한국항행학회 논문지 제11권 제1호 2007년 3월

사용자 인증과 암호화를 위한 키 생성 알고리즘 구현

Implementation of Key Generation Algorithm for User Authentication and Encryption

우찬일*, 전세길**

Chan-Il Woo* and Se-Gil Jeon**

요 약

통신망의 급속한 발전으로 정보보호의 중요성은 점점 더 증가하고 있다. 따라서, 이러한 문제들을 해결하기 위하여 암호시스템이 사용 되었으며 암호시스템의 안전성은 키에 의존하고 있다. 본 논문에서는 암호학적으로 안전한 MD5 해쉬 함수를 기반으로 한 키 생성 방법을 제안한다. MD5 해쉬 함수의 기본 구조는 유한 길이의 입력을 512 비트 블록 단위로 처리하고 128 비트의 고정된 출력을 생성하는 반복적인 구조이다. 제안 방법의 안전성은 해쉬 함수를 기반으로 하고 있으며, 제안 방법은 인증 알고리즘이나 데이터 암호화를 위해 유용하게 적용될 것으로 사료된다.

Abstract

The importance of information security is increasing by the rapid development of the communication network. So, cryptosystems are used to solve these problems and securities of cryptosystems are dependent on keys. In this paper, we propose a key generation method which is based on cryptographically secure MD5 hash function. The basic structure of the MD5 hash function features is a repetitive structure which is processed in a block unit of 512 bits from inputs of limited length and generates a fixed output of 128 bits. The security of proposed method is based on the hash function and the proposed method can be also utilized for authentication algorithm or data encryption algorithm.

Key words : key, authentication, encryption algorithm, hash function

I. 서 론

컴퓨터와 통신 기술의 발전은 최근 들어 언제 어디서나 누구든지 네트워크를 형성하여 통신할 수 있도록 하는 유비쿼터스 컴퓨팅(Ubiquitous Computing) 환경으로 변화시키고 있다.

또한, 인터넷의 급속한 발전은 기존에 유선으로만 제공되던 e-mail, 게임 등이 무선으로 제공되어 이러한 서비스를 이용하고자 하는 무선 인터넷 사용자들이 점점 더 증가하고 있다. 그러나 무선 인터넷은 이동통신과 같은 이동성이 보장되지 않아 제한된 지역 내에서 서비스를 제공받기 때문에 이를 극복하기 위하여 최근 이동성이 보장되면서 인터넷 접속이 가능한 휴대인터넷(WiBro)이 등장하여 서비스 되고 있다.

* 서일대학 정보통신과(Department of Information and Communication Engineering, Seoil College)
** 한국도로공사 도로교통기술원(Korea Highway Corporation HTT(Highway and Transportation Technology Institute))
· 제1저자 (First Author) : 우찬일
· 접수일자 : 2007년 1월 8일

이와 같은 기술의 발전으로 이동통신 시스템은 음성 및 문자 위주의 서비스에서 동영상과 같은 멀티미디어 서비스와 증권거래, 모바일 뱅킹 등의 다양한 서비스를 제공하고 있다. 그러나 이러한 기술들의 발전은 생활의 편리함을 가져다 줄 수 있지만 불법적인 복제 단말기의 사용과 허가되지 않은 제3자에 의한 도청 그리고 창작물에 대한 불법적인 복제 등으로 인하여 사생활 보호나 저작권 보호에 있어서 심각한 문제를 발생시키고 있다[1].

불법적인 복제 단말기의 사용을 방지하기 위하여 스마트카드 등을 이용한 인증 기술이 등장하였으며, 창작물에 대한 저작권 보호를 위해서는 디지털 워터마킹 기술이 등장하여 현재 많은 연구가 진행되고 있다. 그리고 도청이나 전송되는 메시지의 내용 조작을 방지하기 위해 암호 기술이 등장하여 사용되고 있다.

암호 기술은 전송하고자 하는 메시지를 제3자가 알 수 없도록 원본 메시지의 내용을 바꾸어 전송하고 수신자는 암호화된 내용을 복호화 하여 원래 메시지로 변환하는 것으로, 메시지의 암호화와 복호화에는 키(Key)를 사용하며 암호화된 메시지의 안전성 여부는 키의 안전성에 달려있다[2]. 또한, 인증 기술은 일반적으로 인터넷 상에서 ID와 패스워드에 의해 이루어지고 있지만 ID와 패스워드는 쉽게 노출될 수 있어 X.509 인증서 사용이 확대되고 있으며, 이동통신 시스템에서는 사용자 인증과 메시지 암호화를 위해 스마트카드 등을 이용한 방법이 널리 사용되고 있다[3].

암호 알고리즘의 강도와 암,복호화에 사용되는 키는 암호 시스템의 안전성을 좌우한다. 따라서 이러한 키는 제3자에 의해 쉽게 추측될 수 없도록 랜덤하게 생성 되어야 하며 키의 노출을 방지하기 위하여 키의 비밀 유지에 중점을 두어야 한다[1],[2].

본 논문에서는 스마트 카드를 사용하는 휴대 인터넷 단말에 적용하기 위한 키 생성 알고리즘을 해쉬 함수를 사용하여 구현한다. 그리고 이를 위해 이동통신 시스템에서의 정보보호와 해쉬 함수 그리고 스마트카드 등에 대하여 살펴본다.

Ⅱ. 관련 연구

2-1 GSM 시스템의 보안

유럽 이동통신 시스템인 GSM(Global System for Mobile Communication)의 가입자는 망 등록 정보가 내장된 SIM(Subscriber Identity Module)이라는 스마트카드를 단말기에 삽입하여 통화를 시도한다. 스마트카드에는 인증알고리즘(A3), 암호 키 생성 알고리즘(A8), 마이크로 프로세서 등이 내장되어 있어 가입자 번호와 인증키 등의 정보를 보관하며 외부에서 읽을 수 없도록 설계되어 있다[4].

표 1. GSM 시스템의 암호 알고리즘
Table 1. Encryption algorithm of GSM system.

종류	용도	전송매체	비고
A3	가입자 ID인증	무선채널	인증센터
A5/ A5X	암호 알고리즘	무선채널	단말기, 기지국
A8	키 생성 알고리즘	스마트카드	가입자 휴대

GSM(Global System for Mobile Communication)에서의 가입자 인증 절차는 그림 1과 같다. 가입자 인증은 기지국에서 난수가 발생되어 이동국으로 전달함으로써 시작되며 기지국에서는 난수(RAND)와 인증키(Ki)를 A3 인증 알고리즘의 입력으로 사용하여 SRES(Signed Response)를 계산한다. 이와 마찬가지로 이동국에서도 수신한 난수(RAND)와 인증키(Ki)를 사용하여 SRES'를 생성하여 기지국으로 전송하며, 기지국에서는 생성된 SRES와 수신된 SRES'를 비교하여 동일한 값을 가질 경우에만 정당한 가입자로 간주한다.

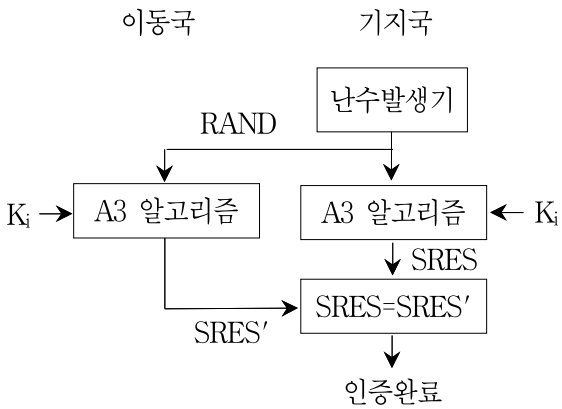

그림 1. 가입자 인증 절차
Fig. 1. Authentication processing of subscriber.

2-2 스마트카드

스마트카드는 IC 칩을 내장한 카드로 카드 내에 CPU와 카드 운영체제인 COS(Card Operating System)를 보관하고 있는 ROM 그리고 RAM 등의 메모리로 구성되어 있다. 또한, 외부 장치와의 통신을 위해 8개의 접촉 부분이 마련되어 있어 스마트카드 내의 메모리는 재 프로그래밍이 가능하고 하나의 카드에서 여러 개의 애플리케이션 들이 사용될 수 있다[5].

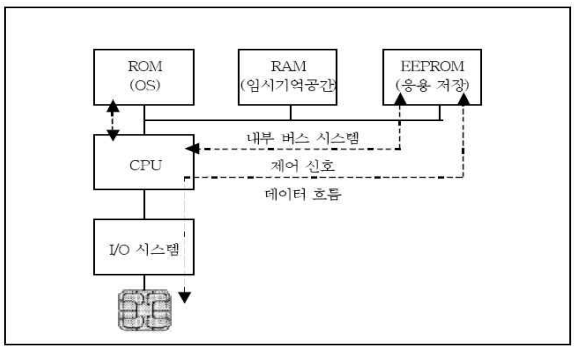

그림 2. 스마트카드 구조
Fig. 2. Architecture of smart card.

스마트카드는 저장매체로서의 기능뿐만 아니라 키 페어의 개발 그리고 데이터 보호의 역할을 수행 할 수 있으며 스마트카드의 물리적인 규격과 기능적인 특징은 대부분 ISO 7816 표준을 따르고 있다.

스마트카드의 COS는 각각의 응용 분야별 개별적으로 개발되어져 있어 활용분야에 맞추어 작성된 스마트카드 애플리케이션이 필요하며, 카드가 발급된 이후에는 스마트카드 애플리케이션을 업그레이드 하거나 추가하기가 쉽지 않다[6].

2-3 휴대인터넷(WiBro) 보안

고속 이동 중에도 인터넷 접속을 가능하게 하는 휴대인터넷은 EAP(Extensible Authentication Protocol) 기반의 인증과 보안 프로토콜의 지원이 가능하고, 단말기와 스마트카드를 이용한 가입자 인증 기능이 제공된다. 휴대인터넷의 MAC 보안 구조는 IEEE 802.16을 기반으로 정의되어, 인증과 키 관리를 위한 PKM(Privacy Key Management) 프로토콜과 TEK (Traffic Encryption Key) 암호화 및 데이터 암호화를 위한 암호 프로토콜로 구성된다. 휴대인터넷은 상호 양방향 인증과 단방향 인증을 지원하며, 주기적인 재 인증과 키 갱신 절차를 지원하여 상향링크와 하향링크에서 트래픽 암호화를 위한 키는 갱신된다[7].

WiBro 네트워크 인증을 위해 단말기에는 다음과 같은 정보가 내장되어야 한다[8].

표 2. 단말 정보
Table 2. Terminal information.

항목	내용
WNID (WiBro Network ID)	단말인증 ID 서비스 업체에서 부여
K (Subscriber key)	다른 정보로부터 유추될 수 없도록 RFC1750에 따라 랜덤하게 생성하여 단말 제조시 내장.
IMEI (International Mobile Equipment Identity)	UICC와 단말간 lock-in을 위한 번호
OPc	$OPc = OP \oplus E[OP]_K$, E:AES(Advanced Encryption Standard) 알고리즘 OP 및 OPc는 128 비트로 OP는 서비스 업체에서 지정
무인증용 K, OPc	인증서버 다운에 대비한 무인증용 인증 정보

Ⅲ. 해쉬 함수를 이용한 키 생성 방법

3-1 해쉬 함수

해쉬 함수는 입력 데이터 스트링을 고정된 길이의 출력인 해쉬 코드로 대응시키는 함수로, 해쉬 코드는 다음과 같은 함수 H에 의해 만들어 진다.

$$h = H(M) \quad (1)$$

식 1에서 M은 가변 길이의 메시지이고, H(M)는 고정 길이의 해쉬 코드이다. 해쉬 함수는 입력 데이터의 한 비트가 바뀌어도 서로 다른 해쉬 코드를 생성한다. 해쉬 함수 중 널리 사용되고 있는 MD5 해쉬 함수는 임의의 길이의 메시지를 512 비트 블록으로 처리하여 128 비트 해쉬 코드를 생성한다. 그림 3은 MD5 해쉬 함수의 처리 과정을 나타내고, 그림 4는 각 블록의

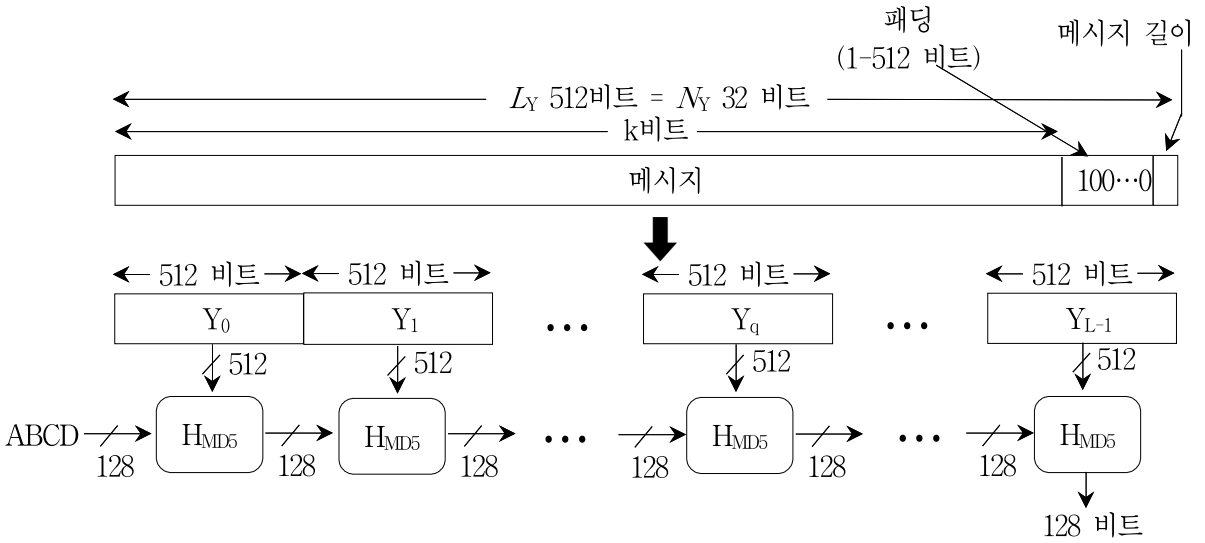

그림 3. MD5 메시지 다이제스트 알고리즘
Fig. 3. MD5 message digest algorithm.

512 비트를 H_{MD5}에서 처리하는 과정을 나타내고 있다. 여기서, 덧셈(+)은 mod2^{32}에서 수행된다[1],[2].

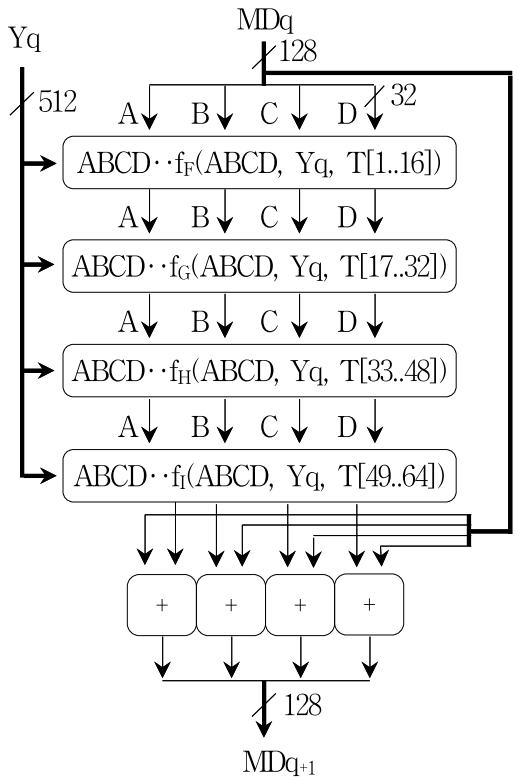

그림 4. 512 비트의 MD5 처리
Fig. 4. MD5 processing of 512 bits.

그림 3에서 128 비트 크기의 버퍼는 4개의 32 비트 레지스터(A, B, C, D)로 표현되며, 각 레지스터들은 다음과 같은 16진수 값으로 초기화된다.

A = 01234567, B = 89ABCDEF
C = FEDCBA98, D = 76543210

MD5 알고리즘에서 해쉬 코드의 모든 비트는 입력에서의 모든 비트의 함수라는 성질을 가진다. 그리고 랜덤하게 선택한 두 개의 메시지가 유사한 규칙성을 가지고 있다 하더라도 똑같은 해쉬 코드를 생성할 수 없다. 즉, 같은 해쉬 코드를 가지는 두개의 메시지를 추적하는 어려움은 2^{64} 연산의 정도인 반면, 주어진 해쉬 코드를 가지고 원래의 메시지를 찾는 어려움은 2^{128} 연산을 수행해야 한다.

3-2 알고리즘 구현

본 논문에서는 WiBro 단말에 내장할 키를 생성하기 위해 MD5 해쉬 함수를 이용하여 구현하였다. 기존에 제안된 키 생성 방법은 해쉬 함수 또는 대칭키 암호 알고리즘 등을 사용한 여러 방법들이 제안되었으나, 제안 방법에서는 암호학적으로 강력한 의사난수 발생기중의 하나인 ANSI X9.17에 명시된 방법을 이용하여 구현하였다.

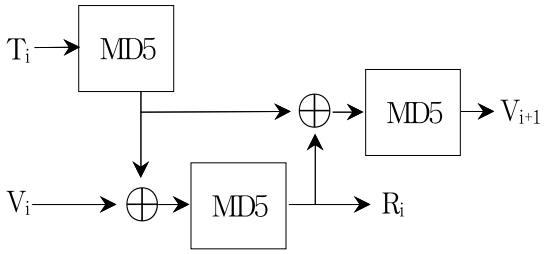

그림 5. 제안 방법
Fig. 5. Proposed method.

그림 5의 입력으로는 두 개의 의사 난수 값을 사용하여 알고리즘을 구동한다. Ti는 i번째 생성 단계 시점의 날짜와 시간으로 구한 랜덤 값으로 키 생성마다 갱신된다. 그리고 Vi는 i번째 생성 단계 시점에서의 난수 값(128비트)으로 생성 과정 중 갱신된다.

Ⅳ. 실험 및 결과

제안 방법에서는 임의 크기의 난수와 128 비트의 난수를 입력으로 사용하여 2개의 128 비트 출력(R_i, V_{i+1})을 생성한다. 일반적으로 대칭키 암호 알고리즘은 128 비트의 키를 사용하지만 AES 암호 알고리즘의 경우 128, 192, 256 비트 크기의 키를 선택하여 사용할 수 있다. 따라서 제안 방법에서는 생성된 2개의 128 비트 출력을 서로 조합하여 128, 192, 256 비트 3개의 키를 생성하고, 각 알고리즘에서 사용할 키를 선택할 수 있도록 하였다. 표 3은 키 생성을 위한 입력(T_i, V_i)과 출력(R_i, V_{i+1})을 나타내고 있다.

표 3. 실험에 사용된 인수
Table 3. The parameter value used for testing.

항목	결과 값(Hexa)
입력 (T_i)	d, 1d, 9, 2a, f0, fc, f1, 8f, 4c, 6, 2c, be, 5d, 15, f4, f1, 4b, 39, d6, b1, c5, 0, 6b, c6, de, 7, 55, 61, 27, c1, 7c, 8d,
입력 (V_i)	17, fb, 5d, e0, ef, b0, bb, 5a, a9, 10, ce, 6, 70, 56, cb, f7,
출력 (R_i)	d9, ca, c0, e7, c0, 20, e3, 39, 8, da, bb, 86, 1f, 6d, 82, ba
출력 (V_{i+1})	4a, ae, ed, 50, 57, ce, 12, 3b, 57, da, 45, 75, 4e, ab, 52, 24
첫 번째 해쉬코드	66, a6, eb, 84, 55, 96, ad, 65, e3, 53, 5d, 2b, 1f, 99, 71, 8b
XOR(1)	71, 5d, b6, 64, ba, 26, 16, 3f, 4a, 43, 93, 2d, 6f, cf, ba, 7c
XOR(2)	bf, 6c, 2b, 63, 95, b6, 4e, 5c, eb, 89, e6, ad, 0, f4, f3, 31

대칭키 암호 알고리즘을 사용한 키 생성 방법에서는 고정된 크기의 입력이 사용되고, 암호화에 사용되는 키의 비밀을 유지해야 하는 단점이 있다. 그러나 제안 방법에서는 입력 변수 T_i는 다양한 크기를 가지며, V_i는 XOR 연산을 위하여 128 비트의 고정된 크기의 난수를 사용한다. 또한, 일방향 함수인 해쉬 함수의 특성으로 R_i나 V_{i+1} 중 하나가 노출되었다 하더라도 해쉬 코드를 생성하는 입력 데이터 스트링을 찾는 것이 어려워 나머지 하나의 출력 값을 찾아내는 것은 불가능 하다는 특징을 가진다.

Ⅴ. 결 론

정보통신망의 기술적인 발전은 언제, 어디서나, 누구와도 네트워크를 통한 정보 전송이 가능한 장점이 있어 그 중요성은 매우 증가하고 있다. 그러나 불법적인 침입자로부터 중요한 정보들이 도청 되거나 내용이 변조될 수 있는 문제점들이 발생할 수 있어 이를 해결하기 위한 보안 대책으로 암호 알고리즘의 강도와 암,복호화에 사용되는 키에 의해 안전성이 보장되고 있는 암호 시스템을 기반으로 하는 정보보호 기술의 중요성은 점점 더 증가하고 있다.

본 논문에서는 사용자 인증과 암호 알고리즘의 키 생성을 위한 방법을 암호학적으로 강력한 의사난수 발생기중의 하나인 ANSI X9.17에 명시된 방법을 해쉬 함수를 이용하여 구현 하였다. 제안 방법에서는 두 개의 난수를 입력으로 128, 192, 256 비트 크기의 3개의 키를 생성할 수 있도록 하여, 각각의 알고리즘에서 사용할 키를 선택할 수 있도록 하였다.

향후 연구 과제로는 제안 방법의 처리 속도 향상을 위하여 저 전력과 적은 수의 게이트로 구성되는 H/W 개발이 필요할 것으로 생각된다.

감사의 글

본 논문은 2006년도 서일대학 학술연구비에 의해 연구되었음.

참 고 문 헌

[1] William Stallings, *Network and Internetwork Security*, Prentice Hall, 1995.

[2] Bruce Schneier, Applied Cryptography, Willey, 1996. *Conf.*, vol. 2, pp. 815-819, July 1995.

[3] Jose Luis Zoreda, Jose Manuel Oton, "Smart cards," Artech House, 1994.

[4] 신인철 외, “공개키 암호화 알고리즘에 관한 연구”, 연구보고서, 한국전자통신연구원, 1998. 12.

[5] Wolfgang Effing and Wolfgang Rankl, "Smart Card Handbook," Jahn Wiley & Sons, 2000.

[6] 구은희, 우찬일, “자바카드를 이용한 파일 접근제어 시스템의 설계 및 구현,” *전자공학회논문지*, 제43권 IE편 1호, pp. 46-51, 2006. 3.

[7] *물리 계층 및 매체접근제어 계층*, 2.3GHz 휴대인터넷 표준, 한국정보통신기술협회, 2005. 12.

[8] *WiBro 단말 인증 정보 생성 가이드*, KT, 2005. 7.

우 찬 일 (禹讚溢)

1993년 2월 : 단국대학교 전자공학과(공학사)
1995년 2월 : 단국대학교 전자공학과(공학석사)
2003년 2월 : 단국대학교 전자공학과(공학박사)
2004년 3월~현재 : 서일대학 정보통신과 교수
관심분야 : 정보보호 시스템, 디지털 워터마킹, 스마트 카드 보안, 데이터베이스 보안

전 세 길 (全世拮)

1998년 2월 : 단국대학교 컴퓨터공학과(공학사)
2000년 2월 : 단국대학교 컴퓨터공학과(공학석사)
2004년 2월 : 단국대학교 전자컴퓨터공학과(공학박사)
2006년 1월~현재 : 한국도로공사 도로교통기술원 책임연구원
관심분야 : 정보보호 시스템, 데이터베이스 보안, 시공간 데이터베이스