International Journal of Computer Applications (0975 – 8887)
Volume 128 – No.8, October 2015

Let It Encrypt (LIE)

Mukta Sharma
Research Scholar
Teerthanker Mahaveer University, Moradabad

Surbhi Dwivedi
Sr. Software Engineer
NIIT Technologies
Greater Noida

R.B. Garg, PhD
Ex-Professor
University of Delhi
Delhi

ABSTRACT
Living in the era of Information technology has leveraged the mankind. The technology has made the life so easy and convenient. It has given the power to speed up the task. Starting from the very basic daily routine shopping, to paying bills, updating passbooks, reserve a table, book a movie ticket or plane ticket etc. has widened the horizon of thinking and relying so much on the technology in the form of Microwave, Washing Machines, GPRS enabled cars and many more. The society experiences the benefits from the technology; at the same time the technology has its own ill effects. Which are horrifying the customers, the customers are little more reluctant, cautious and hesitant to share their information; especially when it comes to the finances and personal demography. The technology advancement has proven as a boon until someone becomes a victim of the same.

The banks have turned more vigilant and they are concerned for their customer's privacy, confidentiality and integrity. The banks are going a step forward to help the customers feel more secure to transact online. Therefore, banks are coming up with better security measures like virtual keyboard, OTP, 3D secure pin, Grid matrix etc. Banks are simultaneously looking for a good secure algorithm so that the transactions could be more secure in case they reach wrong hands.

In this paper, LIE (Let it Encrypt) as the name suggests an algorithm has been proposed with a vision to secure the online transactions. This paper focuses on Symmetric Key Cryptography algorithm. This paper proposes a new encryption algorithm – LIE and discusses and compares it with few of the symmetric key algorithms like DES, 3DES, Blowfish and AES.

General Terms
Security, Algorithms et. al.

Keywords
Cryptography, Symmetric & Asymmetric Cryptography, Plain Text, Cipher Text, Encryption, Decryption, Key, DES, AES, LIE

1. INTRODUCTION
With every new invention it gives the society a new horizon to think and believe. Similarly in the field of Information Technology there has been a tremendous growth. Especially talking about Internet it has actually revolutionized the way of conducting business and many more things.Banking industry is also not untouched from this boon. Banks are upgrading so as to fully utilise the benefits of the technology. Banks had been offering varied services online starting from the informative details, to check the balance and now to transact online. As Banking industry has finance as a product needs to be more vigilant for security. Specially, while making online payments the transaction ought to be very secure; as reaching in wrong hands may lead to disaster and may ruin the banks reputation. To achieve security for each transaction detail many researches have been conducted and are still going on in the field of cryptography. The objective is to find a secure algorithm which should be difficult to decipher by any cryptanalyst.

Cryptography
It is an art of mangling information into obvious incomprehensibility in a way permitting a secret method of unmangling.[2] Since ages human has a requirement to share private information with only intended recipients. Cryptography gives a solution to this requirement. Using its technique Encryption, the plain text message is coded or encrypted into a Cipher text. That cipher text is send across any network. The only recipient will be able to decode or decrypt it back into plain text using again the cryptography technique, Decryption.

Encryption/ Decryption Algorithms are a mathematical way to substitute/transpose the plain text to cipher text and vice-versa. To perform cryptography, one requires the secure algorithm which helps the conversion efficiently, securely if performed with a key.

1.1 Types of Cryptography
1.1.1 Symmetric encryption
also popular with a name conventional encryption. Symmetric encryption is known and used since long especially before 1970s prior to the development of public key. In this type of technique same key is used to encipher & decipher the text. For better security in symmetric encryption one should keep the following criteria's in mind:*A strong encryption algorithm- [6] A strong algorithm which is robust & resilient against a potential breach using combinations of cipher texts & key.*

Key should be exchanged very safely and should be kept secretly because if key is known the entire algorithm is compromised.

1.1.2 Asymmetric Encryption is a two-key
cryptosystems, which has enciphering and deciphering keys.[4] The keys are non-feasible to determine computationally. In the year 1976, Diffie and Hellman conceptualised Public key cryptography each user has a set of both public and private keys and communication can be done only by knowing one's public key. The concept of dual keys makes it more secure, authentic and integrity was well maintained.

Plain Text can be Processed in the following ways:-

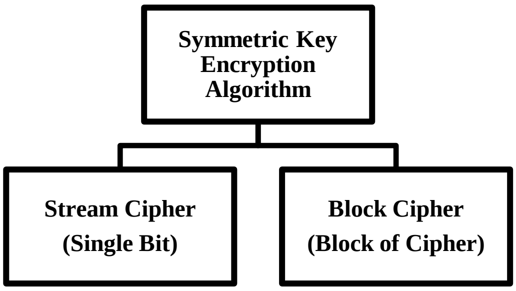


Figure1: Symmetric Key Encryption Algorithm

A block cipher as the name suggests breaks the plain text into blocks, the output (cipher text) after encrypting the plain text is of equal length. Typically, a block size of 64 or 128 bits was initially used. It is the most commonly preferred symmetric encryption algorithms are Block ciphers. The concept of block ciphers defines a function which takes k-bit key subset & n- bit of the plain text as parameters. The function maps the n-bit of plain text to n-bit of cipher text. Here the value 'n' defines the block length. The key is randomly generated from the key space 'K'. The function is so designed that for n-bit plain text, cipher text & a fixed key, the encryption function is a bijection. With each potential key, there is a different bijection. This whole process further allows unique decryption in invertible manner following mapping one-to-one. In short, block cipher can be defined as the function which breaks the plaintext or message into blocks, each of which is then encrypted and produces a block of Cipher text of equal size for each plaintext block.

A Stream Cipher is also known as State Cipher. A stream cipher is a symmetric cipher which operates with a time-varying transformation on individual bit of plaintext. In short, it is a method which encrypts the data one bit or one byte at a time. A sequence of plain text digits p0, p1 is encrypted into a sequence of cipher text digits c0, c1 followed by running key also called as Key-Stream. One time pad is one of the most popular examples of Stream cipher. The random key stream makes it very difficult to break. Stream ciphers have several advantages like; they are usually faster and have a lower hardware complexity than block ciphers.

1.2 Two techniques are used for cryptography algorithm

Substitution techniques substitutes plaintext elements (characters, bits) into cipher text elements.[3] The rule in substitution cipher is the letter which is substituted can be used only once. A substitution cipher is one in which letters are represented by other letters; can be deciphered by the one who knows the order. Two thousand years ago Julius Caeser, roman emperor invented Caeser Cipher. Rotor machines are hardware devices that use substitution techniques. Cryptanalyst can try to break the Substitution cipher via Frequency Analysis- Word Frequency Analysis and Letter Frequency Analysis.

Transposition techniques methodically rearrange the locations of plaintext components. Mathematically the alphabets are permutated, so transposition can be said as Permutation. In short, transposition can hide the message by rearranging the letter order, without altering the actual letters used. Rail Fence is a good example of Transposition.

Scope of the paper

The paper proposes a new encryption algorithm to ensure security of the online transactions. The symmetric cipher algorithm uses the concept of Feistel network, expansion, substitution, permutation etc along with 256 bit key for ensuring better security. A comparative analysis of existing symmetric algorithm and the current algorithm has been depicted in a tabular format.

Outline of the paper

The paper is strategically bifurcated into six parts, starting from the introduction about the subject, moving on to the Technical Groundwork. Part III, discusses the proposed algorithm; how it actually works. Later section discusses the comparison between the proposed algorithm and existing algorithms. Finally, summarizing with a conclusion and the last section shows the provisions to enhance the algorithm in near future.

2. Technical Groundwork

The preferred symmetric encryption algorithms are block ciphers. As discussed above in the paper block cipher breaks the plaintext in fixed-sized blocks and produces the same size block of cipher text. The paper depicts comparison of various symmetric block ciphers algorithms: the Data Encryption Standard (DES), triple DES (3DES) and Advanced Encryption Standard (AES) etc.

Claude Shannon has given the concepts of Diffusion and Confusion.[6] The concepts of confusion-diffusion have become the Corner stone of modern block cipher design. As it makes the algorithm more secure which is the essence of cryptography. Therefore, it has become so successful.

The term diffusion means to spread something widely. Here the term defines the process to dissipate the plain text into long range of cipher text. On the other hand, confusion is created by making the relation between cipher & key highly complex making it tougher for attackers to deduce the key. A complex substitution algorithm helps to resolve this problem.

The Feistel network was named after Horst Feistel, IBM-Crytographer. Feistel network was first implemented in 1973 in Lucifer cipher by Horst Feistel and Don Coppersmith.[2] It is used by symmetric block ciphers. In general, a symmetric block cipher consists of a sequence of rounds, where in each round substitution and permutations are performed conditioned by a secret key value. LIE is also a symmetric key algorithm which is based on feistel network. Therefore, it also input plaintext; divide it into two halves (left and right). Later it goes through 8 rounds iteration for security; better security can be attained by using minimum 16 rounds. LIE iterates only 8 times but with unique keysets which make LIE more secure. Fiestel cipher has the benefit that encryption and decryption operations are very similar, that only a reversal in the key schedule can attain the result.

Substitution: Each plaintext element is uniquely replaced/substituted into cipher text.

Permutation: Changing the order of plaintext. The new ordered elements replace the previous one. They don't change the unit but just rearrange them in a complex order.

Fiestel encryption depends on the following parameters

Round function: round function (F) plays an important part. The more complex it is the more secure the algorithm will be. It will have greater resistance to break.

Block size: The large the block size greater is the security and slower will be the speed of processing. A block size of 128 bits is a reasonable trade off and is nearly universal among recent block cipher designs.

Key size: Security of an algorithm depends on Key size also as if the key size is less it is observed the security is also less. Like, DES uses 56 bits of key which can be easily breached. But if key size is more it increases the security but it may increase the time for encryption/decryption. Generally, 128 bits key is used.

Number of rounds: It's the base of symmetric key algorithm, where it has been observed a single round offers inadequate security but that multiple rounds offer better security. A typical size is 16 rounds.

Subkey generation algorithm: The more complex the sub-key generation is the more difficult it will be to break by cryptanalysis.

Speed: For every algorithm time and space are basi complexities. Therefore, it is important factor to check th speed of execution of the algorithm.

3. Proposed Algorithm

LIE (Let it Encrypt) is a symmetric key block ciphe algorithm. The algorithm comprises of various good feature required for an encryption algorithm. Principles like confusion, diffusion, Permutation, substitution & feistel network makes the algorithm more secure. The algorithm is considered to be fairly secure, if the keys for the inner rounds are discrete. Following which, the number of rounds may be reduced. LIE has 256 bit key. This key is used to generate 8 discrete sub-keys. Each sub key is individually used in each round. The paper discusses all the permutation tables, function & keys required by the algorithm.

Encryption Process

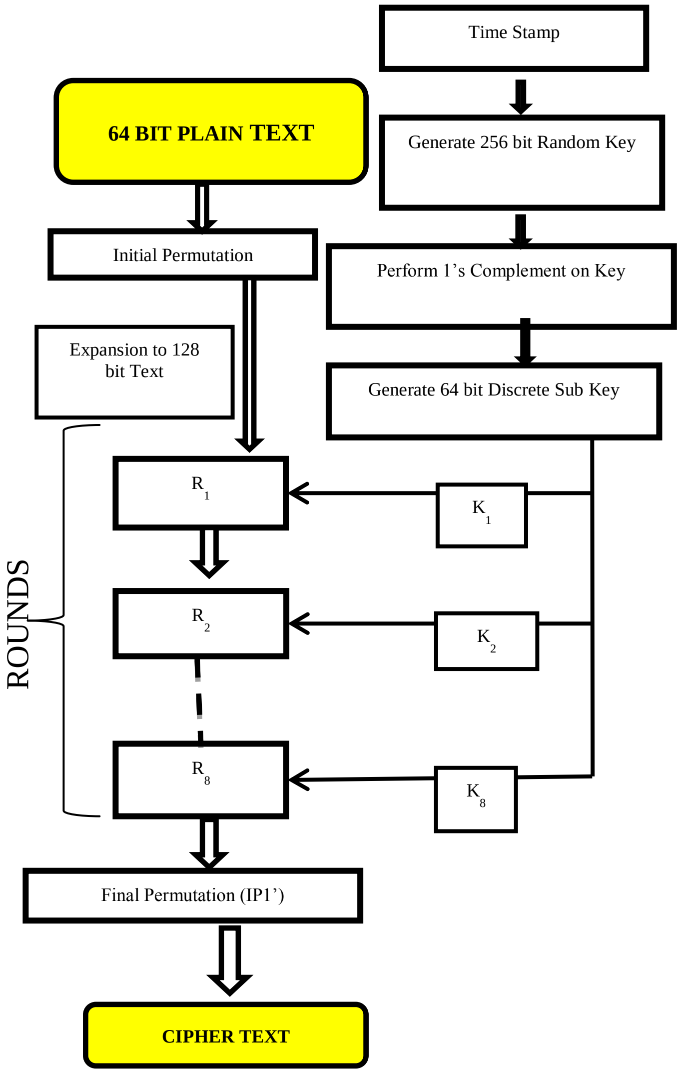


Figure 2: Encryption Process

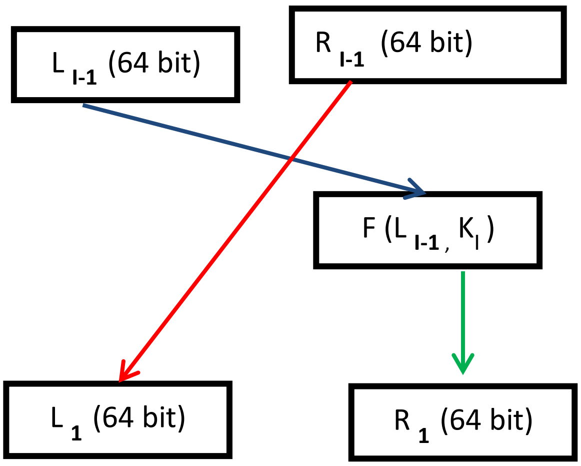


Figure 3: Round Function Insight

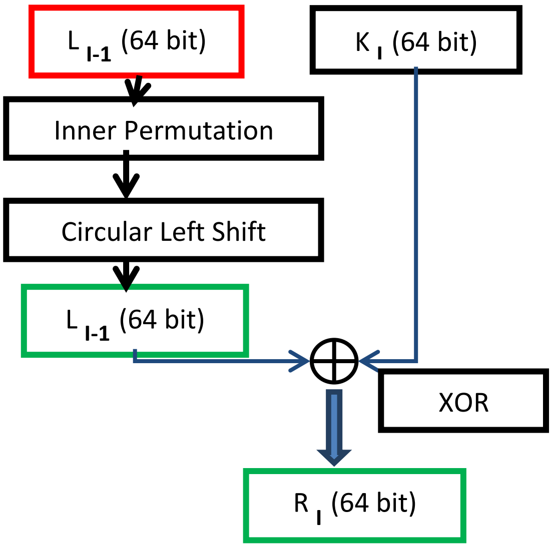


Figure 4: Function

Pseudo Code

Step 1. Initialize Key matrix k[] = 0

Step 2. Take Time stamp -> TS

Step 3.

3.1 Add all digits of TS.

Sum = 0

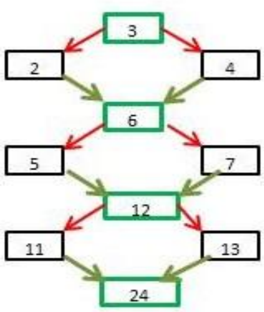
Sum = TS modulo 10 + Sum

Loc = sum

3.2 for loc <=255

K[loc] = 1

Loc = (loc-1) + (loc+1)



Step 4. Perform 1's Complement of the key matrix k[]

Step 5. Generate subkeys k1 to k8 using subkeys matrices.

Step 6. Take 64 bit plain text as input ->PT

Step 7. Perform Initial Permutation using Table 1

Step 8 While I <>8

Step 9 Divide PT(128 bits) into L0 & R0 each 64 bit.

Step 10. Li = Ri-1

Ri = F(Li-1, ki)

Step 11. F(Li-1, ki)

a) Permutate Li-1 using table 2 Inner Permutation
b) Perform Left Circular Shift
c) Li-1 XOR Ki

Step 12. I-> i+1

Step 13. Obtain CT' = R8L8

Step 14. CT = Perform Final Permutation using Table 3

Reading Sequence in the Key Matrix

Table1: Reading Sequence in the Key Matrix

0	1	2	3	4	5	6	7
8	9	10	11	12	13	14	15
16	17	18	19	20	21	22	23
24	25	26	27	28	29	30	31
32	33	34	35	36	37	38	39
40	41	42	43	44	45	46	47
48	49	50	51	52	53	54	55
56	57	58	59	60	61	62	63
Key Sequence							

Subkeys

Table2: Subkey1

0	51	3	48	4	55	7	52
8	59	11	56	12	63	15	60
64	115	67	112	68	119	71	116
72	123	75	120	76	127	79	124
128	179	131	176	132	183	135	10
136	187	139	184	140	191	143	188
192	243	195	240	196	247	199	244
200	251	203	248	204	255	207	252
Key 1							

Table3: Subkey2

205	223	254	236	201	219	250	232
197	215	246	218	193	211	242	224
141	159	190	172	137	155	186	168
133	151	182	164	129	147	178	160
77	95	126	108	73	91	122	104
69	87	118	100	65	83	114	96
13	31	62	44	9	27	58	40
5	23	54	36	1	19	50	32
Key 2							

Table4: Subkey3

1	103	117	84	74	107	121	88
138	171	185	152	134	167	181	148
10	43	57	24	14	47	61	28
78	111	125	92	130	163	177	144
194	227	241	208	198	231	245	212
2	35	49	16	6	39	53	20
66	99	113	80	142	175	189	156
202	235	249	216	206	239	253	220
Key 3							

Table5: Subkey4

17	34	33	18	85	102	101	86
153	170	169	154	221	238	237	222
29	46	45	30	89	106	105	90
149	166	165	150	209	226	225	210
21	38	37	22	217	234	233	218
25	42	41	26	213	230	229	214
81	98	97	82	157	174	173	158
145	162	161	146	93	110	109	94
Key 4							

Table6: Subkey5

48	112	176	240	193	129	65	1
50	114	178	242	195	131	67	3
52	116	180	244	197	133	69	5
54	118	182	246	199	135	71	7
56	120	84	248	201	137	73	9
58	122	186	250	203	139	75	11
60	124	188	252	205	141	77	13
62	126	190	254	207	143	79	15
Key 5							

Table7: Subkey6

102	119	136	153	105	120	135	150
103	104	121	137	152	151	134	118
0	1	16	17	44	45	60	61
170	171	186	187	224	225	240	241
34	35	50	51	74	75	90	91
238	239	254	255	194	195	210	211
68	69	84	85	14	15	30	31
204	205	220	221	164	165	180	181
Key 6							

Table8: Subkey7

0	17	34	51	132	149	166	183
72	89	106	123	204	221	238	255
4	21	38	55	136	153	170	187
76	93	110	127	192	209	226	243
8	25	42	59	140	157	174	191
64	81	98	115	196	213	230	247
12	29	46	63	128	125	162	179
68	85	102	119	200	217	234	251
Key 7							

Table9: Subkey8

0	33	18	51	65	98	83	112
130	163	144	177	195	224	209	242
5	38	23	52	70	103	84	117
135	164	149	182	196	229	214	247
10	43	24	57	75	104	89	122
136	169	154	187	201	234	219	248
15	44	29	62	76	109	94	127
141	174	159	188	206	239	220	253
Key 8							

Table 10: Initial Permutation

	1	2	3	4	5	6	7	8
1	0	9	18	27	1	2	3	10
2	11	19	8	16	17	24	25	26
3	3	10	17	24	11	18	19	25
4	26	27	0	1	2	8	9	16
5	36	45	54	63	37	38	39	46
6	47	55	44	52	53	60	61	62
7	39	46	53	60	47	54	55	61
8	62	63	36	37	38	44	45	52
9	32	41	50	59	33	34	35	42
10	43	51	40	48	49	56	57	58
11	35	42	49	56	43	50	51	57
12	58	59	32	33	24	40	41	48
13	4	13	22	31	5	6	7	14

14	15	23	12	20	21	28	29	30
15	7	14	21	28	15	22	23	29
16	30	31	4	5	6	12	13	20

Table 11: Inner Permutation for Function 'F'

63	55	47	39	30	22	14	6
7	15	23	31	38	46	54	62
61	53	45	37	28	20	12	4
5	13	21	29	36	44	52	60
59	51	43	35	26	18	10	2
3	11	19	27	34	42	50	58
57	49	41	33	24	16	8	0
1	9	17	25	32	40	48	56

Table 12: Final Permutation

	1	2	3	4	5	6	7	8
1	19	28	54	95	38	62	81	32
2	12	105	71	8	91	24	4	45
3	102	43	31	58	118	76	21	108
4	49	3	83	107	16	113	124	65
5	98	110	23	55	72	52	11	39
6	20	77	36	101	26	106	89	61
7	42	6	109	46	69	120	13	125
8	67	48	88	1	90	53	78	33
9	73	17	104	51	7	22	97	84
10	92	41	10	35	82	112	47	5
11	64	122	94	60	18	79	126	50
12	99	57	25	119	37	100	44	74
13	30	114	85	66	96	2	115	34
14	70	9	80	15	116	59	128	68
15	121	111	75	56	123	29	103	86
16	40	87	27	117	63	127	93	14

Decryption process

The decryption process can be explained in a very simpler way. The same algorithm is used except the order of the keys is reversed. That is, the keys will be used in order K8, K7 …. K1. Using the permutation tables, the plain text can be obtained.

4. COMPARISON

Table 13: Comparative Analysis of Algorithms

	Year	**Inventor**	**Key Size**	**Block Size**	**Feistel network**	**Confusion & Diffusion**	**S-Keys**	**P-Keys**	**Possible Keys**	**No. of Rounds**
DES	1975, registered in 1979	IBM	56 bits	64 bits	Yes	Yes	8 s-boxes (48 bit input and 32 bit output) each set of 6 bits reduced to 4	permutes 32 bits, 4	2^{56}	16 rounds
3DES	1978	ANS X9.52	128-192 bits	64 bits	Yes	Yes			2^{112} Or 2^{168}	
AES	1998	Vincent Rijmen, Joan Daemen	128, 192, or 256 bits	128 bits	No	Yes	It does not use S & P boxes. 4×4 column-major order matrix of bytes based on modular arithmetic with non-linear polynomials		2^{128} or 2^{192} or 2^{256}	10 rounds for128 bit keys. 12 rounds for 192

										bit keys. 14 rounds for 256 bit keys.
Blowfish	1993	Bruce Schneier	(variable) 32-448 bits	64 bits	Yes	Yes	4*32 S-boxes with 256 bits	18*32	2^{32} or 2^{448}	16 rounds (64 bit data element)
LIE	2015	Mukta, Surbhi, R.B Garg	256bits	64 bits	Yes	Yes	Does not use S-boxes, It use 8 discrete Keys of 64 bits	3	2^{256}	8 rounds
3DES	1978	ANS X9.52	128-192 bits	64 bits	Yes	Yes			2^{112}Or 2^{168}	

5. CONCLUSION

LIE, Let it Encrypt has been designed with a vision to secure the online transaction. Key size plays a significant role in cryptographic security; therefore the key length is 256 bits. Key generation is done automatically with the help of time stamping. To make key more strong, 1's compliment is used.

The concept of Feistel cipher, expansion, confusion, substitution, permutation, discrete Key matrix, makes this very secure and fast. LIE is very easy to analyse. It has only 8 rounds which make it faster. All Sub keys are discrete which makes it difficult to break.

LIE needs to be implemented, tested and compared with other algorithms with regard to Time and space complexity.

6. FUTURE SCOPE

The Key generation process can be enhanced further. Here, the timestamp yields a 1 digit number using which the first location in key matrix is assigned value '1'. This can be major flaw for this algorithm. Thus, in future work some design to generate the key randomly can be build. Besides this, the key size can also be increased for more security. The number of rounds here is 8. Even though, discrete keys are used but if rounds are increased then certainly it will be more secure algorithm. The cryptanalysis can be done & implementation using C++ or java can also solve some issues around the algorithm. Good quality of testing of this algorithm is required so as to uncover the bugs around it.

7. REFERENCES

[1] A. Kumar, S. Jakhar and S. Makkar, "Comparative Analysis between DES and RSA Algorithm's", International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 2, Issue 7, Jul 2012

[2] A. Menezes, P. van, Oorschot, and S. Vanstone, "Handbook of Applied Cryptography", CRC Press, 1996.

[3] B.Guttman and E. Roback, " An Introduction to Computer Security: The NIST Handbook", Special Publication, 1995

[4] B. Schneier, "Applied Cryptography", Second Edition, John Wiley & Sons, Inc., 1996

[5] W. Stallings, "Network Security Essentials Applications and Standards", 4th edition, Pearson, 2011

[6] W. Stallings, "Cryptography and Network Security: Principles and Practice",5th edition, Pearson, 2011