韓國通信情報保護學會誌
第1卷, 第1號, 1991. 4

암호방식과 키 분배

원 동 호*

1. 서 언

컴퓨터의 급속한 보급과 전기통신기술의 발달로 컴퓨터 네트워크의 진전과 함께 명실상부한 종합 정보시스템이 구축되고 있으며 이러한 정보시스템의 보급 확대로 우리 사회는 고도 정보화 사회로 진입되고 있다.

이에 따라 정보시스템의 사회적 중요성은 한층 높아지고 있으며 이러한 정보시스템의 정상적인 기능 유지는 건전하고 효율적인 사회를 건설하는데 무엇보다 중요한 요소가 되고 있다.

정보화 사회란 컴퓨터와 정보통신 기술이 결합하여 정보의 축적, 처리, 전달 능력이 획기적으로 증대되면서 정보의 가치가 산업사회에서의 물질이나 에너지 이상으로 중요해지는 사회로 정보가 상품으로서의 가치를 인정받아 시장에서 유통되는 사회를 말한다.

이러한 정보시스템 내에서 처리, 축적, 전달되는 정보는 전기적 현상을 이용하여 디지탈화, 대용량화 되고 있어 정보에 대한 적절한 보호조치가 없으면 전송, 처리 혹은 기억 장치에 보관된 상태에서 불법 유출, 삭제 및 수정 등의 위험에 노출되기 쉽다[1,2]. 이러한 원치않는 불법적인 사고로 인하여 프라이버시가 침해될 뿐만 아니라 막대한 경제적 손실을 당할 우려가 있어 정보보호에 대한 관심이 고조되고 있다.

정보시스템상에서의 정보보호를 위한 대책으로는 설비면에서의 물리적 대책, 관리 운영면에서의 인적 자원에 대한 대책, 기술면에서의 대책, 법과 제도면에서의 대책 등이 있을 수 있다. 이 가운데 가장 경제적이면서도 보안 수준에 따라 효율적이고 계층적인 보안 대책을 제공할 수 있는 방법이 기술적인 면에서의 정보보호 대책인 암호방식을 이용하는 방법이다[3].

암호방식은 암호키의 분배와 관리방법에 따라 관용 암호방식(conventional cryptosystem)과 공개키 암호방식(public key cryptosystem)으로 나눌 수 있다. 관용 암호방식은 암호화 키와 복호화 키를 공통으로 사용하는 방법으로 암호계 사용자는 사전에 암호키를 나누어 갖고 있어야 한다. 한편 공개키 암호방식은 암호화 키와 복호화키를 분리하여 복호화키는 비밀리에 간직하고 암호화키를 공개하는 방식이다[4].

암호방식이란 보호하려는 정보를 작은 길이의 암호키로 관리하는 것이라 말할 수 있다. 따라서 암호방식에서 효율적인 정보보호를 위해서는 암호키를 안전하게 관리해야 한다.

암호키 관리는 키생성과 폐기를 비롯하여 키의

* 정회원, 성균관대학교 정보공학과 부교수

분배 및 보관으로 나누어 생각할 수 있는데 이중 가장 문제가 되는 것이 제삼자(침해자)에게 암호키를 노출되지 않게 분배하는 것이다. 특히 분배해야 할 암호키가 많은 대규모 암호통신망과 신규 가입자가 수시로 변동되는 환경에서는 암호키를 제삼자로부터 안전하게 분배하는 것이 커다란 문제로 부각되고 있다.

본고에서는 암호방식에서의 암호키의 성질을 살펴보고 키의 안전한 분배를 위한 대표적인 암호키 분배방식을 소개하고 그 특징을 고찰한다.

2. 암호방식

정보란 추상적인 개념을 갖고 있으나 정보는 그 내용인 정보내용과 정보내용을 지니고 전달하는 정보 캐리어로 나누어 생각할 수 있다. 정보 캐리어에는 부호, 주파수, 시간, 공간, 물질 등의 다양한 모양을 갖고 있다. 예를 들어 정보 캐리어가 부호라 해도 이 정보를 전송하는데는 여러가지의 부호가 있을 수 있어 동일한 정보내용도 외관상 서로 다른 캐리어로 전달할 수 있다.

즉 암호방식이란 정보내용과 정보 캐리어 사이에 존재하는 다양성을 이용하여 정보내용과 정보캐리어의 대응관계를 침해자에게 비밀로 하여 정보를 교환하는 방법을 말한다[1]. 따라서 비밀정보를 교환하려고 하는 사람은 정보내용과 정보캐리어 사이의 대응관계인 암호키를 사전에 나누어 갖고 있어야 한다.

정보의 전달과정에서 정보를 제삼자로부터 보호하기 위한 암호방식의 기본 구성은 그림 1과 같다.

비밀정보를 전달하려는 송신자는 보통의 평문 M을 암호화 알고리즘 E와 암호화키 K_e를 이용하여 암호문 C를 생성시켜서 공중통신 채널을 통하여 상대 수신자에게 전달한다. 수신자는 공중통신 채널을 통해서 전송된 암호문 C를 수신하여 복호화 알고리즘 D와 복호화키 K_d를 이용하여 송신자가 보내고자 했던 평문 M을 얻는다.

만일, 제삼자가 공중통신 채널을 통해 전송되는 암호문 C를 가로채게 되더라도 복호화 알고리즘 D와 복호화키 K_d를 알지 못하면 암호문 C로부터 평문 M을 얻을 수 없어 정보를 보호받을 수 있다.

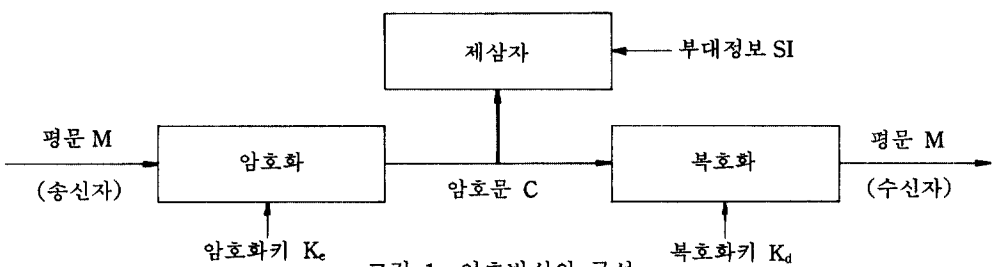

그림 1. 암호방식의 구성

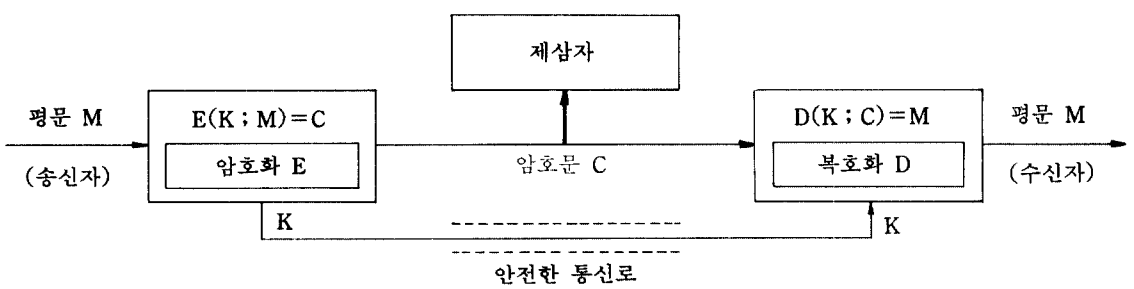

그림 2. 관용 암호방식

그러나 제삼자가 평문의 성질을 알고 있으면 암호문 C의 통계적 성질과 그 밖의 부대정보 SI(Side Information)를 이용하여 암호문 C에서 평문 M을 얻으려고 노력한다. 이와 같이 제삼자의 위협으로부터 정보를 보호하는 것을 암호기술이라 한다.

암호기술이 목표로 하는 정보보호는 다음 세가지로 분류된다[1].

1. 정보의 보호(secrecy) : 불법적인 정보내용의 노출을 방지하고 합법적인 상대자에게 안전하게 정보내용을 전달한다.

2. 정보 인증(authentication) : 송신자가 보낸 정보내용이 불법조작 없이 합법적인 상대에게 전달되도록 한다.

3. 사용자 인증(user authentication) : 정보내용을 교환하는 상대방을 확인한다.

한편, 기억을 정보의 시간적인 통신이라 간주하면 위의 세가지 암호기술은 데이타 베이스 시스템에 그대로 적용시킬 수 있다.

실제로 암호방식은 위의 세가지 정보보호를 기본으로 시스템 엑세스 제어의 고도화, 전자우편의 배달증명, 전기통신에 의한 무기명 투표, IC 카드의 정보보호, 소프트웨어의 부정사용 방지 등 다양한 정보보호 방법으로 유력하다.

가. 관용 암호방식

관용 암호방식은 공통키 암호방식, 또는 공개키 암호방식에 대응되는 비밀키 암호방식이라 불리우는 암호방식으로 그림 2와 같이 비밀정보를 교환하고자 하는 상호 암호통신망 가입자는 사전에 비밀 공통키 K를 제삼자에게 노출되지 않게 나누어 가진 다음, 암호통신을 필요로 할 때 평문 M을 암호 알고리즘 E와 공통키 K로 암호문 C를 생성시켜 공중통신 채널을 통해서 전달하고 암호문 C를 수신한 가입자는 복호화 알고리즘 D와 공통키 K로 평문 M을 얻는 방법으로 오래전부터 사용되어 온 암호방식이다.

관용 암호방식에서 암호강도를 결정하는 암호화 알고리즘 E와 복호화 알고리즘 D는 다음 세가지 조건을 만족해야 한다. 여기서 알고리즘이란 입출력 대응관계만을 문제로 하는 함수가 아니라 입력으로부터 출력을 계산하는 방법과 그 과정을 말한다. 입력 K, M의 알고리즘 E의 출력을 E(K ; M)으로 표시한다.

조건 1. D(K ; E(K ; M))=M이 임의의 공통키 K에 대해서 항상 성립해야 한다.

조건 2. 알고리즘 E, D가 임의의 입력에 대해서도 출력을 계산하는 계산량이 적어야 한다.

조건 3. 공통키 K에 대해서 i), ii)의 성질을 갖는 임의의 알고리즘 e_k, d_k를 알고리즘 E, D와 부대정보 SI로부터 계산하는 계산량이 충분히 커야 한다.

성질 i) $e_k(M)=E(K ; M)$, $d_k(C)=D(K ; C)$가 모든 M, C에 대해서 성립해야 한다.

성질 ii) e_k, d_k의 계산량이 적어야 한다.

여기서, 부대정보 SI에는 평문 M의 정보원 성질, 약간의 노출된 평문 M에 해당하는 암호문 C 등 여러가지가 있을 수 있다.

마지막 조건 3)은 알고리즘 e_k와 d_k를 구하는 계산량이 많을 것을 요구하지만 이것은 우리가 현재 갖고 있는 지식으로는 논리적인 입증이 대단히 어려운 일이다. 다만 조건 3)의 만족여부는 경험적으로 판단할 수 밖에 없다.

조건 1), 2)를 만족하는 알고리즘 E, D를 대칭 암호방식(symmetric cryptosystem)이라 하고, 부대정보 SI에 대해서 대칭 암호방식 E, D가 조건 3)을 만족할 때 SI에 대해서 안전하다고 한다.

따라서, 임의의 부대정보 SI_0에 대해서 현재 안전한 알고리즘 E, D가 언제까지 안전하다고 할 수 없다. 만일 알고리즘 E, D가 조건 3)의 성질 i), ii)를 만족시키는 e_k, d_k가 발견되면 그 순간 알고리즘 E, D는 부대정보 SI_0에 대하여 안전성을 잃게 되며 흔히 알고리즘 E, D가 부대정보 SI_0에 의해 해독되었다고 한다.

또한 알고리즘 E, D로 구성되는 대칭 암호방식이 모든 부대정보 SI에 대하여 안전하다면 알고리즘 E, D를 암호통신망 가입자가 비밀로 할 필요없이 공개할 수 있다. 암호 알고리즘을 공개한다는 것은 매우 중요한 의미를 갖는다. 즉 많은 암호통신망

가입자들이 암호시스템을 공동으로 사용할 수 있으며 알고리즘 E, D를 실현하는 장치의 제작단가가 저렴해진다.

물론 암호 알고리즘 E, D가 부대정보 SI에 대해서 안전하다고 해도 알고리즘 E, D를 비밀로 하는 것이 암호시스템이 보다 안전하다는 것은 말할 나위가 없다. 공개된 암호 알고리즘 E, D의 안전성은 오로지 암호키를 바꾸어 사용함으로써 보장받기 때문에 암호키의 생성, 보관 및 분배에 신중을 기해야 한다.

이러한 대칭암호인 관용 암호방식에는 문자의 치환을 이용한 환자식 암호(substitution cipher)로 단순환자암호(simple substitution), 동음이의환자암호(homophonic substitution), 다표식환자암호(polyalphabetic substitution), 철자환자암호(polygram substitution)와 문자의 전치를 이용한 전치식암호(transposition cipher)로 단순 전치암호(simple transposition), Nihilist 암호 등이 있으며, 암호강도를 향상시키기 위해 환자식 암호와 전치식 암호를 혼합한 적암호(product cipher)로 ADFGVX 암호를 비롯한 무라사끼 암호, DES(Data Encryption Standard) 등이 있다[5].

관용 암호방식은 암호통신망 가입자가 n명일 때 서로 교환해야 할 공통키의 수가 $n(n-1)/2$으로 가입자의 증가에 따라 키의 수가 급증하여 공중통신망을 이용한 암호시스템 구축에 키분배가 문제가 된다. 따라서 적절한 암호키 분배방식을 필요로 한다.

나. 공개키 암호방식

공개키 암호방식은 관용 암호방식과 달리 암호화키와 복호화 키를 분리하여 암호화 키는 암호통신망 가입자 모두에게 공개하고 복호화 키는 가입자 각자가 비밀리에 보관하는 방법으로 구성은 그림 3과 같다.

공개키 암호방식은 그림 3과 같이 암호통신망 가입자 전체가 암호화키 Y_i와 복호화키 X_i 한 쌍을 생성시켜 암호화키 Y_i는 공개화일에 등록하고 복호화키 X_i는 가입자 모두가 비밀리에 보관한다. 따라서 암호화키 Y_i는 공개키, 복호화키 X_i를 비밀키라고 한다.

암호통신을 하려는 암호통신망 가입자는 공개화일에서 암호통신의 상대 가입자의 공개키 Y_i를 제

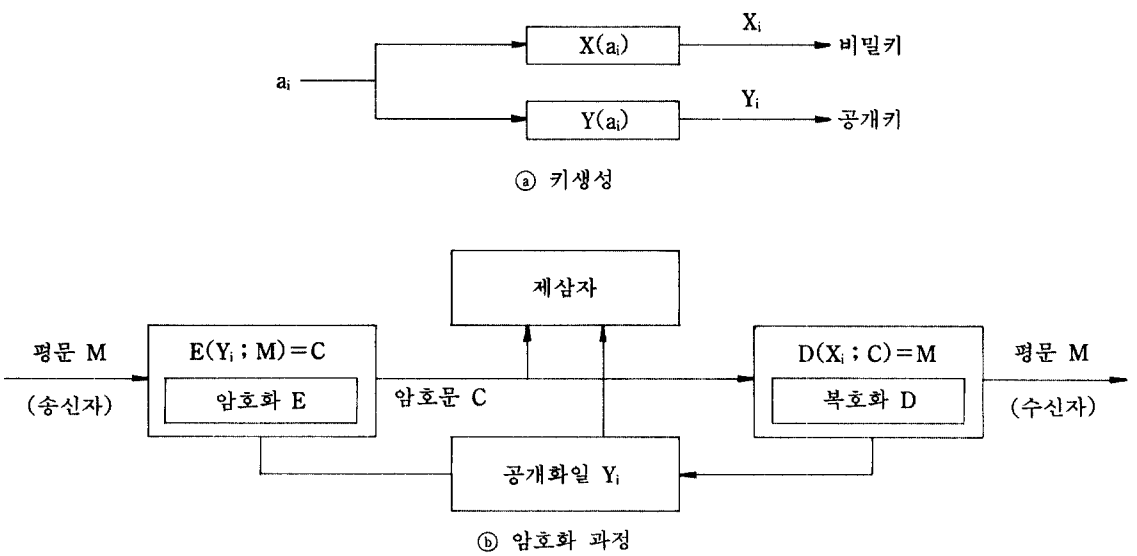

그림 3. 공개키 암호방식

공받아 그 공개키로 평문 M을 암호화하여 암호문 C를 전송하면 상대 가입자는 이를 수신하여 자신이 비밀리에 보관하던 복호화키 X_i로 평문 M을 복원한다. 물론 이때 가입자의 공개키 Y_i로부터 그에 대응하는 복호화키 X_i를 간단히 구할 수 없어야 한다.

공개키 암호방식에서 비밀키와 공개키 생성을 위한 알고리즘 X, Y와 암호화와 복호화를 위한 알고리즘 E, D는 다음 조건을 만족해야 한다.

조건 1. D(X(a) ; E(Y(a) ; M))=M이 임의의 값 a, 임의의 평문 M에 대하여 성립해야 한다.

조건 2. 알고리즘 E, D, X, Y가 임의의 입력에 대해서도 출력을 계산하는 계산량이 적어야 한다.

조건 3. 모든 a에 대해서 성질 i), ii)의 알고리즘 d_a를 (E, D, Y, X, Y(a))와 부대정보 SI로부터 계산하는 계산량이 충분히 많아야 한다.

성질 i) $d_a(C)=D(X(a) ; C)$가 모든 C에 대해서 성립해야 한다.

성질 ii) d_a의 계산량이 적어야 한다.

조건 1), 2)를 만족시키는 알고리즘 E, D와 X, Y를 제 일종 비대칭 암호방식(asymmetric cryptosystem of the first kind)이라 한다. 제 일종 비대칭 암호방식 E, D와 X, Y가 부대정보 SI에 대하여 조건 3)을 만족시키는 경우 알고리즘 E, D와 X, Y는 SI에 대하여 안전하다고 한다.

공개키 암호방식으로 구성된 암호통신망 가입자는 암호화 키와 복호화키 두개가 필요하게 되므로 전체 가입자가 n명일 때 암호키의 수는 2n개이고, 실제로 비밀리에 보관해야 하는 복호화키의 수는 n개로 각 가입자가 자기 소유의 복호화키 하나만을 보관하게 되므로 관용 암호방식 보다 보관해야 할 키의 수가 적고 또한 암호화키를 공개하므로 키 분배가 필요없어 키 관리가 용이하다. 그러나 공개키 암호방식도 문제가 없는 것은 아니다. 예를 들어 암호통신망 가입자 A가 가입자 B를 사칭하여 공개화일에 암호화키를 등록하면 B에게 전송되어야 할 비밀정보가 A에게 전송된다. 따라서 공개키 암호방식에서는 공개키 화일관리가 매우 중요한 문제가 된다.

지금까지 발표된 공개키 암호방식에는 소인수 분해의 어려움을 이용한 RSA 암호방식과 Rabin 암호방식, Knapsack 문제를 이용한 MH Knapsack 암호방식과 Graham-Shamir 암호방식, 선형 오류정정부호를 복호화할 때의 어려움을 이용한 McEliece 암호방식 등이 있다[5,6,7,8].

3. 암호키 분배

암호방식이란 보호하려는 정보를 작은 길이의 암호키로 관리하는 것이라 말할 수 있다. 현대 암호에서는 암호 알고리즘을 공개하고 있지만 관용 암호방식의 암호화 키와 복호화 키는 물론 공개키 암호방식에서도 복호화키는 비밀로 하고 있다[4].

따라서, 비밀로 해야 하는 암호키의 관리방법이 매우 중요한 과제 중의 하나가 되고 있다. 암호키 관리는 키 생성, 키 분배, 키 보관 및 폐기 등으로 나누어 생각할 수 있는데 이중 가장 중요한 것은 제삼자에게 노출되지 않도록 키를 암호통신 상대자에게 분배하는 문제이다.

암호키 분배방식으로 가장 간단하고 안전한 방법은 사람이 직접 키를 전달하는 방법이나 암호통신망 가입자 증가에 따른 보조를 맞출 수 없을 뿐만 아니라 시간 지연이 문제가 되고 있다.

암호키 분배 절차에서 이러한 문제점을 해결하기 위한 방안으로 암호키 분배방식이 제안되었다. 관용 암호방식에서는 암호통신망 가입자 증가에 따른 암호키 증가문제를 해소하고 키 분배의 동시성을 갖는 암호키 분배방식으로 키 분배소(KDC : Key Distribution Center)를 이용한 방식과 이산대수문제를 이용한 공개키 분배방식이 제안되었다. 또한 공개키 암호방식에서의 암호화 키를 등록한 공개화일의 관리문제를 해결하기 위한 방안으로 ID 정보에 의한 키 분배방식이 제안되었다[9].

가. 중앙 집중식 키분배

중앙집중식 키 분배방식은 KDC를 설치하여 암호통신망 가입자가 비밀통신을 할 때마다 KDC로부터 암호화에 사용할 세션키(SK : Session Key)를 분배받는 방식으로 관용 암호방식의 공통키와

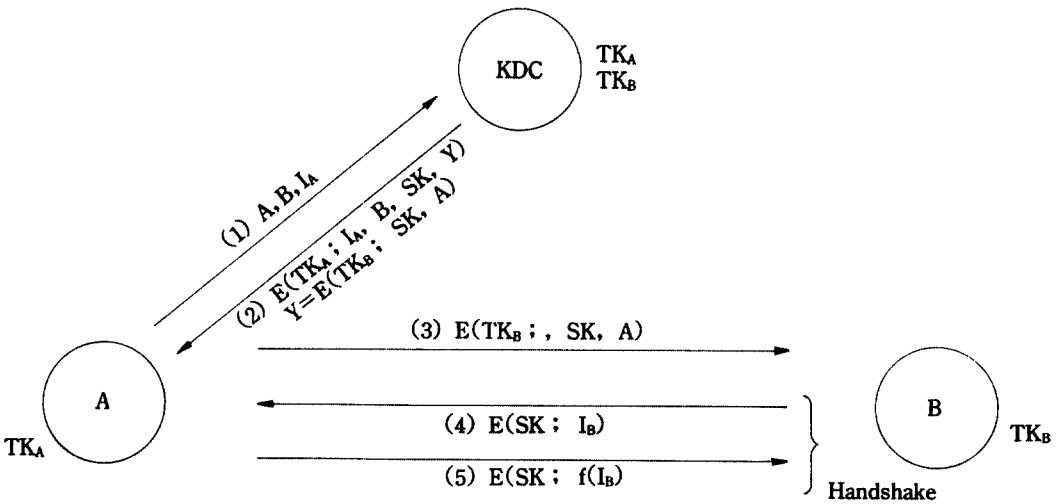

그림 4. 공통키 분배

공개키 암호방식의 공개키를 KDC가 분배해준다[10, 11].

관용 암호방식으로 구성된 암호통신망에서는 공통키 분배를 위해서 사전에 KDC에 가입자 모두가 터미날키(TK : Terminal Key)를 하나씩 비밀리에 등록해야 한다.

암호통신망 가입자 A가 B와 암호통신을 원할 때 A B간의 세션키인 공통키를 KDC로부터 분배받기 위한 순서는 그림 4와 같다.

먼저, 가입자 A는 KDC에 B와의 암호통신을 요청한다. 이때 I_A는 A가 KDC와의 통신에서 이전의 통신이 아님을 확인하기 위해 추가한 확인정보이다.

순서 1. A → KDC : A, B, I_A

KDC는 A로부터 전송된 통신요구에 따라 암호통신을 원하는 A, B의 터미날키 TK를 확인하고 A, B간에 세션키로 사용할 공통키 SK를 생성하여 A에게 순서 2)의 메시지를 전송한다.

순서 2. B →A : $E(TK_A; I_A, B, SK, E(TK_B; SK, A))$

여기서 TK_A와 TK_B는 A와 B의 터미널키이다. 가입자 A는 KDC로부터 송신된 메시지를 TK_A로 복호화하여 자신이 요청한 B와의 암호통신 요구에 대한 KDC의 응답임을 메시지 내용의 I_A와 B로 확인한다.

가입자 A는 공통키 SK를 보관하고 TK_B로 암호화된 부분을 가입자 B에게 전송한다.

순서 3. A → B : $E(TK_B; SK, A)$

가입자 B는 A로부터 수신한 메시지를 자신의 TK_B로 복호화하여 메시지가 KDC로부터 전송되었다는 것과 암호통신 상대자 A, 그리고 공통키 SK를 확인할 수 있다. 이상으로 가입자 A, B간에는 통신세션키 SK로 암호통신을 할 수 있다.

그러나 가입자 B는 가입자 A로부터의 수신 메시지 순서 3)이 이전에 사용된 메시지를 제삼자가 다시 사용한 것인지를 확인할 수 없으므로 가입자 A가 전송한 사실을 핸드쉐이크 과정을 통하여 확인해야 한다.

순서 4. B → A : $E(SK; I_B)$

순서 5. A → B : $E(SK; f(I_B))$

가입자 B는 핸드쉐이크 식별자 I_B를 공통키 SK로 암호화한 메시지를 A에게 전송한다. 이를 수신한 가입자 A는 SK로 복호화하여 I_B를 대입한 A, B만이 알고 있는 함수값 $f(I_B)$를 SK로 암호화하여 B에게 전송한다. 가입자 B는 A로부터의 전송 메시지에서 $f(I_B)$ 값을 확인하여 제삼자의 개입 여부를 확인한

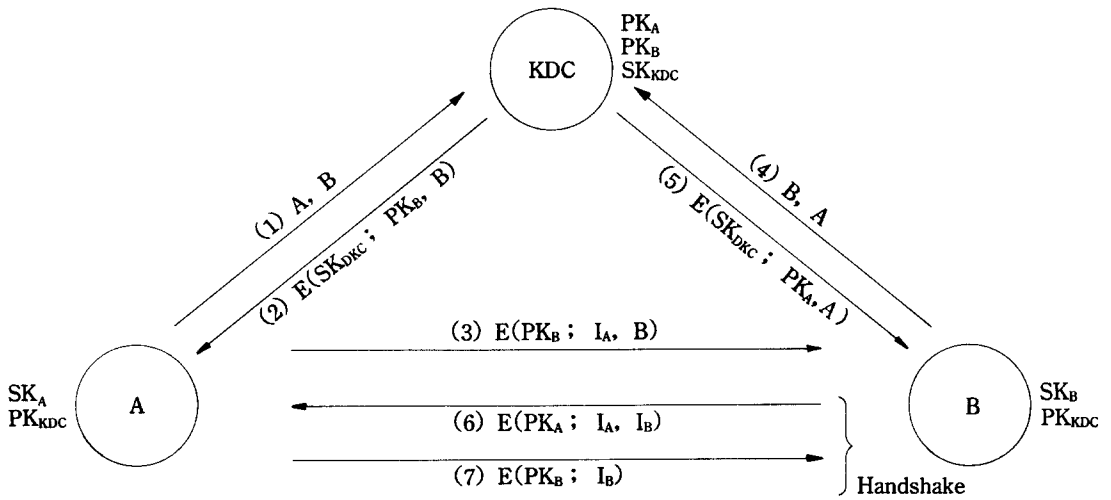

그림 5. 공개키 분배

다.

이 관용 암호방식도 한번 사용한 공통키 SK와 핸드쉐이크 함수가 노출되면 제삼자로부터의 개입을 막을 수 없어 Time stamp를 추가하는 방법으로 제삼자의 개입을 막을 수 있다[11].

공개키 암호방식에서의 공개키는 공개화일에 등록하여 암호통신망 가입자 전체에게 공개하는 것이 원칙이나 공개키 화일에 제삼자가 위장 등록 공개하는 경우 암호통신 정보가 노출될 위험이 있다. 따라서 KDC가 가입자의 공개키의 등록과 갱신을 관리하고 가입자가 암호통신을 원하는 상대 가입자의 공개키를 공급한다[10].

PK_A와 SK_A가 가입자 A의 공개키와 비밀키이다. 공개키의 분배절차는 그림 5와 같으며, 그 순서는 다음과 같다. A는 KDC에게 암호통신 대상 가입자 B의 공개키를 요구한다.

순서 1. A → KDC : A, B

KDC는 가입자 A의 요구에 따라 B의 공개키 PK_B를 자신의 비밀키로 암호화하여 전송한다.

순서 2. KDC → A : $E(SK_{KDC}; PK_B, B)$

SK_{KDC}는 KDC의 비밀키이며 이에 대응되는 공개키 PK_{KDC}는 모든 암호통신망 가입자에게 공개한다. 공개키 암호방식은 비대칭 암호방식으로 암호화 키와 복호화 키의 역할을 바꿀 수 있으므로 KDC로부터 비밀키 SK_{KDC}로 암호화해서 전송받은 메시지는 PK_{KDC}로 복호화하여 B의 공개키 PK_B를 얻을 수 있다. 이때 KDC가 가입자 B의 공개키 PK_B를 SK_{DKC}로 암호화하는 것은 PK_B를 보호하려는 것이 아니라 가입자 A에게 B의 공개키임을 확인시키기 위한 것이다. 즉 PK_B가 제삼자로부터 제공받은 것이 아님을 가입자 A는 확인할 수 있어야 한다.

다시 가입자 A는 KDC로부터 받은 상대 가입자 B의 공개키로 이전의 통신이 아님을 확인하는 I_A와 A를 암호화하여 B에게 보낸다.

순서 3. A → B : $E(PK_B; I_A, B)$

가입자 B는 자신의 비밀키 SK_B로 A로부터 수신한 메시지를 복호화하여 암호통신을 요청하고 있는 A를 확인하고 다시 KDC에게 가입자 A의 공개키 PK_A를 요구한다.

순서 4. B → KDC : B, A

순서 5. KDC → B : $E(SK_{KDC}; PK_A, A)$

순서 5의 암호화 과정은 순서 2)에서의 공개키 확인과정과 같다.

암호통신에 앞서 가입자 A와 B는 서로 상대방을 확인해야 할 필요가 있으므로 순서 6), 7)의 핸드

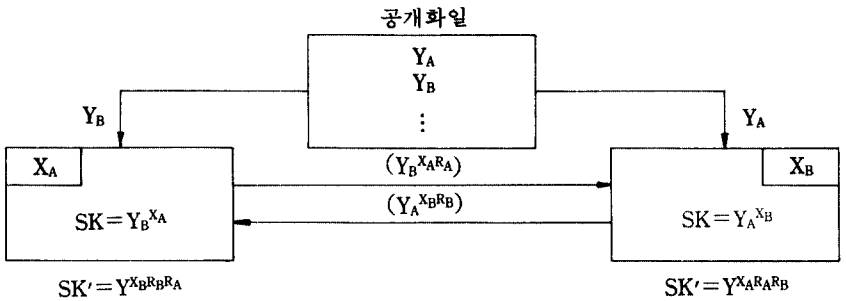

그림 6. 공개키 분배방식

쉐이크 과정을 거쳐야 한다.

순서 6. B → A : $E(PK_A ; I_A, I_B)$
순서 7. A → B : $E(PK_B ; I_B)$

나. 공개키 분배방식

앞에서 설명한 관용 암호방식의 세션키 분배에는 터미날키 분배문제와 가입자간의 암호통신에 앞서 세션키 분배를 위한 사전통신 등의 문제가 있다. 이러한 문제를 해결할 수 있는 방법이 공개키 개념을 이용하여 상대 가입자의 공개정보와 자신의 비밀정보로부터 관용 암호방식의 세션키를 얻는 방법으로 이 방법을 공개키 분배방식이라 한다[6, 12, 13].

이산대수 문제를 이용하면 공개키 분배방식을 실현할 수 있다. 그 실현방법만 간단히 설명한다.

암호통신망 가입자 A는 유한체 GF(P)상의 원소중 임의의 원소 X_A를 선택하여 $Y_A = g^{X_A} \bmod P$를 계산해서 공개화일에 등록한다. 여기서 g는 GF(P)상의 원시원소이고, Y_A는 가입자 A의 공개정보이다. 이때 공개화일의 공개정보 등록은 신뢰성이 있는 기관의 책임하에 이루어져야 한다.

공개키 분배방식에서 세션키 SK의 계산은 그림 6과 같이 가입자 A가 공개화일에서 통신을 원하는 상대 가입자 B의 공개정보 Y_B를 찾아 자신이 비밀리에 보관하고 있는 비밀정보 X_A를 멱승하면 세션키 SK를 얻게 된다.

$$SK = Y_B^{X_A} \bmod P = g^{X_B X_A} \bmod P$$

이 경우 세션키 SK는 공개정보의 변화가 없는 한 항상 일정하므로 장기간 이용시 제삼자에게 노출될 염려가 있다. 이것을 방지하기 위해 가입자 A는 $(Y_B^{X_A})$에 임의의 난수 R_A를 다시 멱승하여 가입자 B에게 전송한다. 가입자 B는 수신된 $(Y_B^{X_A})^{R_A}$에 자신이 선택한 난수 R_B를 멱승하여 세션키 SK′를 얻는다.

$$SK' = (Y_B^{X_A R_A})^{R_B} = g^{X_B X_A R_A R_B} \bmod P$$

마찬가지로 가입자 B도 $(Y_A^{X_B R_B})$를 가입자 A에 전송하면 가입자 A도 자신이 선택한 난수 R_A를 멱승하여 세션키 SK′를 얻는다.

$$SK' = (Y_A^{X_B R_B})^{R_A} = g^{X_A X_B R_B R_A} \bmod P$$

위와 같이 가입자 양측이 난수를 선택하여 멱승해 주면 통신할 때마다 다른 세션키 SK′를 얻을 수 있다[14].

다. ID 정보에 의한 키 분배방식

지금까지 설명한 키 분배방식은 암호통신을 하기 위해서 비밀 세션키를 KDC에서 제공받거나 자신이 직접 관리해야 하며, 공개키의 경우도 공개화일을 유지하거나 KDC에서 제공받는 문제점이 있다.

이러한 단점을 해결하기 위한 방법이 ID 정보에 의한 키 분배방식이다[9]. 이 방법은 세션키를 생성할 수 있는 ID 정보만을 가입자가 보관하고 암호통신을 할 때마다 각 가입자가 직접 세션키를 생성한다.

ID 정보에 의한 키 분배방식은 모든 가입자들이

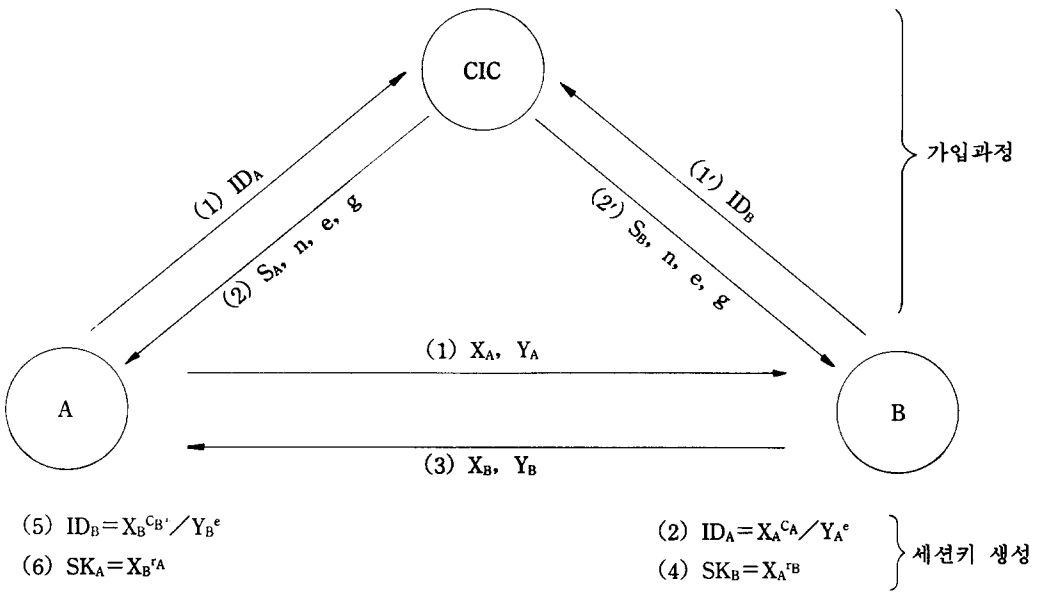

그림 7. ID 정보에 의한 키분배 방식

세션키를 생성할 수 있도록 카드발급센타(CIC ; card issue center)가 세션키 생성에 필요한 정보를 IC 카드에 수록시켜 발급하고 CIC는 폐쇄한다.

CIC는 소수 p, q를 생성하고 소수의 곱 $n = p \cdot q$와 다음 e, d를 결정한다.

$$e \cdot d = 1 \pmod{(p-1) \cdot (q-1)}$$

ID 정보에 의한 키 분배방식은 암호통신망 가입과정과 통신 세션키 생성과정으로 나누어 생각할 수 있다.

가입과정은 암호통신망에 가입을 희망하는 가입자의 신원을 확인한 후(ID_A, n, e, g, S_A)를 가입자 A의 IC 카드에 입력시켜 발급한다. 가입자 A의 ID는 ID_A로 $S_A = ID_A^{-d} \bmod n$이다.

순서 1. A → CIC : ID_A

순서 2. CIC → A : S_A, n, e, g

한편 가입자 A와 B 사이의 통신 세션키를 생성시키는 순서는 다음과 같다.

순서 1. A → B : $X_A = g^{e \cdot r_A} \bmod n$, $Y_A = S_A \cdot g^{c_A r_A} \bmod n$, Time

r_A는 가입자 A가 선택한 난수이고, c_A는 가입자 A, B만이 공유하는 hash 함수로 X_A, ID_A, ID_B와 Time을 변수로 하는 $c_A = \text{hash}(X_A, ID_A, ID_B, \text{Time})$이다.

순서 2. $ID_A = X_A^{c_A} / Y_A^e \bmod n$

가입자 B는 A에서 전송된 메시지로부터 가입자 A를 확인한다. 순서 2)의 값이 ID_A이면 A로부터의 암호통신 요청과 X_A, Y_A가 A로부터의 메시지 전송임을 알 수 있게 된다. 단 c_A'는 가입자 B가 hash 함수로 계산한 c_A 값이다.

마찬가지로 가입자 B도 난수 r_B를 선택하여 X_B, Y_B를 A에게 전송한다.

순서 3. B → A : $X_B = g^{e \cdot r_B} \bmod n$,
$Y_B = S_B \cdot g^{c_B r_B} \bmod n$

순서 4. $SK_B = X_A^{r_B} \bmod n = g^{e \cdot r_A r_B} \bmod n$

가입자 B는 순서 4)와 같이 세션키 SK_B를 계산한다.

가입자 A는 순서 5)와 같이 가입자 B로부터의 메시지를 확인한다.

순서 5. $ID_B = X_B^{c_B'} / Y_B^e \bmod n$

순서 6. $SK_A = X_B^{r_A} \bmod n = g^{e \cdot r_A r_B} \bmod n$

순서 6과 같이 가입자 A도 세션키 SK_A를 계산한다. 따라서 가입자 A, B는 순서 4)의 SK_B와 순서 6)의 SK_A로 서로 같은 공통 세션키를 얻게 된다. 위 과정을 그림으로 표시하면 그림 7과 같다.

4. 결 언

고도 정보화 사회의 급속한 도래에 따라 정보시스템내에서 축적, 처리, 전송되는 정보량이 급격하게 증가하고 있다. 이에 따른 개인의 프라이버시를 비롯한 각종 정보에 대한 보호와 인증문제가 중요한 과제로 부각되고 있으며, 정보시스템과 관련된 각종 범죄행위의 방지 대책은 건전한 정보화 사회 건설에 선결과제가 되고 있다. 이러한 문제를 해결하기 위한 방안으로 암호방식이 이용되고 있다.

정보를 보호한다는 측면에서 암호방식의 발전은 새로운 암호 알고리즘 개발과 함께 정보시스템에 암호방식을 적용시킬 때 문제가 되고 있는 유한체상의 고속 연산, 고속 소수판정, 암호표준화 등의 응용기술이 병행해서 연구 개발되어야 하며, 특히 대단위 암호통신망에서 문제가 되고 있는 암호키 분배방식이 함께 연구되어야 한다.

암호통신망 가입자가 증가하면 암호통신용 세션키를 분배하기 위한 사전통신과 그로 인한 시간지연, 상대방 확인 및 그 절차가 복잡해져 암호통신의 장해가 된다. 그러므로 암호통신 환경에 따라서 효과적이고 적절한 암호키 분배방식이 채택되어야 하며, 또한 암호통신 환경의 변화에 영향이 적고 신속한 암호통신과 효율성을 증대시킬 수 있는 암호키 분배방식이 연구되어야 한다.

參 考 文 獻

1. 今井秀樹, 松本勉, "暗號技術" テレビ"ョジン學會誌, Vol. 39, No. 3, pp. 1140-1147, 1985.

2. 一松信, "暗號の數理, 講談社, 1980.

3. 원동호, "암호학", 한국정보과학회, 정보통신연구회, 정보통신기술 4권, 1호, pp. 110-122, 1990.

4. D.W. Davies and W.L. Price, "Security for Compute Network," John Wiley & Sons. 1984.

5. 池野信一, 小山謙二, "現代暗號理論," 日本電子情報通信學會, 1987.

6. W. Diffie and M.E. Hellman, "New Direction in Cryptography," IEEE. Trans. Inform. Theory, Vol. IT-22, pp. 644-654, Nov. 1976.

7. R.C. Merkle and M.E. Hellman, "Hiding Information and Signatures in Trapdoor Knapsacks," IEEE Trans. Inform. Theory, Vol. IT-24, No. 5, pp. 525-530, Sep. 1978.

8. R.L. Rivest, A. Shamir and L. Adleman, "A Method for Obtaining Digital Signatures and Public Key Cryptosystem," Comm. ACM. Vol. 21, No. 2, pp. 120-126, Feb. 1978.

9. 岡本榮司, 田中和惠, "ID 情報に基つく 暗號鍵配送方式の提案," 電子情報通信學會, Vol. J72-D-I, No. 4, pp. 293-300, 1989.

10. R.M. Needham and M.D. Schroeder, "Using Encryption for Authentication in Large Networks of Computer," Comm. ACM, Vol. 21, No. 12, pp. 993-999, Dec. 1979.

11. D.E. Denning and G.M. Sacco, "Time stamps in Key Distribution Protocols," Comm. ACM. Vol. 24, No. 8, pp. 533-536, Aug. 1981.

12. 松本勉, 高嶋洋一, 今井秀樹, "古典的 PKDSと新しい PKDS," 電子通信學會 技術研究報告, IT 85-19, 1985.

13. 권창영, 원동호, "공개키 분배방식에 관한 연구," 한국통신학회, 논문지, 제 15권, 제 12호, pp. 981-989, 1990.

14. 岡本榮司・中村勝洋, "公開鍵 配送方式の 一檢討," 電子通信學會, 通信部門 全國大會, 講演論文集 (分冊 I), No. 15, 1984.

■ 著者紹介

원 동 호

1976년 成均館大學校 電子工學科 卒業(學士)
1978년 成均館大學校 大學院 電子工學科 卒業(碩士)
1988년 成均館大學校 大學院 電子工學科(博士)
1978년～1980년 韓國通信技術研究所 先任研究員
1985년～1985년 日本 東京工大 客員研究員
現 成均館大學校 情報工學科 副教授
관심분야 : 정보이론, 암호이론