CIPHERING OF TEXT BY USING SHFIT REGISTER TECHNIQUE AND ITS TRANSMISSION OVER OPTICAL FIBER

Haider J. Abd
Departement of Electrical Engineering
Babylon University

Mohanned Hassan Ali
Department Engineering of Technical Electrical Power
Technical College/ Musayab

Abstract

Stream cipher is one of important branch of cryptography that can be implemented by using software and hard ware components .this system is divided into two types :

1.linear stream cipher system .

2. Non- linear stream cipher system .

In this work, we deal with the two type of stream cipher system , the first type doesn't have top secret degree due to weakness of the linear complexity for the sequence generated from Linear Feedback Shift Register (LFSR) .There are many algorithm ms that are designed by using the process of non- linear combination for more than one linear shift register ,one of these algorithm ,that is called adder algorithm ,is used to generate a key sequence for encryption and deciphering process .The data in form of speech or waveform have been recorded by using computer microphone .these digital speech were encrypted .the encrypted speech has been sent via RS232 standard interface at a bit rate 19.6 kbps to another computer ,and then will be decrypted .

The encrypted data were transmitted through the optical system .a multi mode optical fiber is used as a channel and PIN photo diode is used as an optical detector.

Keyword: **Cipher, Shift Register, Optical Fiber, Encryption, Decryption.**

تشفير لكلام نصي باستخدام تشفير مولد المفاتيح وإرساله عبر ليف بصري

مهند حسن علي
الكلية التقنية/المسيب
قسم تقنيات هندسة القدرة الكهربائية

حيدر جبار عبد
كلية الهندسة\ جامعة بابل
قسم الهندسة ا الكهربائية

الخلاصة

تعتبر انظمة التشفير الانسيابي من الانظمة الشفرية المهمة . حيث تعتمد امنيتها على درجة التعقيد لمولد متتابعة المفاتيح ولذلك شهدت هذه الانظمة دراسات تحليلية وبحوث عديدة في تقويم تصاميم المولدات الخطية واللاخطية وحساب التعقيد الخطي للمتتابعات الناتجة عن المكافئات الخطية لهذه المولدات اللاخطية .

يتناول هذا البحث تصميم وبناء خوارزميات لمحاكاة مولدات مفاتيح خطية ولاخطية باشكال وتراكيب مختلفة وحساب التعقيد الخطي لهذه المولدات ودمجها مع رسائل نصية باشكال مختلفة لتوليد بيانات تشفيرية بصور مختلفة . يتم ارسال هذه البيانات عن طريق الالياف البصرية بحسب مواصفاتها والمعدة لهذا النوع من البيانات واخيرا يتم استلام هذه البيانات وفك تشفيرها باستخدام انواع المفاتيح. تم استخدام لغة البرمجة (C^{++}) الاكثر ملائمة لهذه الانواع من التشفير.

Introduction

A communication is an important part of our daily lives .it helps us to get close to one another and exchange important information . The communication process involves information generation , transmission , reception , and interpretation (Hioki,1998),(Lubbe,1998).

Fiber optics is finding use in virtually every application involving the transmission of information .Computer can now be link together with fiber optics cables capable of transmission data several orders of magnitude faster than copper circuit . The computer can now be found in all layers of our society and the possibilities for communication have grown immensely. Cryptology is the science which concerned the method of providing secure storage and transportation of information it widest since .

Internal Architecture and Opertion of Optical Fiber

An optical fiber is a cylindrical dielectric waveguide that transmits light along its axis, by the process of total internal reflection. The fiber consists of a core surrounded by a cladding layer. To confine the optical signal in the core, the refractive index of the core must be greater than that of the cladding. The boundary between the core and cladding may either be abrupt, in step-index fiber, or gradual, in graded-index fiber. STEP-INDEX MULTIMODE FIBER (Amon,1997) has a large core, up to 100 microns in diameter. As a result, some of the light rays that make up the digital pulse may travel a direct route, whereas others zigzag as they bounce off the cladding. These alternative pathways cause the different groupings of light rays, referred to as modes, to arrive separately at a receiving point. The pulse, an aggregate of different modes, begins to spread out, losing its well-defined shape. The need to leave spacing between pulses to prevent overlapping limits bandwidth that is, the amount of information that can be sent. Consequently, this type of fiber is best suited for transmission over short distances, in an endoscope, for instance. GRADED-INDEX MULTIMODE (Gred,1984) FIBER contains a core in which the refractive index diminishes gradually from the center axis out toward the cladding. The higher refractive index at the center makes the light rays moving down the axis advance more slowly than those near the cladding. Also, rather than zigzagging off the cladding, light in the core curves helically because of the graded index, reducing its travel distance. The shortened path and the higher speed allow light at the periphery to arrive at a receiver at about the same time as the slow but straight rays in the core axis. The result: a digital pulse suffers less dispersion.

There are two different types of optical fiber: multimode and single-mode. Both are used in a broad range of telecommunications and data networking applications. These fiber types have dominated the commercial fiber market since the 1970s. The distinguishing difference, and the basis for the naming of the fibers, is in the number of modes allowed to propagate in the core of a fiber.

A “mode” is an allowable path for the light to travel down a fiber (John,1996). A multimode fiber allows many light propagation paths, while a single-mode fiber allows only one light path.

In multimode fiber (Piper,1982)the time it takes for light to travel through a fiber is different for each mode resulting in a spreading of the pulse at the output of the fiber referred to as inter modal dispersion. The difference in the time delay between the modes is called Differential Mode Delay (DMD). Inter modal dispersion limits multimode fiber bandwidth. This is significant because a fiber’s bandwidth determines its information carrying capacity, i.e., how far a transmission system can operate at a specified bit error rate .The optical fiber guides the light launched into the fiber core (**Figure.1**). The cladding is a layer of material that surrounds the core. The cladding is designed so that the light launched into the core is contained in the core.

Components Used in the Optic Fiber Communication System

1. Light Source:-

Light source is often considered to be the active component in an optical fiber transmission link. Its fundamental function is to convert the electrical signal into a corresponding light signal that can be injected into the fiber .The common light sources for optical fiber system are semiconductor light sources , which are light emitting diode (LED) and laser diode(LD) .

Comparison of the advantages of (LED) and LD is shown in (**Table 1**) (Becker&Piper,1982). Light emitting diodes may be used with either multimode or single mode fibers when lower light levels and the lower information capacity (lower modulation bandwidth) are acceptable .laser diode achieve higher performance at the expense of higher cost and complexity.

2. Light Detectors:-

Semiconductor based photodiodes are used as optical detectors in the optical fiber communication systems. They have small size, high sensitivity and fast response. There are two types of photodiodes which consists:

1. A positive-intrinsic-negative (P-I-N) photodiode consists of p and
n regions separated by a very lightly n doped intrinsic region. Silicon (P-I-N) photodiodes are used at 0.8 μm wavelength and InGaAs (P-I-N)photodiodes are used at 1.3 μm and 1.55 μm wavelengths. In normal operation, the p-i-n photodiode is under high reverse bias voltage. So the intrinsic region of the diode is fully depleted of carriers.
2. Avalanche photodiodes (APDs):
It consists of four regions p^+ -i- p-n^+ in order to
develop a very high electric field in the intrinsic region as well as to impart more energy to photoelectrons to produce new electron-hole pairs by impact ionization.

Types of Encryption

The simplest type is called secret-key or symmetric-key encryption where one key is used for both encryption and decryption. It is very fast but only useful for encrypting data that is not "going" anywhere. A security breach can take place because the sender and receiver of the date have to share the key .The second type of encryption is called public key encryption. This is an asymmetric scheme where there is a pair of keys that are used. There is a public key, which encrypts the data and a corresponding private (or secret) key for the decryption. This is often used in conjunction with a digital signature. The primary benefit is that it allows people to exchange messages securely without a preexisting security arrangement. All communications involve only public keys and the private key is never transmitted or shared. Pretty Good Privacy is a combination of the secret-key and the private key encryption (Robling,1982). It first compresses the data which strengthens the security by reducing the patterns associated with encryption. Then it creates a session key that is a one time only secret key. The key is a random number generated by the keystrokes made and the movements of the mouse. The session key is used like the secret key to encrypt the data so it is very fast. The block diagram of the cryptography is shown in (**Figure 2**).

The Relationship Between Encryption and Message

plaintexts of length a positive multiple of some block length N if a message (M) is encrypted by the function of encryption (E) to yield a cipher text(C) or in the mathematical notation (Schneier,1996)

$E(M) = C$ ……………………………………………………………….(1)

and we can recover (M) by appliance the function of the description (D) on the cipher text :

$D(C)=M$ ……………………………..………………………….(2)

and we can obtained the message (M) by appliance the functions of the encryption and description on the plane text:

$D[E(M)]=M$ ……………………………..……………………(3)

The Link Between Algorithms and Key

The meaning of the algorithm is the mathematical function used for encryption and description. In the cipher system there are two types of the algorithm the first type using the same algorithm , in encryption and description, and the second type the algorithm which it is used in the encryption differs from the algorithm used in the description (Harris).
In the past time these algorithms have low security because that anyone can change the algorithm so to solve this problem they used keys.

$E_k(M)=C$ ……………………………..…………..………(4)

$D_k(C) =M$ ……………………………..…………………......(5)

This key increasing the security of the algorithms then some type of algorithms used the same key in encryption and description and other type using different keys in encryption and description as shown (**Figure 3**):

$E_{k1}(M)=C$ ……………………………………………………….. (6)

$D_{k2}(C) =M$ ……………………………………..…………... (7)

$D_{k2}[E_{k1}(M)]=M$ ……………………………...…………...……..…(8)

Plaintext

The transmitted information between the transmitter and the receiver units represent the plain text or original massage .This information represents the deduced information in a binary system . This work shown in (**Figure 4**).

The Stream Cipher and Blocking Cipher

The stream cipher is one that encrypts a digital data stream one bit or byte at the time (such that vigenere cipher (Piper,1987),(Kitab) ,the block cipher is one in which a block of plane text is treated as a whole and used to produce a cipher text block of equal length .Block cipher can be used to achieve the same effect as a stream cipher. The stream represents the most using in the encryption system because of its important properties like high reliability and ease of use in practical application and high speed of execution.(**Figure 5**) show stream cipher.

The Technique of Stream Cipher

The operation of the stream cipher is that an algorithm is feeding by the key to produce the pseudo random sequence (Piper,1982),(Alhamadni,1997). This sequence is mixed with the plane text (which contains alphabet or data ………etc) to yield the cipher text.In the other way we can get the plane text from mixing the cipher text with the pseudo random sequence to produce the plane text.

There are two types of the stream cipher , the first is periodic (the key stream repeats after character or bit) and the second is non periodic (which is used for one time only such as one -time pad cipher). A key stream generator outputs(2^N-1)where N is the no. of register .A key stream of bits K1, K2 , K3, (Electrical) …..Ki (6) .

This key stream is XORed with a stream of plaintext bits :P1 ,P2, P3…Pi.

To produce the stream of cipher text bits.

$C_i = P_i + K_i$ ……………………………………………………...(9)

At the decryption end ,the cipher text bits are XORed with an identical key stream to recover the plaintext bits .

$P_i = C_i + K_i$ ………………………………………………………(10)

Finally the system security depends only on the insides of the key stream generator (Alhamadni & Shakar,1995)

Types of Stream Ciphper System

There are two basic kinds of stream cipher system:

1-Linear stream cipher system: in this type the algorithm is a shift register with linear feedback function. In this type the algorithm is a shift register with linear feedback function as shown in (**Figure 6**) (Arab).

For this example the no. of register =3 and the initial value =101

and the length of key generator 2^3-1 =7

The key is (1011100). The plaintext is (TAKE ME TO YOUR LEADER)

And we need to convert it to the askycode (binary number). The cipher text is obtained by equation:

$C_i = P_i + K_i$

The cipher text is:

(0001000000111010010111001100100100010011001000100000100110000101001001100010010001
110001000100110010011101001110000110000001110),

and we can obtain the original plain text (TAKE ME TO YOUR LEADER) by equation below:

$P_i = C_i + k_i$

The second example for shift register(linear stream cipher) is shown in (**Figure 7**) .In this type the number of register =5 ,and the length of key (2^5-1=32-1=31)

The initial value =11011 and we take the plaintext (COPY ALL ITEMS),and we need to convert this plaintext into askycode (Binary number) .The key generator is (1101100011111001101001000010101).

and we can get the cipher text by equation below

$C_i = P_i + K_i$

The cipher text is:
(0101110111000111001000011011001110000010110101010000000111111110011101011000101111010).

The original plaintext (COPY ALL ITEMS) can be obtained by the equation

$P_i = C_i + K_i$

2-Non linear stream cipher system: in this type the algorithm is different either one shift register with the combining function which is XORING or more than one shift register with combining function. This type shown in (**Figure 8**).

For this example the no. of register =4 and the length of the key $=2^4-1=15$ .and the initial values =1100 and the plain text (MACDONALD),and we need to convert it to asky code in (Bainary number), The key generated outputs :
(010110010001111).so the cipher text can be obtain from the equation below:

$C_i = P_i + K_i$

The ciphertext is
(110000100000110001010111001110100100101111101101000000001000111110)
And we can get the original plain text (MACDONALD) by the formula below:

$P_i = C_i + K_i$

For another example on the nonlinear feedback we take the (**Figure 9**)
This type consist of two linear shift register ,the first consist of two registers and its initial S1=1,S2=0.the length of key $=2^2-1= 3$ and the second consist of three registers and its initial values S3=1,S4=0,S5=1, and the length of the key
$(2^3-1=7)$ .The over all length of key out puts equal(3*7=21)and is:(001001010000011010011).
So the cipher text can be obtaind by:

$C_i = P_i + K_i$

and cipher text is
(101000000001101001001010100010001010001101110100110010110001100010101100001110000001001011100) .
and we can get the original plain text (BLACK HAWK DOWN) By:

$P_i = C_i + K_i$

Results and Discussion

In this part, we deal with the program and results which is calculated in the previous part and key sequence generation from adder algorithm. And the ciphering of the plaintext and access the plaintext or original message from cipher text by deciphering process is discussed.

1. The Cipher And Deciphering Process

Using XOR Boolean function to make a bit wise operation between the plaintext or original message with a binary sequence generation from adder algorithm to obtain the cipher text, and we can access or recover the plaintext from the cipher text by XORing the cipher text and sequence generation from adder algorithm.

The Askycode of the alphabets shown in the (**Table 2**).

For the (**Figure 6**) (Linear stream cipher) the no. of register =3.

The initial value of the register are: S_1=1, S_2=0, S_3=1.

and length key generation =2^3-1=7 .The key is (1011100)

As shown in the (**Table 3**)

The plain text is (TAKE ME TO YOUR LEADER).and the askycod for the plain text of our example and ciphering is shown in the (**Table 4**).

The cipher texts are:

(0001000001110100101110011001001000100110010001000001001100001010010011000100100 01110001000100110010011101001110000110000001110**).**

And we can obtain the original plain text (TAKE ME TO YOUR LEADER) by XORing the cipher text with the key generation. For the figure (1-7) (linear cipher type) the no. of registers =5. And the initial values in the registers S_1=1, S_2=1, S_3=0, S_4 =1, S_5=1.And the length of the key generation is 2^5-1=31 as shown in the (**Table 5**)

The plain text (TOM CROUSE). And the askycode for this example and ciphering are shown in the(**Table 6**).

The cipher text is: -

(01110001110000111110010000001000111100010000110011001101111101110).

And we can obtain the original plaintext (TOM CROUSE) by XORing the cipher text with the key generation. For the figure (1-8) (NON LINEAR CIPHER TYPE) the no. of registers =4 .The initials values in the registers are S_1=1 ,S_2 =2 ,S_3=0 ,S_4=0 .The length of the key generation=2^4-1=15.As shown in the (**Table 7**).

The plain text (MACDONALD) and the askycode for this example and ciphering are shown in the (**Table 8**)**..**

The cipher text is (110000100001100010101110011101001001011111011010000001000111110).

And We can obtain the original plaintext (MACDONALD) by XORing the cipher text with the key generation.

For the (**Table 9**). This type consists of two linear shift register, the first consist of two registers and its initial S_1=1, S_2=0.the length of key =2^2-1= 3 and the second consist of three registers and its initial values S_3=1, S_4=0,S_5=1, and the length of the key (2^3-1=7).The over all length of key out puts equal (3*7=21) .

The plain text (ALI) and the askycode for this example and ciphering as shown in the (**Table 10**).

The cipher text is :-(101001100011010011010)

and we can obtain the original plaintext (ALI) can be obtained by XORing the cipher

2. Software Implementation:

In this part the program was implemented using C^{++} language and Matlab 7.0. The program represent the message as Askycode of the alphabets and representscipher text (linear feedback shift register)and cipher text.(non linear feedback shift).(**Figure 10**) shows the flowchart of the load specification program.

Conclusions

1. Use ciphering (LFSR) by optical fiber is more accurate and more secure than ciphering by other methods.
2. Transmission of the information using laser is better and faster than other methods (linear stream cipher system).
3. The research was done by C^{++} , Matlab, and flow charts in order to illustrate the method.

References

- Bruce Schneier ,"Applied Cryptography" second edition, John Wiley And Sons,Inc.,1996.
- Dorothy Elizabeth Robling Denning " Cryptography And Data Security " Addison-Wesley Publishing company , 1982.
- Farnell Semiconductors Data Sheet CD-ROM , Sponsored by Harris Semiconductor . WWW .Semi.Com
- Heny Beker and Fred Piper , "Cipher systems " Northwood Publication, 1982.
- Keiser. Gred , " Optical Fiber Communications " , second edition , Mc. Grow Hill ,1984.
- Piper F. C. , "Stream Ciphers" , Cryptography :proceedings of the workshop on Cryptography , Germany , 1982.
- Piper , F.C.," Cipher systems" , Egham , England ,1987.
- Piper , F.C.," Cipher systems",1982.
- Senior John M.," Optical Fiber Communications principles and practice ", second edition, prentice Hall ,1996.
- The web site http: // www.kitab.com
- The web sit http: //www. electricalsclub.com
- The web sit http: // www.Arab-engineering.com
- Van Der Lubbe , "Basic Methods Of Cryptography " , prentice Hall ,1998.
- Waseem Alhamadni "Cipher systems ", Baghdad ,1997.
- Waseem Alhamadni & Wasan Shakar,' stream cipher system'', Baghdad ,1995.
- Warren Hioki ,"Telecommunication ", 3'rd edition , prentice Hall ,1998.
- Yarif. Amon, " Optical Electronics In Modern Communications", fifth edition, Oxford university press, 1997.

Table(1) Comparison of light sources

property	Light emitting diode	Laser diode
Optical power	lower	Higher
Life time	longer	shorter
cost	cheap	Expensive
Line width	Wide	Narrow
Modulation bandwidth	lower	Higher
Distance	short	long

Table(2) The ASCII of the alphabets

Alphabet	**ASCII**	**ASCII in binary**
A	65	1000001
B	66	1000010
C	67	1000011
D	68	1000100
E	69	1000101
F	70	1000110
G	71	1000111
H	72	1001000
I	73	1001001
J	74	1001010
K	75	1001011
L	76	1001100
M	77	111101
N	78	1001110
O	79	1001111
P	80	1010000
Q	81	1010001
R	82	1010010
S	83	1010011
T	84	1010100
U	85	1010101
V	86	1010110
W	87	1010111
X	88	1011000
Y	89	1011001
Z	90	1011010

Table (3) Length key generation

I/P	S_1	S_2	S_3	O/P
Initial	1	0	1	------
1	1	1	0	1
2	1	1	1	0
3	0	1	1	1
4	0	0	1	1
5	1	0	0	1
6	0	1	0	0
7	1	0	1	0

Table (4) ASCII for the plain text

Alphabet	ASCII	ASCII in binary XOR key	Cipher text
T	84	1010100+1011100	0001000
A	65	1000001+1011100	0011101
K	75	1001011+1011100	0010111
E	69	1000101+1011100	0011001
M	77	1001101+1011100	0010001
E	69	1000101+1011100	0011001
T	84	1010100+1011100	0001000
O	79	1001111+1011100	0010011
Y	89	1011001+1011100	0000101
O	79	1001111+1011100	0010011
U	85	1010101+1011100	0001001
R	82	1010010+1011100	0001110
L	76	1001100+1011100	0010001
E	69	1000101+1011100	0011001
A	65	1000001+1011100	0011101
D	68	1000100+1011100	0011100
E	69	1000101+1011100	0011000
R	82	1010010+1011100	0001110

Table (5) length of the key generation

I/P	S_1	S_2	S_3	S_4	S_5	O/P
Initial	1	1	0	1	1	-------
1	0	1	1	0	1	1
2	0	0	1	1	0	1
3	0	0	0	1	1	0
4	1	0	0	0	1	1
5	1	1	0	0	0	1
6	1	1	1	0	0	0
7	1	1	1	1	0	0
8	1	1	1	1	1	0
9	0	1	1	1	1	1
10	0	0	1	1	1	1
11	1	0	0	1	1	1
12	1	1	0	0	1	1
13	0	1	1	0	0	1
14	1	0	1	1	0	0
15	0	1	0	1	1	0
16	0	0	1	0	1	1
17	1	0	0	1	0	1
18	0	1	0	0	1	0
19	0	0	1	0	0	1
20	0	0	0	1	0	0
21	0	0	0	0	1	0
22	1	0	0	0	0	1
23	0	1	0	0	0	0
24	1	0	1	0	0	0
25	0	1	0	1	0	0
26	1	0	1	0	1	0
27	1	1	0	1	0	1
28	1	1	1	0	1	0
29	0	1	1	1	0	1
30	1	0	1	1	1	0
31	1	1	0	1	1	1

Table (6) The ASCII and ciphering.

Alphabet	ASCII	ASCII in binary XOR key	Cipher text
T	84	1010100+1101100	0111000
O	79	1001111+0111110	1110001
M	77	1001101+0110100	1111001
C	67	1000011+1000010	0000001
R	82	1010010+1011101	0001111
O	79	1001111+1000111	0001000
U	85	1010101+1100110	0110011
S	83	1010011+1001000	0011011
E	69	1000101+0101011	1101110

Table(7) Length of the key generation

I/P	S_1	S_2	S_3	S_4	O/P
Initial	1	1	0	0	-------
1	1	1	1	0	0
2	1	1	1	1	1
3	0	1	1	1	0
4	1	0	1	1	1
5	0	1	0	1	1
6	1	0	1	0	0
7	1	1	0	1	0
8	0	1	1	0	1
9	0	0	1	1	0
10	1	0	0	1	0
11	0	1	0	0	0
12	0	0	1	0	1
13	0	0	0	1	1
14	1	0	0	0	1
15	1	1	0	0	1

Table (8) The ASCII and ciphering

Alphabet	ASCII	ASCII in binary XOR key	Cipher text
M	77	1001101+0101100	1100001
A	65	1000001+1000111	0000110
C	67	1000011+1010110	0010101
D	68	1000100+0100011	1100111
O	79	1001111+1101011	0100100
N	78	1001110+0010001	1011111
A	65	1000001+1110101	0110100
L	76	1001100+1001000	0000100
D	68	1000100+1111010	0111110

Table(9) Length of the key generation.

I/P	S_1	S_2	S_3	S_4	S_5	O/P
Initial	1	0	1	0	1	-------
1	1	1	0	1	0	0
2	0	1	0	0	1	0
3	1	0	1	0	0	1
4	1	1	1	1	0	0
5	0	1	1	1	1	0
6	1	0	0	1	1	1
7	1	1	1	0	1	0
8	0	1	0	1	0	1
9	1	0	0	0	1	0
10	1	1	1	0	0	0
11	0	1	1	1	0	0
12	1	0	1	1	1	0
13	1	1	0	1	1	0
14	0	1	1	0	1	1
15	1	0	0	1	0	1
16	1	1	0	0	1	0
17	0	1	1	0	0	1
18	1	0	1	1	0	0
19	1	1	1	1	1	0
20	0	1	0	1	1	1
21	1	0	1	0	1	1

Table (10) The ASCII and ciphering.

Alphabet	ASCII	ASCII in binary XOR key	Cipher text
A	65	1000001+0010010	1010011
L	76	1001100+1000001	0001101
I	73	1001001+1010011	0011010

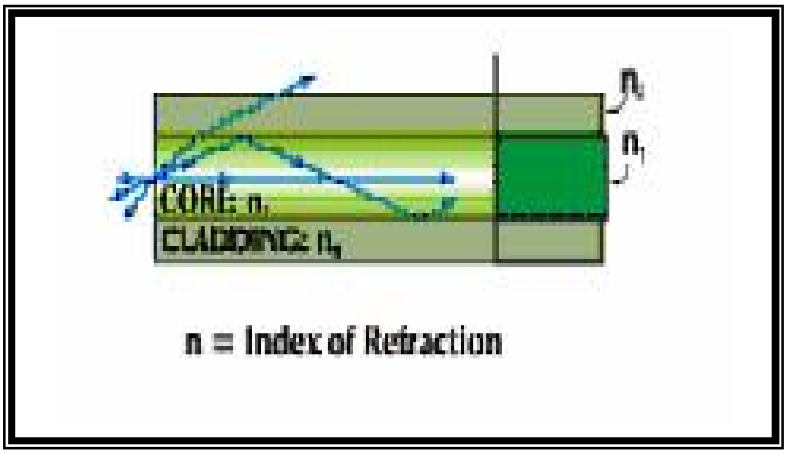

Figure (1) optical fiber scheme (John, 1996)

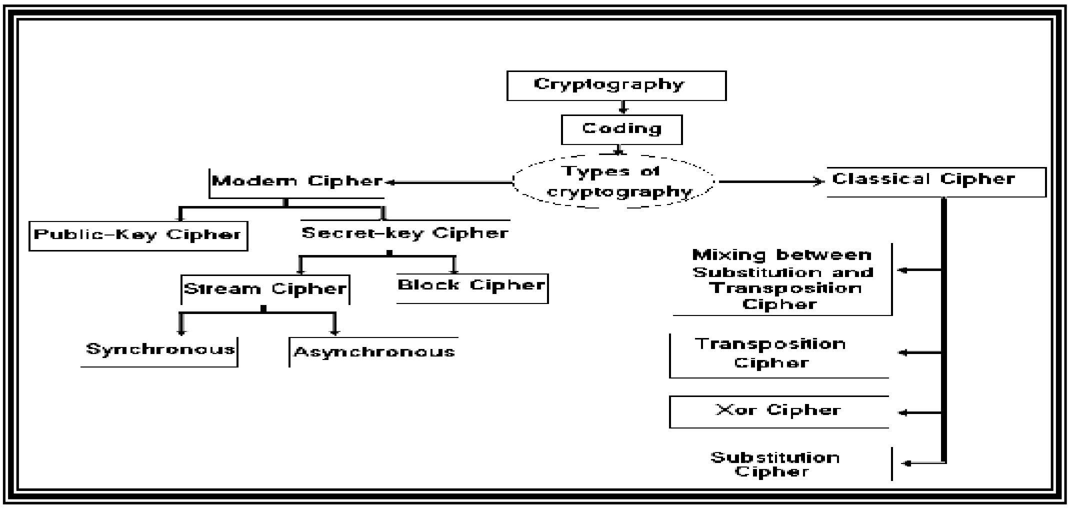

Figure (2) block diagram of the cryptography (Robling, 1982)

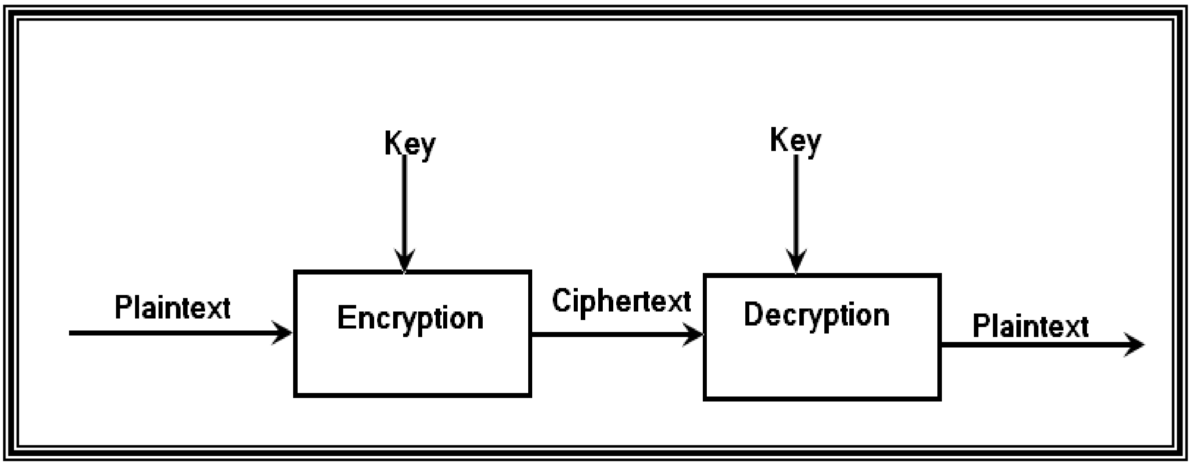

Figure (3) Encryption and decryption with the different key

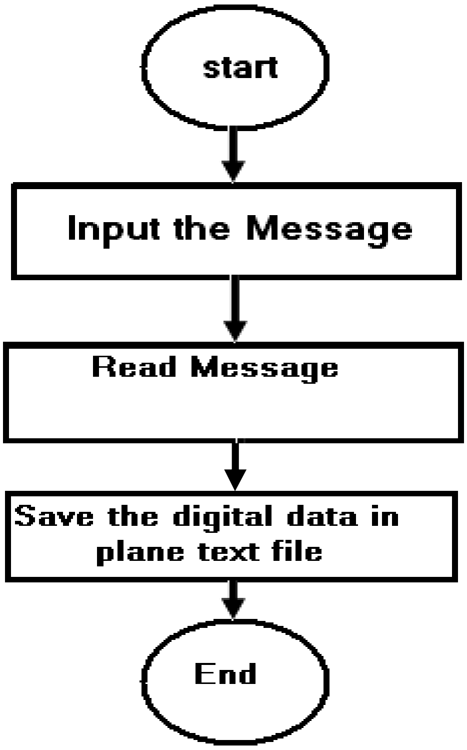

Figure (4) Flowchart for converting the message to the digital data (Harris)

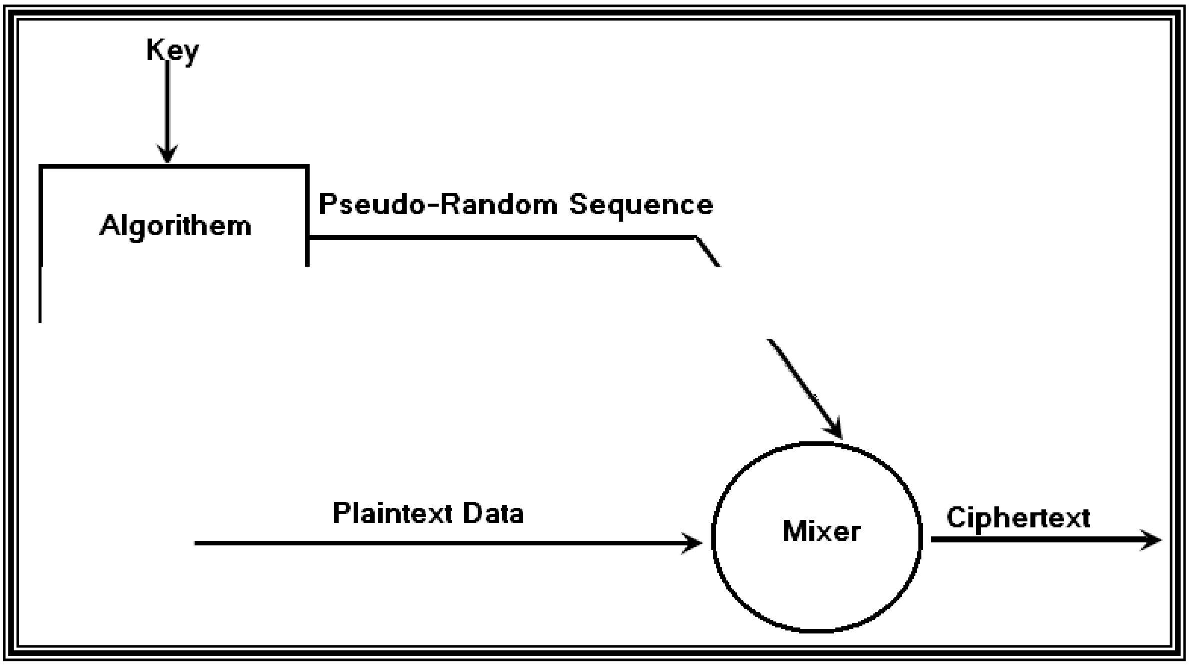

Figure (5) The stream cipher (Kitab)

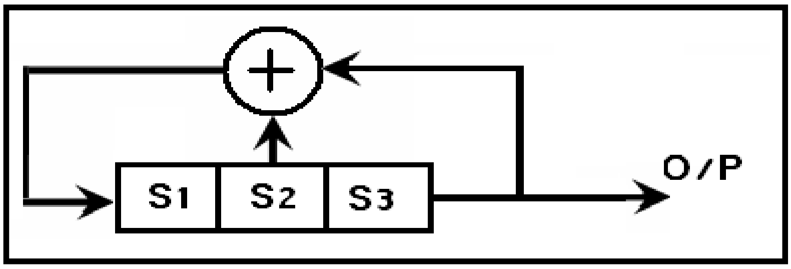

Figure (6) linear feedback shift register with N=3

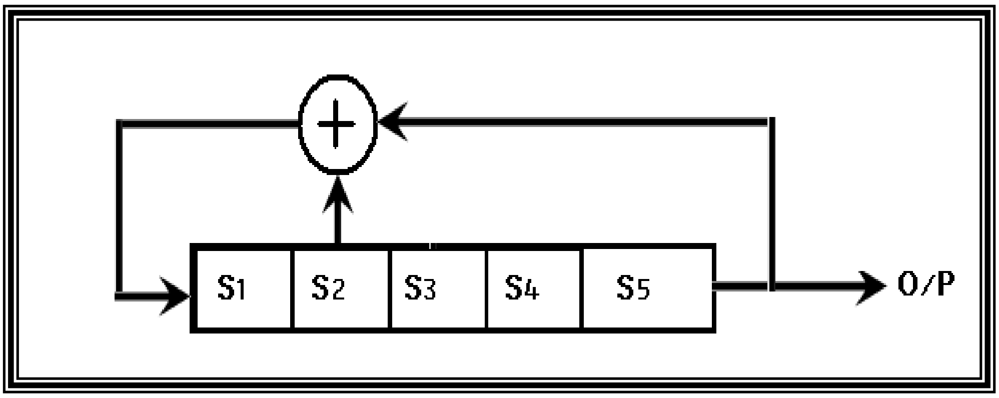

Figure (7) Linear feedback shift register with N=5

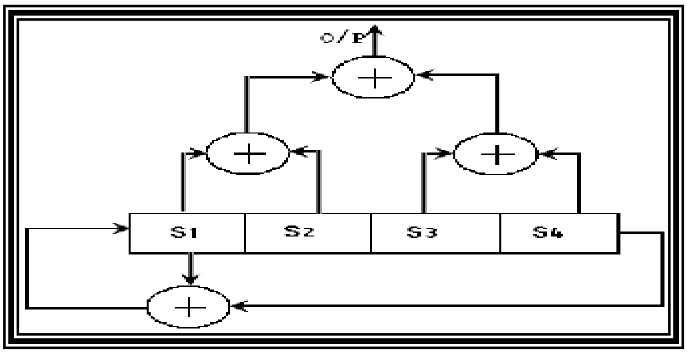

Figure (8) Non linear feedback shift register with N=3

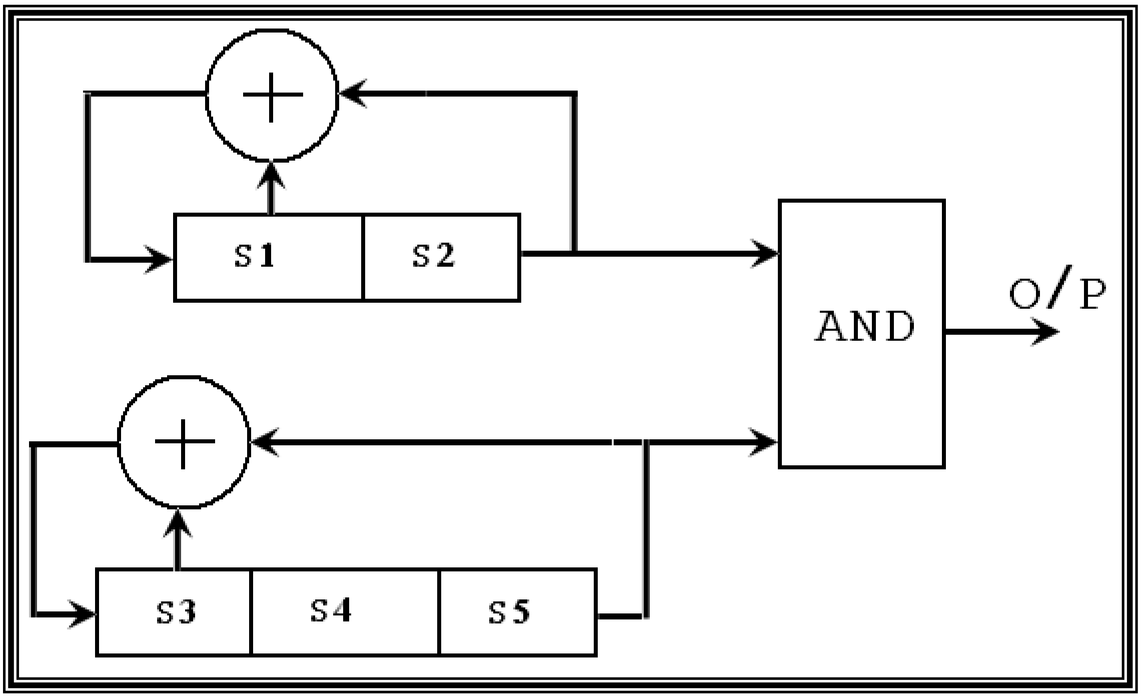

Figure (9) Non linear feedback shift register with N=3

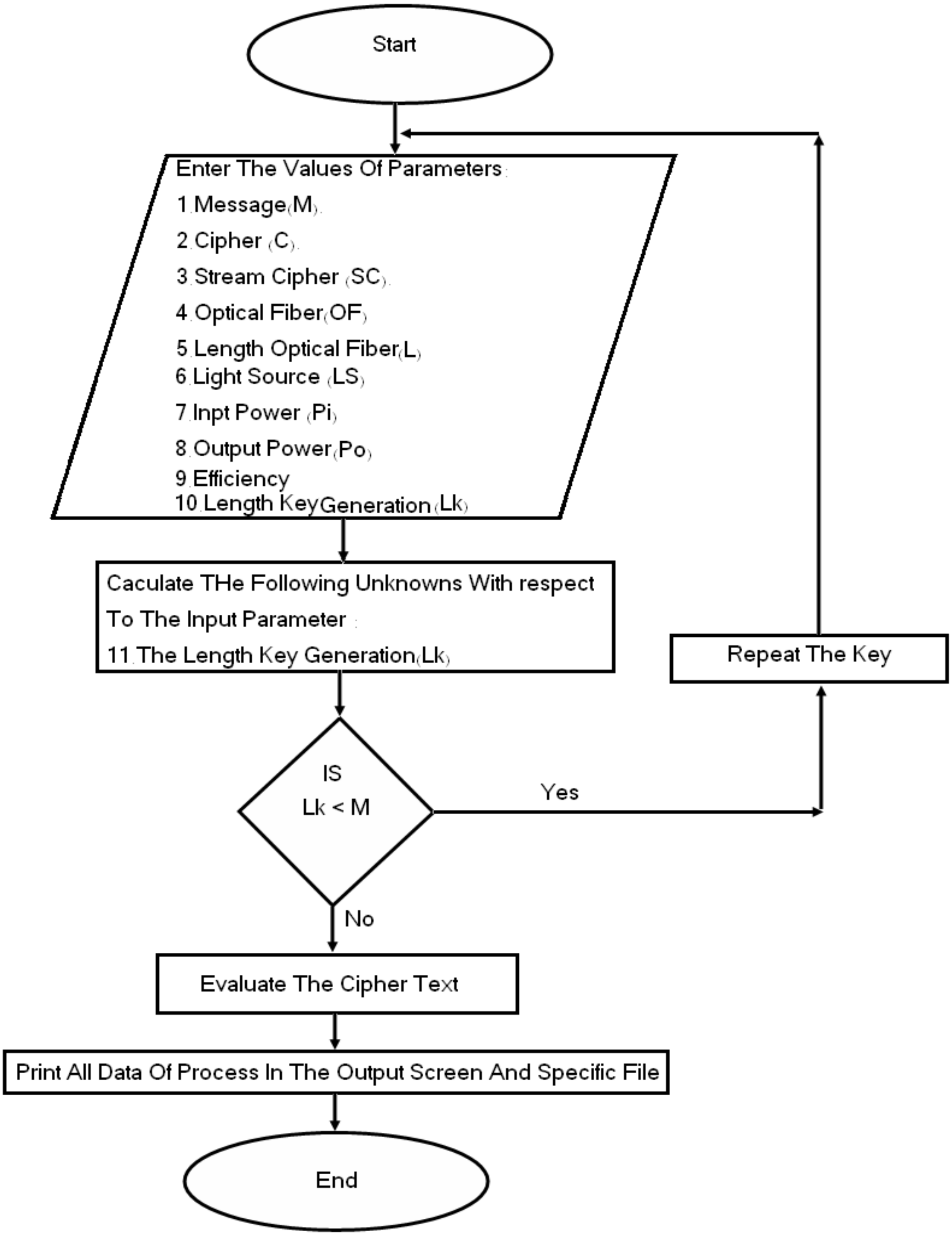
Start
Enter The Values Of Parameters:
1.Message(M).
2.Cipher (C).
3.Stream Cipher (SC).
4.Optical Fiber(OF)
5.Length Optical Fiber(L)
6.Light Source (LS)
7.Inpt Power (Pi)
8.Output Power(Po)
9.Efficiency
10.Length Key Generation (Lk)
Caculate THe Following Unknowns With respect To The Input Parameter :
11.The Length Key Generation(Lk)
IS Lk < M
Yes
Repeat The Key
No
Evaluate The Cipher Text
Print All Data Of Process In The Output Screen And Specific File
End

Figure (10) The flowchart of the load specification program