ISSN No. 0976-5697

Volume 5, No. 7, September-October 2014

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Block Ciphers in Cryptograpy

Prof. Saroj Singh
Dept. Computer Science & Engineering
Applied College of Management & Engineering
Mitrol, Palwal, India

Abstract: Block cipher is a type of key cipher which operates on a fixed length group of bits known as block ciphers. It is most widely used cryptographic algorithm. It is not necessary that the input should be only 128 bits. Size may vary. A message longer than 128 bits is encrypted by breaking the message into blocks and encrypted them individually. Block ciphers are important elementary components in the design of many cryptographic protocols, and are widely used to implement encryption of bulk data.

Keywords: symmetric; algorithm; codes; cipher; message; elementary; cryptography; decryption; encryption; protocols;

I. INTRODUCTION

Block cipher is a type of key cipher which operates on a fixed length group of bits known as block ciphers. In cryptography[1] a block cipher is a deterministic algorithm operating on fixed-length groups of bits, called blocks, with an unvarying transformation that is specified by asymmetric key. Block ciphers are important elementary components in the design of many cryptographic protocols, and are widely used to implement encryption of bulk.

A. Block cipher encryption:

Block cipher encryption requires three parameters.

a) 128 bit block of plaintext which acts as an input
b) 128 bit block of ciphertext which acts as an output
c) Secret key

B. Block cipher decryption:

Block cipher decryption: Block cipher encryption requires three parameters.

a) 128 bit block of plaintext which acts as an input
b) 128 bit block of ciphertext which acts as an output
c) Secret key

C. Features:

a) Provides secrecy
b) Provides authentication

D. Shannon principles of cipher design:

Shannon principles of cipher design: Shannon provides two principles for designing the cipher. The modern design of block ciphers is based on the concept of an *iterated* product cipher. Product ciphers were suggested and analyzed by Claude Shannon in his seminal 1949[2].

a) Confusion: the relation between the key and ciphertext is made to be as complex as possible. For example: replacement of every letter with the letter on the keyboard.

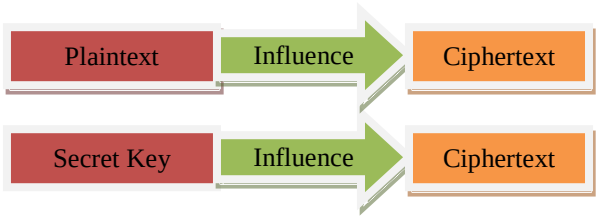

Fig: 1

b) Diffusion: each digit of the plaintext should influence many digits of the ciphertext and each digit of the secret key should influence many digits of the ciphertext.

E. Criteria for evaluating block cipher[3]:

Criteria for evaluating block cipher: following are the criteria for evaluating block ciphers:

a) Security level: Some ciphers are considered more secure than others. This distinguish is done on the basis of the performance on cipher component and design criteria.

b) Key size: Size of the key defines the security of the cipher. As per the size of the key increases so does the cost increases.

c) Throughput: Throughout is related with the complexity of the cryptographic algorithms

d) Block size: Block size affect security, complexity, & performance of the cipher.

e) Complexity of cryptographic mapping: Its affects the implementation cost in terms of development and fixed resources. The .implementation is either hardware & software.

f) Data expansion: It is mandatory the encryption should not increase the size of the plaintext inputs.

g) Error propagation: It is the cipher text contains errors then it may lead to error propagation to subsequent plaintext blocks.

F. Design principles:

There are three design principles[4]:

a) Number of rounds: As the number of rounds increases, the difficulty in performing cryptanalysis increases. This criterion is used to compare the strength of different algorithms.

b) Design of function F: the function F imparts confusion in a Feistel cipher. As F tends to non linear so does the difficulty of cryptanalysis.

c) Key schedule algorithm: the key is used to generate one sub key to each round. Sib key leads to difficulty in deducting individual sub keys. Thus deducing back to main key becomes difficult.

II. TYPES OF BLOCK CIPHERS

A. *Block ciphers can be classified as:*

- Feistel ciphers
- Data encryption
- Data Encryption Standard (DES)
- Avalanche Effect
- Advanced Encryption standard (AES)
- Linear Cryptanalysis
- Differential cryptanalysis
- Brute Force Attack
- Replay Attach
- Triple DES

Publication Communication Theory of Secrecy Systems as a means to effectively improve security by combining simple operations such as substitutions and permutations[5]. Iterated product ciphers carry out encryption in multiple rounds, each of which uses a different sub key derived from the original key. One widespread implementation of such ciphers is called a Feistel network, named after Horst Feistel, and notably implemented in the DES cipher. Many other realizations of block ciphers, such as the AES, are classified as substitution-permutation networks.

The publication of the DES cipher by the U.S. National Bureau of Standards (now National Institute of Standards and Technology, NIST) in 1977[6] was fundamental in the public understanding of modern block cipher design. Both differential and linear cryptanalysis arose out of studies on the DES design. Today, there is a palette of attack techniques against which a block cipher must be secure, in addition to being robust against brute force attacks.

Even a secure block cipher is suitable only for the encryption of a single block under a fixed key. A multitude of modes of operation have been designed to allow their repeated use in a secure way, commonly to achieve the security goals of confidentiality and authenticity.

III. FEISTEL CIPHERS

Definition: Feistel cipher is a scheme used by modern block ciphers where the ciphertext is calculated the plaintext by the repeated application of the round function.its implemented Shannon's substitution–permutation network concept.

B. *Shannon's substitution-–permutation network concept:*

Shannon's substitution–permutation network concept is a series of linked mathematical operations. The input of this network concept is a block of plaintext and key. Ciphertext is produced by applying round of S (substitution) box and p (permutation)-box on the plaintext[7]. Decryption is done by using the inverse of S-boxes, p-boxes and key.

S-box: it is substitutes a small block of bits by another block of bits. The length of the output should be same as that of input. Also each of output bit depends upon the input bit.

P-box: it is permutation of all the bits. It takes the outputs of all the S – boxes of one round permutes the bits and feeds them into the S – boxes of next round. At each round, the round key is combined by XOR function.

A. *Properties:*

- Security depends upon the size of the key.
- Security also depends upon the irreversibility of the hash function

B. *Design Principles:*

The design principles of the feistel cipher are:

- **Block Size:** As the size of the block increases so so does the security. But the increasing block sizes makes the cipher slow.
- **Key size:** as the key size increases the security of the cipher also increases. But the disadvantages are the slow cipher and the exhaustive searching.
- **Sub key generation:** it slows down the ciphers.
- **Number of rounds:** As the number of rounds increases, the security of the cipher also increases.
- **Round functions:** it slows down the cipher and makes it complex.

C. *Advantages:*

- Encryption and decryption process is quite similar.
- Round function F does not have to be invertible.

C. *Working:*

F is the function and $K_0, K_1, \ldots\ldots\ldots K_n$ are the sub keys of the round 0,1, ……n.

- Input is divided into two equal size blocks called left(L) and right(R)
- Feistel round occurs with an internal function known as round function.
- Hash function F is applied to right block(R) and the key.
- The result of the hash function is XOR-ed with the left block (L).
- Blocks are swapped, block which is XOR-ed becomes the right block and unchanged block becomes the left block.
- Process is repeated.

a) **Encryption Process:** this process is computed by

$\mathbf{L_{i+1} = R_i}$

$\mathbf{R_{i+1} = L_i \oplus F(R_i , K_i)}$

b) **Decryption Process:** this process is computed by

$\mathbf{R_i = L_{i+1}}$

$\mathbf{L_i = R_{i+1} \oplus F(L_{i+1} , K_i)}$

D. *Unbalanced Feistel Cipher:*

Unbalanced Feistel cipher: is cipher where L_0 and R_0 are not of equal length. For example THORP SHUFFLE

Thorp Shuffle: it is an unbalanced Feistel cipher where length of one side is only a single bit.

E. Advantage:

Provide better security than a balanced Feistel cipher.

F. Disadvantages:

Requires more rounds.

IV. DATA ENCRYPTION STANDARD (DES)

Data Encryption Standard(DES): is the most widely used block cipher that is based on symmetric key algorithm using 56 bit key

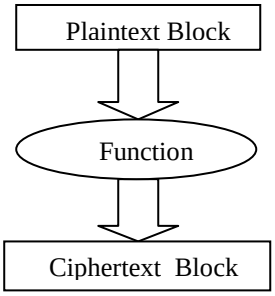

Fig: 2

A. History of DES:

a) The data encryption standard was developed in 1970 by NBS with the help of National SecurityAgency. IBM created the draft of algorithm known as LUCIFER DES[8].
b) In 1973, NBS called for encryption algorithms for use in unclassified government applications.
c) IBM submitted LUCIFER DES design.
d) LUCIFER standard became a federal standard in November 1976.

B. Technique used by DES:

DES uses two techniques:
a) Confusion: it achieved through XOR operations.
b) Diffusion: it achieved through numerous permutations.

C. Applications of DES

a) Banking industry
b) Financial applications

D. Advantages:

a) Suited for implementation in hardware
b) Suited for voice and video

E. DES Encryption:

a) 64 bit plaintext
b) 64 bit key

F. Working:

a) Initial permutation IP
b) Key dependent computation
c) Inverse initial permutation IP^{-1}

G. Enciphering

a) The 64 bits of the input block to be enciphjered are subjected to the initial permutation

IP							
58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

Table: 1

b) The permuted input block then acts as the input to a key-dependent computation. The output of that computation is called pre-output and is subjected to inverse permutation IP^{-1}

IP^{-1}							
40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	69	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

Table: 2

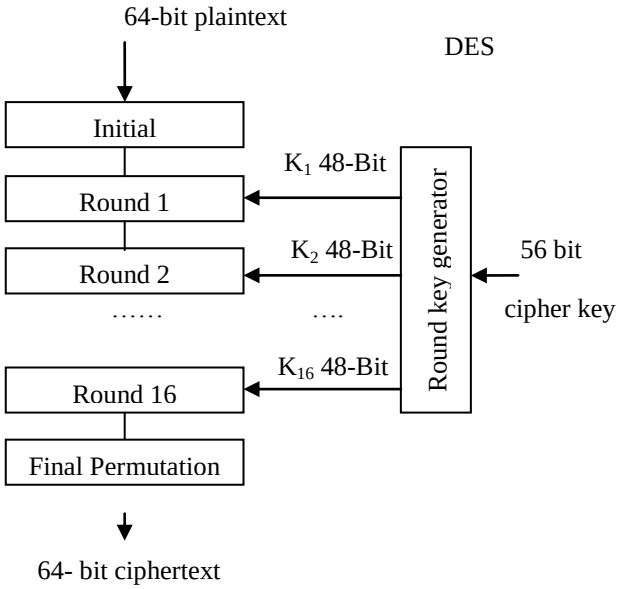

Fig: 3

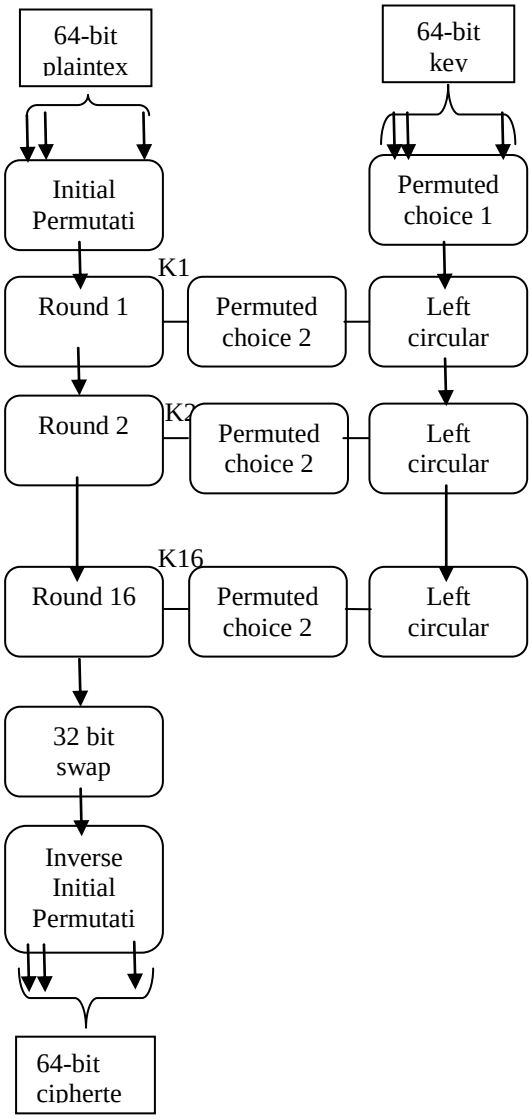

Fig: 4

H. Des Decryption:

a) CC:64 bits of ciphertext
b) K_{16},K_{15} ……K_1 round keys
c) IP initial permutation
d) FP: Final Permutation
e) F(): Round function
f) The output of DES decryption is: TT : 64 bits clear text

I. Algorithm:

a) Initial permutation is applied:
CC = IP (CC).
b) CC is divided into two 32 bit parts:
(LL_0, RR_0) = CC
c) (LL_1,RR_1) = (RR_0, $LL_0 \wedge f(RR_0, K_{16})$)
d) (LL_2,RR_2) = (RR_1, $LL_1 \wedge f(RR_1, K_{15})$)
e) ……
f) The two parts now swapped:TT = (RR_{16}, LL_{16})
g) Final permutation is applied: TT = FP(TT)

J. Key Schedule Algorithm:

The input of the key schedule [9]Algorithm is:
a) K is the 64 bit key
b) PC_1 is the permuted choice 1
c) PC_2 is permuted choice 2
d) R_1 $r_{2\ldots\ldots}$ r_{16},are the left shift rotations
The output of the key schedule algorithm is:
a) K_1, k_2,….k_{16} are the sixteen 48 bit round keys

K. Algorithm

a) Applying permuted choice 1 and thus returning 56 bits: K' = PC_1 (K).
b) K' is divided into two 28 bit parts: (C_0, D_0) = K'
c) Left shifting is permuted (C_1, D_1) =(r_1, (C_0), $r_1(D_0)$)
d) Applying permuted choice 2 and thus returning 48 bits : k_1= $PC_2(C_1,D_1)$
e) Left shifting is permuted (C_2, D_2) =(r_2, (C_1), $r_2(D_1)$)
f) Applying permuted choice 2 and thus returning 48 bits : k_2= $PC_2(C_2,D_2)$
g) K_{16} = $PC_2(C_{16}, D_{16})$

L. DES schedule tables

a) Permuted Choice 1 – PC1:

PC1

57	49	41	33	25	17	9
1	58	50	42	34	26	18
10	2	59	51	43	35	27
19	11	3	60	52	44	36
63	55	47	39	31	23	15
7	62	54	46	38	30	22
14	6	61	53	45	37	29
21	13	5	28	20	12	4

Table: 3

b) Permuted Choice 2 – PC2:

PC2

14	17	11	24	1	5
3	28	5	6	21	10
23	19	12	4	26	8
16	7	27	20	13	2
41	52	31	37	47	55
30	40	51	45	33	48
44	49	39	56	34	53
46	42	50	36	29	32

Table: 4

c) Left shift (number of bits to rotate):

Left Shift (number of bits to rotate):

r_1	r_2	r_3	r_4	r_5	r_6	r_7	r_8	r_9	r_{10}	r_{11}	r_{12}	r_{13}	r_{14}	r_{15}	r_{16}
1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

Table: 5

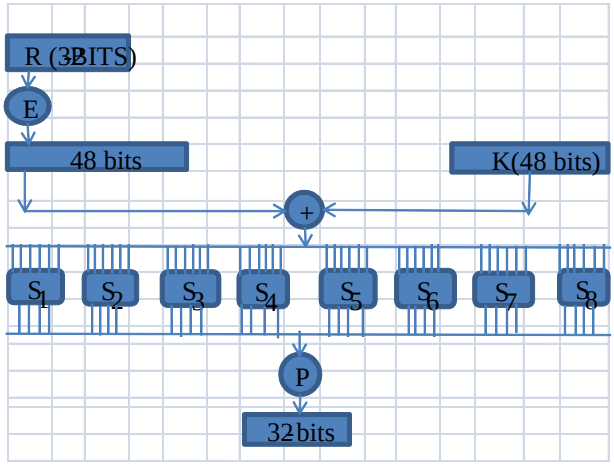

Fig: 5

V. AVALANCHE EFFECT

Definition: Avalanche effect is a key desirable property of cryptographic algorithms like block ciphers and cryptographic hash functions[10]. DES exhibits strong avalanche.

A. Properties

a) When there is slight change in input, output changes drastically.
b) Primary design objective is to construct such a cipher or hash function which xhibits such effect.
Example: In SHA-1, when a single bit is changed the hash sum becomes completely different

A. Disadvantages:

If a cryptographic hash function does not exhibit avalanche effect, then the cryptanalyst can make predictions about the input through the output. Thus the algorithm can be either partially or completed.

B. Strict Avalanche criterion:

a) Introduced by Webster and traverse in 1985.
b) Generalization of the avalanche effect.
c) Holds whenever a single bit is complemented each output bit changes with a fifty percent probability.

C. Bit independence criterion:

Output bit changes independently when any single bit is inverted.

VI. DES MODES

Modes can be classified as single mode and multiple modes of operation [11].

- **Single Mode operation:** these are used to hide patterns in the plaintext and protect against the chosen plaintext attacks. Example: ECB, CBC, CFB, OFB, CTR and PCBC.
- **Multiple Modes:** with the exhaustive search of keys multiple modes of operation came into existence these are more secure than a single mode of operation.

A. Electronic code book mode (ECB):

Message is dividing in blocks and is encrypted separately. The whole process is of encryption is independent of each other.

B. Cipher Block chaining mode(CBC):

The cipher block chaining mode was developed by IBM in 1976. Before encryption each block of plaintext input is XORed with the previous ciphertext block. An initialization vector is ued in the first block to make each message unique.

Disadvantages:

1. Encryption is sequential and can not be parallelized
2. Each ciphertext block depends on all the message block.
3. Thus a change in the message affects all ciphertext block as well as the original block.
4. Requires initial values (IV) which should be known to the sender and receiver but if the IV is sent in a clear form, an attacker can change bits of the 1st block.

CBC Encryption
$C_i = E_k (P_i \oplus C_{i-1})$, $C_0 = IV$
CBC Decryption
$P_i = D_k (C_{i)} \oplus C_{i-1}$, $C_0 = IV$

C. Propagating cipher block chaining (PCBC):

It is also known as plaintext cipher block chaining mode. This mode was basically developed or causing small changes in ciphertext to propagate infinitely in the encryption and the decryption process.

Encryption algorithm:
$C_i = E_k (P_i \oplus P_{i-1,} \oplus Ci_{-1})$, $P_0 \oplus C_0 = IV$

Decryption Algorithm:
$P_i = D_k (C_i) \oplus P_{i-1,} \oplus Ci_{-1}$, $P_0 \oplus C_0 = IV$
Applications: used in Kerberos IV and WASTE[12].

D. Cipher Feedback mode(CFB):

Here a block cipher is transformed into a self synchronizing stream cipher. The decryption process is similar to the CBC encryption in reverse.
$C_i = E_k(Ci_{-1}) \oplus P_i$
$P_i = E_k(Ci_{-1}) \oplus C_i$
$C_0 = IV$

Advantages:

a) The block cipher is only used in the encrypting direction.
b) Message does not need to be padded to a multiple of the cipher block size.
c) It is appropriate when data arrived in bits/bytes
d) It is the most common stream mode

Disadvantages:

a) Any change in the plaintext continues forever in the ciphertext
b) Encryption and decryption process can not be parallelized
c) During encryption a one bit change in the ciphertext affects two plaintext blocks.

E. Output Feedback (OFB) mode:

The output feedback mode makes a block cipher into a synchronous stream cipher. In this mode key stream blocks are XOR-ed with the plaintext block to get the ciphertext. Many errors correcting codes function normally even when applied before encryption. The encryption and decryption process are same.

$C_i = P_i \oplus O_i$
$P_i = C_i \oplus O_i$
$O_i = E_k(O_{i-1})$
$O_0 = IV$

F. Counter (CTR) mode:

CTR allows a random access property during decryption and is also known as integer counter Mode (ICM) and Statement Integer Counter (SIC) mode.

Applications: It suits to the operations on a multi-processor machine where blocks can be encrypted in parallel.

VII. BRUTE-FORCE ATTACK

Definition: brute force attack[13] is also known as exhaustive key search. The main idea of brute force attack is systematically checking all possible keys until the correct key is found.

Feasibility of such attacks is dependent on the key length which is used in the encryption process. Longer keys are difficult to break than the shorter keys.

VIII. REPLAY ATTACK

Definition: it is a type of network attack in which a valid data transmission is either repeated or delayed. The captured packet is first exploited then sent again. It leads to unexpected results.

Protection against replay attacks:
a) Using session tokens: there are choosing randomly.
b) One time passwords: password expires after a short span of time.
c) Time – stamping
d) Synchronization: it is achieved through a secure protocol.

IX. TRIPLE DES

Triple DES, a variant of DES is also known as 3DES and encrypts data thrice. Three 64 bit keys[14] are used for a key length of 192 bits.

a) 1st plaintext is encrypted with a key
b) The output of the encryption is again encrypted with a sound key and resulting ciphertext is again encrypted with a 2nd key and
c) The resulting ciphertext is again encrypted with a 3rd key.

A. Usage:

a) Electronic payment industry
b) Microsoft OneNote
c) Microsoft Outlook

B. Advantages:

a) Used widely than DES since it offers much more security.
b) Reliable
c) Longer key length reduces probability of an attack

C. Disadvantages:

Slower than DES

D. Mode of operation of triple DES:

there are two modes of operation of triple DES[15].
a) Triple ECB (Electronic Code Book): this type of triple DES works in the same way like ECB mode of DES. It is used by private encryptor.
b) Triple CBC (Cipher Block Chaining): this type of triple DES works in the same way like ECB mode of DES. Key length is of 168 bits and the first 64 bits are used as initialization vectors. This is not widely used and is more secure.

X. ADVANCED ENCRYPTION STANDARD (AES)

The Advanced Encryption Standard[16] is symmetric – key block cipher published by the National Institute of Standards and Technology (NIST) in December 2001 for encrypting and decrypting data.

NIST Selected AES mainly because of three reasons:
a) Security
b) cost
c) implementation

A. Properties :

a) Based on substitution permutation network.
b) Does not use Feistel network.
c) Fixed block size of 128 bits.
d) Key size of 128,192 or 256 bits
e) Operates on a 4*4 column major order matrix of bytes.

B. Transformations Used by AES:

AES uses four types of transformations:
a) Substitution
b) Permutation
c) Mixing
d) Key-adding

C. Attack Against AES:

a) Brute- Force Attack
b) Statistical attack
c) Differential attack
d) Linear attack

D. Implementation of AES:

AES can be implemented in software, hardware and firmware. The implementation can use table lookup process or routines that use a well-defined algebraic structure. These can be implemented using cheap processors and a minimum amount of memory.

XI. LINEAR CRYPTANALYSIS

Definition: Linear cryptanalysis[17] is the attacks which are developed for block ciphers and stream ciphers. It is basically a general form of cryptanalysis and was discovered Mitsuree Matsu.

Parts of Linear Cryptanalysis: linear cryptanalysis consists of two parts:

a) Construction of linear equations relating to plaintext, ciphertext and key bits. Linear equations are constructed for those whose probability of holding is as close as possible to 0 or 1

b) Linear equations are used with known plaintext and ciphertext pair to drive bits.

Construction of linear equations: Linear equations express the equality of two expressions. The binary variables of these expressions are combined with XOR operation.

XII. DIFFERNTIAL CRYPTANALYSIS

Definition: Differential cryptanalysis[18] is the study of how the difference in input can affect the resultant difference at the output.

Differential cryptanalysis is applicable to block cipher, stream cipher and cryptographic hash function. It was developed by Eli Biham and ADI Shamir[19].

Differential cryptanalysis is used for tracing the difference through network of transformations[20].

XIII.REFERENCES

[1] Menezes, Alfred J.; van Oorschot, Paul C.; Vanstone, Scott A. "Chapter 7: Block Ciphers". Handbook of Applied Cryptography, 1996 .

[2] Shannon, Claude "Communication Theory of Secrecy Systems". Bell System Technical Journal **28** (4): 656–715, 1949.

[3] Martin, Keith M. "Everyday Cryptography: Fundamental Principles and Application"s. Oxford University Press. p. 114. ISBN 9780199695591,2012 .

[4] William Stallings, "Cryptography and Network Security, principles and practices", 4th Edition, March, 2007

[5] Keliher, Liam et al "Modeling Linear Characteristics of Substitution-Permutation Networks". In Hays, Howard & Carlisle, Adam. Selected areas in cryptography: 6th annual international workshop, SAC', 2000.

[6] Morris Dworkin , "Recommendation for Block Cipher Modes of Operation – Methods and Techniques", Special Publication 800-38A NIST, December 2001

[7] Chakraborty, D. & Rodriguez-Henriquez F. "Block Cipher Modes of Operation from a Hardware Implementation Perspective", 2008.

[8] Van Tilborg, Henk C. A.; Jajodia, Sushil, eds. "Encyclopedia of Cryptography and Security" 2011 .

[9] William Stallings NIST Special Publication 800-57 Recommendation for Key Management — Part 1: General (Revised), March, 2007.

[10] ISO/IEC "Information technology — Security techniques — Hash-functions — Part 2: Hash-functions using an n-bit block cipher" 10118-2:2010

[11] ISO/IEC "Information technology — Security techniques — Modes of operation for an n-bit block cipher", 10116:2006 .

[12] Cusick, Thomas W. & Stanica, Pantelimon "Cryptographic Boolean functions and applications", 2009 .

[13] Matsui, M. and Yamagishi, A. "A new method for known plaintext attack of FEAL cipher". Advances in Cryptology - EUROCRYPT 1992.

[14] Bruce Schneier Description of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish), 1993.

[15] ISO/IEC 9797-1: "Information technology – Security techniques – Message Authentication Codes (MACs) – Part 1: Mechanisms using a block cipher", ISO/IEC, 2011.

[16] James Nechvatal, Elaine Barker, Lawrence Bassham, William Burr, Morris Dworkin, James Foti, Edward Roback, "Report on the Development of the Advanced Encryption Standard (AES)", National Institute of Standards and Technology (NIST), October 2000.

[17] Junod, Pascal & Canteaut, Anne "Advanced Linear Cryptanalysis of Block and Stream Ciphers" , 2011.

[18] Biryukov A. and Kushilevitz E. "Improved Cryptanalysis of RC5", EUROCRYPT 1998.

[19] Baigneres, Thomas & Finiasz, Matthieu "Dial 'C' for Cipher". In Biham, Eli & Yousseff, Amr. Selected areas in cryptography: 13th international workshop, SAC 2006, Montreal, Canada, August 17-18, 2006 : revised selected papers. Springer. p. 77.ISBN, 2007.

[20] Bellare, Mihir, Rogaway, Phillip, "Introduction to Modern Cryptography", 11 May 2005.