i.e. it varies from round to round.

- Confusion & Diffusion

Cryptographic strength ∝ Confusion and diffusion in the cipher

i.e. more the confusion and diffusion, secure the cipher.

Function F provides element of confusion and diffusion. More the complexity of F, more the confusion and diffusion. Confusion and diffusion can be achieved by complex substitution and permutations respectively.

Following table gives the various level of confusion and diffusion in block ciphers, this table provides the complexity of F and also ranks these ciphers accordingly.

TABLE IV
CONFUSION & DIFFUSION ANALSIS

Cipher	Complexity Of F	Confusion & Diffusion	Comment
SDES	L	L	Less Secure
DES	L	L	Less Secure
2DES	L	L	Less Secure
BLOWFISH	I	I	Intermediate Secure
CAST-128	H	H	Highly Secure

L: - Low; I: - Intermediate; H: - High

As we have seen in above table Confusion and diffusion property is high in CAST-128 (as a result of which it is highly secure) because of the high complexity of F (confusion and diffusion is directly related with function F).

- S-boxes

Cryptographic strength ∝ S-boxes.

More the complexity of S-box, greater the security.

S- boxes provides non-linearity to the encryption algorithm, more the non-linearity more the security, So we S-boxes provide security i.e. cryptographic strength to the cipher.

Now we discuss the S-boxes of various ciphers as shown below.

a) SDES :-

Number of S-boxes : 2 namely (S_0,S_1)

Dimension (of each) : 4 * 2, Number of Rows : 4

Number of Columns : 4

Here S- boxes are fixed i.e. values of S_0,S_1 are constant which will decrease the cryptographic strength. Moreover if S-boxes are made public, then by trying various combinations security can be broken.

b) DES: -

Number of S-boxes : 8 namely (S_0,S_8)

Dimension(of each) : 6 * 4, Number of Rows : 4

Number of Columns : 16

In SDES we were having very less number of S-boxes, and S-boxes were also having small dimensions. Due to which they do not give high non-linearity. So SDES is vulnerable to Brute Force, Linear and Differential attacks. Improvement over this is DES which has 8 S-boxes with dimensions 6* 4 each. So Strength of DES lies in S-boxes.

c) 2DES: -

Number of S-boxes : 16 (2 * 8)namely (S_0...S_8)

Dimension(of each) : 6 * 4, Number of Rows : 4

ISSN: 0976-5425

Vol-5-Issue-6-November-December-2019

Number of Columns : 16

In the encryption algorithm, DES is applied twice with two different keys, hence total number of S- boxes are twice the individual DES encryption cipher, Increase in S-boxes will increase the cryptographic strength.

d) BLOWFISH :-

Number of S-boxes : 4

Dimension (of each) : 8 * 32, Number of Rows : 256

Number of Columns : 32

The S-boxes have 256 32 –bit entries. Here S-boxes are produced by repeated application of the cipher. S-boxes are random and key dependent. Every bit of the input to F is only used as input to one S-box, in contrast with DES where many bits are used as inputs to two S-boxes, which strengthens the algorithm considerably against differential attacks.

e) CAST-128 :-

Number of S-boxes : 8

Dimension (of each) : 8 * 32

Number of Rows : 256

Number of Columns : 32

Here we use Bent functions while designing S-boxes, as a result of which cipher has high non-linearity, S-boxes are non-key dependent i.e. fixed. Due to this method of designing plaintext attack is impossible.

Following table shows S-boxes of these ciphers.

TABLE V
S-BOXES ANALYSIS

Cipher	**Number of S-boxes**	**S-boxes Type**	**Comment**
SDES	2	NKD	Less Secure
DES	8	NKD	Intermediately Secure
2DES	16	NKD	Intermediately Secure
BLOWFISH	4	KD	Highly Secure
CAST-128	8	NKD	Secure

NKD: - Non-Key Dependent; KD: - Key-Dependent;

From above table on the basis of S-boxes we find that BLOWFISH is highly secure because of the dimensions of s-boxes (8×32), nature of entries in s-boxes (random and key dependent) and production of s-boxes by repeated applications of algorithm. SDES is less secure because of non-key dependent nature and small dimensions.

- Number of Operators involved

Cryptographic strength ∝ Mixed Operators i.e.

More the Number of Operators, More the security. BLOWFISH uses 2 operators and CAST-128 uses 5 operators. Whereas other cryptographic algorithms have only single operator. So, we find that in CAST-128 complicated 5 operators are involved, which add to its cryptographic strength with respect to other algorithms.

- Number of Cycles

Cryptographic strength ∝ Number of Cycles i.e.

More the number of rounds, more security.

As the number of rounds increases, it is difficult of perform cryptanalysis, even for a relatively weak, F. Another aspect of about number of rounds is that as you increase the number of rounds, cryptographic strength increases, but beyond a certain value there is one drawback that it will result in Encryption/Decryption speed.

Following table shows number of rounds in the ciphers

TABLE VI
NUMBER OF OPERATORS INVOLVED ANALSIS

Cipher	Number of Rounds	F Type	Ranking
SDES	2	F	Less Secure
DES	16	F	Less Secure
2DES	32	F	Intermediately Secure
BLOWFISH	16	F	Intermediately Secure
CAST-128	16	V	Highly Secure

F:- Fixed; V:- Variable.

From the above table we that CAST-128 is highly secure algorithm based on the number of cycles metric.

V. CONCLUSION

In the beginning, five symmetric block ciphers were selected namely SDES, DES, 2DES, BLOWFISH, CAST-128 then identified measurement scales namely Block size, Encryption key length, Complexity of round function F, Confusion & Diffusion, S-boxes, Number of operators involved and Number of Cycles; using these scales analysis was made. The following table gives the net conclusion of the study of various measurement scales. CAST-128 has maximum number of five stars and SDES is the weakest cipher because it has not come up even with 3 stars.

- Ranking of Ciphers Based on Parameters

Cipher	**Confusion & Diffusion**	**S-Boxes**	**Number of Cycles**	**NOOI**
SDES	**	**	**	*
DES	**	***	**	*
2DES	**	***	**	*
BLOWFISH	***	*****	***	**
CAST-128	*****	****	*****	*****

ISSN: 0976-5425

Vol-5-Issue-6-November-December-2019

Cipher	Block Size	Encryption Key Length	Complexity of Round Function F
SDES	*	*	**
DES	**	**	**
2DES	**	***	**
BLOWFISH	*****	*****	***
CAST-128	****	****	*****

*:- Not Secure ; **:- Less Secure ; ***:- Intermediately Secure ; ****:- Secure ; *****:- Highly Secure ; NOOI : - Number of operators involved

In the above table, ciphers are ranked according to their security levels by stars. Single star means cipher is not secure, two stars means cipher is less secure, three stars means cipher has intermediate security, four stars means cipher is secure, and at last, five stars means cipher is highly secure.

- Arrangement of ciphers according to their Cryptographic Strengths
  - CAST-128
  - BLOWFISH
  - 2DES
  - DES
  - SDES

  ↓ Toward Decreasing Cryptographic Strength
- SDES is the weakest cipher.
- CAST-128 is the strongest cipher.

REFERENCES

[1] Andrew S. Tanenbaum, Computer Network, Prentice Hall of India.
[2] William Stallings, Data and Computer Communications, 5th edition, Prentice Hall India.
[3] "IT Papers", ZDNet.com, http://itpapers.zdnet.com[21/8/2014]
[4] "Networking Solutions White Papers", Cisco Systems, USA, http://www.cisco.com [31/7/2014]
[5] "Search Engine", http://www.google.com.
[6] Rivest, Shamir & Adleman", an official site of RSA, http://www.rsa.com.
[7] Schneier, Bruce, Applied Cryptography, 2nd Edition, New York, John Wiley and Sons,1995