Proceedings of International Conference
on Cryptology and Information Security

A Key Distribution Scheme with Directly Mutual Authentication

Jeong-Hyun Park*, Sang-Ho Lee**

* : ETRI section 0920, 161 Kajeong-Dong, Yusung-Gu, Daejeon, 305-350, KOREA

e-mail : jhpark@satserv.etri.re.kr

** : Chungbuk National University, Department of Computer Science, 48 Kaeshin-Dong,
Hyungduck-Gu, Cheongju 360-763, KOREA

e-mail : shlee@cbucc.chungbuk.ac.kr

Abstract

This paper presented a key distribution scheme based on the Yacobi scheme that does not use the secret key provided by key distribution center, but uses instead a random number generated by the user. The scheme is independent of the exposure of the secret key. This paper also presented the key distribution schemes based on the Diffie-Hellman (DH) and ID (identity). The schemes based on the solving of the discrete logarithm and prime resolution into factors are better on the expose of secret key. The proposed scheme based on the DH has directly mutual authentication between users and is able to defend the network from impostors. The proposed key scheme based on the DH was applied to point- to - multipoint, and broadcasting networks via satellite.

1. Introduction

The significance of computer and communications technologies, economically, socially and politically is widely accepted in the information age. Moreover, the global information society has arrived. It is borderless, unconstrained by distance or time. But explosive growth in use of data and computers for all manner of application in all parts of life will be considered the inadequencies of social, ethic, cultural, and criminal aspects. Especially we need to solve problems such as protection from the invasion of privacy, unauthorized access to important data and tampering with transmitted data. So, security is becoming an essential requirement of information networks for these. A protective technology which is called cryptography is used to secure transmissions for privacy. Cryptography can be categorized into conventional cryptosystems and public key cryptosystems which are based on the distribution and management of keys. Conventional cryptosystems, used from ancient times, must share the same key for secret communication. The sender sends the ciphered data using a secret key and the receiver retrieves the plain data by deciphering the ciphering data using the same key. Therefore, each user in this scheme must have the secret key of all users in the group. Moreover if each user has to keep as many keys as the number of users, then large communication networks that use conventional key distribution schemes face a great difficulty due to complicated key management.

Public key cryptosystems use different keys for ciphering and deciphering. Each user must keep a decryption key for himself and the encryption keys of all user are registered on a central public key directory. Therefore, this scheme improves the problem of conventional cryptosystems which require a large memory to keep and protect the session keys, but still has the problem of reliable and consistent management of the central key directory when new users join the group or when keys are changed. To overcome these problems, several key distribution systems have been proposed since Shamir proposed the key distribution scheme based on ID (Identity : birthday, address, ID No., etc).

In this paper, after briefly describing the existing public key distribution schemes and their

handicaps, the modified key distribution scheme based on the Yacobi is proposed and the modified key distribution schemes based on the Diffie-Hellman (DH) and ID are presented. And then the proposed scheme based on DH and ID is applied to point - to - multipoint, and broadcasting networks via satellite.

2. Review of key distribution schemes

In this section, we will review briefly the public key distribution scheme proposed by Diffie and Hellman in 1976 and simpler Yacobi scheme, and then describe the ID scheme first proposed by Shamir in 1984 and improved by Okamoto and Tanaka in 1989. After that, this paper will summarize other schemes and issues.

2.1 Diffie-Hellman scheme[3]

Diffie-Hellman scheme for working key distribution is as follows ;

1) User i sends user j the integer X_i after calculating $X_i = g^{Si} \bmod p$.

2) User j sends user i the integer X_j after calculating $X_j = g^{Sj} \bmod p$.

3) User i and user j generate the working key, $WK_{ij} = (X_i)^{Sj} = (X_j)^{Si} = g^{Si \cdot Sj} \bmod p$.

Here S_i and S_j are secret keys from key distribution center and g is the integer which is a primitive element in GF(p). The p is the prime number and GF is Galois Field. This scheme has the disadvantage that user k can impersonate user i to user j and can then make a working key. User i and user j must change their secret key and working key periodically. This scheme also requires a basically reliable key distribution center. Moreover, since each user's modulus differs from those of the other users, it requires rather complicated processing.

2.2 Yacobi scheme[8]

Yacobi scheme for working key distribution is as follows ;

1) User i and user j open their public keys X_i ($X_i = g^{Si} \bmod p$) and X_j ($X_j = g^{Sj} \bmod p$).

2) User i sends user j the integer Y_i and random number R_i after generating R_i and calculating $Y_i = (R_i + S_i)$

3) User j sends user i the integer Y_j and random number R_j after generating R_j and calculating $Y_j = (R_j + S_j)$.

4) User i and user j generate the working key, $WK_{ij} = (g^{Yj} \cdot Xj^{-1})^{Ri} = (g^{Yi} \cdot Xi^{-1})^{Rj} = (g^{Si \cdot Sj}) \bmod p$.

Here S_i and S_j are secret keys from key distribution center, and R_i and R_j are random numbers by user i and user j. The g is the integer which is a primitive element in GF(p). The p is the prime number. This scheme is susceptible to passive attack when S_i and S_j are disclosed.

2.3 Okamoto - Tanaka scheme[4]

This scheme is similar to the Diffie-Hellman scheme and solves the public key management problem by introducing the ID concept[4]. This is a relatively secure scheme.

1) User i send user j the integer X_i after calculating $X_i = S_i \cdot g^{Ri} \bmod n$ using random number R_i and secret key S_i.

2) User j send user i the integer X_j after calculating $X_j = S_j \cdot g^{Rj} \bmod n$ using random number R_j and secret key S_j.

3) User i and user j generate the working key, $WK_{ij} = (X_j^e \cdot ID_j)^{Ri} = (X_i^e \cdot ID_i)^{Rj} = g^{e \cdot Ri \cdot Rj} \bmod n$ using X_i, X_j, R_i, R_j, e, S_i and S_j.

Here S_i and S_j are secret keys from key distribution center, and R_i and R_j are random numbers. The g is the integer which is a primitive element in GF(p) and GF(q). ID is identification information and e is encryption key. The p and q

are the prime numbers. The n is p x q. Under passive attack, this scheme's security depends on solving $g^{e.Ri.Rj}$ from $g^{e.Ri}$ and $g^{e.Rj}$.

Under impersonation attack from disguised user j, it depends on finding X and R that satisfy $X = ID_j^{-1/e} \bmod n$. The followings are simple definitions of passive and impersonation attack.

Ciphertext Only Passive attack (COP) : This means to find the session key illegally via wire tapping and only observing the exchanged data between user i and user j. It is a simple attack scheme. Ciphertext Only Impersonation attack (COI) : Attacker gets data by means similar to the COP scheme but disguised as user j by modifing the transmitted data. Known Key Passive attack (KKP) : This means to find the new session key illegally via the old session key and additional data obtained via wire tapping and observing the exchanged data between user i and user j. Known Key Impersonation attack (KKI) : Attacker obtains data by means similar to the KKP and COI schemes and disguises as user j by modifing the transmitted data.

2.4 Other schemes

Blom proposed a symmetric key generation system (SKGS) based on secret key sharing systems. A trusted authority generates a matrix G of size k x n and a secret matrix D of size k x k[6]. The *i*th column of G, namely g_i, is set as the address of user i or the like. Then, the authority delivers the *i*th row S_i of G^TD to user i. In the communication phase, user i uses $S_i g_j$ as a working key to user j. Since G^TDG is a symmetric matrix, the working key equals $S_j g_i$, which can be by user j. In this system, any k users among all n users can obtain the top secret matrix D in cooperation with each other, while k - 1 or fewer users cannot. Weak points in the SKGS are the difficulty in choosing a suitable size for integer k and the large memory space required for maintaining S_i. Tanaka proposed a key distribution system similar to the SKGS using the RSA (Rivest, Shamir, Adleman) cryptosystem. Tsujii, Itoh, and Kurosawa showed the threshold type of cryptosystem based on the ElGamal cryptosystem[5].

3. Proposal of key distribution schemes and application

3.1 Proposal of key distribution schemes

This section describes a more secure scheme than Yacobi. A random number is generated by a user and the secret key (unique key) is provided by a key distribution center. Another key distribution scheme based on the Diffie-Hellman scheme but with ID(identity) independent of the exposure of the secret key is proposed as a kind of public key distribution scheme. It is more practical than conventional key management and can authenticate directly between users or among one sender and multi users with the same security level as Okamoto and Tanaka scheme. This scheme will be adapted to point - to - point, point to - multipoint, and broadcasting system using satellite. The procedure for key distribution is as follows ;

(Initial key generation and distribution)

1) When the network is set up, the key distribution center produces two prime numbers p and q, each about 256 bits long and then determines a prime number e(encryption key)and an integer d(decryption key), satisfying $e.d \{\bmod ((p-1).(q-1))\} = 1$, with both e and d less than $n = p \cdot q$.

2) It also determines an integer g, which is a primitive element in GF(p) and GF(q).

3) For user i whose identification information is ID_i , the center calculates integers S_i (i = 1, 2, ...) : $S_i = ID_i^{-d} \pmod n$, where $S_i^e \cdot ID_i \pmod n = 1$.

4) Then, the center stores the set of integers (n, g, e, S_i) in the smart card for user i and distributes it to him.

5) For user j whose identification information is ID_j, the center calculates integers S_j(j = 1, 2, ...) : $S_j = ID_j^{-d} \pmod n$, where $S_j^e \cdot ID_j \pmod n = 1$.

6) Then, the center stores the set of integers (n, g, e, S_j) in the smart card for user j and distributes it to him.

7) After smart cards are distributed to all users, the users can authenticate each other. The integer d can be aborted after all the cards are distributed. If there are no new users expected, even the key distribution center can close down. Hence, d is kept secret from any user, S_i is known only to user i, and n, g, e and ID_i are common to all the users. Figure 3-1 illustrates the card issue phase.

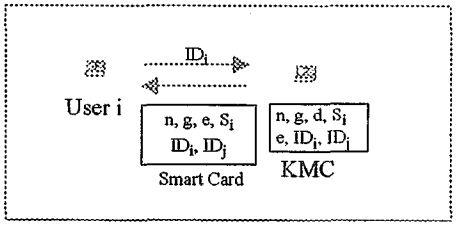

Figure 3-1 Initial Key Generation and Distribution

3.1.1 The modified Yacobi scheme

The modified Yacobi scheme has more security than Yacobi scheme. Because the proposed scheme uses mod n instead mod p. It is difficulty to find p and q from n. This scheme authenticates user indirectly by way of common working key. The procedure for working key generation between user i and user j is as follows. Steps 1) to 7) for initial key generation are same.

8) When users i and j wish to obtain a working key, user i generates a random number r_i and sends user j the integer x_i : $x_i = g^{si} \bmod n$ and $y_i = (r_i.e + s_i)$.

9) User j also generates a random number r_j and sends user i the integer x_j : $x_j = g^{sj} \bmod n$ and $y_j = (r_j.e + s_j)$.

10) Then, users i and j compute working keys WK_i and WK_j, repectively, as follows : $WK_{ij} = WK_j = WK_i = (g^{yi} \cdot x_j^{-1})^{ri} = g^{e.ri.rj} \bmod n$. Figure 3-2 illustrates the working key generation phase of the modified Yacobi scheme.

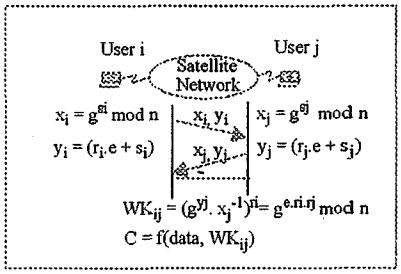

Figure 3-2 Working Key Generation based on the Modified Yacobi Scheme

3.1.2 The modified Diffie-Hellman scheme (case1)

The modified Diffie-Hellman scheme (case1) for working key does not use the secret key from key distribution center, but use the random number from user. The proposed scheme can be independent of key distribution center for working key between user i and user j. User i and user j can change their working key without key distribution center help. The modified Diffie-Hellman scheme also uses mod n instead mod p. This scheme also authenticates user indirectly by way of common working key. The procedure for working key generation between user i and user j is as follows. Steps 1) to 7) for initial key generation are same.

8) When users i and j wish to obtain a working key, user i generates a random number r_i and sends user j the integer x_i : $x_i = ID_j \cdot g^{ri.si} \bmod n$.

9) User j also generates a random number r_j and sends user i the integer x_j : $x_j = ID_i \cdot g^{rj.sj} \bmod n$.

10) Then, users i and j compute working keys WK_i and WK_j using $S_i^e \cdot ID_i \bmod n = 1$, repectively, as follows : $WK_{ij} = WK_j = WK_i = (ID_j^{-1} \cdot x_i)^{rj.sj} = g^{ri.rj.si.sj} \bmod n$. Figure 3-3 illustrates the working key generation phase based on the modified DH scheme.

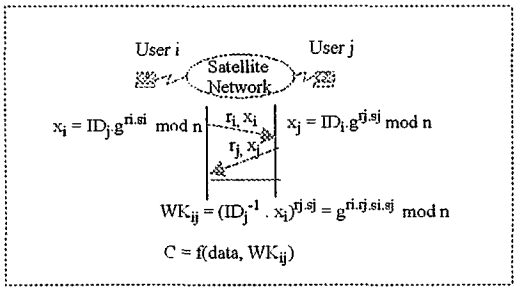

Figure 3-3 Working Key Generation based on the Modified DH Scheme (case1)

3.1.3 The modified Diffie-Hellman scheme (case2)

The modified Diffie-Hellman scheme (case2) for working key also has same features with modified Diffie-Hellman scheme (case1). In addition to the proposed scheme (case2) can be authenicated directly between user i and user j before they use their working key for secret communications. The procedure for working key generation between user i and user j is as follows. Steps 1) to 7) for initial key generation are same.

8) When users i and j wish to obtain a working key, user i generates a random number r_j and sends user j the integer x_i ($x_i = g^{(ri.si+IDj)} \pmod n$), y_i ($y_i = g^{ri.si.ci} \pmod n$) and $c_i = hash(x_i, ID_i, ID_j, t)$.

9) User j also generates a random number r_j and sends user i the integer x_j ($x_j = g^{(rj.sj+IDi)} \pmod n$), y_j($y_j = g^{rj.sj.cj} \pmod n$) and $c_j = hash(x_j, ID_i, ID_j, t)$.

10) Then, users i and j compute working keys WK_i and WK_j, repectively, as follows : $WK_{ij} = WK_j = WK_i = (g^{-IDj} \cdot x_i)^{rj.sj} = g^{ri.rj.si.sj} \bmod n$.

11) User j can authenticate the sender, if the following equation holds : $S_j = x_i^{ci'}/(y_i \cdot g^{IDj\ ci}\ IDj^d) \pmod n$.

Here c_i' is the number calculated by user j with c_i. This is direct authentication. If x_i is changed to another number by an unauthorized user, c_i' is not equal to c_i (c_i is dependent on x_i). t is the time stamp with date and time. Figure 3-4 illustrates the working key generation and authentication phase based on the modified DH scheme.

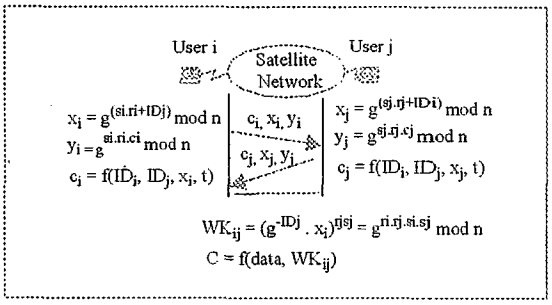

Figure 3-4 Working Key Generation and Authentication based on the Modified DH Scheme (case2)

The schemes described above have an improved security because they use the discrete logarithm function and prime resolution into factors. The schemes do not use the secret keys by center as a power, but use the random number by the user.

3.2 Characteristics of Modified Key Distribution Schemes

1) The modified Yacobi scheme is independent of the exposure of the secret key. Because the scheme does not use the secret key provided by key distribution center as a power, but uses instead a random number generated by the user.

2) The modified Diffie-Hellman (DH) and ID (identity) is better on the exposure of secret key.

3) The second modified DH scheme has direct mutual authentication between user i and user j.

4) The second modified DH scheme also has non-repudiation function which can protect the deny of it after sending and receiving the data.

5) The second modified DH scheme is able to defend the network from impostors.

6) The second modified DH scheme has the same security level as the Okamoto and Tanaka

scheme because the scheme is based on the discrete logarithm and prime resolution into factors.

7) The second modified DH scheme does not require any key distribution center to be active in each communication.

8) The second modified DH scheme randomly determined the working keys.

3.3 Application

Modern networks provide point-to-multipoint communication services such as electronic mail, multiple teleconference, electronic transfer, and direct satellite broadcasting using satellite broadcasting networks, satellite data networks, and multi media. Ciphering algorithms and key distribution schemes are required to secure these services. In this section the proposed key distribution scheme based on the DH (case2) is applied to satellite broadcasting communications and satellite data communications.

(Broadcasting communication via satellite)[5],[6]

Assume that transmitter station provides the key generation and management function.

1) Users register their IDs at the transmitter station.

2) Transmitter station i generates x_i ($x_i = g^{(ri.si+IDj)} \pmod n$), y_i ($y_i = g^{ri.si.ci} \pmod n$) and $c_i = hash(x_i, ID_i, ID_j, t)$ for all users.

3) Transmitter station i generates the group working key $W_k = g \prod_{i \le i \le k} ^{ri.si} \pmod n$.

4) Transmitter station stores r_j, s_j, c_j, x_j, y_j, w_k, n, e, and d into smart cards for each user and transfers it to each user by mail or other transfer scheme.

5) User j receives a smart card with r_j, s_j, c_j, x_j, y_j, w_k, n, e, and d from the transmitter station and inserts it into his set-top box.

6) After that, user j can authenticate the transmitter station, and t receives broadcast programs transmitted from the transmitter station.

This scheme will be more efffective when applied to CATV (Cable Television) using satellite.

(Multicasting data communication via satellite)[2, 4, 6, 7]

Assume a star network and users have a sequential key generation and distribution function in the network. It is also assumed that the key distribution center has already generated each user's unique key including s, e,d, ID, p, q, n for each user, stored this information in smart cards and transfered the cards to each user by mail or other transfer scheme.

1) User i generates a random number r_i and sends to user i+1 the x_i ($x_i = g^{(ri.si+IDj)} \pmod n$), y_i ($y_i = g^{ri.si.ci} \pmod n$) and $c_i = hash(x_i, ID_i, ID_j, t)$.

2) User i receives x_{i-1}, y_{i-1} and c_{i-1} from user i-1 and then authenticates each other. $S_i = x_{i-1}^{ci-1'} / (y_{i-1}.g^{IDi.ci-1}. IDi^d) \pmod n$, where c_{i-1}' is the number calculated by user i with c_{i-1}. This is direct authentication. If x_{i-1} is changed to another number by an unauthorized user, c_{i-1}' is not equal to c_{i-1} (c_{i-1} is dependent on x_{i-1}).

3) If authentication is successful, it means that the message received by user i is transmitted via i-1, i-2, i-3, ..., i-j+1. User i then sends c_i, x_i and y_i to user i+1.

x_i ($x_i = g^{(ri.si+IDj)} \pmod n = g \prod_{i \le i \le k} ^{(ri-k.si-k+IDi-k)} \pmod n$).

y_i ($y_i = g^{ri.si.ci} \pmod n = g \prod_{i \le i \le k} ^{(ri-k.si-k.ci-k)} \pmod n$).

$c_i = hash(x_i, ID_i, ID_j, t) = hash(x_{i-k}, ID_{i-k}, ID_{i+1}, t))$.

4) When the last user of the group receives x, c, y and authenticates it to the group, the working

key of the group is generated as follows ; the group working key, $W_k = g \prod_{i \le i \le k} ri.si \pmod n$.

5) Now, the group has secure communication by using the specified cryptography algorithmin the group using the group working key.

This scheme will be more efffect if applied to VSAT (Very Small Aperture Terminal) data communication using satellite.

4. Conclusions

Existing key distribution schemes encounter the key management problems when changing key and adding new users. First, this paper presented a key distribution scheme that does not use the secret key provided by center as a power, but uses instead a random number generated by the user. The scheme based on the Yacobi is independent of the exposure of the secret key. The scheme based on the Diffie-Hellman (DH) and ID (identity) also proposed. The scheme based on the DH has direct mutual authentication between user i and user j. The scheme also has non-repudiation function which can protect the deny of it after sending and receiving the data. The scheme is able to defend the network from impostors. The scheme has the same security level as the Okamoto and Tanaka scheme because the proposed scheme is based on the discrete logarithm and prime resolution into factors. In the scheme based on the DH, users do not require any key distribution center to be active in each communication. Other things are as follows ; A KMC (Key Management Center) is needed only when starting up a network; An individual user need not maintain a public key directory; When a new user joins, other users need not renew their card; The working keys are randomly determined; Even if secret keys were to be exposed, it would still remain secure. In the DH-PKDS (Diffie- Hellman Public Key Distribution Scheme), working keys between two fixed users are always a constant; All users have the same modulus n, although in the RSA (Rivest, Shamir, Adleman) cryptosystem each user uses a different modulus n. The proposed scheme based on the DH and ID was applied to point- to - multipoint, and broadcasting networks via satellite. We expect the proposed scheme can solve the vulnerable satellite data communication problem over VSAT networks via satellite or satellite broadcasting services such as CATV via satellite, and will be widely extended when these networks expand to private networks.

References

[1] A. Shamir, "Identity-based Cryptosystems and Signature Schemes", Proc. Crypto 84, pp. 47-53, 1984.

[2] I. Ingemarson, D.Tang, C.K. Wong, "A Conference Key Distribution System", IEEE Trans. IT-28, No.5, pp. 714-720, 1982.

[3] W. Diffie and M.E. Hellman, "New directions in cryptography", IEEE Trans. on Inform. Theory, Vol.IT-22, pp.644-654, 1976.

[4] K. Koyama, K. Ohta, "Identity-based conference key distribution systems", Proc. Crypto 87, pp. 175-184, 1984.

[5] EIJI OKAMOTO, KAZUE TANAKA, "Key Distribution System based on identification information", IEEE Journal on selected areas in communications, Vol.7,No.4, pp.481 - 485, May 1989.

[6] Shimshon Berkovits, "How to broadcast a secret", Proc. EUROCRYPT 91, pp.535 - 541, May 1991.

[7] Shamir, "How to share a secret", Communication of the ACM, Vol.22, No.11, pp.612 - 613, November 1979.

[8] Y. Yacobi and Z. Shmuely, " On key Distributions", Proc. Crypto '89, pp.335-346, 1989.

[9] A. Fujioka, T. Okamoto, S.. Miyaguchi, "ESIGN : An Efficient Digital Signature Implementation for Smart Cards", Proc. EUROCRYPT 91, pp.446 - 457, May 1991.

[10] E.T.R.I, "Modern Cryptology", December, 1991.