Aircraft Identification Technique using Public-Key Cryptosystem

Sadiq J. Abou-Loukh, Ph.D.
University of Baghdad,
College of Engineering,
Electrical Dept.

ABSTRACT
A new approach for identifying a friend aircrafts from foe (IFF) using public-key cryptosystem is introduced. Two schemes of public-key cryptosystem namely: RSA and knapsack public-keys are considered, which provide higher security than conventional identification methods. The practical aspects of using such systems for aircraft identification purposes are discussed. Computer simulation examples are also presented to illustrate the identification procedure.

Keywords
Public-key cryptosystem, IFF, Cryptographic security.

1. INTRODUCTION
Conventional method of identification of a friend aircraft from foe can be accomplished using beacon system. This system consists of interrogator on the ground station and transponder on the aircraft. The interrogator transmitter operates in the L-band and transmits a long coded pulse, asking the aircrafts seen on the screen of the ground radar to identify themselves. If the aircraft is a friend, then the transponder can discriminate and decode the long coded poles and send back an identity reply to the ground station (interrogator receiver) identifying itself [1].

In order to prevent a third party who is listening to the channel from copying the code and using it later, it is necessary to change the code with time and use different codes. In the classical system, the long coded pulse consists of N short data pulses (N-bits) which can provide 2^N-1 different identify codes; therefore this technique has limited security. For example, if N=12, there are 4095 different codes.

An identification code is changed daily in interrogator and correspondingly in the transponder. This change can be achieved either manually or automatically. However, sophisticated techniques for electronic countermeasures and spoofing have made this type of system unsuitable for nowadays high secure military identification.

This paper introduces the use of a complex cryptographic procedure instead of the identification codes to provide a very high degree of security by using public-key cryptosystems [2,3].

Public-key cryptography is a set of techniques that allow people to share secret information by exchanging entirely in public. Cryptography is a practical way by which secure private communication can be conducted while using insecure media to carry the transmission. There are two main types of cryptosystems: conventional cryptosystem and public-key cryptosystem.

In conventional cryptosystem, one key is used for ciphering and deciphering, this key must be kept secret. However, public-key cryptosystem operates on the basis of different ciphering and deciphering algorithm and only the deciphering key is kept secret [4,5].

In the public-key cryptosystem, each user on the network, generates two distinct keys, an enciphering key E which serves to implement the system's enciphering algorithm and deciphering key D which serves to implement the system's deciphering algorithm [3]. The trick is that it is computationally infeasible to drive D of E; the computation should require a vast amount of computing time. Hence, in a network of users each one can publish files, such as a telephone book without compromising his deciphering key which is kept secret. Therefore, when user j wants to transmit the message **X** to user i, the transmitted message is

$$Y = E_i(x) \tag{1}$$

This ciphertext Y is transmitted over an insecure channel. Only the intended receiver (the receiver of user **i**) who knows the corresponding secret key Di will be able to decipher the transmitted message

$$D_i(E_i(x)) = x \tag{2}$$

2. PUBLIC-KEY CRYPTOSYSTEM
Two well-known public-key cryptosystems are presented, namely: RSA and Knapsack.

2.1 RSA Public-Key Cryptosystem
The name of the system RSA is referred to the names of its discoverers Rivest, Shamir and Adelman [6]. They make use of the fact that finding large prime numbers is computationally easy, but that factoring the product of two such numbers appear to be computationally infeasible.

RSA public-key cryptosystem, the key generation, encryption and decryption include the following steps [6, 7]:

1. User i generates two long prime numbers p_i & q_i and computes their product

$$n_i = p_i \times q_i \tag{3}$$

2. Calculate $\Phi(n_i)$

$$\Phi(n_i) = (p_i - 1)(q_i - 1) \tag{4}$$

3. User i generates long integer number e_i where $e_i < n_i$ and must be relatively prime to $\Phi(n_i)$, that is

$$GCD[e_i, \Phi(n_i)] = ae_i + b\Phi(n_i) = 1 \tag{5}$$

Where, GCD is the greatest common divisor.

4. User i publishes his ciphering key n_i, e_i in public dictionary available for all users of the network

$$E_i = \{n_i, e_i\}$$

5. User j sends the message M to user i using the public ciphering key of user i $\{n_i, e_i\}$ and as follows:

$$C = M^{e_i} \bmod n_i \quad (6)$$

Where, C is the cipher text.

6. User i decrypts the cipher text C using his secret deciphering key $D_i = \{d_i\}$ and as follows

$$M = C^{d_i} \bmod n_i \quad (7)$$

Where, $\{d_i\}$ the secret deciphering key of user i and it is found from

$$d_i = a \bmod \Phi(n_{i)} \quad (8)$$

With a is calculated from Eq.(5).

2.2 Knapsack Public-Key Cryptosystem

The use of the knapsack problem in public-key cryptography is due to Merkle and Hellman [8]. This type of cryptosystem is based on trapdoor one-way functions. These functions are called one-way because they are easy to compute in one direction but they are computationally infeasible to compute inverse functions. They are called trapdoor functions since the inverse functions are in fact easy to compute once certain private trapdoor information that was employed in the design of the functions is known.

The Merkle-Hellman trapdoor knapsack algorithm for key generation, encryption and decryption involves the following steps [9,10]:

1. User i randomly generates an N-integer vector $[a'_1, a'_2, a'_3, \ldots a'_N]$ with the property that each element is greater than the sum of preceding elements

$$a'_k > \sum_{l=1}^{k-1} a_l' \qquad \text{where, } k = 2, 3, \ldots, N$$

This vector is the deciphering key of user i and it must be kept secret

$$Di = [a'_1, a'_2, a'_3, \ldots a'_N]$$

2. User i generates two large numbers m and w, such that w is invertible modulo m, i.e.,

GCD (w, m) =1 and $m > \sum_{i=1}^{N} a_i'$

These two integers are also kept secret by user i

3. User i computes vector of integers $a_1, a_2, a_2, \ldots a_N$ via

$$ai = a'_i \,.\, w \bmod m \quad \text{where, } i = 1, 2, 3, \ldots N$$

This vector of integers $[a_1, a_2, \ldots a_N]$ are published in a public file and represents the ciphering key of user i

$$Ei = [a_1, a_2, a_3, \ldots a_N]$$

4. The sender (user j) transmits the message M to user i by converting the message M into its binary representation and divide this binary representation into block each of length N-bits. Encryption of message M is accomplished by encryption of each block, let $x_1, x_2, \ldots x_N$ be one of these blocks, the encryption of this block is:

$$C = a_1x_1 + a_2x_2 + \ldots + a_Nx_N \quad (9)$$

Which is transmitted by user j via insecure channel to user i

5. User i compute first w^{-1} from the two secret integer w and m as follows:

$$w.w^{-1} = 1 \bmod m \quad (10)$$

Then $\acute{C}$ is computed by

$$\acute{C} = C * w^{-1} \bmod m \quad (11)$$

Receiver of user i begins to recover x_i by comparing $\acute{C}$ with a'_N. If $\acute{C} > a'_N$ then x_N is equal to 1, otherwise x_N is equal to zero. If $x_N = 1$ then a'_N is subtracted from $\acute{C}$ and a new value is found, then comparing this value with a'_{N-1}, if the new value of $\acute{C}$ is greater than a'_{N-1}, then x_{N-1} is equal to 1, otherwise x_{N-1} is equal to zero. This process is repeated until x_1 is computed.

3. COMPUTER SIMULATION RESULTS

For the purpose of illustrating the idea of using public-key cryptosystem for identification of an aircraft, a small computer simulation example is given for each RSA and knapsack by considering a ground station user 1 and one aircraft as user 2. The encryption of decryption keys of user 1 and user 2 is determined according to the procedure explained in section 2.

3.1 RSA Computer Simulation Example

Firstly, the keys of the ground station (user 1) and the aircraft (user 2) are generated as follows:

Ground Stations (user 1) chooses: $p_1 = 47$, $q_1 = 59$

Then $n_1 = p_1 * q_1 = 2773$

$\Phi(n_1) = (p_1\text{-}l)\,(q_1\text{-}l) = 2668$

$e_1 = 17$

Hence, the public encryption key of the ground station is

$E_1 = \{2773, 17\}$

The secret key of the ground station d_1 is calculated such that

$e_1 * d_1 = 1 \bmod \Phi(n_1)$

So, $d_1 = 157$

Secret key of ground station $D_1 = \{157\}$

Aircraft station (user 2) chooses

$p_2 = 73$

$q_1 = 151$

$n_2 = p_2 * q_2 = 11023$

$\Phi(n_2) = (p_2\text{-}l)\,(q_2\text{-}l) = 10800$

$e_2 = 11$

Hence, the public encryption key of the aircraft is $E_2 = \{11023, 11\}$

The secret key of the aircraft d_2 is calculated from

$e_2 * d_2 = 1 \bmod \Phi(n_2)$, so $d_2 = 5891$

Secret key of aircraft $D_2 = \{5891\}$

a- When the ground station wishes to send a message asking the aircraft how are you?

Then the message is

M = "HOW ARE YOU?"

This message consists of 13 characters, including three spaces. The ASII code transformation of this message is M = [87 72 79 32 65 82 69 32 89 79 85 32 63]. The ground station ciphered this message using the public encryption key of the aircraft

E2 = {11023, 11} to get cipher-text C, where

$C = M^{11} \bmod 11023$

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

Then, the aircraft receiver which receives the ciphertext C, start to decipher C using its secret decryption key

D2 = {5891} and as follows:

$M = C^{5891} \bmod 11023$

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

By using the ASCII code transformation, the original message is obtained as:

HOW ARE YOU?

b- The aircraft must send a reply to the ground station identifying itself, for example if the aircraft identify itself as BMW, then the aircraft sends back the answer (message):

M = I AM BMW!

The ASCII –code transformation of the message is M = [73 32 67 77 32 66 77 87 32 33]. Then the aircraft ciphered this message using the public encryption key of the ground station E_1 = {2773, 17} and as follows:

$C = M^{17} \bmod 2773$

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

The ground station received the cipher-text C and decipher it using its secret decryption key D_1 = {157} and as follows:

$M = C^{157} \bmod 2773$

M = [73 32 67 77 32 66 77 87 32 33]

Again, by using ASCII –code transformation the original message is recovered as:

I AM BMW!

3.2 Knapsack Computer Simulation Example

Ground stations (user 1) keys generation.

Let N = 9, length of the vector a' and select

$[a'_1\ a'_2\ a'_3 \ldots a'_9]$ = [3 6 12 24 48 96 193 386 771]

Let m = 2731 such that $m > \sum_{i=1}^{9} a_i'$

And w =1761

Then w^{-1} =1129

Vector a is computed via $a_i = 1761\ a'_i \bmod m$

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

Ground station public encryption key is

E_1 = {vector a}

Ground station secret decryption key is

D_1 = {vector a′, m, w}

Aircraft (user 2) keys generation

Let N = 10, length of the vector a′ and select $[a'_1\ a'_2 \ldots a'_{10}]$ =

[2 5 10 19 38 77 154 308 616 1231]

Let m = 2398 such that $m > \sum_{i=1}^{10} a_i'$

And w =1605

Then $w^{-1} = 665$

Aircraft secret decryption key is D_2, where D_2 {vector a′,m,w}

Aircraft public encryption key is E_2, where E_2 = {vector a}

Vector a = $[a_1\ a_2 \ldots a_{10}]$, and is computed via

$a_i = 1605\ a'_I \bmod 2398$ where, i = 1, 2,….

a. The ground station asks the aircraft to identify itself by sending the message:

M = HOW ARE YOU?

The ground station cipher this message using aircraft public encryption key E_2 via

$$C_j = \sum_{i=1}^{10} a_i . x_{ij}$$

Where x_{ij} is the binary representation of block j of message M.

C = [5537 1921 4586 485 1918 351 2996 485 4571 4586 4888 485 6003]

The aircraft receives the ciphertext C and start to decrypt it by computing Ć using

$\acute{C}_j = 665 * C \bmod 2398$

Ć = [209 173 190 77 156 197 166 77 213 190 204 77 151]

By using a comparison process between $\acute{C}_i$ and a'_i the binary representation of the original message is obtained, then

M = HOW ARE YOU ?.

b. The aircraft will send reply to the ground station :

I AM BMW!

This message is ciphered by the aircraft using ground station public encipher key to obtain the cipher-text:

C = [5080 2465 3781 7095 2465 3602 7095 10767 2465 5017]

The ground station decipher the received cipher-text C by computing C′ firstly using its secret key D1, then

C′ = [220 96 196 232 96 199 232 262 96 99]

Again, using the comparison process to obtain the original message

I AM BMW!

4. CONCLUSIONS

The RSA and knapsack public-key cryptosystems are successfully applied for the identification of a friend aircraft from foe. The security of RSA based on the fact that factoring large number is computationally infeasible, while the security of the 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 systems 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.

However, these limitations are not a real problem today due to the revolution in computer and microcomputer technologies.

In these 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 the transmitter and interrogator receiver.

5. REFERENCES

[1] Faulconbridge, I., 2002. Radar Fundamentals. Argos Press pty. Ltd.

[2] Grigoriev, D., Hirsch, E., and Pervyshev, K. 2009. A Complete Public Key Cryptosystem. Groups Complexity Cryptology, Vol.1, No.1, 1-12.

[3] Naccache, D., and Stern, J. 1997. A New Public Key Cryptosystem. In : W. Fumy (Ed.). Advances in Cryptology, EUROCRYPT 97. 27-36.

[4] Wiener, M. J. 1994. Efficient DES key Search. Technical Report TR-244, School of Computer Science. Carleton University.

[5] Ajtai, M. and Work, C. D. 1999. A Public Key Cryptosystem. In Proc. 39th Annual ACM Symposium on the Theory of Computing.

[6] Marjono, M. 2002. The Rivest, Shamir, Adelman (RSA) Public Key Cryptosystem and Cyclic Code. Journal Integral. Vol. 7, No. 1, 1-6.

[7] Abood, Q., Younis, M., and Othman, M. 2011. RSA Security Enhancement. ECCCM 2011. 241-245.

[8] Nguyen, P., and Stern, J. 1997. Merkle-Hellman Revisited: A Cryptoanalysis of the Qu-Vanstone Cryptosystem Based on Group Factorizations. In: B.S. Kaliski (Ed.). Advances in Cryptology-CRYPTO 97 (LNCS 1294). 198-212.

[9] Wang , B., Wu, Q. and Hu, Y., 2007. A Knapsack Based Probabilistic Encryption Scheme. Information Sciences. Vol.77, Issue 19, 3981-3994.

[10] Lee, M. S. 2013. Improved Cryptanalysis of a Knapsack Based Probabilistic Encryption Scheme. Journal Information Science, Vol. 222, 779-783.