*Journal of Engineering and Development, Vol. 9, No. 4, December (2005)* **ISSN 1813-7822**

# *Aircraft Identification Scheme using Public-Key Cryptosystem*

***Asst. Prof. Saad Mohammed kaliphs***
***Electrical and Electronical Engineering Department***
***University of Technology, Baghdad, Iraq***

## Abstract

***A novel approach for identifying friend aircrafts from foe (IFF) using public-key cryptosystem is introduced. Tow schemes of public-key cryptosystem which provide higher security than convention(IFF) are presented computer simulation examples are also included to illustrate the identification procedure.***

## 1. Introduction

The introduction 0f a friend aircraft from foe can be accomplished by transmitting to the interrogating ground station a certain codes that only the friend aircraft knows it. In order to prevent a third party who is listening to the channel from copying the code and using it later ,it is necessary that each time an aircraft identifies it self , a different codes should be used . There are two generating a dynamically changing code:

**1.** The ground transmits to the aircraft a random message (m) together with the identification code , then the aircraft transmit back "IAMX" together with $f^{-1}{}_{(m)}$

**2.** The aircraft operators on message m, such a message contains the time and date of transmission , the content of m should be known on the ground after operating on the signal received from the aircraft with the function f .

We stand today on the development of the public-key cryptosystem. The public-key cryptosystem has the following properties:

**a)** f and $f^{-1}$ from the message m yields m. Formally $f^{-1}$ [f(m)]= m.

**b)** Both f and $f^{-1}$ are easy to computer for user. But it is computationally infeasible to derive $f^{1}$ from f for any eavesdropper.

**c)** For these reasons the public-key cryptosystem can be used for the identification of the aircraft.

## 2. Public-Key Cryptosystem

In the public-key cryptosystem, each user generates two distinct keys, an enciphering key E which serves to implement the enciphering algorithm and a deciphering key D which serves to implement the enciphering algorithm [2]. In the public-key cryptosystem each user places in a public-file an enciphering procedure. That is, the public-file is a directory giving the enciphering procedure of each user. The user keeps secret the details of his corresponding deciphering key. In a public-key, each two users can get private communication over an insecure channel. Each user sends his enciphering key to the key of all recipients.

### 2-1 Some of Public-Key Cryptosystem

We list here two well known public-key cryptosystem:

#### 2-1-1 RSA Public-Key Cryptosystem

The name of this system RSA is referred to the names of its discoverers Rives, Shamir and Adleman [3]. They make use of the fact that finding large numbers is computationally easy, but that factoring the product of two such numbers appear to be computationally infeasible.

A user a select two very large prime numbers p and q at random and multiplies them together to obtain a number n. The number n is made public, but it's factors p and q kept secret. Using p and q also to compute the Euletotient function $\Phi(n)$ the number of integers less than $\Phi(n) = (p^{-1})(q^{-1})$. Then he chose another number E (which is enciphering key) at random from the interval 2 through $[\Phi(n)-1]$. This numbers is also made public [4].

A message is than represented as a sequence of integers $M_1$, $M_2$, ….. with each $M_i$ an integer between 0 and n-1. Enciphering is carried out on each block $M_i$ using the public information E and n as:

$$\mathbf{C = M^E \bmod n}$$

where C represents the enciphering block. Using the secret $\varphi(n)$ user can easily calculate a number D (which is the deciphering key) by the equation [4]:

$$\mathbf{E*D = 1 MOD\ \text{Ø}(n)}$$

Equivalently, $ED = K\,\text{Ø}(n)+1$. where K =1,2,3,…….

Then because:

$$\mathbf{X^{k\text{Ø}(n)+1} = X \bmod n}$$

For all integers X between 0 and n-1 and for all integers K , deciphering is easily accomplished by raising C to the D$^{th}$ power:

$$C^{D} = M^{ED} = M^{KØ(N)+1} = M \bmod n$$

The security of RSA system is:

$$Z = Ln(n)\sqrt{\frac{Ln(n)}{Ln(ln(n))}}$$

### 2-1-2 Knapsack Public-Key Cryptosystem

This system is based on the well known problem which is knapsack problem, given a vector of integers a=$a_1$, $a_2$, ..... $a_n$ and the integer C, the knapsack problem is to find a subset of the [$a_i$] such that the sum of the elements of subset is equal to equivalently, given a and C. Find a binary n-vector X such that a. X =C.

The vector a can be used to encipher a message by dividing the message into N-bits block $X_1$, $X_2$, ...... $X_N$ and forming the dot product.

$$C = a_i \, . \, X_I$$

The C from the cipher text [3]. Recovering of $X_i$ from C involves solving a knapsack problem and is thus believed to be computationally infeasible, if (a) and X are randomly chosen, the vector a is chosen such that each element is greater than the sum of the preceding elements.

This vector a is chosen by the receiver and kept secret, also the receiver generate two large number m and w such that invertible modulo m (i.e. g c d (w, m) =1).
where g c d =Greatest common divisor. And:

$$M \geq \sum_{I=1}^{N} ai$$

These two also kept secret at the receiver. Then the receiver compute the integers $a_1$, $a_2$,.....$a_n$. (The hard solved knapsack problem) via the relation:

$$ai = (a_i * w) \bmod m$$

These integers are transmitted to the sender or in a public file.

The sender converts the message into it's binary representation and divided this into blocks each block of length N-bits [4].

Let $X_1$, $X_2$, ……$X_N$ be one of these block, the encryption of this block is accomplished as follows:

$$C = a_1\ x_1 + a_2\ x_2 + \ldots\ldots + a_N\ x_N$$

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

Then the receiver computers $w^{-1}$ via the relation:

$$\mathbf{w^{-1} * w = mod\ m}$$

The C (the transformed cipher text) is computed by the following relation:

$$\mathbf{\acute{C} = C * w^{-1} \bmod m}$$

The comparison between $\acute{C}_I$ ś and $å_i$ ś is used to recover the $X_i$ ś (which represent the binary representation of the message) as following:

First if $\acute{C}>å_N$ then set $X_N$ equal to 1 otherwise $X_N$ =0 .IF $X_N$ =1 then he subtracts $å_N$ form C and a new value is found ,then comparing this value with $å_{N-1}$ if the new value of C is greater than a $X_{N-1}$ then $X_{N-1}$ is set equal to 1 otherwise $X_{N-1}$ equal to 0. This process is repeated until the $X_i$ ś computed.

## 3. Computer Results

To clear the idea of using the public-key-cryptosystem for identification of an aircraft, we give small computer simulation examples for each (R S A and Knapsack).

### 3-1 RSA Computer Simulation Example

*The User (Aircraft) Choose:*

p = 73

q = 151

Then, n = p*q =11023

Ø(n) = (p-1)(q-1) =10800

*The User Also Choose:*

E (The public-key) = 11

Then calculate D (secret –key), such that E*D=1 mod Ø(n).

Hence, D = 5891

When the ground stations wish to send a message to the aircraft, it uses the public-key (E and n) to cipher the plaintext M.

**M = "WHO ARE YOU ?"**

where the message contain (14) characters include 4 spaces. The cipher text of this message is:

$$C=M^E \bmod n$$

**C=[1024 10355 4306 1583 1024 2929 2369 2320 1024 10841 1583 3777 1024 5497]**

Then the receives the cipher text C, extract the information by calculating:

$M=C^D \bmod n$

**M=[32 87 72 79 32 65 82 69 32 89 79 85 32 63 ]**

By using the ASCII code transformation we get the original message:

**"WHO ARE YOU"**

the sender (aircraft ) answer the ground station with the message:

**M = "I AM BMW"**

*By using the Same Procedure, the Aircraft Choose:*

P = 47

q = 59

n = p*q = 2773

Ø(n) = (p-1)(q-1) = 2668

E = 17

E*D=1 mod Ø(n)

Hence, D = 157

Then the aircraft encrypts the message M, and send the cipher text C:

$C= M^E \bmod n$

**C=[2227 928 2227 332 729 2227 872 762 652 2227 207]**

Then the receiver deciphers the cipher text C ,to obtain the message M by:

$M= C^D \bmod n$

**M=[32 37 32 67 77 32 66 77 87 32 33]**

Again by using code transformation, we get the original message:

**"I AM BMW"**

## 3-2 Knapsack Computer Simulation

*The User (Aircraft) Choose the Following:*

N =10: where N is the length of the vector å

**å = [$å_1$, $å_2$ ,……, $å_{10}$ ]=[2,5,10,19,38,77,154,308,616,1231]**

**M = 2398 such that:**

$M \geq \sum_{I=1}^{10} å_i$, **W=1605, $w^{-1}$ = 665**

Then he calculates a, which is the public- key,

**$A=[a_1, a_2, \ldots\ldots\ldots, a_{10}] =[748,639,1278,951,1902,485,970,1940,1418,1231]$**

Then the ground station uses this public-key to cipher the message:

**"WHO ARE YOU"**

The cipher text**:**

$$C_{jJ} = \sum_{I=1}^{10} \mathring{a}_i \cdot \chi_{ij}$$

where $\chi_{ij}$ is the binary representation of block j

**$C=[C_1, C_2, \ldots\ldots\ldots\ldots, C_{14}]=[485,5537,1921,4586,485,1918,$
$3511,2996,485,4571,4586,4888,485,6003]$**

Hence, the receiver (aircraft) wills receiver the cipher text C of the message and he calculates the transformed cipher text C where:

$$\acute{C}=C*W^{-1} \bmod m$$

**$\acute{C}=[\acute{C}_1, \acute{C}_2, \ldots, \acute{C}_{14}] =[77,209,173,190,77,156,197,166,77,213,190,204,77,151]$**

By using comparison process between Ćj ś and å we get binary representation of the original message:

**"WHO ARE YOU"**

*By using the same procedure, the aircraft will be the sender and the ground station will be the receiver:*

**N=9**

**$\mathring{a}=[\mathring{a}_1, \mathring{a}_2, \ldots\ldots, \mathring{a}_9] =[3,6,12,24,48,96,193,386,771]$**

m=2731

w=1761

w =1129

**$a=[a_1, a_2, \ldots.., a_9]=[2552,2373,2015,1299,2598,2465,1229,2458,422]$**

The message is:

**"I AM BMW"**

The cipher text is:

**$C= [C_1, C_2, \ldots., C_{11}]=[2465,5080,2465,3781,7095,2465,3602,7095,10767,2465,5017]$**

$\acute{C} = [\acute{C}_1, \acute{C}_2, \ldots, \acute{C}_{11}] = [96,220,96,196,23,96,199,232,262,96,99]$

And by using the comparison process, we obtain the original message:

**"I AM BMW"**

## 4. Conclusion

We have proposed a method for implementing the identification of an aircraft by using public-key cryptosystem either the RSA or knapsack .the security of based on the fact that factoring large number is computationally in feasible while the security of knapsack is based on the knapsack problem which can be solved by the enumeration technique. The knapsack technique is computationally infeasible for large n.

The limitations of the RSA and knapsack system are:

**1.** Slow in ciphering and deciphering procedure when compared with the conventional method due to the large amount of computing steps.

**2.** Large amount of storage is required to store the public file and ciphering and deciphering procedures.

In our methods the information and authenticators can also be hidden, but in addition a code must be exchanged first. Also in conventional identification, the authenticators only prevent third party forgeries and cannot be used to settle disputes between a transmitter and receiver.

## 5. References

**1.** Rivest, R. L., Hamir, A. S., and Adleman, L., ***"A Method of Obtaining Digital Signature and Puplic-Key Cryptosystems"***, Comm. of the ACM, Vol. 21, No. 2, Feb. 1978.

**2.** Martin, E. Hllman, ***"The Mathematics of Public-Key Cryptography"***, Scientific American, Vol. 241, No. 2, Aug. 1977.

**3.** Diffie, and Hellman, ***"An Introduction to Cryptography"***, Proceeding of the IEEE, Vol. 67, No. 3, March, 1979.

**4.** Brain Be Chett, ***"Introduction to Cryptography and PC Security"***, McGraw-Hill Co. Ltd., 1997.

**5.** Knuth, D. E., ***"The Art of Computer Programming"***, Vol. 2, Seminumerical Algorithm, Addison-Wesley, Mar. 1968.

**6.** Achim Jung, ***"Implementing the RSA Cryptosystem"***, Computer and Security, No. 6, North-Holland, 1987.