個別通信 및 放送通信시스팀에 適合한 暗號方式의 硏究

○이 차 연, 이 민 수, 이 만 영

한양대학교 전자통신공학과

A Study on the Cryptosystem for Private and Broadcasting Communication System

Lee Cha Youn, Lee Min Soo, Rhee Man Young

Dept. of Electronic Communication Eng. Hanyang Univ.

요 약

개별통신 및 방송통신시스팀에 적합한 암호방식으로서 동일한 통신시스팀내에 가입된 모든 이용자의 개별키에 공통으로 대치할 수 있는 마스터키방식을 적용하였다. 사용된 암호방식으로는 키관리가 편리하고 인증기능이 좋은 RSA공개키암호방식을 사용하여 RSA마스터키의 생성법을 제시하고 실제 마스터키를 생성하여 개별암호통신 및 방송암호통신의 방법을 보였다.

1. 서 론

현대의 통신망이 고도화, 다양화됨에 따라 위성통신망, 방송매체등을 이용하여 전자우편, 전자송금, 다자간회의등과 같이 일대다수의 방송통신기능이 요구됨에 따라 개별통신 뿐 만아니라 일대다수 방송통신기능을 수행할 수 있는 암호방식이 요구되고 있다.

본 논문에서는 RSA암호를 이용하여 위성통신등에서 개별통신 과 일대다수방송통신이 모두 가능한 암호방식을 제안하고 제안한 방식을 이용하여 암호통신 및 디지틀서명이 가능함을 보였다. 2절에서는 RSA암호방식의 원리, 3절에서는 개별통신 및 방송통신에 적합한 암호방식으로서 마스터키방식을 적용하여 안전성 및 키관리법과 키 생성법을 제시하고 개별 및 방송암호통신방법과 일대다수 디지틀서명방법을 보이고 4절에서 결론을 내렸다.

2. RSA 공개키 암호방식[1][2]

2.1 RSA 암호알고리듬

마스터키와 구별하기위해 이용자 i($1 \le i \le m$)의 암호화개별키를 K_{ei}, 복호화개별키를 K_{di}라 하고, 평문(plaintext)P에 대한 암호화함수를 E(P), 암호문(ciphertext) C에 대한 복호화 함수를 D(C)라 하면 암호문 C 및 복호문 P의 생성 알고리듬은 다음과 같다.

암호화 : $E(P) = C \equiv P^{K_{ei}} \pmod{n_i}$ ·····(2-1)

복호화 : $D(C) = P \equiv C^{K_{di}} \pmod{n_i}$ ·····(2-2)

P 와 C 를 대신하여 M 이라 하면

$$E(D(M)) = D(E(M)) = M \cdots\cdots(2\text{-}3)$$

$$M^{K_{ei} \cdot K_{di}} \equiv M \pmod{n_i} \cdots\cdots(2\text{-}4)$$

2.2 키의 생성법

RSA암호방식의 개별키(K_{ei}, K_{di}, n_i)는 다음과 같은 과정을 통해 얻어 진다.

(1) 임의의 서로다른 큰 소수(prime) p_i, q_i 를 선택하여, n_i 를 계산한다.

$$n_i = p_i q_i \cdots\cdots(2\text{-}5)$$

(2) p_i-1 과 q_i-1 의 최소공배수인 L_i(LCM(p-1),(q-1)) 와 서로소이고, 이것보다 적은 임의 정수 K_{ei} 를 선택한다.

(3) 다음식을 풀어 K_{di} 를구한다.

$$K_{ei} \cdot K_{di} \equiv 1 \pmod{L_i} \cdots\cdots(2\text{-}6)$$

3. 개별통신 및 방송통신시스템에 적합한 암호방식

개별통신이란 망 가입자간 일대일 또는 통신단말간 지점대지점통신을 말하며, 방송통신이란 1개의 망가입자 또는 통신단말이 다수의 망가입자 또는단말과 동시에 통신하는 것을 말한다. 개별통신시스템에서는 일대다수 방송통신이 곤란하고 방송통신시스템에서는 일대일개별통신의 비밀성을 보장하지 못하는 단점이 있다 본장에서는 방송통신시스템에서 개별통신의 비밀성을 보장하면서 지정된 가입자그룹의 모든 가입자에게 방송통신을 할 수 있는 암호방식을 제시한다.

3.1 방송통신시스템에 적합한 암호방식의 마스터 키 요구조건[4]

일반적으로, 암호화키와 복호화키가 동일한 비밀키 암호방식을 이용한 통신망에서 마스터키라 함은 각각의 개별키를 암호화하기 위한키를 지칭하지만, 본 논문에서의 마스터키는 RSA 암호방식의 모든 개별키 대신에 사용할 수 있는 키를 말하며, 비밀키암호에서의 마스터키와는 개념이 다르다. 따라서, 본 논문에서의 마스터키라 함은 비밀키

암호방식에서와는 달리 개별 및 방송통신시스팀에서의 모든 개별키 대신에 이용될 수 있는 키 이다. 암호화 함수 E, 복호화 함수 D를 가진 암호 시스팀에서, m개의 개별키K_i에 대한 마스터키 K_M의 존재조건은 다음과 같다.

(1) 모든 평문 P와 암호문 C에 대해, 다음이 성립한다.

$$E_{K_M}(P) = E_{K_i}(P) \quad (i = 1,2,\cdots m) \cdots\cdots (3\text{-}1)$$

$$D_{K_M}(C) = D_{K_i}(C) \quad (i = 1,2,\cdots,m) \cdots\cdots (3\text{-}2)$$

(2) 마스터키의 길이는 각 개별키의 길이에 대해· 다음 관계가 성립한다.

$$|MK| \leq m \cdot |K_i| \quad \cdots\cdots (3\text{-}3)$$

여기서 |MK|:마스터키의 bit수이고 $|K_i|$:개별키의 bit수이다.

3.2 RSA암호방식에서의 마스터키[5]

RSA암호방식은 두종류의 키가 존재한다. 즉, 암호(복호)시 멱승하는 멱지수키 $K_{ei}(K_{di})$와 법성분 n_i가 있다. 이것을 구분하기 위하여 멱지수에 대한 마스터 키를 멱지수마스터키라 하고, 법성분에 대한 마스터키를 법마스터키라 칭한다.

(1) 멱지수마스터키

마스터키와 각 개별키와의 관계는 임의의 평문 P와 암호문C 에 대해, 식(3-1),(3-2)이 성립해야 하므로, RSA암호방식에서의 암호화(복호화)멱지수마스터키 K_{eM} (K_{dM})과 암호화(복호화)개별키 K_{ei} (K_{di})간에는 다음관계식이 성립한다.

$$P^{K_{eM}} \equiv P^{K_{ei}} (\mathrm{mod}\ n_i) \cdots\cdots (3\text{-}4)$$

$$C^{K_{dM}} \equiv C^{K_{di}} (\mathrm{mod}\ n_i) \cdots\cdots (3\text{-}5)$$

P와 C를 M, K_{eM}과 K_{dM}을 K_M, K_{ei}과 K_{di}를 K_i로 대치하면 식(3-4), (3-5)의 일반형은 다음과 같다.

$$M^{K_M} \equiv M^{K_i} (\mathrm{mod}\ n_i) \cdots\cdots (3\text{-}6)$$

즉; 어떠한 평문(암호문)에 대해서도, 임의의 암호화(복호화)개별키에 의해 암호(복호)한 결과와 마스터키에 의한 암호화(복호화)한 결과가 같아야 한다. 식(3-6)가 성립하는 구체적인 조건들을 검토하여, 멱지수마스터키의 존재조건들을 도출한다. $n_i = p_i \cdot q_i$이므로 식(3-6)은 다음과 같이 나눌 수 있다.

$$M^{K_M} \equiv M^{K_i} (\mathrm{mod}\ p_i) \cdots\cdots (3\text{-}7)$$

$$M^{K_M} \equiv M^{K_i} (\mathrm{mod}\ q_i) \cdots\cdots (3\text{-}8)$$

윗식은 다음과 같이 쓸수있다.

$$K_M \equiv K_i (\mathrm{mod}(p_i - 1)) \cdots\cdots (3\text{-}9)$$

$$K_M \equiv K_i (\mathrm{mod}(q_i - 1)) \cdots\cdots (3\text{-}10)$$

식(3-6)이 어떠한 $M(0 \leq M \leq \min(n_1, n_2, \cdots, n_m)-1)$에 대해서도, 성립할 필요충분조건은

식(3-9)와 (3-10)을 동시에 만족해야 하므로, 식 (3-9),(3-10)을 동시에 만족하는 식을 구하면,

$$K_M \equiv K_i \pmod{L_i} \qquad (L_i = LCM((p_i-1),(q_i-1))) \cdots\cdots\cdots (3\text{-}11)$$

이 된다. 따라서, 식(3-11)을 m개의 개별키 $K_i, (i = 1,2,\cdots,m)$에 대해서 멱지수마스터키가 존재할 조건은 $i = 1,2,\cdots,m$에 대한 ${}_mC_2$개의 연립합동식을 만족하는 K_M, K_i가 존재할 때이다. 식(3-11)의 임의의 두 식 $i,j(i \neq j, 1 \le i,j \le m)$을 뽑으면, 다음과 같다.

$$K_M \equiv K_I \pmod{L_I} \cdots\cdots\cdots (3\text{-}12)$$

$$K_M \equiv K_j \pmod{L_j} \cdots\cdots\cdots (3\text{-}13)$$

윗식은 다음과 같이 나타낼 수 있다.

$$K_M = K_i + AL_i \cdots\cdots\cdots (3\text{-}14)$$

$$K_M = K_j + BL_j \cdots\cdots\cdots (3\text{-}15)$$

(단, A,B는 임의의 정수)

각 개별키의 관계를 알기 위하여, K_M을 소거하면,

$$K_i - K_j = BL_j - AL_i \cdots\cdots\cdots (3\text{-}16)$$

이다. 식 (3-16)이 정수해 A,B를 갖기 위한 조건은 $K_i - K_j$가 L_i와 L_j의 최대공약수(GCD)로 나누어 질 때이다. $GCD(L_i,L_j) = d$라 하면, $d|(K_i - K_j)$이므로, K_i 와 K_j의 관계는 다음과 같이 쓸수 있다.

$$K_i \equiv K_j \pmod{d} \cdots\cdots (i \neq j, 1 \le i,j \le m) \cdots\cdots\cdots (3\text{-}17)$$

식(3-17)를 만족하는 개별키 $K_i, (i = 1,2,\cdots,m)$ 에 대해, 식(3-11)은 다음과 같이 쓸 수 있다.

$$\begin{aligned} K_M &\equiv K_1 \pmod{L_1} \\ K_M &\equiv K_2 \pmod{L_2} \\ &\vdots \\ K_M &\equiv K_m \pmod{L_m} \end{aligned} \qquad \cdots\cdots\cdots (3\text{-}18)$$

그러므로, 식 (3-11)은 중국인 잉여정리에 따라 K_M은 존재하며, $LCM(L_1,L_2,\cdots,L_m)$을 법으로 하여, 오직 한개 존재한다.

RSA암호방식에서 암호화개별키와 복호화개별키의 관계는 식(2-6)와 같다. 각 개별키와 멱지수마스터키와의 관계식(3-11)으로 부터 다음과 같이 쓸수 있다.

$$K_{eM} \equiv K_{ei} \pmod{L_i} \cdots\cdots\cdots (3\text{-}19)$$

$$K_{dM} \equiv K_{di} \pmod{L_i} \cdots\cdots\cdots (3\text{-}20)$$

식(3-19),(3-20)을 개별키 생성조건식(2-6)에 대입하면 다음과 같다.

$$K_{eM} \cdot K_{dM} \equiv 1 \pmod{L_i} \cdots\cdots\cdots (3\text{-}21)$$

1부터 m까지의 모든 i에 대해서 식(3-21)가 성립하는 조건식은 중국인잉여정리에 의해, 다음과 같이 쓸 수 있다.

$$K_{eM} \cdot K_{dM} \equiv 1 \pmod{LCM(L_1,L_2,\cdots,L_m)} \cdots\cdots\cdots (3\text{-}22)$$

즉, K_{eM}, K_{dM}중 한개가 존재하면, 나머지하나도 존재한다.

이상과 같은 멱지수마스터키와 개별법성분 n_i를 이용하여 디지틀서명이 가능하다. 디지틀 서명이 가능한 조건은 식(2-3), (2-4)가 성립할 때이다. 이때, 암호화개별키와 복호화개별키의 관계는 식(2-6)이다. 멱지수 마스터키와 개별키와의 관계식 (3-19),(3-20)을 식(2-6)에 각각 대입하면, 다음식이 성립한다.

$$K_{ei} \cdot K_{dM} \equiv 1 \pmod{L_i} \cdots\cdots (3\text{-}23)$$

$$K_{eM} \cdot K_{di} \equiv 1 \pmod{L_i} \cdots\cdots (3\text{-}24)$$

식(3-21)에서 K_{eM}과 K_{dM}의 관계식은 $K_{eM} \cdot K_{dM} \equiv 1 \pmod{L_i}$이므로, 다음의 어떠한 조합에서도 디지틀 서명이 가능하다.

(가)암호화 개별키 K_{ei} 와 복호화 마스터키 K_{dM}

(나)암호화마스터키 K_{eM} 과 복호화 개별키 K_{di}

(다)암호화마스터키 K_{eM} 과 복호화마스터키 K_{dM}

즉, 다음식이 성립한다.

$$M^{K_{ei} \cdot K_{dM}} \equiv M \pmod{n_i} \cdots\cdots (3\text{-}25)$$

$$M^{K_{eM} \cdot K_{di}} \equiv M \pmod{n_i} \cdots\cdots (3\text{-}26)$$

$$M^{K_{eM} \cdot K_{dM}} \equiv M \pmod{n_i} \cdots\cdots (3\text{-}27)$$

(2) 법 마스터키

멱지수 마스터키($K_{eM} \cdot K_{dM}$)를 사용시, m개의 개별법성분 n_i에 관한 마스터키 n_M 을 유도한다. 식(2-5)에서 $n_i = p_i \cdot q_i$이므로,

$$M^{K_{eM} \cdot K_{dM}} \equiv M \pmod{p_i} \cdots\cdots (3\text{-}28)$$

$$M^{K_{eM} \cdot K_{dM}} \equiv M \pmod{q_i} \cdots\cdots (3\text{-}29)$$

로 분해할 수있다. 이들 2m개의 식중 서로 다른 소수를 법으로한 합동식만 모으면, 중국인잉여 정리에 의해 다음식을 얻을 수있다.

$$M^{K_{eM} \cdot K_{dM}} \equiv M \pmod{n_M} \cdots\cdots (3\text{-}30)$$

$$n_M = LCM(n_1, n_2, \cdots\cdots, n_m) \cdots\cdots (3\text{-}31)$$

$$0 \le M \le \min(n_1, n_2, \cdots\cdots, n_m) - 1 \cdots\cdots (3\text{-}32)$$

n_M은 개별법성분 n_i의 배수이기때문에, n_i에 대해 다중화가 가능하다. 즉, 멱지수마스터키($K_{eM} \cdot K_{dM}$)를 사용할 경우, 법의 개별키 n_i 대신에 n_M을사용하여도 원래의 평문을 얻을 수있다. 여기서 n_M을 개별 법성분 n_i에 대한 법마스터키라 한다. 이후에서는 마스터키라함은 멱지수마스터키와 법마스터키를 모두 가르킨다.

3.3 마스터키의 안전성

본절에서는 전절에서 구한 마스터키의 안전성을 검토한다.

(1) 멱지수마스터키의 안전성

$K_{dM} \equiv K_{di} \pmod{L_i}$ ($L_i = LCM((p_i-1),(q_i-1))$로 부터, 다음과 같이 K_{dM}을

구할 수가 있다.

$$K_{dM} = K_{di} + T_i \cdot L_i (T_i는\ 임의의\ 정수) \cdots\cdots\cdots (3\text{-}33)$$

사용자 i가 p_i, q_i 를 알고 있다면, 자신의 비밀키 K_{di} 를 이용하여, K_{dM}을 구할 수가 있다. 그러므로, 마스터키의 안전성을 보장하기 위해서는 p_i, q_i 는 마스터키 관리자 (masterkey manager, 이하에서는 MM이라 칭한다)만이 생성 및 보관해야 한다. 또한, $K_{eM} \equiv K_{ei} (\mathrm{mod}\ L_i)$는 공개되어 있으므로, $K_{eM} - K_{ei} = RL_i$(R은 임의의 정수)가 되어 $K_{eM} - K_{ei}$가 인수분해된다면 L_i 가 추정될 수 있다. L_i 가 추정된다면 K_{ei}로 부터 K_{di} 가 쉽게 계산되어 안전성이 파괴된다. 이것을 방지하기 위해, 모든 i 에대해,

$$K_{eM} = K_{ei} \cdots\cdots\cdots (3\text{-}34)$$

로 하면 $K_{eM} - K_{ei} = 0$ 이 되어 L_i를 계산하는 것이 불가능하다. 즉, 공개암호화키는 개별키와 마스터키를 동일하게 하여 공개한다. 이렇게 해도 복호화 개별키 K_{di}를 추정하기 위해서는 $K_{ei} \cdot K_{di} \equiv 1 \pmod{L_i}$($L_i = LCM((p_i-1),(q_i-1))$를 계산해야 한다. 이식을 계산하기 위해서는 L_i 를 구해야하므로, 이것은 n_i를 소인수분해해서 p_i, q_i를 구해야 가능하다. n_i를 소인수분해하는 것은 계산량적으로 불가능하기 때문에 K_{di}를 추정하는것은 불가능하다. 또한 식(3-34)같이 해도 복호화마스터키와 복호화개별키와의 관계는 $K_{dM} \equiv K_{di} (\mathrm{mod}\ L_i)$이므로 안전상 문제가 없다.

(2) 법마스터키의 안전성

RSA암호 체계는 법성분 n_i의 소인수분해 어려움에 기초를 둔 암호이므로 법마스터키 n_M으로 부터 개별법성분 n_i의구성요소인 p_i, q_i가 구해진다면 이것을 이용하여 복호화키가 쉽게 구해지므로 곤란하다. 그러므로 법마스터키 n_M과 p_i, q_i의관계를 검토할 필요가 있다. $n_M = LCM(n_1, n_2, \cdots, n_m)$, $n_i = p_i \cdot q_i$에서 p_i, q_i는 소수이므로, 각사용자의 법성분을 구성하는 총 2m개의 서로다른 소수만으로 n_M 을 구성한다면,

$$n_M = LCM(n_1, n_2, \cdots, n_m) = \prod_{i=1}^{m} n_i \cdots\cdots\cdots (3\text{-}35)$$

가 된다. 이때는 n_M 으로 부터 p_i, q_i를 추정하기는 불가능하나 이중 일부가 중복될 경우를 검토한다. m=2 인 경우에 일부중복, 전부중복되는 경우로 나누어서 검토한다.

$p_1 = p_2$, $q_1 \neq q_2$와 같이 일부중복된 경우, $n_M = LCM(n_1, n_2) = p_1 \cdot q_1 \cdot q_2$가 된다. $n_1 \cdot n_2 / n_M = p_2$, $n_1 / p_2 = q_1$, $n_2 / p_2 = q_2$가 쉽게 구해져, n_1 과 n_2의 소인수 분해값이 구해지게 된다.

$p_1 = p_2, q_1 = q_2$와 같이 전부중복되는경우는 $n_M = LCM(n_1, n_2) = n_1 = n_2$ 가 된다. 이경우는 법성분을 인수분해할 수는 없으나 $L = L_1 = L_2$가 되어 $K_{dM} \equiv K_{d1} (\mathrm{mod}\ L(=L_1=L_2))$, $K_{dM} \equiv K_{d2} (\mathrm{mod}\ L(=L_1=L_2))$가 되어, 모든 멱지수 개별키가 멱지수마스터키인 것을 의미한다. 따라서 p_i, q_i를 일부 또는 전부중복시키는 것은 안전상 부적합하다. 그러므로 각 법성분의 요소 p_i, q_i는 서로소인 것이 가장 바람직하며, 이때, n_M은 식(3-35)가 된다.

3.4 마스터키 관리

암호체계의 안전성은 비밀키의 적절한 보호 관리를 전제로 하기 때문에, 키관리는

실제응용측면에서 매우 중요하다. 키의 관리는 생성,분배,보호관리의 세단계로 구분할 수 있다. 특히, 키의 생성자, 키생성에 필요한 정보의 소유자가 누구냐에 따라, 키관리의 안전성에 큰 차이가 있기 때문에, 마스터키 관리의 안전성을 검토할 필요가 있다.

(1) 마스터키의 생성

마스터키는 MM이 기본키정보(p_i,q_i)와 개별키(K_{ei},K_{di})를 바탕으로 하여 생성한다.

(2) 기본키정보(p_i,q_i)와 개별키(K_{ei},K_{di})의 생성

기본키정보(p_i,q_i)와 개별키(K_{ei},K_{di})의 생성은 사용자 또는 MM이 할 수 있으나, 기본키정보(p_i,q_i)와 개별키(K_{ei},K_{di})를 사용자가 직접 생성할 경우에는 MM이 마스터키를 생성하기 위해, 모든 가입자가 기본키정보(p_i,q_i)를 MM에게 송신해야 하기 때문에 통신량이 많아진다. 또한, 각각의 이용자가 기본키정보(p_i,q_i)를 알고 있기 때문에 법마스터키가 증복되었을 경우, n_i를 소인수 분해하는 경우가 생기므로 안전상 타당하지 않다. 그러므로, 마스터키와 기본키정보(p_i,q_i)와 개별키(K_{ei},K_{di})는 MM이 일괄 생성하여 K_{ei},K_{eM},n_i,n_M 은 공개화일에 등록하고, p_i,q_i,K_{dM},는 비밀리에 보관하며, 비밀개별키 K_{di}만을 각 이용자에게 송신하는 방법이 바람직하다.

이상을 종합하면, 이용자와 각 키들의 억세스관계는 그림 3-1과 같다.

3.5 마스터키의 생성법

마스터키의 생성은 다음과 같은 방법에 의해 생성한다.

(단계 1) 법마스터키 안전조건인 n_i가 서로소가 되도록, 소수 p_i,q_i($1 \le i \le m$)를 선택한다.

(단계 2) 멱지수마스터키 안전조건 $K_{eM} = K_{ei}$와 RSA 기본원리식(2-6)를 만족하도록, K_{eM}, K_{di}, K_{ei}를 구한다.

(단계 3) (단계 2)에서 구한 K_{eM}을 이용하여 식(3-22)을 만족하는 K_{dM}을 구한다.

이상의 도출순서를 이용하여 간단한 예를 들어보면 다음과 같다.

표 3-1. 개별키

	p_i	q_i	K_{ei}	K_{di}	n_i
R_1	569	887	773	241533	504703
R_2	823	677	773	86981	557171
R_3	479	907	773	20729	434453
R_4	857	503	773	197901	431071

표 3-2. 표 3-1.의 개별키를 가진 그룹에 대한 마스터키

그룹	가입자	K_{eM}	K_{dM}	n_M
1	R_1, R_2, R_3, R_4	773	12162600028214237717	5266426138305009161 6719
2	R_1, R_2, R_3	773	529566665110949	122170736103913489
3	R_2, R_3, R_4	773	368575988536325	10437034559037873
4	R_1, R_4	773	2902472749	217562826913

3.6 마스터키의 응용

(1) 개별암호통신 및 방송암호통신

마스터키와 개별키의 정합성을 이용하여, 일대일 개별통신 및 다수 가입자에게 동시에 방송암호통신을 할 수 있다. 지정된 가입자 그룹에 대한 마스터키와 개별법성분은 공개되어 있기 때문에 임의의 송신자가 송신국이 된다.

(가) 개별암호통신

임의의 송신자 S는 공개되어있는 멱지수마스터키 K_{eM}과 각가입자의 개별법성분n_i를 이용하여 다음순서로 개별통신할 수 있다.

(단계 1) 송신국 S는 평문 P를 공개되어 있는 멱지수마스터키 K_{eM} 와 개별법성분 n_i을 이용하여 암호화하여 송신한다.

$$C = P^{K_{eM}} \pmod{n_i}$$

(단계 2) 수신국 i는 수신된 암호문 C를 자신의 비밀키 K_{di}와 n_i를 이용하여 복호화하여 평문 P를얻는다.

$$P = C^{K_{di}} \pmod{n_i}$$

이때, i를 제외한 타수신국도 암호문 C를 수신할 수 있지만, K_{di}를 알 수 없기 때문에 P를 얻을 수 없다.

(나) 방송암호통신

방송암호통신시에는 송신국은 평문 P를 마스터키(K_{eM}, n_M)으로 암호화하여 송신하면, 수신국은 자신의 법성분 n_i로 분리한후 복호화 D 를 수행하여 평문 P를 얻는다. 통신순서는 다음과 같다.

(단계 1) 송신국 S는 평문 P을 암호화마스터키 ($n_M, K_{eM},$)를 이용하여 암호화하여 송신한다.

$$C = P^{K_{eM}} \pmod{n_M}$$

(단계 2) 각 수신국은 수신된 C 를 다중분리화한다.

$$C_i = C \pmod{n_i}$$

(단계 3) 수신국은 자신만 알고 있는 복호화키 K_{di}를 이용한 복호화로 평문을 얻는다.

$$P = C_i^{K_{di}} \pmod{n_i}$$

(2) 마스터키를 이용한 디지틀 서명

RSA암호방식에서 식(2-3)이 성립하기 때문에 디지틀서명이 가능하다. 마스터키를 이용하면 개별통신뿐만 아니라 방송통신에서 일대 다수 디지틀서명이 가능하다.

(가) 개별통신에서의 디지틀서명

임의의 송신자는 공개되어 있는 멱지수 마스터키 K_{eM}과 개별법성분 n_i를 이용하여 일대일 개별통신에서 디지틀서명 및 인증이 가능하다. 디지틀서명을 위한 통신순서는 다음과 같다.

(단계 1) 임의의 송신국 S는 인증이 필요한 통신문 P를 자신만 알고 있는 비밀복호화키 K_{do}, n_o로 복호화하여 서명문 P_s를 생성한다.

$$P_s = P^{K_{do}} \pmod{n_o}$$

(단계 2) 송신국 S는 공개된 멱지수마스터키 K_{eM} 과 수신국의 법성분 n_i를 이용하여 암호화하여 송신한다.

$$C = P_s^{K_{eM}} \pmod{n_i}$$

(단계 3) 수신국 R_i는 수신된 암호문 C를 자신의 비밀복호화키 K_{di}, n_i를 이용한 복호화에 의해 서명문 P_s를 구한다.

$$P_s = C^{K_{di}} \pmod{n_i}$$

(단계 4) 수신국 R_i은 공개되어 있는 송신국의 암호화키 K_{eo}, n_o를 이용하여 P_s를 암호화하여 통신문 P를 얻는다.

$$P = P_s^{K_{eo}} \pmod{n_o}$$

(나) 방송통신에서의 일대다수 디지틀서명

마스터키(K_{eM}, n_M)를 이용하면 방송통신에서 일대다수 디지틀 서명이 가능하다. 통신순서는 다음과 같다.

(단계 1) 임의의 송신국 S는 인증이 필요한 통신문 P를 자신의 비밀복호키 K_{do} 로 복호화하여 서명문 P_s를 구한다.

$$P_s = P^{K_{do}} \pmod{n_o}$$

(단계 2) 송신국 S는 공개된 마스터키 (n_M, K_{eM})를 이용하여 서명문 P_s를 암호화하여 송신한다

$$C = P_s^{K_{eM}} \pmod{n_M}$$

(단계 3) 각 수신국 R_i는 C를 수신하여 n_i로 다중분리화한다.

$$C_i = C \pmod{n_i}$$

(단계 4) 수신국 R_i는 자신의 비밀복호화키 K_{di}를 이용하여 복호화하여 서명문 P_s를 구한다.

$$P_s = C_i^{K_{di}} \pmod{n_i}$$

(단계 5) 수신국 R_i는 공개되어 있는 송신국의 개별키 (K_{eo}, n_o)를 이용하여 암호화하여 통신문 P를 구한다.

$$P = P_s^{K_{eo}} \pmod{n_o}$$

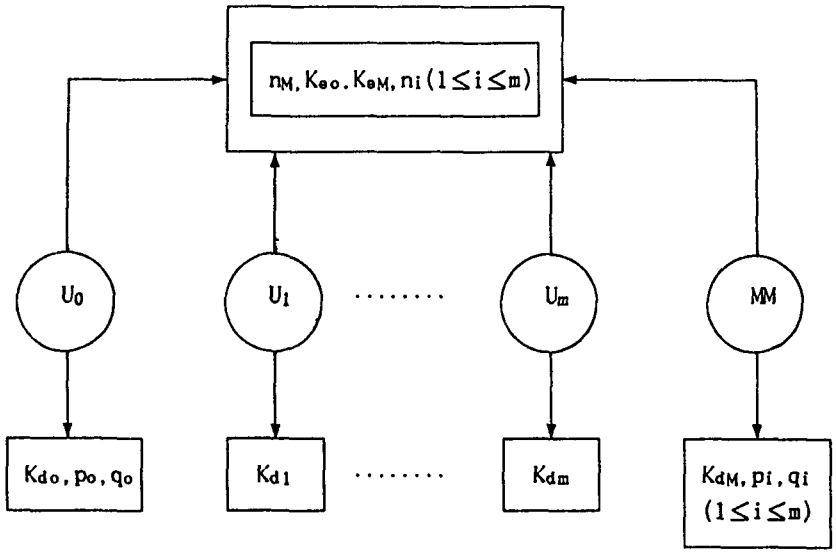
4. 결론

최근 통신망이 다방면으로 발전함에 따라 위성통신망 및 근거리통신망에서 일대일통신을 기반으로 하는 개별통신 및 일대다수통신망을 기반으로하는 방송통신에 대한 요구가 증대되고 있으며 이들 시스팀상에서의 정보보호를 목적으로 하는 연구역시 활발히 진행되고 있다.

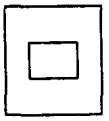
본 논문에서는 개별통신 및 방송통신을 동시에 수행할 수 있을 뿐만아니라 정보보호를 위한 암호방식으로서 RSA 마스터키암호방식을 적용하였다.RSA마스터키암호방식은 개별통신과의 정합성이 좋으며 키관리가 편리하고 암호의 안전성은 RSA암호방식과 동일한 정도의 안전성이 있는 방송암호통신방식임을 보였다. 본 논문에서 제안된 방식은 위성 및 근거리통신망에서의 암호시스팀에 직접 적용될 수 있을 것으로 기대된다..

참 고 문 헌

1. 李晩榮 : "公開키 暗號시스템에 관한 硏究" 通信情報保護學會紙, 제1권 제 1 호, pp 94-99 (1991), 제1권 제2호,pp 63-75 (1991)
2. Rivest. R.L, Shamir.A, and Adleman.L: "A method for obtaining digital signatures and public key cryptosystem," Commun. ACM, 21, 2, pp 120-126(1978).
3. Kent, S.T : "Security requirement and protocals for a broadcast scenario." IEEE Trans. Commun. COM-29, 6, pp 778-786(1981)
4. Dorothy.E, DENNING, Fred B, Schneider : "Master keys for group sharing." Inform Proc. Letters, Vol 12, No1.(1981)
5. 池野, 小山 : "現代暗號理論" 電子通信學會(1986)



U_0 : 임의의 이용자
$U_i((1 \le i \le m)$: 그룹내이용자


: public key


: secret key

*. 기본키 정보(p_i, q_i, K_{ei}, K_{di})및 마스터키(n_M, K_{eM}, K_{dM})는 마스터키 관리자가 생성

*. n_M, K_{eM}, n_i는 공개화일에 등록하고 개별 비밀키 K_{di}는 각 가입자에게 비밀통신채널을이용 송신

그림 3-1. 암호키의 관계도