정보화 사회와 암호

박 두석*, 권 창영*
(대유공업전문대학 사무자동화과*)

◀ 차 례 ▶

1. 서 론

현대는 정보의 검색/전송/처리/제어 등이 사회 전반의 경제 활동에 있어서 중추적 역할을 하는 사회이므로 언제 어디서든지 누구라도 필요한 정보를 손쉽게 그리고 신속하게 입수할 수 있어야 한다. 따라서 컴퓨터를 비롯한 정보화 기기를 이용한 정보처리 및 통신을 이용한 정보의 전송이 필요 불가결해지고 컴퓨터와 통신이 결합된 정보 시스템을 이용하지 않으면 안되게 되었다. 그 결과 필연적으로 문자 정보나 화상 정보 등이 전자 정보로 변환, 처리되는 추세이며 최근에는 모든 정보가 전자 정보화 되어 종이 없는(paperless) 사회로 진전되고 있으며 정보 시스템이 사회 전반에 확산되어 감에 따라 전자 정보의 가치가 높아져 전자 정보가 제품이나 에너지보다 우선하여 생산의 중심이 되고 있다[ETRI90]. 또한, 정보 시스템이 단독으로 활용되지 않고 대규모 네트워크로 구축되어 정보처리가 집중형으로 진전되고 있으며, 사무 자동화(office automation)가 기업의 핵심 전략이 되면서 최종 이용자가 자신의 정보관리를 하는 단계에 이르러 정보처리가 분산 처리형으로 진전되고 있다. 특히, 퍼스널 컴퓨터의 보급은 정보 통신의 보급에 커다란 기여를 했으며 비디오텍스나 PC통신 서비스가 일반화되면서 정보 엑세스의 대중화는 더욱 진전될 것이다.

고도 정보화 사회를 지탱하는 정보 시스템의 발달은 인류에게 생활의 편리함을 가져다 준

동시에 정보 시스템의 신뢰성과 안전성을 위협하는 기회 역시 늘어나고 있다. 정보 시스템에 이상이 발생했을 경우 사회에 미치는 영향에 대해서는 굳이 언급하지 않아도 될 것이다. 따라서 정보 시스템엣 신뢰성 및 안전성의 확보 즉, 정보 시큐리티는 매우 중요한 비중을 차지하며 정보화 사회를 지탱하는 주요한 요서가 되는 것이다.

정보 시스템 내에서의 정보 시큐리티는 설비면의 대책, 관리 운영면의 대책, 법 제도면의 대책, 기술면의 대책 등을 들 수 있으나 가장 안전하고 효과적이면서도 경제적인 방법은 기술적인 면의 대책인 암호 방식을 이용하는 것이다. 즉, 정보의 분실이나 도청으로부터 정보의 누출을 방지하고, 보안을 요구하는 정보의 보안 수준에 따라 효율적인 계층적 보안 대책을 제공하기 위해서는 암호 방식을 이용하는 것이 효과적이다. 즉, 암호 기술을 이용하여 시큐리티기능과 인증 프로토콜 기능이 보장된 정보 시스템을 통해 편리함을 향유하는 고도 정보화 사회를 이루어야 한다.

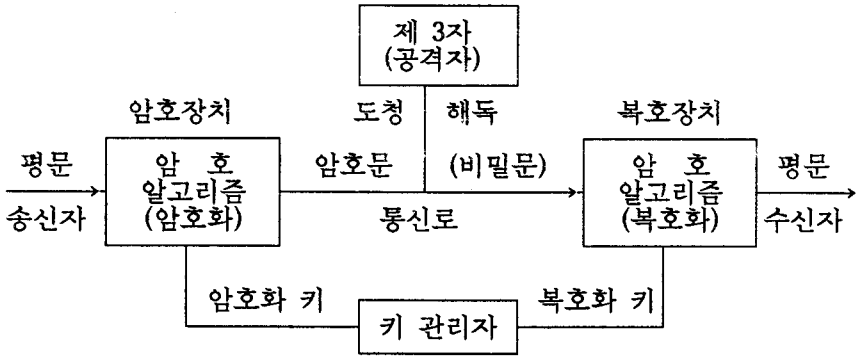
정보화 사회에서의 암호는 현대 사회의 특성에 비추어 전송 중 또는 축적 중인 가치 있는 정보를 보호하고 정보의 축적, 집중에 따른 플라이버시 침해를 방지하기 위해 필요하다. 또한, 정보 시스템에 대한 불법 엑세스를 막고, 다양한 전자 거래 결재를 안전하게 수행하기 위해 필요하다.

본고에서는 정보 시큐리티의 핵심이 되는 암호의 정의 및 기본 용어에 대하여 살펴보고, 실제 각종 암호 방식을 컴퓨터 네트워크상에서 효율적으로 제공하기 위하여 현대 암호 방식의 대표적인 방식인 관용 암호 방식, 공개키 분배 방식, 공개키 암호 방식의 성질을 분석하고 각각의 특성에 대하여 살펴본다.

2. 암호의 정의 및 기본 용어

미국의 FIPS(연방 정보 처리 규격)에 의하면 암호(cryptography)란 '평문을 해독 불가능한 형태로 만들거나, 암호화된 통신문을 해독 가능한 형태로 변환하기 위한 원리, 수단, 방법 등을 취급하는 기술 또는 과학'이라고 정의하고 있다. 또한, 1976년 Diffie, Hellman은 암호학을 '플라이버시(privacy)와 인증(authentication)의 두 가지 문제를 해결하기 위한 수학적 방식(mathematical system)에 관한 학문'이라고 전의했다[DH76].

암호학을 이론적 근거로 하여 생성된 여러 가지 암호 기법을 적용한 암호화 과정 및 복호화 과정으로 구성된 방식을 암호 방식이라 하며 송신자가 수신자에게 전송하려는 통신문(message)를 평문(plaintext)이라 하며, 평문을 그냥 보아서는 이해할 수 없는 암호문(ciphertext)으로 변환시키는 조작을 암호화(encipherment)라 한다. 역으로 암호문을 본래의 평문으로 바꾸는 조작을 복호화(decipherment)라 한다. 복호화는 정규의 수신자가 정규의 절차를 통하여 평문을 복원할 경우를 말하며, 부당한 제 3자 (도청자) 가 다른 수단을 통하여 평문을 추정하는 것을 암호 해독 (cryptanalysis)이라 한다.



[그림 2.1] 암호 방식의 기본 원리

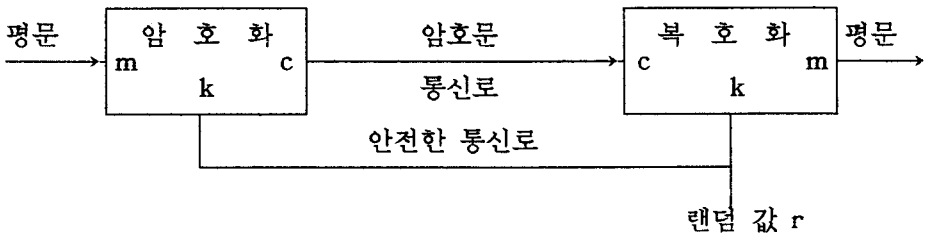
암호화와 복호화의 조작 원리를 암호 알고리즘이라 하며, 암호 알고리즘에 의한 변환을 제어하는 파라메터를 키(key)라고 한다. 일반적으로 하나의 암호계에서 아무리 많은 암호문을 입수할 수 있다고 하더라도 그 평문이 무엇인가를 확정하는데 있어서 충분한 정보를 얻지 못하면 그 암호계는 절대적으로 안전하다고 말하며 이 같은 암호계를 안전계라고 한다.

정보 통신 방식에서 정보를 공격자(제3자)로부터 보호하기 위한 암호 방식의 기본 원리는 그림2.1로 표시된다.

3. 관용 암호 방식

공개키 암호 방식이 발표되기 전의 암호 방식인 관용 암호 방식(conventional cryptosystem)은 암호화키와 복호화키가 동일하며, 두 사용자가 암호화키와 복호화키를 비밀리에 보관하여야 한다. 따라서, 관용 암호 방식을 공통키 암호 방식(common kiy crtptosystem)이라고도 하며 비밀키 암호 방식(secret key cryptosystem)이라고도 한다.

관용 암호 방식의 기본 원리를 그림으로 나타내면 다음과 같다.



[그림 3.1] 관용 암호 방식의 기본 원리

그림 3.1에서 암호화, 복호화 알고리즘(E, D)은 입출력 대응 관계만을 문제로 하는 함수가 아니라 입력으로부터 출력을 계산하는 방법과 그 과정을 말한다. 또한, E와 D는 식(3.1)과 같은 관계를 갖는다.

$$E^{-1} = D \qquad (3.1)$$

관용 암호 방식은 비보호 통신로를 통해 송신자 A가 수신자 B에게 메시지를 전송할 때 제 3자가 불법 유출을 못하도록 송신자 A는 평문 m를 암호화한다.

송신자 A의 암호화 과정은, 입력 (k ; m)으로부터 암호화 알고리즘 E의 출력을 E(k ; m)로 표시하면, 식(3.2)로 나타낼 수 있다. 즉, 암호화 과정의 결과로 암호문 c를 얻는다.

$$E(k ; m) = c \qquad (3.2)$$

수신자 B의 복호화 과정은, 입력(k ; m)으로부터 복호화 알고리즘 D의 출력을 D(k : c)로 표시하면, 식(3.3)으로 나타낼 수 있다. 즉, 복호화 과정의 결과로 평문 m를 얻을 수 있다.

$$D(k ; c) = D(k ; E(k ; m)) = m \qquad (3.3)$$

관용 암호 방식의 알고리즘은 암호화키 k를 알고 있는 합법적인 수신자는 암호문 c로부터 평문 m를 복호화할 수 있으나, 암호화키 k를 모르는 제 3자는 암호문 c로부터 평문 m를 복호화할 수 없도록 설계되어 있다.

관용 암호 방식은 암호화키와 복호화키가 동일하다. 즉, 정보의 송·수신자가 공유하는 비밀키(secret key)를 사용한다. 관용 암호 방식은 송·수신자 A와 B가 비밀키를 사전에 나누어 갖고 있어 A에서 B로 또는, B에서 A로 비밀 통신(secret communication)이 가능한 대칭 암호 방식(symmetric crytosystem)이다. 따라서 이 관용 암호 방식은 송·수신자 A, B를 구분할 필요가 없으며 양쪽 어느 방향으로도 안전한 통신로를 제공한다.

알고리즘 (E, D)는 송/수신자가 비밀로 할 필요 없이 공개할 수 있다. 여기서 암호 알고리즘을 공개한다는 것은 매우 중요한 의미를 갖는다. 왜냐하면 많은 사용자들이 암호 방식을 공동으로 사용할 수 있으며, (E, D)를 실현하는 장치의 제작 단가가 저렴해지기 때문이다.

물론 부대 정보 SI(Side Information)에 대하여 안전하다고 해도 알고리즘(E, D)를 비밀로 하는 것이 보다 안전한 것은 말할 필요가 없으며 공개된 알고리즘(E, D)의 안전성은 암호화키를 바꾸어 사용함으로써 보장받는다. 즉, 관용 암호 방식에는 암호 알고리즘을 비밀로 하는 방식과 암호 알고리즘은 공개하고 키(대응표)만을 비밀로 하는 방식이 있다. 그 동안 전자는 여러 가지 통계적 해독 방법이 연구 대상이 되어 왔으며[CP89], 후자의 대표적인 예는 DES(Data Encryption Standard)이다[NBS77].

관용 암호 방식은 전반적인 암호 기술이 충분히 축적되어 있으며 암호화 복호화의 계산량이 적어 처리 속도가 고속인 암호 장치 구현이 용이한 장점이 있으나, 송신자와 수신자가 동

일한 비밀키를 가지고 통신하기 때문에 사전에 키를 비밀리에 분배해야 하는 문제점이 있다. 그러므로 제 3자로부터 비밀키를 보호받기 위한 키 분배 방식이 필요하며, 이로 인한 비용의 증대와 지연 시간으로 통신 방식이 제한을 받게 된다. 또한, 불특정 다수 사이의 비밀 통신인 경우, 가입자가 n명일 때 비밀리에 보관해야 하는 암호화키는 n(n-1) / 2 이고 가입자 수의 증가에 따라 n2 지수 함수적으로 암호화키의 개수가 증가하므로 전자 메일 등 컴퓨터 네트워크의 이용자가 많은 경우에는 키 관리가 용이하지 않은 방식이다.

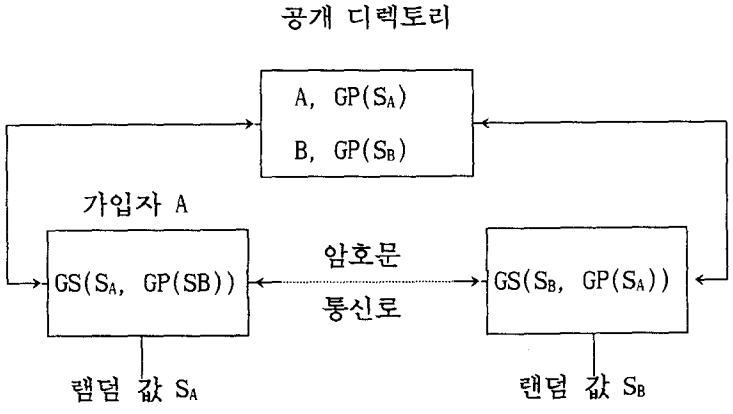
4. 공개키 분배 방식

관용 암호 방식은 송신자와 수신자가 동일한 비밀키를 가지고 통신하기 때문에 사전에 키를 비밀리에 분배해야 하는 문제점이 있다. Diffie,Hellman은 관용 암호 방식의 키 분배 문제를 해결하기 위한 방식으로 새로운 개념인 공개키 분배 방식이 제안되었다[DH76].

공개키 분배 방식의 기본 원리를 그림4.1로 나타내었다.

암호 통신망 가입자 A는 자기의 비밀 정보 SA와 공개 디렉토리에 등록된 상대 가입자 B의 등록 정보 PB로부터 공유 정보를 계산하여 공통키로 사용하는 방식으로 이 방식을 이용하면 관용 암호 방식의 암호화키를 컴퓨터 네트워크 등의 비보호 통신로를 통해 분배할 수 있다.

대표적인 공개키 분배 방식으로는 Diffie, Hellman의 공개키 분배 방식이 있는 데 이 방식은 제 3자의 암호 해독 노력이 지수 함수적으로 증가하며, 더욱이 암호화 키들의 사용을 정보의 공개 디렉토리 내로 제한시킬 수 있는 새로운 개념의 키 분배 방식을 제안하였다. 이 방식은 최초의 공개키 분배 방식이다.



[그림 4.1] 공개키 분배 방식의 기본 원리

이 방식은 유한체 GF(p)상의 이산 대수 계산의 어려움을 이용한 방식으로 먼저 각 가입자는 유한체 GF(p)상의 집합 { 0, 1, 2, ... , p-1 }에서 독립적으로 선택한 임의의 난수 Si 와 공개 정보인 위수가 p인 원시 원소 g를 이용하여 공개키 Pi를 계산한다. 가입자는 가입자의 이름, 주소 등과 함께 공개키를 공개 디렉토리에 등록한다.

$$P_i = GP(S_i) = g^{Si} \pmod p \quad (4.1)$$

가입자 A와 가입자 B가 비밀 통신을 원할 경우, 가입자 A는 공개 디렉토리에 있는 가입자 B의 공개키 PB와 자신의 비밀키 SA를 이용하여 다음과 같이 공통키 KAB를 계산한다.

$$K_{AB} = GS(S_A, P_B)$$
$$= GS(S_A, GP(S_B)) = g^{SASB} \pmod p \quad (4.2)$$

가입자 B도 같은 방법으로 공통키를 계산하며 가입자 A와 가입자 B는 공통키 KAB를 사용하여 비밀 통신을 할 수 있다.

이때 사용자 A와 사용자 B 이외에 제 3자가 KAB를 계산하려 할 경우에

$$Si = Logg\ Pi \pmod p \quad (4.3)$$

을 계산하여야 하는 데 그 계산량은 $O(\exp(c\sqrt{\ln p \ln\ln p}))$이므로, D-H방식의 안전성은 식(4.3)의 계산상 어려움에 근거한다. 이 방식은 공개 디렉토리를 변경하지 않는 한, 특정의 두 가입자 사이에 공유되는 키가 항상 동일하게 되어 시간에 대한 약점을 갖고 있다. 이런 방식을 이용한 비밀 통신의 안전성을 향상시키기 위하여 위의 약점을 보완한 Yamamoto-Akiyama 방식, Okamoto-Nakamura 방식, Matsumoto-Takashima-Imai 방식, Kwon-Won방식 등 다양한 공개키 분배 방식들이 제안되어 있다[MTI86, KW90].

공개키 분배 방식은 관용 암호 방식의 키 분배 문제를 해결한 최초의 공개키 개념의 방식이며, 가입자의 비밀키 S와 공개키 P로 구성되어 진다. (S, P)는 수학적으로 강한 연관성을 가지나 P에서 S를 계산하는 것은 불가능하다. 공개키 P는 비밀성(confidentiality)을 유지하기 위해 보호될 필요는 없다. 그러므로 공개키는 가능한 한 공개적으로 만들어져야 한다는 것이다. 그러나 공개키 방식은 이러한 공개성(publicity)때문에 공개키 디렉토리의 합법적인 공개키(true public key)를 비합법적인 공개키(false public key)로 대치하는 등의 능동적인 공격(active attack)에 부분적으로 공격당할 수 있다. 즉, 공개키 분배 방식은 관용 암호 방식의 키 분배 문제는 해결하였지만, 공개키 디렉토리를 관리해야 하는 새로운 문제점을 야기시켰다.

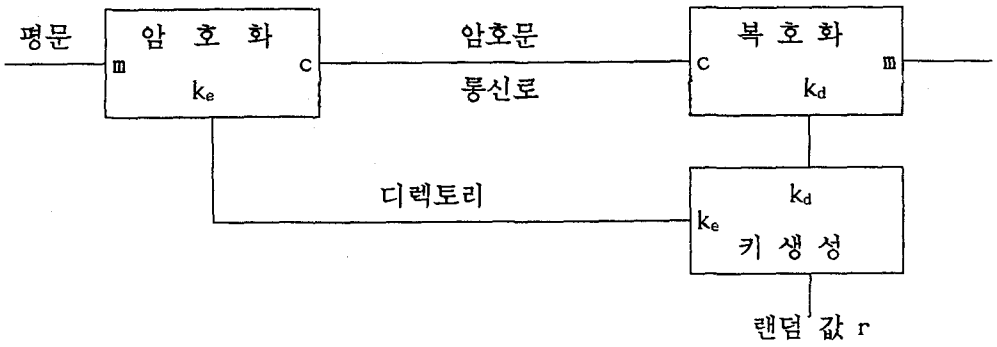
그러므로 공개키 디렉토리에는(S, P)와함께 가입자를 식별하기 위한 가입자의 개인 정보(identity 또는 identification string) I가 추가되어야 하며, P가 가입자 I의 공개키임을 보증하기 위한 가입자의 공개키 증명서(guarantee, certificate)G가 추가되어야 한다.

5.공개키 암호 방식

암호 학계는 1976년 Diffie, Hellman의 논문 'New directions in cryptography'의 발표로 놀랄만한 새로운 발전을 이루었다[DH76]. 그들은 수신자가 복호화 키만 비밀로 보관하고, 암호화키는 공개해도 암호계를 위태롭게하지않는 새로운종류의암호 방식인 공개키암호 방식(public key cryptosystem) 을 제안하여 관용 암호 방식의 키 전송 문제점을 해결하였다.

공개키 암호 방식은 송·수신자가 연관성 있는 서로 다른 두 개의 키를 이용하는 비대칭 암호 방식(asymmetric cryptosystem)이며 한쪽 방향의 비밀 통신만 제공한다. 다른 방향으로 통신을 시작하려면 새로운 한쌍의 키가 필요하다. 비대칭 암호 방식에서 두 통신자를 구분하기 위해 각각 송신자(sender) 수신자(receiver)라 부른다.

공개키 암호 방식의 기본 원리를 그림으로 나타낸 것이 그림 5.1이다.



[그림 5.1] 공개키 암호 방식의 기본 원리

공개 디렉토리에 등록된 가입자 A의 공개 정보 Ke를 공개키(암호화키),가입자 B의 비밀정보 kd를 비밀키(복호화키)라고 한다. 비밀키와 공개키를 생성하는 알고리즘을 각각 X,Y라 하고 암호화, 복호화 알고리즘을 E,D라 하자.

수신자의 공개 디렉토리의 등록 정보 ke 즉, 암호화키를 이용한 암호화 과정 및 수신자가 비밀리에 보관하고 있는 kd 즉, 복호화키를 이용한 복호화 과정은 다음과 같다.

$$E (ke ; m) = c \qquad (5.1)$$

$$D (kd ; c) = D (kd ; E (ke ; m)) = m \qquad (5.2)$$

암호화키와 복호화키는 큰 범위(영역)의 가능한 키들 중에서 동시에 선택되고 공개되어 있는 알고리즘 및 암호화키로부터 복호화키를 구할 수 없어야 하며 암호화키로 암호화한 암호문을 비밀키로 복호화할 수 있어야 한다. 그러므로 그림 5.1에서 보는 바와 같이 무작위 추출된 시드(randomly choosen seed)나 스타트 키(start key)인 r로부터 생성시켜야 한다. 한

편, 앞에서도 언급한 것처럼 많은 사용자들이 공동으로 사용하는 암호 방식을 구현하는 장비의 제작 단가를 낮추기 위해 각 알고리즘 E, D, X, Y 는 공개되어야 한다. 수신자의 X ,Y ,D 는 1개의 마이크로 칩 (micro-electronic chip)으로 구성하는 것이 이상적이다. 알고리즘 E, D, X, Y 는 공개되어 있으므로 복호화키 값은 칩의 해체를 시도하여 복호화키를 알려고 하는 경우 복호화키 값이 파괴되도록 하여야 한다. 즉, 수신자의 칩은 물리적 안전(physical integrity)을 보장하여야 하며 복호화 능력을 제공해야 한다[DP84].

공개키 암호 방식에서 평문을 암호화할 때 암호문이 평문보다 확장(expand)되지 않는 것이 유리하다. 즉, 평문 m과 암호문 c가 같은 범위의 값을 갖도록 하여야 한다[YA83,DP84]. 또한, 알고리즘 E, D에 적용되는 함수(function)는 동일(identical)하게 적용된다. 두 함수가 서로 다른 것은 단지 서로 다른 키를 사용하기 때문이다.

암호화키와 암호화 알고리즘이 공개되어 있으므로 불특정 다수가 이것을 이용하여 임의의 평문을 암호화하여 불특정 다수에게 전송할 수 있다. 따라서 수신자는 이러한 불법적인 통신문과 합법적인 송신자가 전송한 합법적인 통신문을 구별할 수 없게 된다. 또한, 침입자는 위조된 통신문 (bogus message)을 만들 수 있으며 방식은 침입자로부터 위조된 메시지가 전송되어 오는 것을 수신자에게 경계하도록 통보할 수 없다. 즉, 공개키 암호 방식은 관용 암호 방식의 키 전송 문제점은 해결하였지만, 송신자와 통신문의 합법성을 확인해야 하는 인증에 관한 새로운 요구가 대두된다. 그러나, 다양한 디지털 서명(digital signature)[Won94]을 이용하여 공개키 암호 방식의 인증에 관한 문제점을 해결할 수 있다.

공개키 암호 방식의 안전성에 관한 여러 가지 잠재적 문제점(potential problem)은 암호화키와 각종 알고리즘의 완벽한 공개에서 발생한다[DP84]. 공개키 암호 방식의 구체적 예로는 소인수 분해의 난점에 근거한 RSA 암호, Knapsack 문제에 근거한 Kmapsack 암호, 선형 오류 정정 부호의 일반적인 복원 문제에 근거한 McEliece 암호 등이 있다.

공개키 암호 방식에서는 복호화키만을 비밀로 하고, 암호화키는 공개해도 암호의 안전성은 확보할 수 있으므로 가입자 A,B간에 비밀키를 전송시킬 안전한 통신로는 필요하지 않다. 즉, 비밀키를 전화번호부와 같이 공개해도 무방하며 일반 통신 회선을 이용하여 동보 통신 형식으로 전송할 수 있기 때문에 키의 정기적 갱신 등의 키 관리가 매우 용이하다. 또한, n명이 상호 통신하는 방식에서도 필요한 키는 2n개이며 비밀 관리를 해야하는 복호화키는 n개 뿐이다. 즉, 공개키 암호 방식의 가장 큰 장점은 비밀키를 설립하기 위해서 안전한 통신로가 필요가 없다는 것과 비밀리에 관리해야 할 키의 개수가 적다는 것이다.

그러나, 공개키 암호 방식은 암호화 및 복호화의 계산량이 많아 처리 속도가 저속인 단점이 있으며 공개키의 전송은 가능성이 있는 여러 가지 위험 요소에 대한 많은 예방책이 필요하기 때문에 다루기 힘들고 비용이 많이 든다. 비밀키의 저장은 많은 위험 요소를 내포하고 있으며 공개키의 어떤 적용에 있어서 이러한 위험 요소들은 제거되어야 한다. 특히, 키가 다수의 장소에 저장 보관되어야 할 경우, 보안상 필요한 키의 이동은 막대한 비용이 요구된다.

6. 관용 암호 방식과 공개키 암호 방식의 조합

정보 보호 기술과 암호는 정보의 비밀을 지키는 기능이 있고, 송신되는 통신문의 송신자가 공격자가 아니라는 것을 수신자가 확인하는 기능이 있는데 이것에 주목할 필요가 있다.

이런 인증 기능의 실현은 관용 암호 방식을 사용하면 키의 분배가 곤란하고 수신자 자신이 디지털 서명의 위조가 가능하여 비효율적이고, 안전성도 높지 않다. 그러므로 비밀 통신망 내에서 불특정 다수가 전자 송금, 업무상 계약 등을 안전하게 행하려면 공개키 방식의 암호 기술을 이용하여야 한다.

관용 암호 방식은 공개키 암호 방식에 비하여 다음과 같은 장점이 있다.

관용 암호 방식의 역사는 매우 오래되었고, 전쟁 등 세계사의 격동기에 중요한 기능을 담당하며 발전하였기 때문에 전반적인 암호 기술이 충분히 축적되어 있으며 관용 암호 방식의 암호화 알고리즘 및 복호화 알고리즘은 계산적 안전성에 근거하는 공개키 암호 방식의 암호화 알고리즘 및 복호화 알고리즘은 계산적 안전성에 근거하는 공개키 암호 방식의 암호화 알고리즘 및 복호화 알고리즘에 비하여 비교적 간단하여 그 계산량이 적고, 처리 속도가 빠르다. 또한, 관용 암호 방식의 암호화 과정 및 복호화 과정의 계산량이 적으므로 적은 비용으로 암호화, 복호화 속도가 고속인 하드웨어 암호 장치를 비교적 간단히 구현할 수 있다.

공개키 암호 방식에서는 암호화키와 복호화키가 서로 다르며 암호화키는 공개하고 복호화키만을 비밀로 하는 방식이므로 관용 암호 방식에 비하여 다음과 같은 특징이 있다.

관용 암호 방식에서는 송신자와 수신자가 동일한 키를 가지고 비밀 통신을 하므로 사전에 키를 안전하게 분배하여야 한다.

그러나, 공개키 분배 방식에서는 암호화키를 공개적으로 분배하므로 키 전송 문제는 발생하지 않으며 암호화키는 비보호 통신로를 이용하여 전송할 수 있으므로 키 전송이 용이하다. 관용 암호 방식에서는 공중 통신망 내의 비밀 통신 가입자는 통신 상대방 전원의 많은 암호화키를 비밀리에 보관해야 하지만, 공개키 암호 방식에서는 자신의 복호화키 한 종류만을 비밀리에 보관하면 되므로 비밀을 유지해야 하는 키의 종류가 적다.

또한, 공개키 암호 방식을 이용하면, 송신자가 자신을 비밀키로 서명하고, 수신자가 공개키로 서명의 검사를 하면 용이하고 안전한 인증 기능(디지털 서명 등)이 실현된다. 이상과 같은 관용 암호 방식과 공개키 암호 방식의 장단점을 비교 요약하면 다음의 표와 같다.

[표 6.1] 관용 암호 방식과 공개키 암호 방식의 비교

암호방식 / 항목	관용 암호방식		공개키 암호방식
키의 상호관계	암호화키 = 복호화키		암호화키 ≠ 복호화키
암호화 키	비밀		공개
복호화 키	비밀		비밀
암호 알고리즘	비밀	공개	공개
대표적 예	Vernam	DES	RSA
비밀키의 전송	필요		불필요
비밀키의 유지수	많음 통신 상대방의 수 만큼		적음 자신의 키만 비밀 유지
안전한 인증	곤란		용이
암호화 속도	고속		저속
경 제 성	△		▽

그러므로 관용 암호 방식 및 공개키 암호 방식의 특징들을 이용하여 처리 속도가 빠른 관용 암호 방식으로 암호화 및 복호화를 행하고 암호화키의 전송은 공개키 방식으로 행하는 암호 방식을 설계하여 구현하는 것이 경제적이며 효과적인 방식이다. 이런 유형의 조합형 암호 방식은 선진 각국에서 실제로 구현되어 이용되고 있다[Sch82, ETRI91].

7.결 론

본 고에서는 정보 시큐리티의 핵심이 되는 암호의 정의 및 기본 용어에 대하여 살펴보고, 현대 암호 방식의 대표적인 방식인 관용 암호 방식, 공개키 분배 방식, 공개키 암호 방식의 성질을 분석하여 각각의 문제점을 지적하였다. 실제 각종 암호 방식을 이용하여 컴퓨터 네트워크 상에서 고부가가치 서비스를 제공하기 위하여 암호화 및 복호화시 처리 속도가 고속이나, 키 관리에 문제가 있는 관용 암호 방식과 암호화 및 복호화시 처리 속도가 저속이나 키 관리는 용이한 공개키 방식을 조합하는 방안을 고려하여야 한다. 즉, 향후 대규모 컴퓨터 네트워크 상에서 각종 암호 방식을 이용한 고도 정보 서비스 시스템 구현시 조합형 암호 방식으로 구현하는 것이 경제성면에서 효율적이라 확신한다.

즉, MHS(Message Handling System), PCN(Personal Communication Network), DBS(Direct Broadcast by Satellite), ABM(Automatic Banking Machines), EDI(Electronic Data Interchange) 등 각기 다른 다양한 환경에서의 정보 보호 및 인증 문제를 암호학으로 해결하여 조기에 고부가가치 통신 서비스를 제공하기 위한 노력이 필요하다고 생각된다.

부 록

본 부록은 상용으로 널리 사용되고 있는 대표적인 관용 암호 방식인 DES를 이용하여 텍스트 파일을 암호화하고 복호화한 예를 기술하였다.

평문 파일은 test.txt이며, 암호화 비밀키는 '123456789'을 사용하였으며 암호화한 결과 파일은 test1.sec 및 test2.sec이다. test1.sec는 DES를 이용하여 암호화를 행한 결과 파일이며, test2.sec는 압축 및 암호화를 동시에 행한 결과 파일이다.

c:\crypto\test.txt

From : 대유공업전문대학 사무자동화과 권 창 영
To : 한국 OA교육협의회 회장 박 두 석

Message : 본 자료는 현대 암호 방식 중 대표적인 방식인 DES를 이용하여 암호화 및 복호화를 행하기 위한 예제 파일 자료입니다.

가나다라마바사아자차카타파. . . .
ABCDEFGHIJKLMNOPQRSTUVWXYZ. . . .
abcdefghijklmnopqrstuvwxtz. . . .

c:\crypto\test1.sec

From : 대유공업전문대학 사무자동화과 권 창 영
To : 한국OA교육협희회 회장 박 두 석

PCT練)刊其 K칩 縯c轄絲i 빤[illegible]誥N @ [illegible]@そ -j' 育w幀챦f]o *>*H!놉 뵙
[illegible] oy '([illegible]꽸咽)p y ~<; j F M=滄/ NwU譏6d

c:\crypto\test2.sec

From : 대유공업전문대학 사무자동화과 권 창 영
To : 한국OA교육협희회 회장 박 두 석

PCT練)刊其片[illegible] t 쐴簞3빤주誥|뽐 鉛 @ 請 x

참 고 문 헌

1. [CP89] C. P. Pfleeger, Security in computing, Pretice Hall, Inc. 1989.
2. [DH76] W. Diffle, M. E. Hellman, "New Directions in Crytography," IEEE Trans. on Inform. Theory, vol. IT-22, pp.644-654, 1976.
3. [DP84] D. W. Davies, W. L. Price, Security for Computer Network, John Wiley & Sons, 1984.
4. [ETRI90] 컴퓨터 범죄와 암호화 대책, 한국전자통신연구소, 1990. 2.
5. [ETRI91] 현대암호학, 한국전자통신연구소, 1991. 8.
6. [KW90] 권창영, 원동호, "공개키 분배방식에 관한연구", 한국통신학회 논문지, 제 15권, 제 12호, pp.981-989, 1990. 12.
7. [MTI186] 松本勉 高岭洋一 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 84-40, 1985.
8. [NBS77] "Data Encryption Standard," Federal Information Processing Standard Publication No.46, National Bureau of Standard, U. S. Dept of Commerce, 1977.
9. [Sch82] B. P. Schanning, "Applying Public Key Distribution to Local Area Networks," North-Holland Publicing Com., Computers & Security 1. pp.268-274, 1982.
10. [Won94] 원동호, "디지털명의 정의와 개념," 디지털서명 표준화 워크샵 자료집, pp.11-29, 1994. 4.
11. [YA83] T. Yamamoto R. Akiyama, "A data encryption device incor porating fast PKDS," Proceeding of IEEE Global Telecommunitions Conference, pp.1085-1090, 1983.

박두석(朴斗碩) 정회원

1945년 6월 1일생
1965. 3 ~ 1969. 2 영남대학교 전기공학과(공학석사)
1975. 9 ~ 1977. 8 한양대학교 산업대학원 전자통신공학과(공학석사)
1980. 9 ~ 1982. 8 건국대학교 대학원 전자공학과(공학석사)
1985. 9 ~ 1990. 8 광운대학교 대학원 전자통신공학과(공학박사)
1961. 1 ~ 1977. 2 한국전력 정보시스템처 근무
1977. 3 ~ 1977. 12 영진전문대학 전자통신과(전임강사)
1977. 11 ~ 현재 대유공업전문대학 사무자동화과(교수)
관심분야 : 정보 통신 및 마이크로파 분야

권창영(權蒼英) 정회원

1957. 4 22일생
1983. 2 성균관 대학교 수학교육과 졸업 (이학사)
1991. 2 성균관 대학교 대학원 정보공학과 졸업 (공학석사)
1991. 3 ~ 1994. 8 성균관 대학교 대학원 정보공학과 박사과정(공학박사)
1982. 12 ~ 1988. 9 (주) KOLON 정보 SYSTEM실 팀장
1992. 3 ~ 현재 대유공업전문대학 사무자동화과 전임강사
관심분야 : 암호학, 정보관리