Symmetric Cryptosystem Based on Petri Net

Hussein A. Lafta **Rand Abdul-Wahid M. Ali**
College of Science for Women, University of Babylon College of Information Technology, University of Babylon
wsci.husein.attia@uobabylon.edu.iq albeerrand@yahoo.com

Abstract

In this wok, a novel approach based on ordinary Petri net is used to generate private key . The reachability marking of petri net is used as encryption/decryption key to provide more complex key . The same ordinary Petri Nets models are used for the sender(encryption) and the receiver(decryption).The plaintext has been permutated using look-up table ,and XOR-ed with key to generate cipher text

Keyword: pseudo random number , symmetric cryptosystem ,petri net

الخلاصة

يتضمن هذا البحث طريقة جديدة تعتمد على شبكة بتري لتوليد مفتاح سري خاص .يستخدم مؤشر الوصول الذي يشير الى البيانات الموجودة في الشبكة كمفتاح للتشفير وفك التشفير للحصول على مفتاح معقد بشكل جيد. يستخدم كلا الطرفين (المرسل والمستقبل) للتشفير وفك التشفيرشبكة ذات تصميم مطابق لتوليد نفس المفتاح . يتم اعادة ترتيب النص الصريح باستخدام جدول معين قبل عملية التجميع مع المفتاح لتوليد النص المشفر.

الكلمات المفتاحية: بتري نت ، تشفير تناظري ، توليد رقم شبه عشوائي.

1.Introduction

One of the most used in information security is Cryptography ,one of its services is protected sensitive information to discover by unauthorized people or made modification on it during sending or storage. Cryptography depends upon two basic elements: cryptography algorithm and key generator algorithm . key stream generator has a short input(seed) and a long output, the two party(sender and receiver) have the same input and generate the same key, our project use petri net as generator. Petri net is mathematical graphical model ,consists three component ,places , transitions and arc that connect one place to one transition or one transition to one place, each arc labels with its weight(positive integer), each place may hold either zero or a positive number of tokens or mark. A marking of net is denoted by M, it consists tokens of all places, short key(seed) is used as initial marking to the first places of petri net ,firing of enabled transition chance the token in petri net according to the weights of arc and number of firing which can be change according to the agreement between sender and receiver ,this generated random long number . The plaintext has been permutated using look-up table, each plaintext is permutated in differ form according to the key . And finally the plaintext and key have been mixed to generate ciphertext.

2. Related works

There are few paper that used petri net as a tool to generate public key sequence based on the average of token or complicated of more than one petri net .

1-"A Public-Key Cryptosystem Based On Stochastic Petri Net"(Zuohua Dinga, Hui Zhoua, Hui Shena, Qi-wei Geb)2014. They have developed a public-key cryptosystm based on They have developed a public-key cryptosystm based on scope of initial marking and average number of token in places of stochastic petri net, in decryption process used CPN. The markings in coverability tree are used in key generation, and the plaintext can be encrypted in many steps. This system has higher security than other like RSA.

2-"Construction of Petri nets and Calculation of Elementary T invariants for Multi-stage-Encryptions Public-Key Cryptography: MEPKC"(Ryo Yamaguchi , Qi-Wei Ge and Mitsuru Nakata,Graduate School of Education, Yamaguchi University)

2008. They have proposed a method, by collecting two Petri nets, in order to increase complex of petri nets to be used as a key generator of a public-key cryptography.

3. Symmetric Cryptography

Cryptography is the study of information security and provide possibility of connecting over an insecure channel to protect information during transmission. Information security is become most important in general modern business and technology for privacy of communications and transmission. Good cryptography gets its security by using complex keys . [Shafi ,Mihir 08]

Cryptography can be divided into asymmetric cipher and symmetric cipher ,A symmetric cipher which use public key to encrypt message and secret key to decrypt it , while symmetric cipher use the same secret key to encrypted and decrypted the message [Paar & Pelzl 10]

In symmetric cipher , the sender and receiver shared secret key by secure channel which will be used in the encryption/decryption algorithm .Symmetric cipher consists three algorithm the randomized key generation algorithm, encryption algorithm and decryption algorithm .The randomized key generation algorithm are used to generated random number, it considers as basic role in the use of cryptography in various security application, the security of algorithms which use it are based on the assumption that it is infeasible to distinguish when a random sequence is being used . A generator began with short random bit string (as a seed) and extend it to become long complex bit string, it should be as long as plaintext to maintain high security . Random number generator are deterministic functions, so it based on the seed, sender and receiver have been agreed on the same seed which must be randomly and shared it over secure channel to get same secret key, which will be xor-ed with the plaintext. [Andrea 2005]

4.Petri Nets

Petri nets are graphical and mathematical tool, it has been used in many applications including the modeling and analysis of discrete-event systems ,concurrent systems , fault tolerant systems , communication protocols, distributed-software systems , control systems and parallel systems . [Jiacun]

A Petri net is a weighted directed graphs, it consists two types of nodes, the place(represented by circle) and transition(represented by bar), place and transition connected by directed arcs either from place to transition or transition to place ,each arc are labeled with weight. [Bab 01]

A marking of net is labeled by M, (m vector where m is the total number of places), the pth component of M denoted by M(p),is the number of tokens in place p. Transition *t* is enabled when each input place is marked with at least w tokens, where w is the weight of the input arc of that transition).

A firing on an enabled transition deletes token from each input place p, and adds token to each output place according to the weight of associative arc, see fig (1). Token-flow occurs via the firing of transitions. The system achieves a new marking via the firing of a transition. [Mutata 89]

A formal definition of Petri net, is represented by five-element PN = (P,T, F,W,M0) where:

P={p1,p2,p3,….,pn} is a finite set of places,
T={t1,t2,t3,…..,tn} is a finite set of transitions,
F≤ (P*T) (T*P) is a set of arcs (flow relation),
W: F-->{1,2,3,….} is a weight function,
M0:{0,1,2,3,…} is the initial marking
A Petri net structure N= (P,T,F,W)without initial marking is denoted by N. A Petri net with the given initial marking is denoted by (N,M0) [Mutata 89]

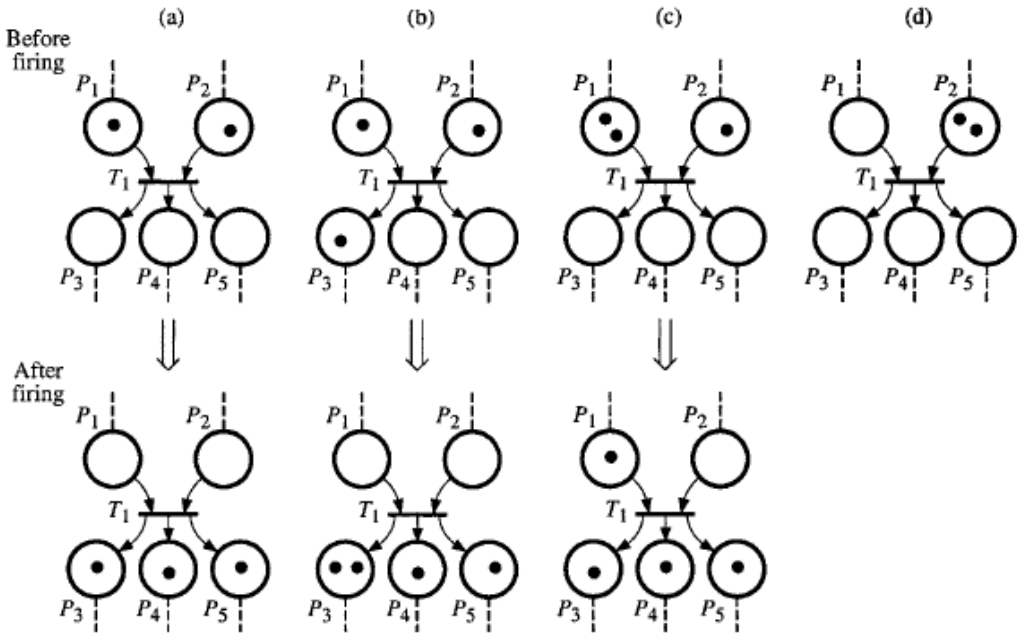


Figure (1) :Firing of transition

5. Design and Implementation of the Proposed System

The Petri net was used as good tools in cryptography. We have developed cryptosystem based on petri net . We can used it to generate nonlinear random number based on the marking of petri net and flow of token according to firing of transitions. this system can supply us with complex key to be used as private key for cryptosystem . the figure (2) depict the suggested petri net model that used in our research. The algorithm

(5.1) is used to generated pseudo random key sequences. The key sequences are used in encryption algorithm (5.2) to generate cipher text and decryption algorithm (5.3) to return the original message.

5.1 algorithm to generate random number .

Input : short secret key(seed) .

Output : long complex key .

Processing includes the following steps:

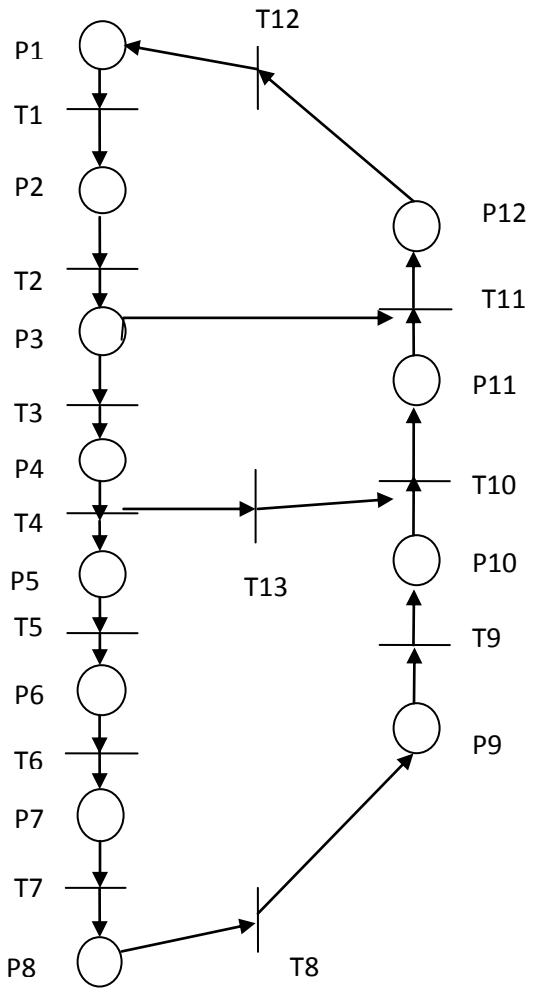
1- Obtain ASCII code of the seed then convert it to binary code and divided into sequence of five bit ,we get sequences S={S0,S1,S2,S3,S4,S5…..}

2-Initialize marking of petri net with S, set P1 with S1,P2 with S2,….,p7 with S7, while p8-p11 set to zero.

3-Set the weight of arc according to table(1),

4- Firing the enabled transitions of petri net n time.

5-Take the marking of petri net as private key



Figure(2): Suggested PN_model for generating a random number

Table(1):Suggested weight of Petri net

1st node	2nd node	Weight	1st node	2nd node	weight	1st node	2nd node	Weight
P1	T1	2	T5	P6	3	P10	T10	4
T1	P2	3	P6	T6	1	T10	P11	1
P2	T2	2	T6	P7	1	P11	T11	1
T2	P3	1	P7	T7	2	T11	P12	1
P3	T3	3	T7	P8	4	P12	T12	3
T3	P4	4	P8	T8	2	T12	P1	1
P4	T4	3	T8	P9	4	T3	P11	2
T4	P5	2	P9	T9	2	P5	T13	1
P5	T5	4	T9	P10	1	T13	P10	1

5.2 Algorithm for encryption

Input : plaintext message
Output: cipher text message
Processing including the following:
1-Obtain ASCII code of the plaintext then convert it to binary code
2-Divided the binary code into 16-bit sequence and permutated the binary code according to table(2),which indexed by S0 .
3- XORed the result with the private key .

5.3 Algorithm for decryption

Input : ciphertext message
Output: plain text message
Processing including the following:
1-Obtain ASCII code of the cipher then convert it to binary code
2- XORed the result with the private key .
3-Applied inverse permutation to binary code according to table(3) which index by S0 to return to original order

Table (2) permutation of plain

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	3	13	7	4	9	8	0	12	1	2	14	15	5	10	11	6
1	10	5	13	1	7	3	0	6	12	14	2	8	9	4	15	11
2	11	6	14	2	8	4	1	7	13	15	3	9	10	5	0	12
3	12	7	15	3	9	5	2	8	14	0	4	10	11	6	1	13
31	8	3	11	15	5	1	14	4	10	12	0	6	7	2	13	9

Table (3) revers permutation of cipher

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	6	8	9	0	3	12	15	2	5	4	13	14	7	1	10	11
1	6	3	10	5	13	1	7	4	11	12	0	15	8	2	9	14
2	14	6	3	10	5	13	1	7	4	11	12	0	15	8	2	9
3	9	14	6	3	10	5	13	1	7	4	11	12	0	15	8	2
31	10	5	13	1	7	4	11	12	0	15	8	2	9	14	6	3

Case study

The word (absyter) used as secret key ,and (my name is ahmed)used as plaintext.
First ,applied random number algorithm according to secret key (absyter) to generate the complex key, use n=32 we get the following key
(00001110110011000100111010111011100101111111101010000101111010100001011
01100110011111011010100100100101010111001101101111011110100110110100101 1
01010010011111010101100010101101011101011011001000101101000100000111110 0
11001110110110001011110101011000111100010100110101000110111011001000100
11001101011010010011101111111100010101110101011101110010110001110111001 1
01110011001110101111100001111010010010101110110111101010001011011100101 0
00001110010011111010011101110000111101110100100010101000111011111111110
01110101000001011010010011001010100000101111011100010001101100010011001 0
01001100001111111010111100101001101010010011000111010001011111110011010 0
10111100100110010010101111110100000111010011111111010010011001001100000 0
10000111011001111000001001100100011101110111000101001010010101000101001 0
01100101011010101000111001001110010010010011001001001110110100100111001 1
10100110100100110001110110001100010110100101110100010011001001010101011 0
10000010101001101010100100110010011011001111010110011111011001001100 0
11101001111111101010011010111010010011001010100001011101001010010110000 1
00110010010011000101101111100111001100101001001100011101110111001110100 1
11110100100110010010101011101011110101001111011010010011001001110001010 1
10110100111100010011001000111010011101100101001110111010100100110010101 1
01010100001010010011110010011001001001111010010111010010111110100100110 0
01110100110000110100111110000001001100100101011011101101001111100000010 0
1100100101011011101)

Obtain binary code of plaintext and applied permutation we get
(10111111000111101110000110011000100011010110110100000010011110110111101 0010001000100110011000111101101010011100 0)
Xor_ed the private key with the plaintext we get (
10110001110100101010111100100011000110101001011110000111100100010110110 0 1000100010110111100101010111111111110000001)

And the cipher text is (XtUr j/ H[<W□). in other side ,the same petri net will be used to generate the same key , XOR-ed with cipher text and applied inverse permutated to get plaintext.

6. Conclusions and future works

In this work, a novel approach based on Petri net is used to encrypted messages. This a new approach is used to generated the private key. The proposed system consists two part, the first one is used to generate a random number based on the token of places, which generate complex long nonlinear random number used to encrypted message, the second part is used to permutated the plaintext and XORed the result with private key.
There are some future works like private key cryptosystem based on coloured petri net, public key cryptosystem based on petri net, using coloured petri net for secure

transmission of message between sender and receiver and using petri net in parallel processing.

7. References

Andrea 2005, Andrea Rö ck, " Pseudorandom Number Generators for Cryptographic Applications", 2005

Bab 01, Bablo G. ,2001, Introduction to stochastic Petri net,(Eds.): FMP2000, LNCS2090 ,pp. 84-115 .Springer –Verlag Berlin Heidelberg.

Jiacun, Jiacun Wang," Petri Nets for Dynamic Event-Driven System Modeling ",Department of Software Engineering Monmouth University

Mutata 89, TADAO MURATA "petri nets properties, analysis and application",IEEE, 1989

Paar, C. ; J. Pelzl 10]C. Paar, J. Pelzl,"understanding cryptography", _c Springer-Verlag Berlin Heidelberg 2010

Shafi ,Mihir 08, Shafi Goldwasser1, Mihir Bellare2, "lecture note on cryptography", July 2008, (1)MIT Computer Science and Arti¯cial Intelligence Laboratory, (2)The Stata Center, Department of Computer Science and Engineering, , University of California at San Diego

Zhijie, Ruby 00 , Zhijie Shi, Ruby B. Lee, "Bit Permutation Instructions for Accelerating Software Cryptography ",Department of Electrical Engineering, Princeton University,2000