

Key Exchange 프로토콜을 이용한 디지털 콘텐츠 보호에 관한 연구

권도윤*, 김정호*

*한밭대학교 컴퓨터공학과

e-mail:dykwon@taekwang.co.kr

A Study on Protection of Digital Contents using Key Exchange Protocol

Do-Yun Kwon*, Jeong-Ho Kim*

*Dept of Computer Engineering, Hanbat National University

요 약

디지털 콘텐츠는 텍스트, 이미지, 비디오, 오디오 등의 디지털 저작물을 포함하는 총체적인 용어로 인터넷 상에서 접근할 수 있는 디지털화된 파일을 의미하는데, 최근 전자상거래의 급속한 발달과 인터넷과 같은 컴퓨터망의 확산으로 디지털 콘텐츠의 활용이 기하급수적으로 증가하고 있다. 디지털 콘텐츠는 저장, 편집, 수정이 용이할 뿐만 아니라 인터넷을 통해 원본의 손상없이 무제한의 복제와 배포가 가능하다는 장점을 가지고 있다. 그러나, 이와 더불어 디지털 콘텐츠의 불법복제 및 배포와 같은 중요한 문제점들을 내포하고 있다. 따라서, 본 논문에서는 Key Exchange 프로토콜과 Triple DES 암호 알고리즘을 이용하여 디지털 콘텐츠 불법 복제 및 배포를 방지하기 위한 디지털 콘텐츠 보호 시스템을 구현하였다.

1. 서론

최근 컴퓨터 통신망의 확산과 인터넷 사용자의 폭발적인 증가로 전자상거래를 이용한 디지털 콘텐츠의 이용이 급증하고 있다. 디지털 콘텐츠는 텍스트, 이미지, 비디오, 오디오 등의 디지털 저작물을 포함하는 총체적인 용어로 인터넷 상에서 접근할 수 있는 전자화된 파일을 의미하는데, 다음과 같은 기본적인 특징들을 가지고 있다. 첫째, 디지털 콘텐츠는 복사가 매우 쉽다. 따라서, 디지털 콘텐츠는 누구나 쉽게 자신의 컴퓨터를 이용하여 쉽고, 빠르게 복사할 수 있다. 둘째, 디지털 콘텐츠의 복제품은 원본과 질적인 면에서 동일하다. 만약 우리가 비디오 테이프를 복사하거나 인쇄된 자료를 복사하면, 복사물은 원본에 비하여 질적으로 낮기 때문에 소비자가 불법적으로 무제한 복사하기 힘들다. 셋째, 디지털 콘텐츠의 확산 속도는 매우 빠르다. 디지털 콘텐츠를 인터넷에 띄어 놓으면, 그 콘텐츠는 순식간에 전세계에 확산될 수 있다. 상기와 같은 편리한 디지털 콘텐츠의 속성은 소비자에게는 매우 반가운 특징이

지만, 그 콘텐츠를 생산하고, 콘텐츠 판매를 통하여 수익을 원하는 저작권자(rights-holders)나 상거래업자(retailers) 측면에서 볼 때 매우 심각한 문제를 발생시킬 수 있다. 특히, 최근에는 전자상거래와 같은 네트워크 망을 통한 상업적 거래(전자상거래)가 확대됨에 따라 디지털 콘텐츠의 저작권 및 소유권 보호와 더불어 디지털 콘텐츠 불법 복제 및 배포에 대한 보호가 더욱 필요하게 되었다. 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 암호 알고리즘을 통해 디지털 콘텐츠를 암호화하여 전송함으로써 전송선로상의 디지털 콘텐츠를 보호하는 특성을 유지할 수 있었다.

2. 관련 기술 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, x 로부터 y 를 구하는 것은 쉬우나, g, p, y 로부터 x 를 구하는 것은 매우 어렵다(NP-complete)는 것이다.

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

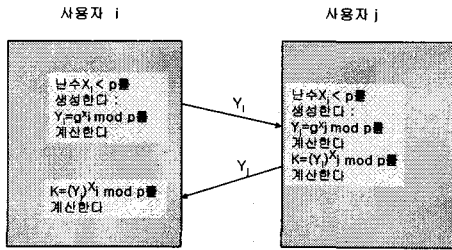


그림 1 Diffie-Hellman 키 교환 프로토콜

이 프로토콜은 두 시스템 파라미터 p 와 g 를 갖는데, 그것들은 모두 공개되고 시스템 안의 모든 사용자들에 의해 사용될 수 있다. 사용자 i 와 j 는 Diffie-Hellman 키 교환 프로토콜을 이용해서 다음과 같이 공통키를 나눈다. 첫 번째로, 사용자 i 는 랜덤한 비밀키 X_i 를 생성하고 사용자 j 는 랜덤한 비밀키 X_j 를 생성한다. 그리고 나서 파라미터 p, g 그리고 비밀키들을 이용해서 그들의 공개키들을 만드는데, 사용자 i 의 공개키는 $Y_i = g^{X_i} \pmod p$ 이고 사용자 j 의 공개키는 $Y_j = g^{X_j} \pmod p$ 이다. 그리고 나서 서로 공개키를 교환하고, 마지막으로 사용자 i 는 $K = Y_j^{X_i} \pmod p$ 를 계산하고 사용자 j 는 $K = Y_i^{X_j} \pmod p$ 를 계산하며, 그 결과 사용자 i 와 j 는 비밀키 K 를 갖게 된다.

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

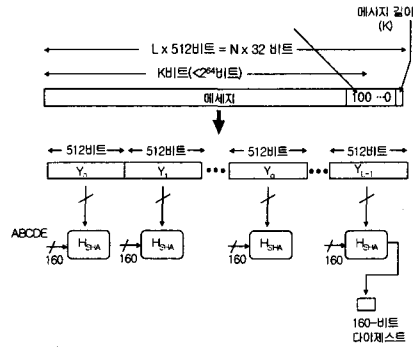


그림 2 SHA 메시지 다이제스트 생성

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 그림 3과 같다.

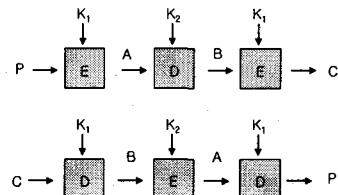


그림 3 Triple DES 알고리즘

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_2 는 암호화 또는 복호화 할 때 사용하는 암호 키이다.

3. 디지털 콘텐츠 보호 시스템 구현

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

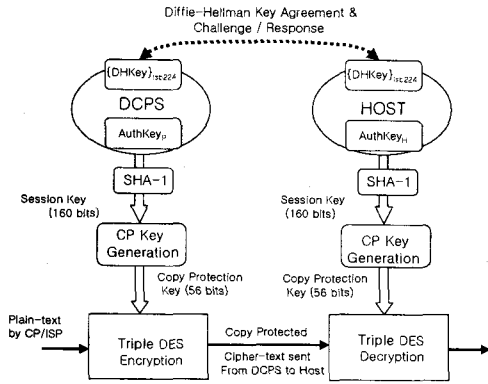


그림 4 디지털 콘텐츠 보호 시스템의 개요

본 논문에서는 디지털 콘텐츠 보호를 위해 공개 키 시스템인 Diffie-Hellman 프로토콜과 블록암호 알고리즘인 Triple DES 알고리즘을 이용하였다. 공개 키 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 공개 키 시스템 기술의 하나인 Diffie-Hellman 프로토콜을 채택하였다. 한편, 전송 선로상의 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.

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 공개 키 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 교환하여 주고받은 공개키를 Base로 하여 각자가 가지고 있던 비밀키로 승산한 후, 모듈러 연산을 취하면 그 결과 값으로 양측이 동일한 값(DHKey)을 얻게 된다.

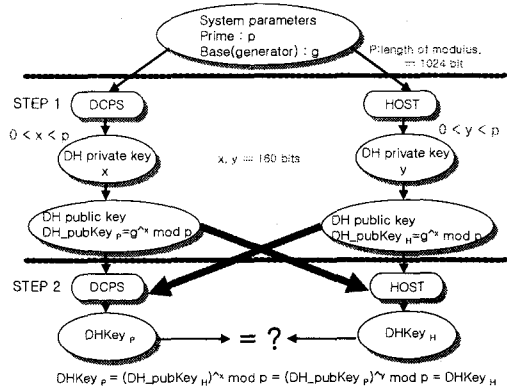


그림 5 Diffie-Hellman Key Exchange

DCPS 측의 공유 비밀키의 유도과정은 다음과 같다.

$$DHKey_p = (DH_pubKey_H)^x \bmod p = (g^y \bmod p)^x \bmod p = g^{xy} \bmod p$$

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 잔직할 수 있는 공유 비밀키가 된다.

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

DCPS 측의 경우 :

$$AuthKey_p = SHA-1[DH_key_p / Host_ID | DCPS_ID]$$

Host 측의 경우 :

$$AuthKey_H = SHA-1[DH_key_H / Host_ID | DCPS_ID]$$

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_2 로 하여 실제 디지털 콘텐츠 암호화에 사용되는 암호화 키인 CPK(Copy Protection Key)를 생성한다. 상기에서 생성한 CPK K_1 , K_2 를 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 비교 결과는 그림 7에 나타내었다.

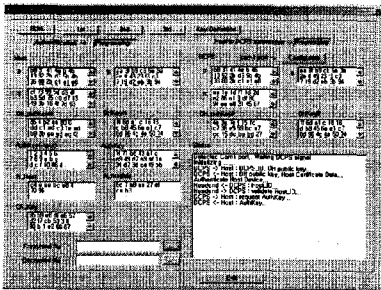


그림 6 DCPS의 동작 과정

00000000: 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16	00000000: 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16
00000016: 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32	00000016: 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32
00000032: 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48	00000032: 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48
00000048: 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64	00000048: 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64
00000064: 65 66 67 68 69 70 71 72 73 74 75 76 77 78 79 80	00000064: 65 66 67 68 69 70 71 72 73 74 75 76 77 78 79 80
00000080: 81 82 83 84 85 86 87 88 89 90 91 92 93 94 95 96	00000080: 81 82 83 84 85 86 87 88 89 90 91 92 93 94 95 96
00000096: 97 98 99 100 101 102 103 104 105 106 107 108 109 110 111 112	00000096: 97 98 99 100 101 102 103 104 105 106 107 108 109 110 111 112
00000112: 113 114 115 116 117 118 119 120 121 122 123 124 125 126 127 128	00000112: 113 114 115 116 117 118 119 120 121 122 123 124 125 126 127 128
00000128: 129 130 131 132 133 134 135 136 137 138 139 140 141 142 143 144	00000128: 129 130 131 132 133 134 135 136 137 138 139 140 141 142 143 144
00000144: 145 146 147 148 149 150 151 152 153 154 155 156 157 158 159 160	00000144: 145 146 147 148 149 150 151 152 153 154 155 156 157 158 159 160
00000160: 161 162 163 164 165 166 167 168 169 170 171 172 173 174 175 176	00000160: 161 162 163 164 165 166 167 168 169 170 171 172 173 174 175 176
00000176: 177 178 179 180 181 182 183 184 185 186 187 188 189 190 191 192	00000176: 177 178 179 180 181 182 183 184 185 186 187 188 189 190 191 192
00000192: 193 194 195 196 197 198 199 200 201 202 203 204 205 206 207 208	00000192: 193 194 195 196 197 198 199 200 201 202 203 204 205 206 207 208
00000208: 209 210 211 212 213 214 215 216 217 218 219 220 221 222 223 224	00000208: 209 210 211 212 213 214 215 216 217 218 219 220 221 222 223 224
00000224: 225 226 227 228 229 230 231 232 233 234 235 236 237 238 239 240	00000224: 225 226 227 228 229 230 231 232 233 234 235 236 237 238 239 240
00000240: 241 242 243 244 245 246 247 248 249 250 251 252 253 254 255 256	00000240: 241 242 243 244 245 246 247 248 249 250 251 252 253 254 255 256
00000256: 257 258 259 260 261 262 263 264 265 266 267 268 269 270 271 272	00000256: 257 258 259 260 261 262 263 264 265 266 267 268 269 270 271 272
00000272: 273 274 275 276 277 278 279 280 281 282 283 284 285 286 287 288	00000272: 273 274 275 276 277 278 279 280 281 282 283 284 285 286 287 288
00000288: 289 290 291 292 293 294 295 296 297 298 299 300 301 302 303 304	00000288: 289 290 291 292 293 294 295 296 297 298 299 300 301 302 303 304
00000304: 305 306 307 308 309 310 311 312 313 314 315 316 317 318 319 320	00000304: 305 306 307 308 309 310 311 312 313 314 315 316 317 318 319 320
00000320: 321 322 323 324 325 326 327 328 329 330 331 332 333 334 335 336	00000320: 321 322 323 324 325 326 327 328 329 330 331 332 333 334 335 336
00000336: 337 338 339 340 341 342 343 344 345 346 347 348 349 350 351 352	00000336: 337 338 339 340 341 342 343 344 345 346 347 348 349 350 351 352
00000352: 353 354 355 356 357 358 359 360 361 362 363 364 365 366 367 368	00000352: 353 354 355 356 357 358 359 360 361 362 363 364 365 366 367 368
00000368: 369 370 371 372 373 374 375 376 377 378 379 380 381 382 383 384	00000368: 369 370 371 372 373 374 375 376 377 378 379 380 381 382 383 384
00000384: 385 386 387 388 389 390 391 392 393 394 395 396 397 398 399 400	00000384: 385 386 387 388 389 390 391 392 393 394 395 396 397 398 399 400
00000400: 401 402 403 404 405 406 407 408 409 410 411 412 413 414 415 416	00000400: 401 402 403 404 405 406 407 408 409 410 411 412 413 414 415 416
00000416: 417 418 419 420 421 422 423 424 425 426 427 428 429 430 431 432	00000416: 417 418 419 420 421 422 423 424 425 426 427 428 429 430 431 432
00000432: 433 434 435 436 437 438 439 440 441 442 443 444 445 446 447 448	00000432: 433 434 435 436 437 438 439 440 441 442 443 444 445 446 447 448
00000448: 449 450 451 452 453 454 455 456 457 458 459 460 461 462 463 464	00000448: 449 450 451 452 453 454 455 456 457 458 459 460 461 462 463 464
00000464: 465 466 467 468 469 470 471 472 473 474 475 476 477 478 479 480	00000464: 465 466 467 468 469 470 471 472 473 474 475 476 477 478 479 480
00000480: 481 482 483 484 485 486 487 488 489 490 491 492 493 494 495 496	00000480: 481 482 483 484 485 486 487 488 489 490 491 492 493 494 495 496
00000496: 497 498 499 500 501 502 503 504 505 506 507 508 509 510 511 512	00000496: 497 498 499 500 501 502 503 504 505 506 507 508 509 510 511 512
00000512: 513 514 515 516 517 518 519 520 521 522 523 524 525 526 527 528	00000512: 513 514 515 516 517 518 519 520 521 522 523 524 525 526 527 528
00000528: 529 530 531 532 533 534 535 536 537 538 539 540 541 542 543 544	00000528: 529 530 531 532 533 534 535 536 537 538 539 540 541 542 543 544
00000544: 545 546 547 548 549 550 551 552 553 554 555 556 557 558 559 560	00000544: 545 546 547 548 549 550 551 552 553 554 555 556 557 558 559 560
00000560: 561 562 563 564 565 566 567 568 569 570 571 572 573 574 575 576	00000560: 561 562 563 564 565 566 567 568 569 570 571 572 573 574 575 576
00000576: 577 578 579 580 581 582 583 584 585 586 587 588 589 590 591 592	00000576: 577 578 579 580 581 582 583 584 585 586 587 588 589 590 591 592
00000592: 593 594 595 596 597 598 599 600 601 602 603 604 605 606 607 608	00000592: 593 594 595 596 597 598 599 600 601 602 603 604 605 606 607 608
00000608: 609 610 611 612 613 614 615 616 617 618 619 620 621 622 623 624	00000608: 609 610 611 612 613 614 615 616 617 618 619 620 621 622 623 624
00000624: 625 626 627 628 629 630 631 632 633 634 635 636 637 638 639 640	00000624: 625 626 627 628 629 630 631 632 633 634 635 636 637 638 639 640
00000640: 641 642 643 644 645 646 647 648 649 650 651 652 653 654 655 656	00000640: 641 642 643 644 645 646 647 648 649 650 651 652 653 654 655 656
00000656: 657 658 659 660 661 662 663 664 665 666 667 668 669 670 671 672	00000656: 657 658 659 660 661 662 663 664 665 666 667 668 669 670 671 672
00000672: 673 674 675 676 677 678 679 680 681 682 683 684 685 686 687 688	00000672: 673 674 675 676 677 678 679 680 681 682 683 684 685 686 687 688
00000688: 689 690 691 692 693 694 695 696 697 698 699 700 701 702 703 704	00000688: 689 690 691 692 693 694 695 696 697 698 699 700 701 702 703 704
00000704: 705 706 707 708 709 710 711 712 713 714 715 716 717 718 719 720	00000704: 705 706 707 708 709 710 711 712 713 714 715 716 717 718 719 720
00000716: 721 722 723 724 725 726 727 728 729 730 731 732 733 734 735 736	00000716: 721 722 723 724 725 726 727 728 729 730 731 732 733 734 735 736
00000732: 737 738 739 740 741 742 743 744 745 746 747 748 749 750 751 752	00000732: 737 738 739 740 741 742 743 744 745 746 747 748 749 750 751 752
00000748: 753 754 755 756 757 758 759 760 761 762 763 764 765 766 767 768	00000748: 753 754 755 756 757 758 759 760 761 762 763 764 765 766 767 768
00000764: 769 770 771 772 773 774 775 776 777 778 779 780 781 782 783 784	00000764: 769 770 771 772 773 774 775 776 777 778 779 780 781 782 783 784
00000780: 785 786 787 788 789 790 791 792 793 794 795 796 797 798 799 800	00000780: 785 786 787 788 789 790 791 792 793 794 795 796 797 798 799 800
00000796: 801 802 803 804 805 806 807 808 809 810 811 812 813 814 815 816	00000796: 801 802 803 804 805 806 807 808 809 810 811 812 813 814 815 816
00000812: 817 818 819 820 821 822 823 824 825 826 827 828 829 830 831 832	00000812: 817 818 819 820 821 822 823 824 825 826 827 828 829 830 831 832
00000828: 833 834 835 836 837 838 839 840 841 842 843 844 845 846 847 848	00000828: 833 834 835 836 837 838 839 840 841 842 843 844 845 846 847 848
00000844: 849 850 851 852 853 854 855 856 857 858 859 860 861 862 863 864	00000844: 849 850 851 852 853 854 855 856 857 858 859 860 861 862 863 864
00000860: 865 866 867 868 869 870 871 872 873 874 875 876 877 878 879 880	00000860: 865 866 867 868 869 870 871 872 873 874 875 876 877 878 879 880
00000876: 881 882 883 884 885 886 887 888 889 890 891 892 893 894 895 896	00000876: 881 882 883 884 885 886 887 888 889 890 891 892 893 894 895 896
00000892: 897 898 899 900 901 902 903 904 905 906 907 908 909 910 911 912	00000892: 897 898 899 900 901 902 903 904 905 906 907 908 909 910 911 912
00000908: 913 914 915 916 917 918 919 920 921 922 923 924 925 926 927 928	00000908: 913 914 915 916 917 918 919 920 921 922 923 924 925 926 927 928
00000924: 929 930 931 932 933 934 935 936 937 938 939 940 941 942 943 944	00000924: 929 930 931 932 933 934 935 936 937 938 939 940 941 942 943 944
00000940: 945 946 947 948 949 950 951 952 953 954 955 956 957 958 959 960	00000940: 945 946 947 948 949 950 951 952 953 954 955 956 957 958 959 960
00000956: 961 962 963 964 965 966 967 968 969 970 971 972 973 974 975 976	00000956: 961 962 963 964 965 966 967 968 969 970 971 972 973 974 975 976
00000972: 977 978 979 980 981 982 983 984 985 986 987 988 989 990 991 992	00000972: 977 978 979 980 981 982 983 984 985 986 987 988 989 990 991 992
00000988: 993 994 995 996 997 998 999 1000 1001 1002 1003 1004 1005 1006 1007 1008	00000988: 993 994 995 996 997 998 999 1000 1001 1002 1003 1004 1005 1006 1007 1008
00001004: 1009 1010 1011 1012 1013 1014 1015 1016 1017 1018 1019 1020 1021 1022 1023	00001004: 1009 1010 1011 1012 1013 1014 1015 1016 1017 1018 1019 1020 1021 1022 1023

그림 7 Encrypted data와 Decrypted data의 비교

4. 결론 및 향후 연구방향

본 논문에서는 최근 인터넷 기반 전자상거래 활

성화와 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 방지키(CPK)를 생성함으로써 인가된 사용자가 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 사용자에게 대한 인증 및 전송선로 상의 디지털 콘텐츠 보호 기능을 제공함으로써 인가되지 않은 사용자에게 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 학술 연구 과제, 2002.
- [2] 김광조 외, "디지털 콘텐츠 관리", 방송공학회지 제5권 제3호, 2000.
- [3] 김용, 이태영, "디지털콘텐츠 유통을 위한 스마트카드기반의 다중인증처리방법 설계 및 구현", 정보관리학회지 제18권 제5호, 2002.
- [4] OC-SP-HOSTPOD-IF-111-021126 OpenCable Host-POD Interface Specification, November 2002.
- [5] ANSI/SCTE 41 2001(Formerly DVS 301) POD Copy Protection System, June 2001.
- [6] NIST FIPS PUB 46-3, U. S. Department of Commerce, October, 1999.
- [7] NIST FIPS PUB 186-1, U. S. Department of Commerce, December 1998.