키 교환 프로토콜을 이용한 디지털콘텐츠 보호 모듈 설계

Design of Security Module using Key Exchange Protocol in Digital Contents

권도윤
한밭대학교 정보통신컴퓨터공학부

이경원
한밭대학교 정보통신컴퓨터공학부

김정호
한밭대학교 정보통신컴퓨터공학부

중심어 : 디지털콘텐츠 보호, 키 교환

요 약

본 논문은 안전하지 못한 DCPS(Digital Contents Protection Systems)와 HOST 사이의 통신채널을 통해 서로 일치하는 암호 키를 생성하기 위한 공개키 적용을 위해 1차적으로 이산대수와 난수를 이용한 Diffie-Hellman 알고리즘을 적용하고, 2차적으로 키 관리 표준인 ANSI X9.17, ISO 8732와 PEM(Privacy-Enhanced Mail) 등에서 채택하고 있는 2개의 서로 다른 암호키를 통해 Triple DES를 적용하여 전송 선로상의 디지털콘텐츠의 안전한 전송을 수행한다. 이에 따라 설계한 정보보호 모듈은 Key Exchange 모듈, Key Derivation 모듈, Copy Protection Processing 모듈로 구성되었으며 사용자 인증 기능과 디지털콘텐츠 암호화 기능을 통해 인가되지 않은 사용자에 의한 디지털콘텐츠의 불법 복제 및 배포를 방지하고, 전송선로상의 디지털콘텐츠를 보호할 수 있도록 하였다.

Do-Yun Kwon (dykwon@taekang.co.kr)
Div. of Info. Communication and Computer Eng., Hanbat National University
Kyung-Won Lee (kwlee@hanbat.ac.kr)
Div. of Info. Communication and Computer Eng., Hanbat National University
Jeong-Ho Kim (jhkim@hanbat.ac.kr)
Div. of Info. Communication and Computer Eng., Hanbat National University

Keyword : Digital Contents Protection, Key Exchange

Abstract

In the paper, designed digital contents security module to check unlawfulness reproduction and distribution of digital contents. This paper applied Diffie-Hellman algorithm that use discrete logarithm and random number as primary for public key application to create encryption key that agree each other through communication channel between DCPS and HOST, and applied Triple DES repeat DES 3 times through 2 different encryption key that is selecting ANSI X9.17 that is key management standard, ISO 8732 and PEM(Privacy-Enhanced Mail) etc. by secondary protection for safe transmission of digital contents in transmission line. Designed security module consist of key exchange module, key derivation module and copy protection processing module. Digital contents security module that design in this thesis checks unlawfulness reproduction and distribution of digital contents by unauthenticated user through user certification function and digital contents encryption function, and protect digital contents of transmission line.

I. 서론

최근 컴퓨터 통신망의 확산과 인터넷 사용자의 증가로 네트워크를 이용한 디지털콘텐츠의 사용이 급증하고 있다. 또한 음반, 영화, 애니메이션, 게임 등의 콘텐츠 제작방식에서의 디지털화를 촉진함과 동시에 상품의 판매에 있어서도 온라인을 통해 사용자들에게 직접 유통하는 방식을 창출하는 등 콘텐츠 산업의 제작과 유통에 있어서 혁신적인 변화를 초래하고 있다.

또한, 디지털콘텐츠는 인터넷의 활성화와 정보통신기술의 발달로 인해 그 의미와 가치 등이 지속적으로 높아지고 있으며, 특히 최근에는 인터넷을 이용한 디지털콘텐츠 유료화 서

접수번호 : #030725-002
접수일자 : 2003년 7월 25일, 심사완료일 : 2003년 9월 19일

*교신저자 : 이경원, e-mail : kwlee@hanbat.ac.kr

비스들이 시작되면서 디지털콘텐츠의 저작권 보호와 더불어 디지털콘텐츠의 불법 복제 및 배포 방지에 대한 관심이 더욱 고조되고 있다[1],[2].

본 논문은 안전하지 못한 디지털 콘텐츠 보호 시스템(DCPS:Digital Contents Protection Systems)와 Host 사이의 통신채널을 통해 서로 일치하는 암호 키를 생성하기 위하여 공개키 적용을 위해 이산대수와 난수를 이용한 Diffie-Hellman 알고리즘을 적용하였으며, 키 관리 표준인 ANSI X9.17, ISO 8732와 PEM 등에서 채택하고 있는 2개의 서로 다른 암호키를 통해 Triple DES를 전송선로상의 디지털콘텐츠의 안전한 전송을 위해 적용한다. 이에 따라 설계된 모듈은 Key Exchange 모듈, Key Derivation 모듈 그리고 Copy Protection Processing 모듈로 구성하였으며 각각에서 유도된 CPK, K1, K2에 의해 암호화된 디지털콘텐츠를 이용할 수 없음을 확인할 수 있다.

II. 디지털콘텐츠의 정보보호 적용

디지털콘텐츠에 대한 개념적 정의는 다양한 관점에서 접근할 수 있고 명칭 또한 정보 콘텐츠, 디지털콘텐츠, 멀티미디어 콘텐츠, 웹 콘텐츠 등으로 다양하게 표현되고 있다. 그러나 일반적으로 디지털콘텐츠는 어원적 측면에서 "디지털+콘텐츠"의 합성어라고 할 때 기존의 콘텐츠를 디지털화 하거나 콘텐츠를 제작할 때 디지털로 제작하는 것 모두를 포함한다[2]. 즉, 디지털콘텐츠는 음악, 영화, 프로그램, 게임, 소프트웨어, 디지털 저작물 등을 포함하는 총체적인 용어로 인터넷 상에서 접근할 수 있는 디지털화된 파일을 의미한다고 할 수 있다.

이러한 디지털콘텐츠는 다음과 같은 본질적인 특징을 가지고 있다[3],[4],[5]. 첫째, 디지털콘텐츠는 복제가 매우 쉽다. 따라서, 디지털콘텐츠는 누구나 쉽게 자신의 컴퓨터를 이용하여 쉽고, 빠르게 복사할 수 있다. 둘째, 디지털콘텐츠의 복제품은 원본과 질적인 면에서 동일하다. 만약 우리가 비디오 테이프를 복사하거나 인쇄된 자료를 복사하면, 복사물은 원본에 비하여 질적으로 낮기 때문에 소비자가 불법적으로 무제한 복사하기 힘들다. 하지만, 디지털콘텐츠는 원본과 동일한 품질을 유지하면서도 무제한의 복사가 가능하다. 셋째, 디지털콘텐츠는 저장 및 편집이 용이하다. 디지털콘텐츠는 디지털화된 파일의 형태로 존재하기 때문에 컴퓨터의 하드디스크나 CD-ROM 등과 같은 보조기억장치에 쉽게 저장할 수 있을 뿐만 아니라, 이를 편집하기도 용이하다. 넷째, 디지털콘텐츠는 배포가 쉽고 빠르다. 디지털콘텐츠를 인터넷에 띄어 놓으면, 그 디지털콘텐츠는 네트워크를 통해 순식간에 다양한 사용자들에게 배포될 수 있다.

위와 같은 편리한 디지털콘텐츠의 특징은 사용자들에게는 매우 반가운 특징이지만, 그 콘텐츠를 생산하고, 콘텐츠 판매를 통하여 수익을 원하는 저작권자나 상거래업자 측면에서 볼 때 매우 심각한 문제를 발생시킬 수 있다. 특히, 최근에는 인터넷을 이용한 전자상거래와 같은 네트워크 망을 통한 상업적 거래에서 음악, 영화 등의 디지털콘텐츠를 중심으로 디지털콘텐츠의 유료화 서비스들이 시작되면서, 디지털콘텐츠의 저작권 보호와 더불어 디지털콘텐츠의 불법 복제 및 배포에 대한 관심이 더욱 고조되고 있다.

III. 적용된 정보보호 기술

1. Diffie-Hellman 알고리즘

최근 많은 상업적 제품 정보제공에 적용되고 있는 Diffie-Hellman 알고리즘은 두 사용자가 키를 안전하게 교환하고 계속해서 메시지의 암호화에 사용할 수 있도록 한다. 암호학적 안전성의 근거는 이산대수(Discrete Logarithm)의 소인수 분해 문제이며 즉, $y = g^x \pmod p$에서 g, p, x로부터 y를 구하는 것은 쉬우나, g, p, y로부터 x를 구하는 것은 매우 어렵기(NP-complete) 때문이다[6],[7].

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

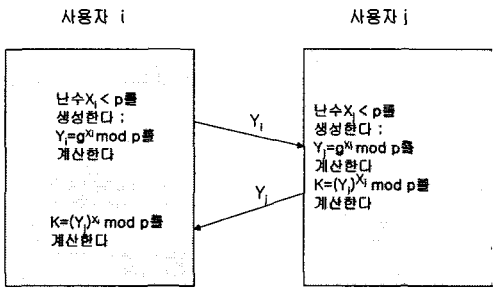

그림 1. Diffie-Hellman 기법의 적용

2. Triple DES

DES(Data Encryption Standard)는 16라운드의 반복적인 암호화 과정을 갖고 있으며 각 라운드마다 전치 및 대치의 과정을 거친 평문과 56비트의 내부 키에서 나온 48비트의 키가 섞여 암호문을 만든다. DES는 64비트의 키를 사용하는데,

64비트의 키 중 56비트는 실제의 키가 되고 나머지 8비트는 패리티 비트로 사용된다. DES는 안전성을 위해 주로 Triple DES를 사용하는데, Triple DES는 56비트인 2개의 서로 다른 암호키 112비트를 사용하여 DES를 3번 중복하여 실행하는 알고리즘으로, 키 관리 표준인 ANSI X9.17, ISO 8732와 PEM 등에서 채택하고 있다. 현재 Triple DES에 대한 실용적인 암호 분석 공격법은 없는 것으로 알려져 있다. Triple DES 알고리즘의 동작은 다음과 같다[8],[9].

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 복호화 할 때 사용하는 암호 키이다.

IV. 디지털콘텐츠 보호모듈의 설계와 평가

1. 제안된 정보보호기법과 모델 환경

본 논문에서 설계한 디지털 콘텐츠 보호 시스템의 모델은 그림 2에 나타내었다.

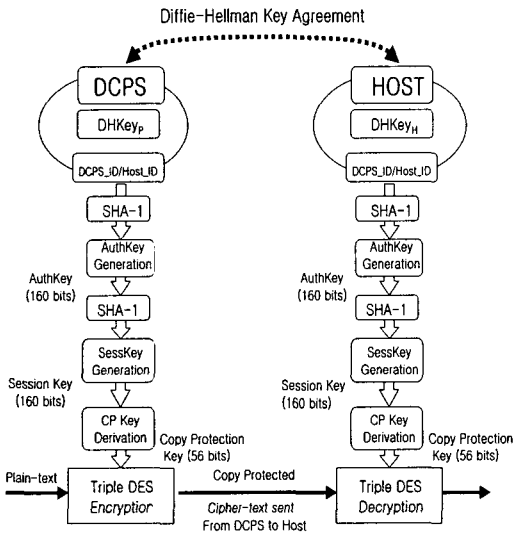

그림 2. DCPS의 모델

안전하지 못한 DCPS와 Host 사이의 통신채널을 통해 서로 일치하는 암호 키를 생성하기 위한 공개키 적용을 위해 이산대수와 난수를 이용한 Diffie-Hellman 알고리즘을 적용하였고, 키 관리 표준인 ANSI X9.17, ISO 8732와 PEM 등에서 채택하고 있는 2개의 서로 다른 암호키를 통해 DES를 3번 반복한 Triple DES를 전송선로상의 디지털콘텐츠의 안전한 전송을 위해 적용하였다[10],[11]. 본 논문에서 설계한 디지털콘텐츠 보호 시스템은 크게 Key Exchange 모듈과 Key Derivation 모듈 그리고 Copy Protection Processing 모듈로 구성되어 있다.

2. 제안된 모델에서의 보호모듈 설계

2.1. Key Exchange 모듈의 설계

본 논문에서 구현한 디지털콘텐츠 보호 시스템에서는 안전하지 않은 DCPS와 Host 사이의 통신채널을 통해 서로 일치하는 키를 공유하기 위해 Diffie-Hellman 키 교환 프로토콜을 적용하였다. DCPS와 Host의 처음 접속시, DCPS는 접속을 시도하는 Host에게 Host_ID를 요청한 후 DCPS는 자신이 가지고 있는 사용자 목록과 접속을 시도하는 Host_ID를 비교한 후, 인가된 사용자일 경우에만 Diffie-Hellman 키 교환 프로토콜을 이용하여 공유 비밀키 DHKey를 생성하게 된다. DCPS와 Host는 Diffie-Hellman 프로토콜에 의해 키 교환을 하게 되며 그 결과로서 160비트의 인증키와 1024비트의 공유 비밀키(DHKey)를 유도하게 되는데, Key Exchange 모듈의 처리 과정은 다음과 같으며 이를 그림 3에 나타내었다.

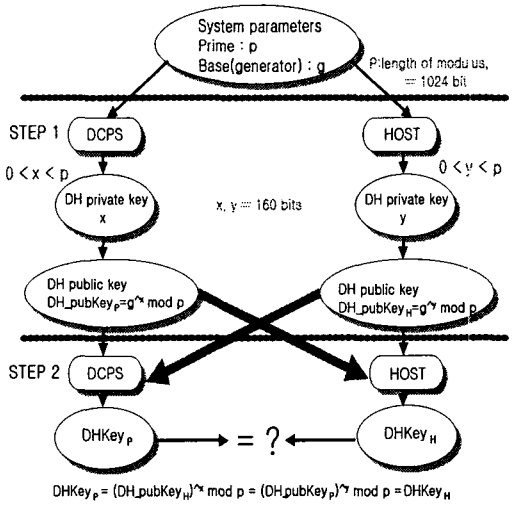

그림 3. Key Exchange 모듈

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 생성한 후, 2단계로 이들 중 공개키(DH_pubKey)를 각각 상대방 측에 전송한다. 마지막 3단계로서 DCPS와 Host는 서로 교차

하여 주고받은 공개키를 Base로 하여 각자가 가지고 있던 비밀키로 승산한 후, 모듈러 연산을 취하면 그 결과 값으로 양측이 동일한 값인 공유 비밀키 DHKey를 얻게 된다.

따라서 DCPS와 Host의 160비트의 인증키 x, y의 생성에 있어서 난수를 발생시켜 이를 이용하였다. 난수는 전체적인 시스템 보안성을 결정하는 중요한 부분으로서, DES, RC2 그리고 RC5와 같은 대칭형 암호알고리즘은 무작위로 생성된 난수를 필요로 한다.

DCPS와 Host의 공유비밀키 DHKey의 유도과정은 다음과 같다.

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

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

DCPS와 Host 사이의 공유 비밀키 DHKey가 유도된 후, DCPS는 Host에 $DHKey_H$를 요청하고 이를 보관하고 있는 $DHKey_P$와 비교하여 일치할 경우에만 다음 단계인 Key Derivation Module을 수행하게 된다. 만일 일치하지 않을 경우에는 초기 상태로 되돌아가게 된다.

2.2 Key Derivation 모듈의 설계

Key Derivation 모듈에서는 DCPS와 Host 사이에서 Diffie-Hellman 키 교환 프로토콜을 통해 유도한 공유비밀키 DHKey를 핵심정보로 이용해서 Host 인증을 위한 160 비트의 AuthKey와 160비트의 세션 키 그리고 실제적으로 디지털콘텐츠를 암호화하는데 사용할 56비트의 암호화 키인 CPK(Copy Protection Key) K_1, K_2를 유도하게 된다.

Key Derivation 모듈의 전체적인 처리과정은 그림 4와 같다.

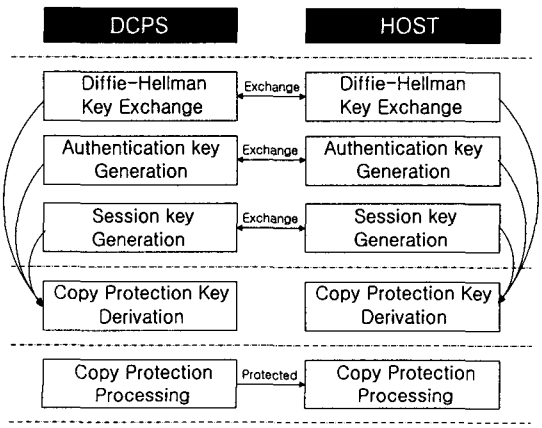

그림 4. Key Derivation 모듈

Key Derivation 모듈에서는 먼저 DHKey(1024비트)와 Host_ID(40비트), 그리고 DCPS_ID(64비트)를 SHA-1 함수의 입력값으로 하여 인증키 AuthKey를 생성하게 되는데, 그 생성과정은 다음과 같다.[9]

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

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

DCPS와 Host의 인증키 AuthKey가 생성되고 난 후, DCPS는 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 AuthKey와 SHA-1[.] 함수를 이용하여 SessKey(160비트)를 생성하게 된다. 만일 Host의 인증키 $AuthKey_H$와 DCPS의 인증키 $AuthKey_P$가 서로 일치하지 않을 경우, Host는 다시 초기 단계로 되돌아가게 된다.

SessKey는 AuthKey(160비트)와 Host_ID(40비트), 그리고 DCPS_ID(64비트)를 SHA-1 함수의 입력값으로 하여 생성하게 되는데, 그 생성과정은 다음과 같다.

$$SessKey_P = SHA-1[AuthKey_P \,/\, Host\_ID \mid DCPS\_ID]$$

$$SessKey_H = SHA-1[AuthKey_H \,/\, Host\_ID \mid DCPS\_ID]$$

따라서 SessKey를 생성한 후, DCPS는 Host 측에 $SessKey_H$를 요구하고 이를 DCPS에서 보관하고 있는 $SessKey_P$와 비교함으로써 Host 인증 기능을 수행하게 된다. 만일 Host 인증이 실패한다면, 다시 초기 상태로 되돌아가게 된다. Host 인증 결과 인가된 사용자임이 확인될 경우, 마지막으로 CPK를 유도하게 된다.

CPK는 Triple DES 알고리즘으로 디지털콘텐츠를 암호화하는 데 사용할 실제적인 암호화 키로서, SessKey의 LSB 56비트와 MSB 56비트를 선택하여 CP Key K_1, K_2를 유도하게 된다.

2.3. Copy Protection Processing 모듈의 설계

Copy Protection Processing 모듈에서는 위에서 생성한 CPK K_1, K_2를 Triple DES의 암호화키로 사용하여 평문(Plain Text) 형태의 디지털콘텐츠를 Triple DES로 암호화하게 되는

데, 이를 그림 5에 나타내었다.

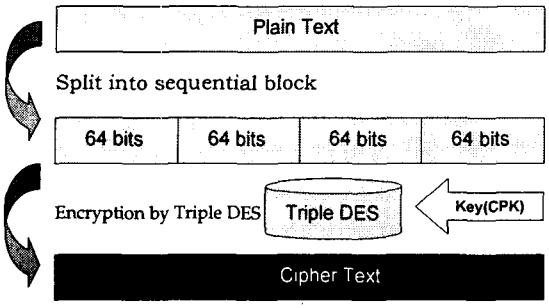

그림 5. Copy Protection Processing 모듈

Copy Protection Processing 모듈에서는 Split 과정과 Encryption 과정을 거쳐 디지털콘텐츠를 암호화하게 된다. Split 과정에서는 먼저 평문(Plain Text) 형태의 디지털콘텐츠를 64비트 블록들로 나누고, 이후 Encryption 과정에서 분할된 디지털콘텐츠 블록들을 CPK K_1, K_2를 이용해 Triple DES 알고리즘으로 암호화하게 된다.

Encryption 과정에서는 평문형태의 디지털콘텐츠 블록들을 암호화 키인 CPK K_1으로 암호화하고 그 결과를 CPK K_2로 복호화한 후, 다시 그 결과를 처음에 사용한 CPK K_1으로 암호화함으로써 암호화된 디지털콘텐츠를 생성하게 된다. 여기에서 두 번째 복호화 함수에서 사용되는 키는 처음 암호화에서 사용한 키와 다르므로 원래의 평문이 해독되지 않는다.

Copy Protection 모듈 수행 결과 생성된 암호화된 디지털콘텐츠를 Host로 전송하면, Host에서는 Key Derivation 과정에 의해 생성한 CPK K_1, K_2를 이용해 역으로 복호화하여 원하는 디지털콘텐츠를 이용할 수 있게 된다.

3. 제안된 보호 모듈의 수행 결과와 적용

3.1. Key Exchange 모듈의 수행 결과

Key Exchange 모듈의 수행 결과는 그림 6에 나타내었다. 그림 6에서 보는 바와 같이 Key Exchange 모듈을 통해 DCPS의 인증키 x와 Host의 인증키 y를 생성하고, 시스템 파라미터인 소수 p와 g를 이용해 DCPS와 Host의 공개키 DH_pubKeyP와 DH_pubKeyH를 계산하고, 이를 서로 교환하여 각각의 공유 비밀키 $DHKey_P$와 $DHKey_H$를 생성하였다. 이렇게 생성된 DCPS의 공유 비밀키 $DHKey_P$와 Host의 공유 비밀키 $DHKey_H$가 동일한 값(value)을 나타냄을 알 수 있다.

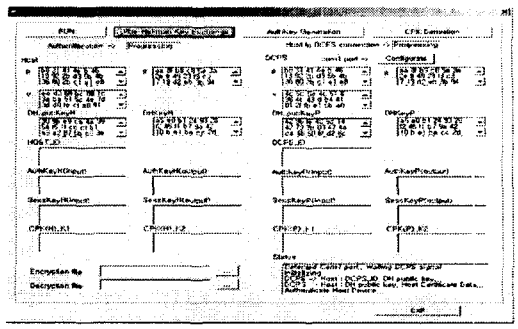

그림 6. Key Exchange 모듈 수행 결과

3.2 Key Derivation 모듈의 수행 결과

Key Derivation Module의 수행 결과는 그림 7에 나타내었다.

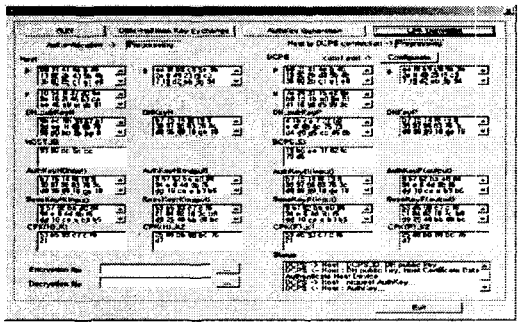

그림 7. Key Derivation 모듈 구현 결과

그림 7에서 보는 바와 같이 Key Exchange 모듈에서 생성된 DCPS와 Host의 공유 비밀키를 핵심정보로 이용하여 동일한 값을 가지는 $AuthKey_P$와 $AuthKey_H$를 생성하고, AuthKey와 DCPS_ID, Host_ID를 SHA-1 함수의 입력값으로 하여 같은 값을 가지는 $SessKey_P$와 $SessKey_H$를 생성하였다. 마지막으로 DCPS와 Host는 각각 $SessKey_P$와 $SessKey_H$의 LSB 56비트와 MSB 56비트를 선택하여 실제적인 암호화 키인 CPK K_1, K_2를 유도하였으며, 그 결과 동일한 값을 가지는 CPK K_1, K_2를 가지게 됨을 알 수 있다.

3.3. Copy Protection Processing 모듈의 수행 결과

Copy Protection Processing 모듈의 수행 결과는 그림 8에 나타내었다.

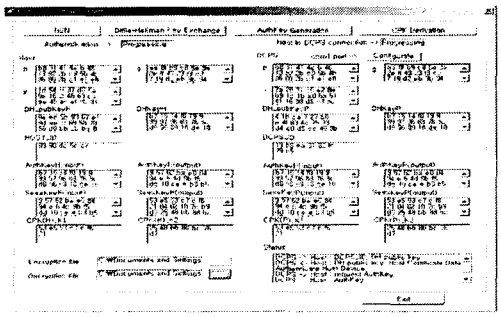

그림 8. Copy Protection Processing 수행 결과

그림 8에서 보는 바와 같이 Key Derivation 모듈에서 생성된 CPK K_1, K_2를 Triple DES의 암호화 키로 사용하여 Encrypted file과 Decrypted file을 생성하였으며, 그 결과 생성된 Encrypted data와 Decrypted data의 비교는 그림 9에 나타내었다[12],[13].

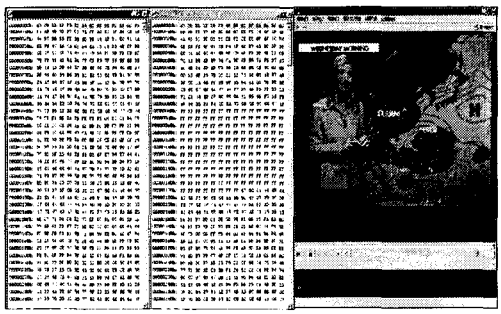

그림 9. Encrypted data와 Decrypted data의 비교

그림 9는 데이터파일의 내용을 UltraEdit v9.0을 이용하여 검색한 것으로 왼쪽부터 순서대로 평문 형태의 디지털콘텐츠를 Triple DES로 암호화한 디지털콘텐츠에 대한 헥사값, 암호화된 디지털콘텐츠를 Host에서 유도한 CP key K_1, K_2로 복호화한 디지털콘텐츠의 헥사값, 그리고 복호화된 디지털콘텐츠를 Windows Media Player에서 실행한 화면이다. 그림 9에서 보는 바와 같이 평문 형태의 디지털콘텐츠는 암호화되어 평문과는 전혀 다른 형태의 암호문을 생성하게 되므로, 이를 복호화할 수 있는 키를 소유하고 있지 않은 사용자는 암호화된 디지털콘텐츠를 사용할 수 없다. 즉, DCPS에 의해 인증을 받지 못한 인가되지 않은 사용자는 Key Derivation 과정에서 DCPS와 Host 사이의 공유 비밀키 DHKey와 이를 핵심정보로 이용하여 유도되는 암호화 키인 CPK K_1, K_2를 유도할 수 없으므로, 결국은 CPK K_1, K_2에 의해 암호화된 디지털콘텐츠를 이용할 수 없을 뿐만 아니라 이를 불법 복제 및 배포할 수 없게 된다[6],[12].

이상과 같이 Key Exchange 프로토콜을 이용하여 CPK K_1, K_2를 유도하고 이를 Triple DES의 암호화 키로 사용하여 디지털콘텐츠를 암호화함으로써 인가되지 않은 사용자에 의한 불법 복제 및 배포를 방지할 수 있는 디지털콘텐츠 Security 모듈을 설계하고 구현하였으며, 그 결과 만족할 만한 결과를 얻었다고 할 수 있다.

V. 결 론

최근 인터넷 기반 전자상거래 활성화와 디지털콘텐츠 유료화 추세에 따라 점차 그 중요성이 부각되고 있는 디지털콘텐츠의 불법 복제 및 배포를 방지하기 위한 디지털콘텐츠 보호가 필요하다.

본 논문은 안전하지 못한 DCPS와 Host 사이의 통신채널을 통해 서로 일치하는 암호 키를 생성하기 위한 공개키 적용을 위해 이산대수와 난수를 이용한 Diffie-Hellman 알고리즘을 적용하였고, 키 관리 표준인 ANSI X9.17, ISO 8732와 PEM 등에서 채택하고 있는 2개의 서로 다른 암호키를 통해 Triple DES를 전송선로상의 디지털콘텐츠의 안전한 전송을 위해 적용하였다.

본 논문에서 설계한 디지털콘텐츠 Security 모듈은 크게 Key Exchange 모듈과 Key Derivation 모듈, 그리고 Copy Protection Processing 모듈로 구성되어 있다. Key Exchange 모듈에서는 Diffie-Hellman 키 교환 프로토콜을 이용해 공유 비밀키 DHKey를 생성하고, Key Derivation 모듈에서는 Key Exchange 모듈에서 생성된 DHKey를 핵심정보로 이용하여 AuthKey와 SessKey를 생성하고 이를 이용하여 CPK를 유도하게 된다. 마지막으로, Copy Protection Processing 모듈에서는 Key Derivation 모듈에서 유도된 CPK K_1, K_2를 이용해 디지털콘텐츠를 Triple DES로 암호화하여 Host로 전송하게 된다. 설계된 보호 모듈의 실행은 3단계의 Host 인증 기능을 수행함으로써 DCPS에 의해 인가된 사용자만이 암호화된 디지털콘텐츠를 복호화 할 수 있는 복제 방지 키 CPK를 유도할 수 있도록 하였으며, 그 결과 DCPS에 의해 인증을 받지 못한 인가되지 않은 사용자는 Key Derivation 과정에서 DCPS와 Host 사이의 공유 비밀키 DHKey와 이를 핵심정보로 이용하여 유도되는 암호화 키 CP Key를 유도할 수 없다. 따라서,

CPK에 의해 암호화된 디지털콘텐츠를 이용할 수 없을 뿐 아니라 불법 복제 및 배포도 할 수 없게 된다. 또한, 전송선로상의 디지털콘텐츠의 안전한 전송을 위해서 Triple DES 알고리즘을 이용하여 디지털콘텐츠를 암호화하여 전송함으로써, 전송선로상의 제 3자에 의한 디지털콘텐츠의 불법적인 도용을 방지할 수 있도록 있었다.

참 고 문 헌

[1] 박창섭, 암호이론과 보안, 대영사, 1999.

[2] William Stallings, Cryptography and Network Security, Pearson Edu., 2003.

[3] David Broberg, Copy Protection in Digital Cable Television Systems, NCTA Publication, 2001.

[4] N. Memon, P. W. Wong, "Protecting Digital Media Content," CACM, Vol. 12, No. 7, pp. 35-43, 1998.

[5] J. Bloom et al, "Copy protection for DVD Video," Proc. of IEEE, Vol. 87, No. 7, 1999.

[6] B.C.Neuman, "Security, Payment, and Privacy for Network Commerce," IEEE Journal on Selective Areas in Comm, Vol. 13, No. 8, pp. 1523-1531, Oct. 1995.

[7] 차재현, "암호키 생성을 위한 실난수와 소수생성 알고리즘에 관한 연구", 박사학위논문, 숭실대학교, 2001.

[8] 고형대, "디지털콘텐츠의 저작권 보호 및 인증 기술에 관한 조사 연구", 정보통신부 정보통신 학술연구 과제, 2002.

[9] D.Davis, R.swick, "Network Security via Private-Key Certificate," Operating Systems eview, Vol. 24, pp. 64-67, 1990.

[10] R.C.Merkle, "Protocols for Public Key Cryptosystems," Proc.of 1980 IEEE Symp. on Security and Privacy, pp. 122-134, 1980.

[11] 이동훈, 임채훈, "국제/업계 표준 암호알고리즘 및 프로토콜의 이해", 퓨처시스템 암호체계센터 기술보고서 (FS-TR 00-13), 2000.

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

[13] OC-SP-PODCP-IF-I09-030210 OpenCable POD Copy Protection System, CableLabs, February 2003.

권 도 윤(Do-Yun Kwon) 정회원

1997년 2월 : 경북대학교 문헌정보학과 (학사)

2001년 2월 : 한밭대학교 전자계산학과 (공학사)

2003년 2월 : 한밭대학교 컴퓨터공학과 (공학석사)

1996년 ~ 현재 : 태광산업 중앙연구소 연구지원팀

<관심분야> : 인터넷 보안, 전자상거래 보안, 콘텐츠 보호

이 경 원(Kyung-Won Lee) 정회원

2000년 2월 : 한밭대학교 전자계산학과 (공학사)

2002년 2월 : 한밭대학교 전자계산학과 (공학석사)

2002년 12월 ~ 2003년 3월 : (주)아이피에스 기술연구소 전임연구원

2003년 3월 ~ 현재 : 한밭대학교 정보통신컴퓨터공학부 조교

<관심분야> : 인터넷보안, 암호학, 콘텐츠 보호

김 정 호(Jeong-Ho Kim) 정회원

1980년 2월 : 경북대학교 전자공학과 (공학사)

1983년 2월 : 경북대학교 전자공학과 (공학석사)

1995년 2월 : 단국대학교 컴퓨터공학과 (공학박사)

1983년 ~ 1996년 : 한국전자통신연구원 책임연구원/실장

1989년 8월 : 정보처리기술사

1990년 8월 : 전자기술사

1991년 12월 : 정보통신기술사

1996년 ~ 현재 : 한밭대학교 정보통신컴퓨터공학부 부교수

<관심분야> : 데이터통신, 프로토콜공학, 인터넷보안