Triple DES 알고리즘을 이용한 디지털 콘텐츠 보호 시스템 설계 및 구현

권 도 윤, 이 경 원*, 김 정 호
한밭대학교, (주)아이피에스*

Design and Implementation of Digital Contents Protection System using Triple DES Algorithm

Kwon do-yun, Lee kyung-won*, Kim jeong-ho
Hanbat National Univ., Intellectual Property Solutions, Inc.*
E-mail : dykwon@taekwang.co.kr

요 약

현재 우리나라의 방송환경은 지난 수십년간 지속되어온 아날로그 방송시스템에서 디지털 방송시스템으로 변모해 가는 과도기를 맞고 있다. 이러한 방송환경의 변화와 더불어 디지털 방송 인프라에 담길 각종 디지털 방송 콘텐츠 산업과 고부가가치의 디지털 방송 콘텐츠에 대한 불법 복제 방지 기술에 대한 관심이 고조되고 있다. 디지털방송 환경으로 전환됨에 따라 복제방지에 대한 관심이 민감하게 대두되는 데에는 이유가 있다. 첫 번째, 아날로그 방송환경에서는 전송시의 오류를 수신기에서 완벽하게 제거할 수 없으나 디지털방송 환경의 경우 오류정정 기능에 의해 원본과 동일한 콘텐츠를 수신기에서 복원할 수 있다. 두 번째로는 아날로그의 경우 복제를 반복할수록 복사본의 품질이 원본에 비해 저하되어 가지만, 디지털의 경우 원본과 동일한 품질을 유지하면서 복사의 횟수와 상관없이 무수히 많은 복사가 가능하다는 점이다. 그리고 세 번째 요소로서 아날로그와 달리 디지털 콘텐츠의 경우 인터넷의 발달과 더불어 온라인으로 누구에게나 손쉽게 전달이 가능하다는 점이다. 이러한 배경 하에서, 본 논문에서는 Triple DES 알고리즘을 이용하여 디지털 콘텐츠 불법 복제 및 배포를 방지하기 위한 디지털 콘텐츠 보호 시스템을 설계 및 구현하고자 한다.

Abstract

Broadcasting environment of present our country is greeting period of transition that undergo a change to digital broadcasting system in analog broadcasting system continued for last several decades. With change of these broadcasting environment, interest about various digital broadcasting contents industry that fill to digital broadcasting infra and unlawfulness reproduction prevention technology for digital broadcasting contents of high added value is rising. According as is converted to digital broadcasting environment, interest about reproduction prevention is well-founded to be risen sensitively. First analog broadcasting environment can not remove perfectly error at transmission in receiver, but can reconstruct contents such as original by error correction function in receiver in the case of digital broadcasting environment. Secondarily, although quality of copy is dwindled than original repeat reproduction in case of analog, many copies are available innumerably regardless of number of times of copy keeping quality such as original in the case of digital. And third element is possible easily to anyone to on-line along with development of internet in case of digital contents unlike analog. Under these background, this thesis wish to design and implement digital contents protection system to prevent unlawfulness reproduction and distribution of digital contents using Triple DES algorithm.

Ⅰ. 서론

현재 우리나라의 방송환경은 지난 수십년간 지속되어온 아날로그 방송시스템에서 디지털 방송시스템으로 변모해 가는 과도기를 맞고 있다. 이미 2002년 3월부터 디지털 위성 방송이 시작되었으며, 지상파에서도 일부 프로그램을 고선명 디지털 프로그램으로 송출하고 있다. 이러한 방송환경의 변화와 더불어 디지털 방송 인프라에 담길 각종 디지털 방송 콘텐츠 산업의 중요성이 날로 부각되어 가고 있으며, 또한 이와 더불어 중요시되고 있는 것이 고부가가치의 디지털 방송 콘텐츠에 대한 불법 복제 방지 기술이다. 디지털방송 환경으로 전환됨에 따라 복제방지에 대한 관심이 민감하게 대두되는 데에는 이유가 있다. 첫 번째, 아날로그 방송환경에서는 전송시의 오류를 수신기에서 완벽하게 제거할 수 없으나 디지털방송 환경의 경우 오류 정정 기능에 의해 원본과 동일한 콘텐츠를 수신기에서 복원할 수 있다. 두 번째로는 아날로그의 경우 복제를 반복할수록 복사본의 품질이 원본에 비해 저하되어 가지만, 디지털의 경우 원본과 동일한 품질을 유지하면서 복사의 횟수와 상관없이 무수히 많은 복사가 가능하다는 점이다. 그리고 세 번째 요소로서 아날로그와 달리 디지털 콘텐츠의 경우 인터넷의 발달과 더불어 온라인으로 누구에게나 손쉽게 전달이 가능하다는 점이다. 상기와 같은 편리한 디지털 콘텐츠의 속성은 소비자에게는 매우 반가운 특징이지만, 그 콘텐츠를 생산하고, 콘텐츠 판매를 통하여 수익을 원하는 저작권자(rights-holders)나 상거래업자(retailers) 측면에서 볼 때 매우 심각한 문제를 발생시킬 수 있다.

따라서, 본 논문에서는 Diffie-Hellman 키 교환(Key Exchange) 프로토콜과 Triple DES(Data Encryption Standard)를 이용한 디지털 콘텐츠 보호 시스템을 구현하였다. 본 논문에서 구현한 디지털 콘텐츠 보호 시스템은 Diffie-Hellman 키 교환 프로토콜을 이용하여 사용자를 인증함과 더불어 안전하지 않은 통신채널에서 비밀정보를 공유할 수 있었고, Triple DES 알고리즘을 통해 디지털 콘텐츠를 암호화하여 전송함으로써 전송선로상의 디지털 콘텐츠를 보호하는 특성을 유지할 수 있었다.

Ⅱ. 관련기술 동향

Diffie-Hellman(DH) 프로토콜은 1976년에 Diffie와 Hellman에 의해 개발된 키 교환 프로토콜로서, 많은 상업용 제품들에 이용되고 있다. 이 프로토콜의 목적은 두 사용자가 키를 안전하게 교환하고 계속해서 메시지의 암호화에 사용할 수 있도록 하는 것이며, 암호학적 안전성의 근거는 이산대수(Discrete Logarithm)의 소인수 분해 문제이다.

즉, $y = g^x \pmod p$에서 g, p, x로부터 y를 구하는 것은 쉬우나, g, p, y로부터 x를 구하는 것은 매우 어렵다(NP-complete)는 것이다.

이러한 배경을 가지고 Diffie-Hellman 키 교환 프로토콜을 정의할 수 있는데, 프로토콜의 처리과정은 그림 1에 나타내었다.

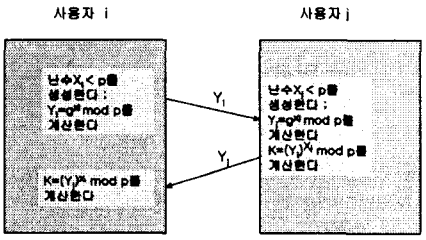

그림 3 Diffie-Hellman 키 교환

이 프로토콜은 두 시스템 파라미터 p와 g를 갖는데, 그것들은 모두 공개되고 시스템 안의 모든 사용자들에 의해 사용될 수 있다. 사용자 i와 j는 Diffie-Hellman 키 교환 프로토콜을 이용해서 다음과 같이 공통키를 나눈다. 첫 번째로, 사용자 i는 랜덤한 비밀키 X_j를 생성하고 사용자 j는 랜덤한 비밀키 X_j를 생성한다. 그리고 나서 파라미터 p, g 그리고 비밀키들을 이용해서 그들의 공개키들을 만드는데, 사용자 i의 공개키는$Y_i=g^{Xi} \bmod p$이고 사용자 j의 공개키는 $Y_j=g^{Xj} \bmod p$이다. 그리고 나서 서로 공개키를 교환하고, 마지막으로 사용자 i는 $K=Y_j^{Xi} \bmod p$를 계산하고 사용자 j는 $K=Y_i^{Xj} \bmod p$를 계산하며, 그 결과 사용자 i와 j는 비밀키 K를 갖게 되다.

SHA-1은 1994년에 발간된 SHA(Secure Hash Algorithm)의 개정판으로 SHA 내에 남아있던 결

함들을 수정한 것이다. 이 알고리즘은 264(2^{64})비트 미만의 길이를 갖는 메시지를 입력으로 160비트의 메시지 다이제스트를 출력시키며, 512비트 단위로 동작되도록 구성되었다. SHA-1은 MD4를 기본으로 MD4와 유사하게 설계되었으며, ANSI X9.30 표준으로도 정의되어 있다. 다이제스트를 생성하기 위한 메시지의 전체 처리는 그림 2에 나타내었다.

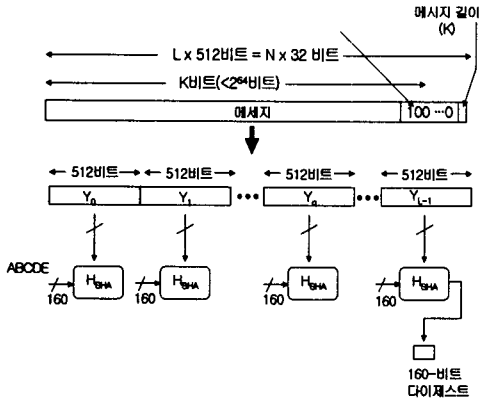

그림 4 SHA 메시지 다이제스트 생성

DES는 지난 20년간 세계적인 표준으로 사용된 64비트 블록암호 알고리즘이다. 최근 컴퓨팅 파워의 향상에 따라 56비트 DES가 22시간만에 해독되어서 64비트 이하의 키 길이를 갖는 DES는 더 이상 안전한 암호가 아니다. 이를 보완하기 위해 고안된 것이 Triple DES이다. Triple DES는 56비트인 2개의 서로 다른 암호키 112비트를 사용하여 DES를 3번 중복하여 실행하는 알고리즘으로 암호학적으로 큰 문제점이 없는 것으로 알려져, 현재 키 관리 표준인 ANSI X9.17, ISO 8732와 PEM(Privacy-Enhanced Mail) 등에서 채택하고 있다.

Triple DES 알고리즘의 동작은 다음과 같으며, 이를 그림 3에 나타내었다.

Triple DES 암호화 : $C = E_{K1}(D_{K2}(E_{K1}(M)))$

Triple DES 복호화 : $P = D_{K1}(E_{K2}(D_{K1}(C)))$

단, P(PlainText)는 평문, C(CipherText)는 암호문, E(Encryption)는 암호화, D(Decryption)는 복호화이다. 그리고, K_1, K_2는 암호화 또는 복호화할 때 사용하는 암호 키이다.

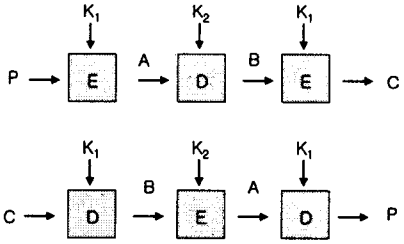

그림 5 Triple DES 알고리즘

Ⅲ. 디지털 콘텐츠 보호 시스템 구현

본 논문에서 구현한 디지털 콘텐츠 보호 시스템의 개요는 그림 4에 나타내었다.

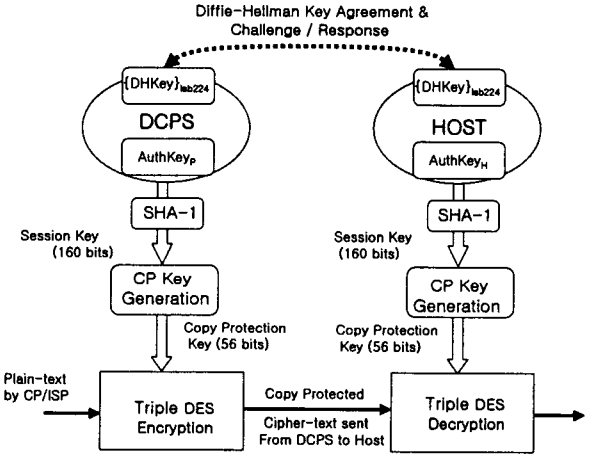

그림 6 디지털 콘텐츠 보호 시스템의 개요

본 논문에서는 디지털 콘텐츠 보호를 위해 공개키 시스템인 Diffie-Hellman 프로토콜과 블록암호 알고리즘인 Triple DES 알고리즘을 이용하였다. 공개키 시스템은 복제방지 기술에 관한 표준 규격에서도 키 공유문제와 인증에 관한 문제를 해결하기 위해 사용되고 있으며, 본 논문에서는 안전하지 못한 DCPS(Digital Contents Protection System)와 Host 사이의 통신채널을 통해 서로 일치하는 암호 키를 공유하기 위해 공개키 시스템 기술의 하나인 Diffie-Hellman 프로토콜을 채택하였다. 한편, 전송선로상의 디지털 콘텐츠의 안전한 전송을 위해서 Triple DES를 통해 디지털 콘텐츠를 암호화하여 전송하는데, Triple DES는 DES의

brute-force 공격에 대한 취약성을 보완하기 위해 기존 DES 알고리즘을 반복적으로 적용하여 보안성을 강화한 구조로서 현재 키 관리 표준인 ANSI X9.17, ISO 8732와 PEM(Privacy-Enhanced Mail) 등에서 채택하고 있다. 본 논문에서 구현한 디지털 콘텐츠 보호 시스템은 Pentium Ⅳ 1.7Ghz CPU와 DDR 256M RAM을 탑재하고, Microsoft Windows 2000 Professional 운영체제를 사용하는 PC(Personal Computer)에서 Microsoft Visual C++ 6.0을 이용하였다.

DCPS와 Host는 처음 접속시 Diffie-Hellman 프로토콜에 의해 키 교환을 하게 되며 그 결과로서 160비트의 인증키와 1024비트의 공유 비밀키(DHKey)를 유도하게 되는데, Diffie-Hellman 키 교환 프로토콜의 처리과정은 그림 5에 나타내었다.

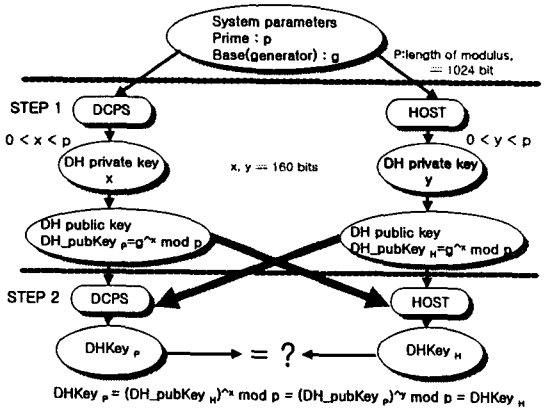

그림 7 Diffie-Hellman Key Exchange

먼저 제 1단계로 DCPS와 Host는 제작 당시 주어진 시스템 파라미터(Prime Number and Base)에 의해 각자 공개키(Public Key)와 개인키(Private Key)의 키 쌍(Key pair)을 생성한다. 이후 2단계로 이들 중 공개키를 각각 상대방 측에 전송한다. 이 경우 전송되는 채널 상에는 이들 객체들의 공개키만 공개되지만 공개키 시스템의 안전성에 기인하여 이들 공개키로부터 각자가 가지고 있는 비밀키 정보를 유도하는 것은 실제적으로 불가능하다고 보기 때문에 각자의 비밀정보는 노출되지 않는 것으로 볼 수 있다. 마지막 3단계로서 DCPS와 Host는 서로 교차하여 주고받은 공개키를 Base로 하여 각자가 가지고 있던 비밀키로 승산한 후, 모듈러 연산을 취하면 그 결과값으로 양측이 동일한 값(DHKey)을 얻게 된다.

DCPS 측의 공유 비밀키의 유도과정은 다음과 같다.

$$DHKey_P = (DH\_pubKey_H)^x \bmod p = (g^y \bmod p)^x \bmod p = g^{yx} \bmod p$$

한편, Host 측에서는 다음과 같다.

$$DHKey_H = (DH\_pubKey_P)^y \bmod p = (g^x \bmod p)^y \bmod p = g^{xy} \bmod p$$

이와 같이 계산된 DHSK(Diffie-Hellman Secret Key)가 DCPS와 Host 간에는 둘만이 공통으로 간직할 수 있는 공유 비밀키가 된다.

DCPS와 Host 사이의 인증을 위한 인증키(AuthKey)의 생성은 공유 비밀키(DHKey)와 DCPS_ID(64비트), Host_ID(40비트)를 이용하여 다음과 같이 계산하여 얻는다.

DCPS 측의 경우 :

$$AuthKey_P = SHA-1[DH\_key_P \mid Host\_ID \mid DCPS\_ID]$$

Host 측의 경우 :

$$AuthKey_H = SHA-1[DH\_key_H \mid Host\_ID \mid DCPS\_ID]$$

여기에서 SHA-1[.] 함수는 해쉬 함수(Hash function)의 일종으로 512비트의 입력을 받아 160비트로 압축된 정보를 생성하는 미국 표준 디지털 서명 알고리즘(DSA : Digital Signature Algorithm)에 사용되는 해쉬 알고리즘이다.

DCPS에서 Host 측의 인증키 $AuthKey_H$를 Host 측에 요구하고, Host에서 전송받은 인증키($AuthKey_H$)와 DCPS에서 보관하고 있는 인증키($AuthKey_P$)를 비교함으로써 사용자 인증 기능을 수행한다. 그 결과 인가된 사용자임이 확인되면, 상기에서 얻은 인증키(AuthKey)와 SHA-1[.] 함수를 이용하여 Session Key(160비트)를 생성한다. 이후 Session Key의 LSB 56비트와 MSB 56비트를 K_1, K_2로 하여 실제 디지털 콘텐츠 암호화에 사용되는 암호화 키인 CPK(Copy Protection Key)를 생성한다. 상기에서 생성한 CPK K_1, K_2를 Triple DES의 암호화키로 사용하여 CP/ISP(디지털 콘텐츠 제공자)에서 제공되는 디지털 콘텐츠를 Triple DES로 암호화하여 암호화된 디지털 콘텐츠를 Host로 전송함으로써 전송 선로상의 디지털 콘텐츠를 보호하도록 하였다.

본 논문에서 구현한 디지털 콘텐츠 보호 시스템의 동작 과정은 그림 6에 나타내었으며, 그 결과로 생성된 Encrypted data와 Decrypted data의 비

교 결과는 그림 7에 나타내었다.

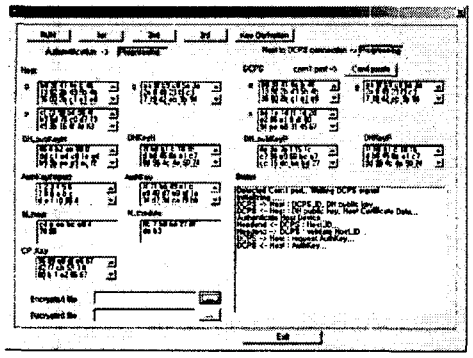

그림 8 DCPS의 동작 과정

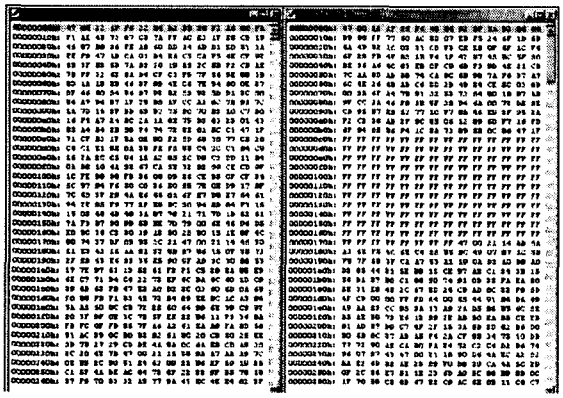

그림 9 Encrypted data와 Decrypted data

Ⅳ. 결론 및 향후 연구방향

본 논문에서는 최근 인터넷 기반 전자상거래 활성화와 디지털 콘텐츠 유료화 추세에 따라 점차 그 중요성이 부각되고 있는 디지털 콘텐츠 보호를 위한 디지털 콘텐츠 보호 시스템을 구현하였다. 본 논문에서 구현한 디지털 콘텐츠 보호 시스템은 Diffie- Hellman 키 교환 프로토콜을 이용하여 안전하지 못한 DCPS와 Host 사이의 통신채널을 통해 서로 일치하는 암호 키인 공유 비밀키(DHKey)를 공유하고, 이를 기반으로 해서 인증키(AuthKey)와 복제 방지 키(CPK)를 생성함으로써 인가된 사용자만이 디지털 콘텐츠를 복호화할 수 있도록 하였다. 한편, 전송선로상의 디지털 콘텐츠의 안전한 전송을 위해서 Triple DES를 통해 디지털 콘텐츠를 암호화하여 전송함으로써, 전송 선로상의 제 3자에 의한 디지털 콘텐츠의 불법적인 복제 및 배포를 방지할 수 있도록 하였다. 본 논문에서 구현한 디지털 콘텐츠 보호 메커니즘을 통해 디지털 콘텐츠 사용자에 대한 인증 및 전송선로 상의 디지털 콘텐츠 보호 기능을 제공함으로써 인가되지 않은 사용자에 의한 디지털 콘텐츠의 불법 복제 및 배포를 방지할 수 있다.

본 논문에서 구현한 시스템은 공개키 기반 구조 하에서 추가적인 비용없이 즉시 적용 가능하며, 최근 그 연구가 활발히 진행되고 있는 전자상거래를 위한 메타데이터 표준인 INDECS와의 연계를 통해 디지털 콘텐츠의 유통 및 저작권 보호를 위한 여러 가지 새로운 메커니즘들을 통합한다면, 더욱 효과적인 디지털 콘텐츠 보호 시스템을 구현할 수 있을 것이다.

참고문헌

[1] 고형대, "디지털 콘텐츠의 저작권 보호 및 인증 기술에 관한 조사 연구", 정보통신부 정보통신 학술연구 과제, 2002.

[2] 정보고, "Diffie-Hellman 키 교환 방식을 이용한 안전한 인스턴트 메신저의 구현", 석사학위논문, 숙명여대, 2000.

[3] 김용, 이태영, "디지털콘텐츠 유통을 위한 스마트카드기반의 다중인증처리방법 설계 및 구현", 정보관리학회지, 제18권, 제5호, 2002.

[4]최용락 외, "통신망 정보 보호", 도서출판 그린, 서울, 1997.

[5]OC-SP-HOSTPOD-IF-I11-021126 OpenCable Host
-POD Interface Specification, November 2002.

[6] ANSI/SCTE 41 2001(Formerly DVS 301) POD Copy Protection System, June 2001.

[7] NIST FIPS PUB 46-3, U. S. Department of Commerce, October, 1999.

[8] NIST FIPS PUB 186-1, U. S. Department of Commerce, December 1998.