ISSN: 2348 9510
International Journal Of Core Engineering & Management (IJCEM)
Volume 2, Issue 8, November 2015

SIMULATION OF MULTISTAGE KNAPSACK PUBLIC KEY CRYPTOSYSTEM

Assist. Prof. Dr. Eng. Saad M. Khalifa
Al-turath university collage
Iraq-Baghdad

M.sc Eng Angham Khalid Hussain
Al-turath university collage
Iraq-Baghdad

ABSTRACT

This system is a multistage knapsack cryptosystem this paper include the simulation of the system by mathlab , for both ciphering and deciphering procedure .The ciphering procedure contain ciphering message by 1st , 2nd ,and 3rd stages the deciphering procedure is reversed from 3rd , 2nd , and 1st to obtain the original message.

Keywords: knapsack, multistage, public-key.

I. INTRODUCTION

Cryptograph is the use of transformation of data intended to make the data useless to an opponents. Such transformation provides solution to the major problem of data security which is the privacy problem: preventing an opponent from extracting information from communication channel. The main problem in using conventional cryptography is the distribution of keys particularly for commercial applications.

A second difficulty which has limited the application of conventional cryptography is inability to deal with the problem of "dispute" [1] which is deal with setting dispute between the sender and receiver as to what message if any , was sent . The public cryptography offers good solution for the dispute problem. This solution is called the digital signatures.

In a public – key cryptosystem each receiver generates two distinct keys ,an enciphering key E which serves to implement the system enciphering algorithm ,and a deciphering D which which serves to implement the system s' deciphering algorithm [2] . The keys are related in the sense that they serves to

ISSN: 2348 9510
International Journal Of Core Engineering & Management (IJCEM)
Volume 2, Issue 8, November 2015

implement inverse operations on a plaintext message, first with transformation specified by E and then with the transformation specified by D reproduce the message. The trick is that it is computationally infeasible to derive D from E , the calculation would required a vast amount of computing time [3].

Therefore anyone who wants to transmit information to a particular person simply enciphers the information with that persons listed key E and sends the ciphertext over an insecure channel .Only the intended receiver knows his own corresponding secret key D will be also to decipher the transit message .

In this paper a public-key cryptosystem simulation is introduced .this system is formed by cascading multi-stage of the well known scheme of trapdoor knapsack cryptosystem. This system offers a grater security than a single trapdoor knapsack cryptosystem of the same length by matlab.

II. KNAPSACK PUBLTC-KEY CRYPTOSYSTBM

This system is based on the knapsack problem. Given a knapsack of length C and a set of n-roods all of the same diameter as the knapsack but of lengths a_1, a_2 , a_3, …..,a_n find a subset of rods that completely fills the knapsack. In general the only known solution is the enumeration technique.

The knapsack system operates as follows:

1. The user generates an n - integer a_1', a_2',….,a_n' (easy solved knapsack problem) with the property that each element is greater than the sum of the preceding elements. These integers with the deciphering key D are kept secret . Also he generates tow large number m and w, such that w is invertible modulo m (i.e. god (m , w)=1)), and $m > \sum a_i'$. These two integers also kept secret by the receiver.

2. Then he computes the integers a_1 , a_2 ,....., a_n (the hard solved knapsack problem) via the relation:

$a_i = a_i' * w \bmod m$

These integers are transmitted to the sender or stored in a public file. These integers is the enciphering key E which is public [3].

3. The sender converts the message into its binary representation , and divides this binary representation into blocks each of length n–bits. The encryption of the message is accomplished by encrypting each block.

Let X_1 ,X_2 , ….. , X_n be one of these blocks, the encryption of this block is accomplished as follows:

$C=a_1 X_1 + a_2 X_2 + ...+ a_n X_n$

Which is the information transmitted via insecure channel to the receiver.

ISSN: 2348 9510
International Journal Of Core Engineering & Management (IJCEM)
Volume 2, Issue 8, November 2015

4. The receiver computes first w^{-1} via the relation:

$w\, w^{-1} = 1 \bmod m$

Then $Ć = C * w^{-1} \bmod m$

Then the receiver begins to recover the X_i s' by comparing Ć with a_n . If $Ć > a_n'$ then he set X_n equal to 1, otherwise $X_n$equal to zero . If $X_n = 1$ then he subtracts a_a from Ć a new value is found , then comparing this value with $a_{a}'_{-1}$, if the new value of Ć is greater than a'_{n-1} then X_{n-1} is set equal to 1 , otherwise X_{n-1} is set to zero . This process is repeated until the X_i s' is computed . the knapsack problem a_1 ,a_2 , ...a_n with constant C is called the trap door knapsack problem it is hard solve, however it has the same solution as the easy solve knapsack problem $á_1$, $á_2$, ...$á_n$ with constant Ć [4].

III. MULTISTAGE KNAPSACK PUBLIC-KEY CRYPTOSYSTEM

Since no techniques exist to prove that an encryption scheme is secure, the only test available is to see whether the enemy can think of a way to break it [2]. The only solution available is the enumeration method search over all 2^N possible vector of x . since each possibility requires N-number of multiplication therefore the total number arithmetic multiplication required to break the trapdoor knapsack cryptosystem is :

$$Z = N \cdot 2^N \qquad (1)$$

It is quite clear that the security of the trapdoor knapsack cryptosystem is increased by using a long knapsack vector . However, it is possible to increase the security of the well known trapdoor knapsack cryptosystem by using the suggested multi – stage trapdoor knapsack cryptosystem . In the first stage, the message is enciphered by a knapsack vector of length N_1. The ciphartext at the output of the first stage is considered as a message for the second stage which is again enciphered by the knapsack vector of the second stage (length N_2) . By proceeding in this manner the transmitted message at the output of the k-th stagein Fig.(1) can be obtained . In the receiver, the enciphered transmitted information is decrypted [6] . The order of deception stages is opposite to the encryption order.

The security of the multi – stage cryptosystem is evaluated is evaluated by number of arithmetic operations required to break it . Since each stage in the knapsack cryptosystem, the knapsack

ISSN: 2348 9510
International Journal Of Core Engineering & Management (IJCEM)
Volume 2, Issue 8, November 2015

vector has 2^{Ni} (where i=1,2, …….k) possibility , then the enemy who knows the final transmitted output of the k – cascaded stage ,is faced with the following number of possibility

$$2^{N1} .2^{N2}. 2^{N3} ……..2^{Nk}$$

The required number of arithmetic multiplication for breaking the multi – stage system , (assuming worst case that the enemy knows the number of stages and the length of each stage) is

$$Z_{multi} = N_1 . N_2.N_3 ……..N_k . 2^{N1} , 2^{N2} .2^{N3} ..2^{Nk}$$

Or

$$Z_{multi} = N_1 . N_2 N_3 . ..... N_k . 2 \times 2^{N1 + N2 + N3 ..... Nk}$$

To evaluate the security of this system , it is necessary to compare it with the security of the well known single stage trapdoor knapsack cryptosystem . This comparison is made under the condition that the length of the single stage is equal to the overall length of the k– stage .

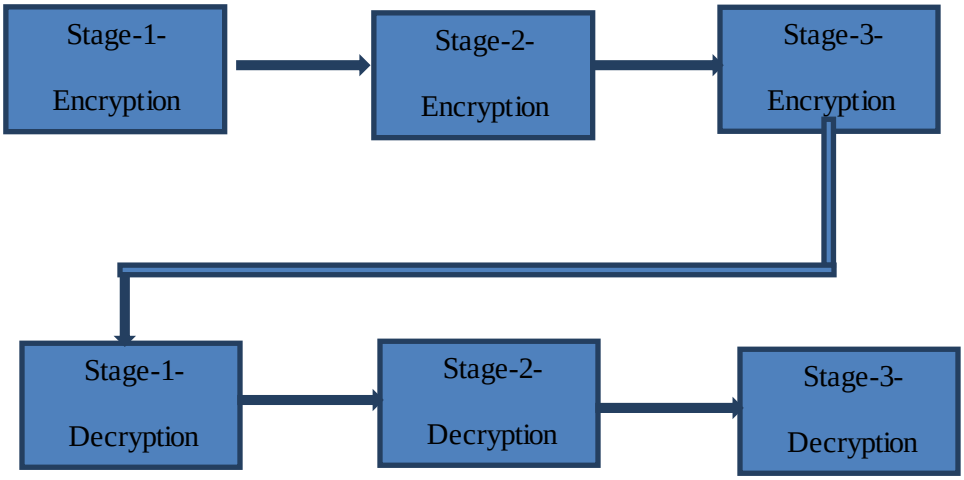
$$r = \frac{1}{K} N_o^{k-1}$$

r is a parameter presenting how many time the security increased

Where N_o is the length of one stage (N_o - N/k) (7)

Table (1) evaluates the security of single stage and K-stage trapdoor knapsack cryptosystem of the same length ($N = KN_o$) .For example if N= 200 and k= 1 (it is the case of single stage N_o = N/k =200) , then the enemy cryptoanalyst need 3.213×10^{62} multiplications to find the vector X(the message) [8], while in the multi – stage system consisting of 10 stages (k=10) each of them has a knapsack of length 20 (N_o =20 , and the overall length = 20x 10= 200 , then the enemy cryptanalyst requires 1.645×10^{73} multiplications to break the system . It is quite clear that the security increased 5.12×10^{10}times.The block diagram of the knapsack public key shown in Fig. (1).

ISSN: 2348 9510
International Journal Of Core Engineering & Management (IJCEM)
Volume 2, Issue 8, November 2015



Fig(1) encryption and decryption stages

ISSN: 2348 9510
International Journal Of Core Engineering & Management (IJCEM)
Volume 2, Issue 8, November 2015

N	K stage cryptosystem			
	K Number Of stages	N_o Length of Each stage	Number of Multiplication Z^{multi}	Improvement Security r
100	1 4 10	100 25 10	1.267×10^{32} 4.951×10^{35} 1.267×10^{40}	1 3906 10^8
200	1 4 10	200 50 20	3.213×10^{62} 1.004×10^{67} 1.645×10^{73}	1 31250 5.12×10^{10}
300	1 4 10	300 75 30	6.111×10^{92} 6.445×10^{97} 1.202×10^{105}	1 1.054×10^5 1.968×10^{13}

Table (1)

ISSN: 2348 9510
International Journal Of Core Engineering & Management (IJCEM)
Volume 2, Issue 8, November 2015

IV. RESULTS

The following table contains the encryption and decryption results of a specific message in each stage where m is the input message and the upper part is for encryption and lower part for decryption.

Table (2)

Encryption									
m	H	E	L	L	O	J	O	H	N
Stage1	132	172	162	162	282	172	282	132	202
Stage2	1927	3055	369	369	3182	3055	3182	1927	1215
Stage3	62843	108682	52274	52274	83341	108682	83341	62843	119998
Decryption									
Stage1	1927	3055	369	369	3182	3055	3182	1927	1215
Stage2	132	172	162	162	282	172	282	132	202
Stage3	72	69	76	76	128	74	76	72	78

The time required for encryption and decryption are shown in following table (Table (3))

Stage	Required time
stage 1	2 sec
stage1 & stage 2	4 sec
stage1 & stage 2 & stage 3	6 sec

Table (3)

CONCLUSIONS

A new cryptosystem is having a higher security and higher speed .while have the following disadvantages:

1-the time required to encryption is increased as the number of stages increased because the operations in each stage increased as the number of stages increased.

2-Big memory size is required.

ISSN: 2348 9510
International Journal Of Core Engineering & Management (IJCEM)
Volume 2, Issue 8, November 2015

3-Encryption and decryption time increased.

REFERNCES

- M.E. "The Mathematic of public- key cryptography", scientific American,vol.241, P.P.130-139,Aug. 1979.
- R.L.Rivest,A.Shamir&L.Ad leman, "A method for obtaining digital signature and public-key cryptosystem", comm. Acm,vol21,no.2,pp.120-126,feb. 1978.
- W.Diffi and M.E.Hellman,"Privacy and Authentication: An Introduction to Cryptography", Proceedings of IEEE,Vol .67,No.3,P.P. 397-427,March 1979.
- S.M.Kalifa and S.N.Saloum, "Implementation of Knapsack Public-Key Cryptosysem",Proceeding of First Scientific Conference on Radar System and Signal Processing,RSSP.87 Baghdad-Iraq 1987.
- B.Arazi,"ATrapdoor Multiple Mapping ",IEEEirans.of Information Theory,Vol.11,No.1, Jan.1980.
- R.M.Goodman& A.J.Mcauly,"ANew Trapdoor Knapsack Public –Key Cryptosystem, In Advance Cryptology, Proc. 48 New York, Springer-Verlag,1985.
- B.Warg,"Knapsack-Type Public Key with High Density", Journal at Electric and Information Technology 2006,P.P 2390-2393.
- Hussien A. Hussien, Jaafer Wade and Saad M. Khalifa , New Multistage Knapsack Public Key Cryptosystem, International Journal of System and Science, Vol. 22, Nov.,1991.