International Journal of Modern Engineering Research (IJMER)

www.ijmer.com Vol.2, Issue.3, May-June 2012 pp-1354-1359 ISSN: 2249-6645

Encryption and Decryption of Data by Using Geffe Algorithm

Hussein Th. Khamees, Jalal A. Kahlf and Ali A. Al-sajee

University of Al-Nhrain College of Engineering Department of Laser and Optoelectronic Engineering

Abstract

In this modern world of communications, cryptography has an important role in the security of data transmission and is the best method of data protection against passive and active fraud. In this paper, we used the stream cipher which is the best way with the algorithm Geffe generator with a specific length to Encryption the information from plain text in the first compute. This has been sent via the cable which called RS-232 standard interface, which connected between the two computers, and receiving the cipher text in the second computer, and then it will be Decryption by added the same algorithm to the cipher text to return to the plain text.,we satisfy the random statistical tests of the sequence generation from the Geffe algorithm .

1. Introduction

Before the modern era, cryptography was concerned solely with message confidentiality (*i.e.*, encryption)—conversion of messages from a comprehensible form into an incomprehensible one and back again at the other end, rendering it unreadable by interceptors or eavesdroppers without secret knowledge (namely the key needed for decryption of that message)[1].Encryption was used to (attempt to) ensure secrecy in communications, such as those of spies, military leaders, and diplomats. In recent decades, the field has expanded beyond confidentiality concerns to include techniques for message integrity checking, sender/receiver identity authentication, digital signatures, interactive proofs and secure computation, among others ,the earliest forms of secret writing required little more than local pen and paper analogs, as most people could not read. More literacy, or literate opponents, required actual cryptography. The main classical cipher types are transposition ciphers, which rearrange the order of letters in a message (*e.g.*, 'hello world' becomes 'ehlol owrdl' in a trivially simple rearrangement scheme)[2], and substitution ciphers, which systematically replace letters or groups of letters with other letters or groups of letters (e.g., 'fly at once' becomes 'gmz bu podf' by replacing each letter with the one following it in the Latin alphabet). Simple versions of either offered little confidentiality from enterprising opponents, and still do. An early substitution cipher was the Caesar cipher, in which each letter in the plaintext was replaced by a letter some fixed number of positions further down the alphabet [2, 3].

It was named after Julius Caesar who is reported to have used it, with a shift of 3, to communicate with his generals during his military campaigns, just like EXCESS-3 code in Boolean algebra. There is record of several early Hebrew ciphers as well. The earliest known use of cryptography is some carved ciphertext on stone in Egypt (ca 1900 BC), but this may have been done for the amusement of literate observers. The next oldest is bakery recipes from Mesopotamia .A stream cipher may be regarded as one of the many modern cipher system, which uses as one secret key in encryption process.As Now days, It is one of the most encryption system, because of its extremely important properties such as error elimination, high reliability and ease of use in practical application, as well as high speed of execution, it's used in voice encryption as well as in text encryption [4].

Stream cipher operates on stream of plain text and cipher text on one bit or byte as a time

A stream cipher consists of two basic parts:

1- Pseudo random sequence algorithm.
2- Mixer

When we use a binary representation for XOR relation, Figure (1) illustrates the operation of a stream cipher [5].

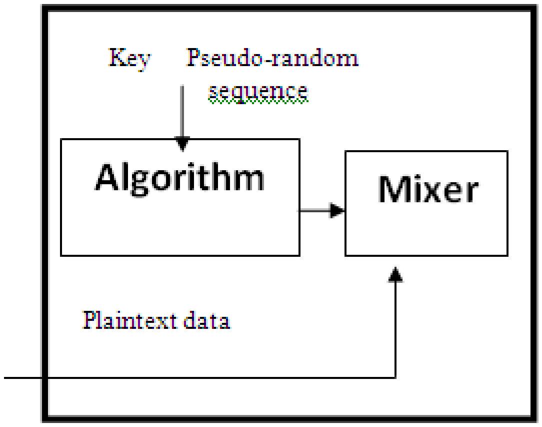


Figure (1): A Stream Cipher.

Many considerations must be taken into account in designing the algorithm in the stream cipher systems are divided into [6]:

1- Speed of key generation.

2- Security degree of the designed system.

3- The time required to decrypt the cipher text.

There are many essential requirements which must be providing by the key stream [7]:

1- Key stream must have a long period.

2- Key stream must have a good statistical property.

3- It must have a large linear complexity.

The security of the stream cipher is depending on the security of key and not on algorithm. So the generation key operation is so important and should be random

2. Statistical test

The statistical Test for Randomness divided as shown below [8]:

2.1frequency test:-

This is applied on sample of (n) bit s of our sequence to ensure that there is roughly the same number of 0s (n0) and 1s (n1) .for this we merely compute**.**

$St=(n0-n1)^2/n$ ....… (1)

To decide if the value (St) obtained is good enough for the sequence to pass, we have merely to compare our value with a table of the x2 distribution, for one degree of freedom. From this table we find that the value of x2 for a 5% significance level is 3.84 the sequence passes. Otherwise we must reject it. (See appendix).

2.2 serial tests:-

The serial test is used to ensure that the transition probability are reasonable; i.e. that the probability of consecutive entries begin equal or different is about the same. Suppose 01 occur n_{01} times, 10 occur n10 times, 00 occur n_{00} times and 11 occur n_{11} times. Thus for this test we compute

$St=4/(n-1)\sum_{i=0}^{1}\sum_{j=0}^{1}(nij)^2-2/n\sum_{i=0}^{1}(ni)^2+1$ ..(2)

This test is successful if St≤5.99 because to two freedom degree, the value of x^2 corresponding to a 5% significant level is 5.99 .

2.3 poker test:-

For any integer (m) there are 2^m different possibilities for a section of length (m) of a binary sequence . In this test we partition our sequence in to blocks of size (m) and then we count the frequency of each type of section of length (m) in our sequence.

If F=n/m, then, we evaluate

$St=2^m/F\sum_{i=0}^{m}\frac{(xi)^2}{i^m}-F$ …………………...... (3)

Where i^m= (m! / (m – i)!)*i!

Where Xi is the number of m-bit blocks having (i) ones and (m-i) zeros. Finally we compare our value with the table for x^2 having 2m -1 degrees of freedom to see if we have a 5% significance level.

2.4runs test:-

For the runs test we divide the sequence in to blocks and gaps. We let r_{01} be the number of gaps of length i and r_{10} be the number of blocks of length i, if r_0 and r1 are the number of gaps and blocks respectively then

$r_0=\sum_{j=0}^{n}r0j$ ……………………………….…(4)

$r_1=\sum_{j=1}^{n}r1j$……………………………………………………………(5)

$n_{01}=r_0-1$ or $r_{0,}$ $n_{10}=r_1-1$ or $r_{1,}$ $n_{00}=n_{0-}r_{0,}$ $n_{11}=n_1-r_1$

The equation is used in this test is:-

$t_0=[\sum_{i=o}^{ro}(roi-\frac{n}{2^{2+i}})^{\wedge}2*2^{2+i}]/n$ …………...(6)

$t_1=[\sum_{i=1}^{r1}(r1i-\frac{n}{2^{2+i}})^{\wedge}2*2^{2+i}]/n$ ……. ..…. (7)

number of freedom degree used with $t_0$and t_1 equal to the value of the length of large gap and length of the large r block respectively .

2.5 auto correlation test:-

Suppose the sequence of (n) bits which we wish to test for randomness properties is a_1, a_2, a_3…... an. Then set:

$A(d)=\sum_{i=1}^{n-d}ai(ai+d),$ 0≤ d ≤ n-1 …….(8)

Clearly A (d) $=\sum_{i=1}^{n}ai=n1$

If the sequence has n_0 zeros and n_1 ones, the expected value of A (d), (d≠0), is

$\mu= n_1^2(n-d)/n^2$ ……(9)

This test is successful if $St \leq 3,841$ to all value of d

Where

$St=(A(d)-\mu)^2/\mu$ ………………………………..…….(10)

3. Experimental work and results

The description of the hardware and software design will be presented in this paper, the system consist of many parts as shown in figure (2).

By using the matlab program the key stream is represented by Geffe algorithm figure (3), to encrypt the plaintext and decrypt the cipher text. The cable RS_232 serial port is connected between two computers ,the sender and receiver programs between two computers are done by visual basic program. Decryption .Geffe algorithm is used linear shift register with different length such as m=5, n=7, and o=11 . and the length of the key is d

Where: $d= (2^5-1)\ (2^7-1)\ (2^{11}-1)$

The 1'st shift register consists of 5 stages with an initial state 10101, the 2'nd consists of 7 stage with an initial state 1010111 and the 3'rd stage of 11 with an initial state 11011101011.

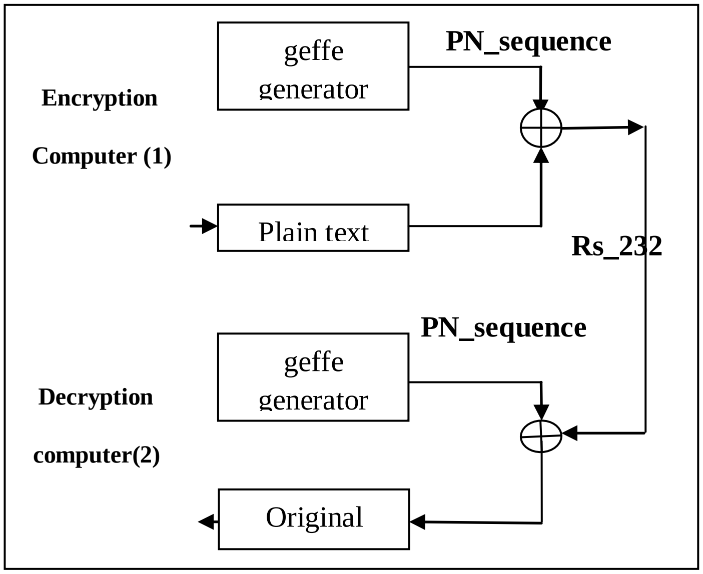


Figure (2): the block diagram of the encryption and decryption.

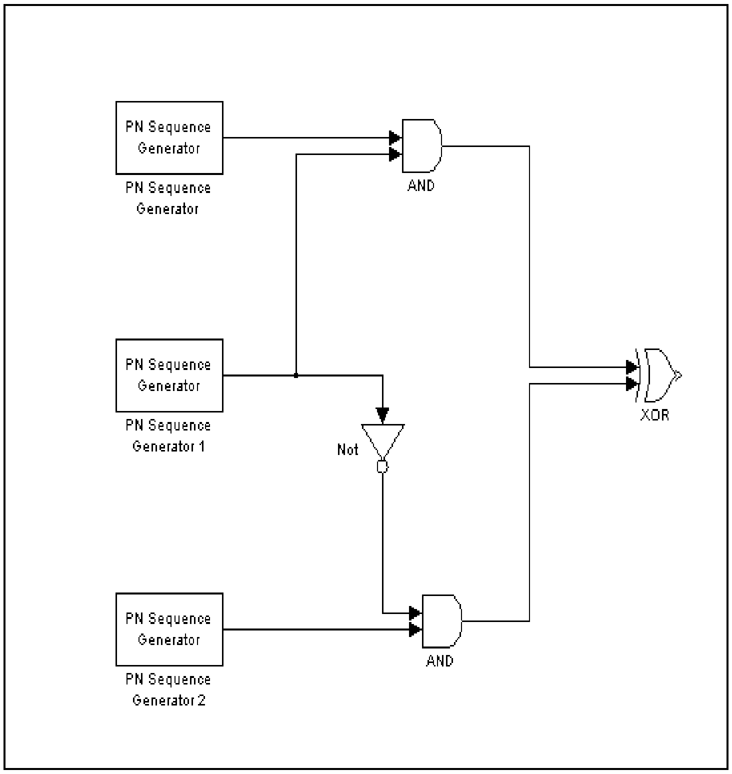


Figure (3): the sequence generation from Geffe algorithm.

It is important to apply statistical test of the generated sequence and to check the key; they also appear to be pseudo random. So that, It was decided whether a sequence has successful or failed in the test. It was took a three different lengths of this sequence which were generated from Geffe algorithm such as (1000, 500 and 300), table (1) shows the results of the statistical testes of the Geffe algorithm.

Table (1): The results of the statistical testes of the Geffe algorithm.

Length of Pseudo	Statistical test	Value of statistical test	Degree of freedom	Value of X^2
1000	Frequency test	0.2560	1	3.841
	Serial test	2.0030	2	5.99
	Poker test	1.0920	7	14.1
	Run test	0.5080	7	14.1
		0.4920	5	11.100
	Autocorrelation test	0.2421	1	3.841
500	Frequency test	0.2000	1	3.841
	Serial test	1.0040	2	5.99
	Poker test	1.7970	7	14.1
	Run test	0.4900	7	14.1
		0.5100	5	11.100
	Autocorrelation test	2.1048	1	3.841
300	Frequency test	0.1200	1	3,841
	Serial test	0.0083	2	5.99
	Poker test	0.6820	7	14.1
	Run test	0.4900	7	14.1
		0.5100	4	9.49
	Autocorrelation test	2.1048	1	3.841

Figure (4) show the block diagram of the encryption and decryption by the simulink_matlab.

The RS232 is the communication line which enables the data transmission by only using three wire links. The three links provides 'transmit', 'receive' and common ground, the 'transmit' and 'receive' line on this connecter send and receive data between the computers. As the name indicates, the data is transmitted serially the next flowchart described the main program of RS_232 transmitter serial port as shown in figure (5).

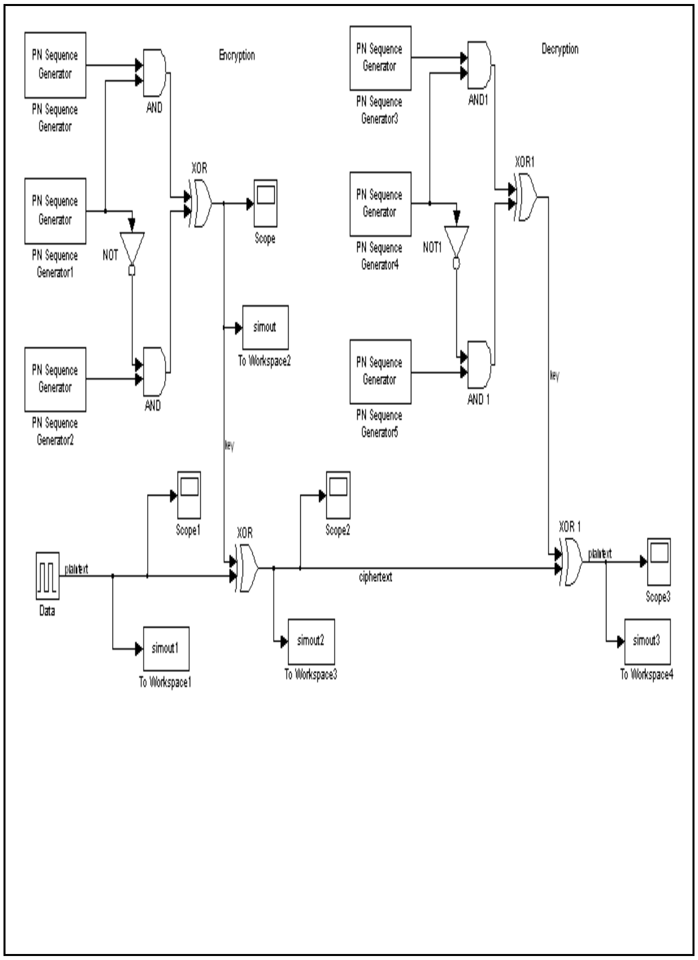


Figure (4): the block diagram of the encryption and decryption by the simulink_matlab.

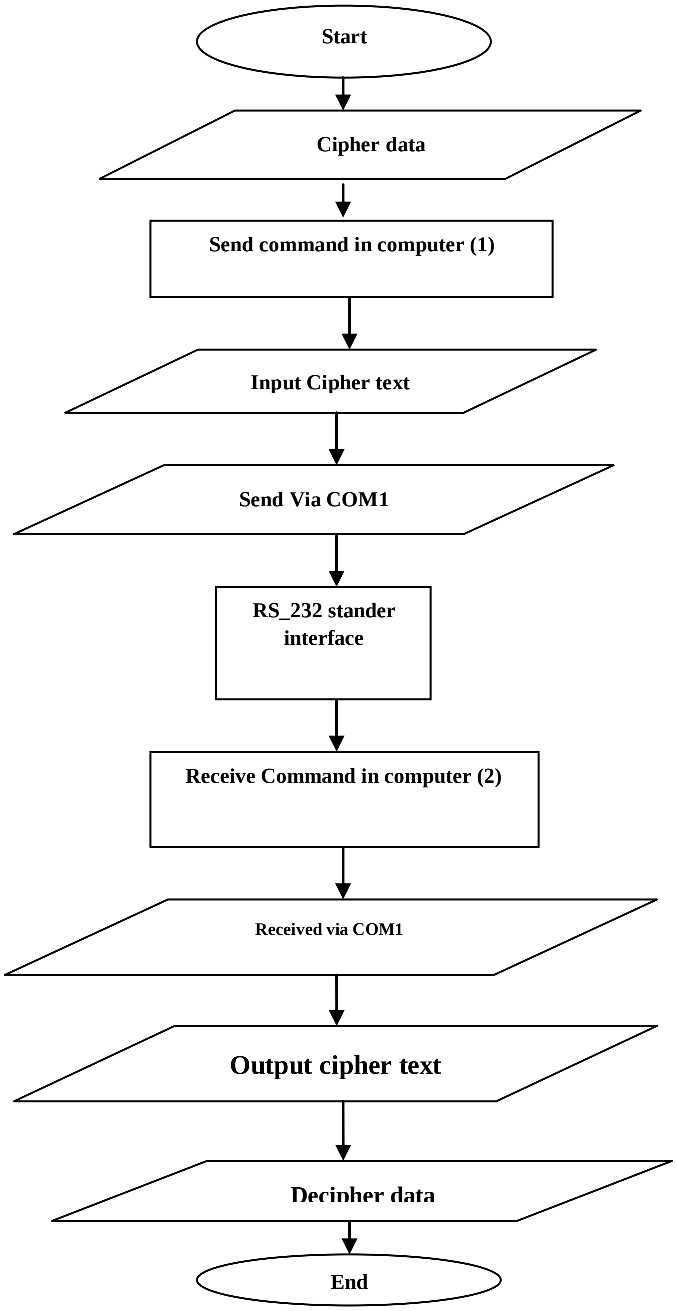


Figure (5): The Flowchart of Main Program of Rs_232 Transmitter link.

The Geffe algorithm was used linear shift register with different length such as m=5, n=7, and o=11.

$d=(2^5-1)(2^7-1)(2^{11}-1)=(31)(127)(1047)=4122039$ bit

The Geffe algorithm will repeat itself after 4122039 bit

The bits are: 1 1 1 1 1 0 0 1 0 1 1 1 0 0 1 0 1 1 0 0 0 1 0 0 0 1 0……….. As shown in figure (6)

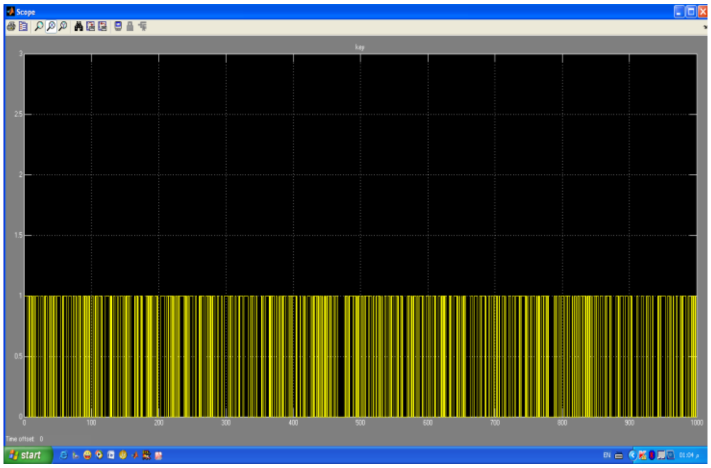


Figure (6): the key generation (Geffe algorithm)

The transmitted data between transmitter and receiver represented the plaintext or original message by a binary system. the input data bits (plaintext) are: 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 0 0 0 0 0 0 0 0 ………… as shown in figure (7)

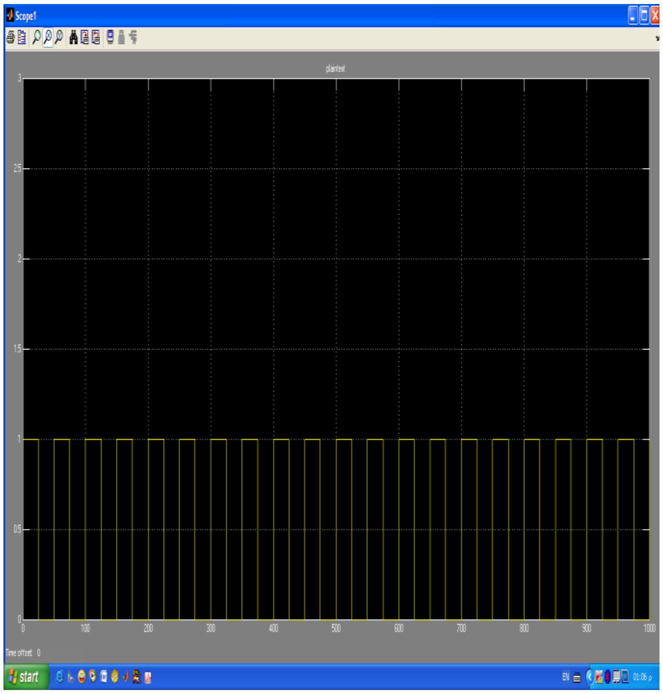
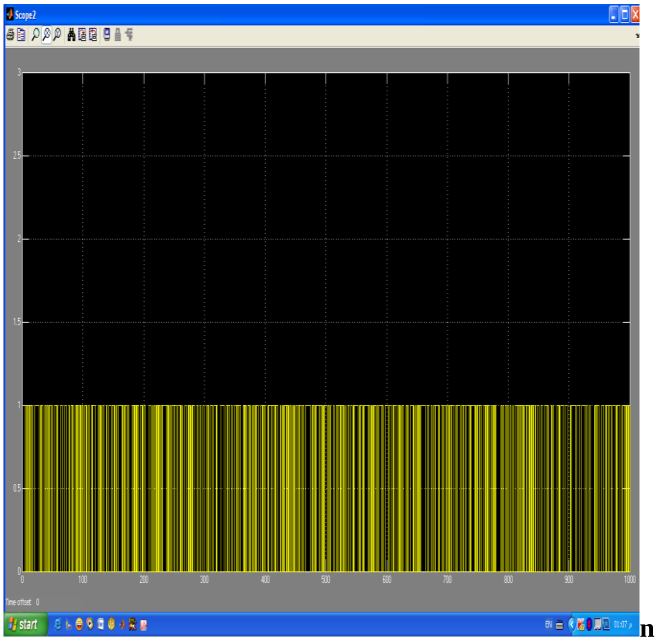


Figure (7): the plaintext (original data).

using XOR boolean function to make a bit wise operation between the plaintext or original data with a binary sequence generation from geffe algorithm to the encryption bits (ciphertext) are: 0 0 0 0 0 1 1 0 1 0 0 1 0 1 0 …………. as shown in figure (8)



n

Figure (8): the encrypted data (after encryption)

The original data will back after the decryption process as shown in figure (9)

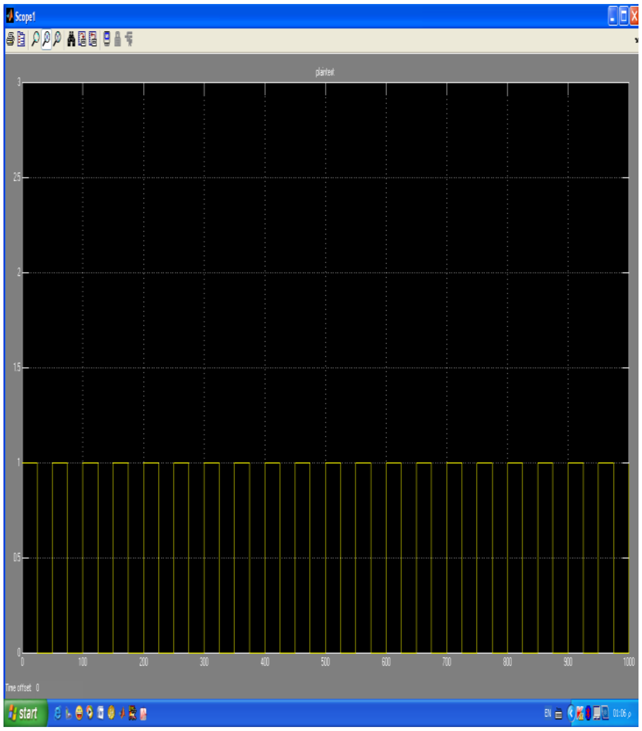


Figure (9): the plaintext (after decryption).

Conclusions

1. The stream ciphering technique is a highly secure and has a high speed to generate the keys.
2. The generator sequence from the nonlinear stream cipher (Geffe algorithm) has a high linear complexity therefore; the nonlinear sequence has a good degree of security.
3. The maximum period length to the generator binary sequence from any generator is much better, which have maximum period length 4122039.

REFRENCES

1- Merriam-Webster's Collegiate Dictionary "Cryptology (Definition)" (11th Editioned.). Merriam-Webster.Retrieved 2008-02-01.

2- Alfred J. Menezes Paul C. Van Oorschot Scott A. Vanstone "Handbook Of Applied Cryptography", 1996.

3- An Introduction To Cryptography Copyright © 1990-1999 Network Associates, Inc. And Its Affiliated Companies. Printed In The United States Of America.

4- Tom Davis" Cryptography" February 7, 2000

5- David R. Kohel ,' Cryptography' July 11, 2008.

6- Rsa Laboratories Technical Report Tr-701 , M.J.B. Robshaw 'Stream Ciphers' Version 2.0|July 25, 1995

7- Tin Lai Win, And Nant Christina Kyaw 'Speech Encryption And Decryption Using Linear Feedback Shift Register (Lfsr) '

8- Tsang-Yean Lee, Huey-Ming Lee, Homer Wu, Jin-Shieh Su 'Data Transmission Encryption and Decryption Algorithm in Network Security Department Of Information Management, September 22-24, 2006