전자결재 시스템에서 보안기법 설계 및 구현

유영모* · 강성수* · 김완규* · 송진국*

*진주산업대학교 컴퓨터공학과

Design and Implementation of Security Technique in Electronic Signature System

Yeng-Mo YOO * · Sung-Soo KANG ** · Wan-kyoo KIM*** · Jin-kuk SONG****

Chinju National University

*E-mail : http://yym0830@netian.com

**E-mail : http:// sskang@chinju.ac.kr

***E-mail : http://wankyoo@chinju.ac.kr

****E-mail : http://jksong@chinju.ac.kr

요 약

본 논문에서는 개방형 통신상에서 전송중인 데이터를 암호화시켜 정보의 노출을 방지하고 송신자가 인정한 수신자만이 이러한 정보를 받을 수 있도록 한 암호화 알고리즘을 제시한다. 암호화의 방법에는 크게 관용키 암호화 방법과 공개키 암호화 방법으로 나누는데 본 논문에서는 혼합형 암호화 방식의 개념을 이용했다. 이 알고리즘은 통신시간과 저장공간을 절약하기 위해 전송할 데이터를 압축한 다음 암호화시키게 되며, 암호화 key를 생성하기 위한 파라미터로서 키를 생성하게 하는 것이 특징이다. 파라미터는 키 값이 생성됨과 동시에 전송되고 매 26회마다 파라미터를 변경시켜 키를 재생성 시킨다. 암호화키의 구성요소인 random number 는 table 형태로 저장되는데 키가 40회마다 table을 재편성 key의 보안을 강화하였다. 이렇게 생성된 키와 원래 데이터는 연산과정을 거쳐 암호화가 이루어진다. 복호화는 전송된 파라미터를 조사해 복호화 키를 구한 다음 암호화 동작의 역순으로 수행한다. 본 논문에서 제시한 알고리즘을 구현 및 평가결과는 100KB 메시지 0.0152/sec 정도로 빠른 수행이 되었다.

abstract

IN this paper we propose an encryption algorithm for security in data communication. this algorithm acts encryption operation after the compression of data in order to reduce the transmission time and storage an encryption key is generated by using a parameter. as soon as key value is generated the parameter is transmitted and key is recreated every 26 times of parameter changing. the random number which is a constituent unit of encryption key is stored in a table . the table is reorganized when the key is generated 40 times in order to intensity the security of encryption key. the encryption of data is made through the operation process of the generated key and sour data and the decryption performs the revers operation of encryption after getting decryption key by searching the transmitted parameter. as this algorithm is performed fastly it is possible to be used in practice.

Ⅰ. 서 론

전 세계는 하나의 전자 시장으로 연결되었다. 특히, 인터넷을 통해 쉽게 정보를 입수 할 수 있다. 그러나 해킹으로 인한 위협 등 보안상의 위협으로 가상공간의 사기와 속임수가 발생할 가능성이 높다. 이런 상황하에서 전자결재 방법으로는 수표의 경우와 같이 결제계좌에 자금을 넣어 두고 이에 대한 지불을 요청하는 방식인 e-debt방식과 크레디트 카드와 같이 신용을 이용하여 지불하고 자금은 후불하는 형태의 e-credit 방식과 그 자체가 현금과 동일한 e-cash방식 등이 있다. 이러한 방식은 거래당사자, 인증기관 및 결재기관 등 3 자 이상의 관계로 진행되는 의사표시이다. 그러나 기본적으로 전자결재에서 반드시 필요한 것이 신뢰성, 확실성, 비밀성 등으로 이러한 요건을 충족하는 방법으로는 현재까지 암

호화 및 전자서명의 방법뿐이기 때문에 전자결재의 경우에도 암호화 및 전자서명이 널리 사용되고 있다 [1]

제안하는 전자결재시스템에서의 보안기법은 암호화 key를 생성하기 위해, 적정 파라미터 값을 주어 그 값에 의해 Key를 생성하는 2중 key 알고리즘을 제안하고 key값을 구성하는 random number table의 내용을 일정한 횟수마다 변경시켜 암호화 key의 보안을 강화하였다.

본 논문의 구성은 다음과 같다. 2장에서는 전자결재시스템에서의 보안기술로써 암호화 방식에 대해서 요약한다. 그리고 3장에서 전자결재 보안 알고리즘 설계 및 구축에 대해서 요약했으며, 4장에서 구축한 알고리즘에 대한 수행평가 결과를 요약하고, 마지막으로 5장에서는 결론과 향후 연구과제를 제시한다.

II. 전자결재 시스템에서의 보안기술

2-1 전자결재 시스템 개요

전자결재시스템은 유·무선 통신장치와 컴퓨터 등을 통신회선으로 연결하고 하드웨어나 소프트웨어 프로그램을 이용한 거래 및 결재를 할 수 있는 전자시스템이다.

특히, 공문서의 기안, 결재, 전송, 공문서 송·수신 대장을 관리하기 위한 공문서 결재 시스템과 금융기관과의 여·수신에 따른 금융 결제 시스템 등이다. 이러한 시스템 상에서 결재 방식은 거래당사자, 인증기관 및 결재기관 등 3자 이상의 관계로 진행되는 의사표시인 것이다. 그러나 기본적으로 전자결재 방법상 반드시 필요한 충족요건이 신뢰성, 확실성, 비밀성 등으로 이러한 요건을 충족하는 방법으로는 암호화 및 전자서명의 방법뿐이기 때문에 암호화 및 전자서명이 널리 사용되고 있다. 현재 개방형 통신망 상에서 안전한 전자결재가 성립되도록 하기 위한 시스템 개발이 이루어지고 있다. [2]

2-2 전자결재 시스템에서의 전자서명 및 암호화

2-2-1 전자서명 개요

전자서명은 전자적 데이터에 대해 비밀키에 의해 생성된 표식으로 인증기관에서 발부한 인증된 공개키로 복호화 될 수 있고 서명키의 소유자 및 데이터가 변개되지 않았음을 확인 할 수 있는 것이다.[1]

2-2-2 전자서명의 종류

(1) 디지털 전자서명

디지털 전자서명은 송신자가 평소자신의 문서에 하는 서명 모양으로 수신자의 컴퓨터 또는 중간매개자에게 미리 등록시킨 다음 송신자가 문서를 작성한 후 특수컴퓨터 펜으로 컴퓨터 스크린 또는 특수패드에 서명하여 문서와 함께 송신하면 수신자 컴퓨터에 그 모양 그대로의 서명이 나타나게 되고 수신자 컴퓨터는 미리 등록되어 있는 송신자의 서명과 비교하여 이를 확인하는 방식이다. 단점은 미리 서명을 등록하여야 한다는 점이다.[2,13]

(2) 기타 전자서명

손가락 지문을 미리 수신자 컴퓨터 또는 중간 매개자에게 등록시킨 다음 송신자가 전자문서 작성 후에 컴퓨터에 부착된 지문인식장치에 손가락을 밀착시켜 그 지문이 수신자 컴퓨터 또는 중간매개자에 도달하면 컴퓨터가 미리 등록된 지문과 대조하여 확인하는 방식이다. 단점은 미리 지문을 등록하여야 한다는 점이다.[2,13]

1) 대칭적 암호방식을 이용한 전자서명

대칭적 암호방식을 이용한 전자서명은 실무에서 전자서명기능 수행목적으로 사용되는 방식으로서 송신자와 수신자는 각자의 컴퓨터에 동일한 종류의 대칭적 암호프로그램을 설치한 다음 각자의 비밀번호를 가진다. 송신자는 전자문서(A)를 작성한 후 자신의 비밀번호(X)와 상대방 비밀번호(Y)를 입력한다. 그러면 코드의 숫자 값과 X Y에 대해 암호화 알고리즘을 적용하여 결과 값(S)을 만드는 방식이다. 복호화는 전자문서에 대해 코드의 숫자 값과 송신자 암호알고리즘과 동일한 방식으로 결과 값을 만드는 방식이다. 이 방식은 위·변조 사실 확인을 하기 위해 코드 값을 비교한다.[2,13]

2) 비대칭적 암호방법을 이용한 전자서명

비대칭적 암호방법을 이용한 전자서명은 송신자는 우선 비밀키와 공개키를 자신의 컴퓨터 스스로 만들거나 통신서비스 사업자로부터 받는다. 비밀키는 개인 비밀번호와 동일한 것이고 공개키는 그 비밀키가 그 개인의 것이 맞는지 여부를 확인해 주는 것을 말한다. 이 방식은 송신자가 전자문서(A)를 작성하면 프로그램은 그 전자문서에 대해 해쉬 알고리즘(Z)를 적용하여 메시지를 만든다. 해쉬 알고리즘은 원래의 메시지 양과 관계없이 일정길이의 컴퓨터 코드로 표현하는 방법이다. 해쉬 함수는 임의길이 메시지를 그 메시지 양과 관계없이 그 메시지와 유일하게 대응하는 일정길이 비트로 표현하는 함수를 말한다. 원래의 메시지(x) 대해서 해쉬함수(f)를 사용하여 나온 결과(X)라고 하는 형식 f(x)=X가 된다. 여기서 x의 내용에 한자라도 수정이 가해지면 X의 값도 달라진다. 비대칭형 암호방식에서 사용하는 이유는 data 처리속도가 느리므로 본래 메시지에 일단 해쉬 알고리즘을 적용하여 data량의 작은 값을 만들고 이 값에 대해서 알고리즘을 적용하는 것이다. 예를 들면 결과 값에 송신자 비밀키(P)를 입력하면 알고리즘에 의해 기계어를 생성되는데 이것이 전자서명(S)이다. 송신자가 전자문서(A)와 관계없이 다른 전자서명(S)을 송신하여 수신자의 컴퓨터에 도착하면 수신자 컴퓨터의 프로그램은 도착 전자문서에 대해서 송신자와 동일한 내용의 해쉬 알고리즘을 적용 새로운 파일을 생성한다. 이어 전자문서를 꺼낸다. 즉 공개키는 비밀키로 암호화되어서 메시지와 함께 전송하여 수신자가 전자서명을 해독하는데 쓰이는 것이다. 그리고 송신자 전자서명 안에 담긴 코드 값과 수신자가 만든 코드 값이 서로 동일하면 위변조가 없는 것으로 확인한다. 이때 공개키가 송신

자의 비밀키와 대응하는 짝이 아닐 경우 코드 값은 다르게 된다.[2,8]

2-2-3 전자문서의 보안

전자문서의 보안기법이 제공 할 수 있는 기능은 다음과 같다.

(1) 신분확인 서비스

신분확인서비스(IDENTIFICATION/AUTHENTICATION)는 네트워크 보안을 위해 상대방의 신분을 확인하는 것이다. 자신의 신분을 증명하는 것을 신분확인이라 하며, 대등실체, 발신처 신분확인을 나눈다.[3,4,5,6]

(2) 엑세스 제어 서비스

엑세스제어 서비스(ACCESS CONTROL SERVER) 는 사용자와 대등한 실체의 엑세스를 위한 자원과 엑세스 동작 유형에 대한 정당성을 점검하는 서비스로서, 특권의 최소화(LEAST PRIVILEGE), 메카니즘의 간소화(ECONOMY OF MECHANISM), 수용성(ACCEPTABLILITY), 완벽한 중재(COMPLETE MEDIATION), 개방된 설계(OPEN DESIGN)와 설계원칙을 따른다.[3,4,7,10]

(3) 자료의 무결성

자료의 정확성(DATA INTEGRITY)은 전송되는 데이터의 정확성을 점검하는 서비스로서 내용의 정확성을 점검하는 내용 무결성(CONTEXT INTEGRITY)과 전송되는 전문의 순서를 점검하는 순서 무결성(SEQUENCE INTEGRITY)으로 나눈다.[3,4]

(4) 비밀보장

비밀보장(DATA CONFIDENTIALITY)은 네트워크에서 데이터가 불법적으로 그 내용이 노출되는 것을 방지하는 서비스로 전체전문에 대한 암호화와 선택적 필드에 대한 암호화로 구분되며, 암호화 메카니즘을 사용하여 전송되는 데이터의 내용을 감출 수 있다.[3,4]

(5) 부인 봉쇄 서비스

발신부인(NON-REPUDIATION ORIGIN)과 수신부인(NON-REPUDIATION, DELIVERY) 이 있다. 발신부인은 전송된 데이터 내용에 대한 발신 사실을 부인 할 수 없게 하며, 수신부인은 수신된 데이터나 내용에 대한 수신 사실을 부인 할 수 없게 한다.[3,4,12]

2-2-4 전자문서 암호화

전자문서에 대한 암호화는 다음과 같다.

(1) 전자문서 암호화 개요와 기법

전자결재 시스템에서 통신문 위협은 도청, 위조, 수정 등 이에 따른 안전대책이 하나로 암호화는 좋은 해결방안이 된다. 암호화(CRYPTOGRAPHY) 란 송신된 자료가 읽혀지거나 복사되거나 누군가에 의해 조작되지 않도록 자료를 전송하기 전에 그 의미를 알 수 없는 암호문(CRYPTOGRAM)으로 변형시켜 전송한 후, 그것을 다시 해독하도록 하는 것을 말한다. 따라서 암호화 알고리즘에 대한 입력 DATA로써 송신자가 수신자에게 보내는 보통의 통신문을 평문(PLAIN TEXT CLEAR TEXT)이라고 하며, 이 평문을 암호화 알고리즘을 통해 나온 출력 데이타인 암호문(CIPHER TEXT)으로 변환시키는 조작을 암호화(ENCRYPTION)라고 한다. 암호화된 데이터를 정상적인 형태로 즉, 원래의 평문으로 조작시키는 과정을 복호화(DECRYPTION)이라고 한다. 복호화는 합법적인 사용자가 정상적인 절차를 거쳐 평문으로 복원된 것만을 말하여, 부당한 사용자가 중간에 도청하여 나름대로의 방법으로 평문을 얻는 것을 해독이라 한다. 따라서 정보를 전송할 때 그 정보를 제3자로부터 보호하기 위해 송신자는 평문을 암호화 알고리즘과 암호화 key로 암호문을 생성하여 침입자에게 노출된 통신채널을 통하여 수신자에게 보내며, 수신자는 암호문을 받아 복호화 알고리즘과 복호화 key로 원래 송신자가 보내고자 했던 평문을 얻게 된다.[3,4,9]

부정접근은 패스워드의 누설 등으로 일어 날수 있으며, 이런 위험에 대한 대책의 하나로서 암호화가 이용된다. 또한 전송로의 고의 또는 사고 등의 침해에 의한 통신내용의 도청, 파괴, 변경 등의 위협에 대한 물리적인 대책도 중요하지만 한계가 있으므로 이에 대한 보완대책으로 암호화는 좋은 해결수단이 된다.[1,4]

암호시스템의 개발과정은 다음과 같이 3 단계로 구분할 수 있다.

제1 단계 : 암호 알고리즘의 개발(암호화 및 복호화 루틴의 개발)

제2 단계 : 보안성 분석 및 효율성 평가

제3 단계 : 암호시스템 활용

암호시스템의 기본적인 기능은 데이터의 비밀성 보장과 사용자 확인을 할 수 있다는 것이다. 정보를 전송할 때 그 정보를 제3자로부터 보호하기 위해 송신자는 평문(PLAIN TEXT)을 암호화 알고리즘과 암호화 KEY로 암호문을 생성하여 침입자에 게 노출된 통신채널을 통하여 수신자에게 보내며, 수신자는 암호문을 받아 복호화 알고리즘과 복호화 KEY로 원래 송신자가 보내고자 했던 평문을 얻게 된다.

암호화 방식의 기본구조는 암호화 KEY 관리를 어떻게 하느냐에 따라 암호화 기법은 크게 관용KEY 암호화방식과 공개KEY 암호화 방식으로 나눌 수 있다. 이러한 암호화 알고리즘은 평문을 암호문으로 바꾸어주는 관용KEY 암호화 방식은 암호화 및 복호화 에 필요한 KEY가 동일하며, 공개KEY 암호화 방식은 암호화 및 복호화 에 필요한 KEY가 다르다. 일반적으로 관용KEY 암호화 시스템은 수행속도는 빠르나 인증성이 결여되며, 공개KEY 암호화 시스템은 인증성은 있으나 수행속도가 늦은 단점이 있다.[3,4]

1) 관용 암호화 방식

관용 암호화 방식(CONVENTIONAL CRYPO SYSTEM) 은 오래 전부터 널리 사용되어온 방식으로 송신측과 수신측에 똑같은 KEY를 준비하여 암호화 및 복호화를 한다. 관용 암호화 방식이란 용어

는 1976년 공개 KEY 암호화 방식의 개념이 발표되면서, 이에 대응하여 붙여진 것으로 위치교환 방법, 문자대치방법, 대수적 방법, 합성암호방법 등이 있다.[3,4,11,16]

① 위치 교환방법(TRANSPOSITION)

위치교환 방법(TRANSPOSITION)은 평문의 각 글자들의 위치를 바꾸어 놓는 방법으로 평문에서 사용된 각 글자는 모두 그대로 사용되나 그 위치가 달라져 본래의 뜻을 알아 볼 수 없고, 이를 전치식(순열방법)이라고 부른다. 이 방법은 다른 암호화 방법과 조합하여 사용함으로써 , 충분한 효과를 얻을 수 있으며, 다음 3가지 종류가 있다.

가. 글자의 순서를 반대로 나열하는 방법

나. 문장전체를 둘로 나누어 적은 다음, 열(column)순서로 나열

다. 정해진 matrix의 크기에 따라 글자의 위치를 바꾸는 방법

이 방법은 matrix를 만들 때 변화를 줄 수도 있다. matrix의 형태에서 글자를 선택하는 순서에 변화를 줌으로써 다른 형태의 암호문을 얻을 수 있다.

② 문자 대치방법

문자대치방법은 (SUBSTITUTION)은 평문의 글자를 다른 체계를 갖는 글자로 치환시키는 것으로 주어진 KEY TABLE에 의해 원문의 글자를 다른 글자로 치환시키며, 본래의 글자 위치는 변하지 않으나 글자를 바꾸어 알아 볼 수 없게 한 방법이다.[3,4]

③ 대수적 방법

대수적 방법(ALGEBRAIC SYSTEM)은 평문의 글자를 미리 정의된 숫자로 바꾸고 수학적인 처리를 한 다음, 다시 문자로 바꾸는 방법이다. 이 방법으로는 BCD코드를 이용한 방법, 연속방정식에 의한 방법, 메트릭스에 의한 방법 등이 있다.[3,4]

④ 합성암호화

합성암호(PRODUCT CIPHER) 는 전치 및 대치 암호화 방식의 혼합형으로 미국IBM이 개발한 DES (Data Encryption Standard),를 일본의 NTT가 모방하여 개량한 FEAL(Fastdata Encipherment Algorithm) 이 여기에 속한다. 미국 상무성 표준국에서 안전성 key 에만 의존되며, 정량적으로 표기될 수 있는 조건으로 암호화 알고리즘을 공개 모집하여 IBM사의 W. L Tuchman이 개발한 암호방식을 1977년 DES(Data Encryption Standard)로 제정되었다.[3,4,11,15,17]

2) 공개키 암호화 방식

공개키 암호화 방식(PUBLIC-KEY CRYPTO SYSTEM)은 1976년에 Diffie와 Hellman에 의하여 발표된 암호계의 개념으로서 DES 등의 관용 암호계에서 중요시되고 있는 키의 배분이 불필요하다.

암호화 key 와 복호화 key를 별도로 가지고 있는 것으로서 사용자는 자기의 암호화 key는 공개하고 복호화 key는 비공개 관리한다.

수신측은 사전에 암호화 key와 복호화 key을 작성하여 암호화 key를 공개적으로 송신측에 보낸다. 송신측은 통신문을 암호화하여 key로 암호문을 수신측에 송신한다. 수신측에서는 이 암호문을 비밀리에 보관시켜 놓은 복호화 key로 복호화 하여 통신문을 얻도록 한다.

즉 암호계 가입자는 각자의 암호화 key와 복호화 key를 서로 다르게 하여 각자의 암호화 key를 공개 key list에 등록하고 복호화 key를 보관한다.

예를 들어 임의의 송신자 A 가 수신자 B 에게 평문을 전송할 때 는 수신자의 공개 암호화 key를 사용하여 암호문을 작성한 후에 B에게 송신한다. 이때 B 이외의 다른 가입자도 이 암호문을 수신할 수는 있지만 이 암호문은 복호화 할 수 있는 복호화 key를 가지지 않기 때문에 복호화 할 수 없다. 즉 수신자 B만이 복호화 Key를 가지고 있기 때문에 평문을 구 할 수 있다.

이러한 시스템은 암호화하기 위한 key와 복호화하기 위한 key를 소유하며, 복호화 key는 비밀로 하고 암호화키는 공개한다. 암호문은 누구라도 작성하여 송신할 수 있지만 그것을 복호화 할 수 있는 것은 상대 수신자뿐이다.

즉 암호계 가입자는 각자의 암호화 key와 복호화 key를 서로 다르게 하여 각자의 암호화 key를 공개 key list에 등록하고, 복호화 Key는 본인이 관리한다. 이 시스템은 key 관리가 양호하며, 디지털 서명이 가능하다. 각 가입자는 자신의 공개 key를 가지고 있다가 암호통신을 할 때 자신의 id와 공개 key로 자신을 보증한다.

따라서 이러한 공개 key 암호방식의 개념을 처음으로 실행시킨 알고리즘은 RSA(미국의 MIT의 Rivest, shamir, adleman)에 의해 1978에 발표되었다. RSA는 두 개의 큰 소수 p, q를 구하는 것은 쉽지만, 곱이 주어졌을 때 인수분해하여 두 개의 소수를 구하는 것은 어렵다는 소인수 분해의 어려움을 이용하여 "trap door function "을 실현한 암호화 방식이다.[3,4,11,14,16]

III 전자결재 보안 알고리즘 구축

3-1 개요

본 논문에서는 유·무선 통신장치 및 컴퓨터 시스템의 안전성, 신뢰성을 확보하는 방법으로 데이터의 분실이나 도청으로부터 보호하고, 보안을 유지하는 방법은 암호화 시스템을 이용하는 것이 효과적이다. 통신회선 상에서 전송중인 데이터를 암호화하여 정보의 누출을 방지하고, 송신자 가 인정한 수신자만이 이러한 정보를 받을 수 있도록 한 암호화 알고리즘을 제시한다.

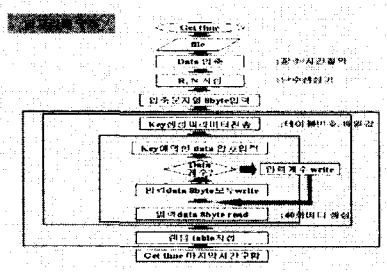
이 알고리즘은 시간을 절약하기 위하여 전송할 데이터를 입·출력한 후 암호화시키며 암호화 key를 생성하기 위하여 parameter 값을 따로 buffer에 두어 key를 생성하게 하는 것이 특징이다. parameter 값은 key값이 생성됨과 동시에 전송되고 26회마다 parameter값을 변경시킴으로써 key를 재생성 시킨

다. 이렇게 생성된 key 값과 원래의 데이터는 연산을 거쳐 암호화가 이루어지게 되며 40회마다 table 내용이 random number생성에 의해 변경되도록 하여 key의 분석을 어렵게 하여 암호화 강도를 높게 하였다.

3-2 알고리즘 설계 및 구성

3-2-1 암호화 처리과정

암호화 처리과정은 [그림1]와 같다.



[그림 1 암호화 처리과정]

여기에서 암호화 시간을 구하기 위해 시작시간(get time)을 구한 후 저장공간과 통신시간을 절약하기 위해 입력 데이터를 압축한다. 난수 생성기는 10개의 6행 5열의 table 형태로 저장되는데 암호화 key 생성을 위한 parameter 값으로 이러한 random number의 위치를 나타내는 table number 와 array 값이 전송된다. 전송된 parameter의 변환에 의해 암호화 key가 생성되고 입력 데이터와 암호화 key는 연산과정을 거쳐 8 byte 단위로 암호화가 이루어진다. table number와 array 값은 26회마다 변경시켜 암호화 key를 재생성 한다. 또한 암호화 의 강도를 높이기 위해 random number를 40회마다 다시 생성하여 table 내용을 변경시켰다.

3-2-2 전자문서 암호화 알고리즘 설계

본 논문에서 제안하는 암호화 알고리즘(Encryption Algorithm)은 다음과 같다.

(1) compress input data using zip

(2) store in buffer A the value of generated by random number generator

(3) generate contents of buffer B the value from the fifth byte of buffer A

(4) store the first 4byte of buffer A rotated in the first 4byte of buffer B

(5) store the value of key generated in the rest 4 byte of buffer B

(6) As soon as generate the contents of buffer B, buffer A is transfered

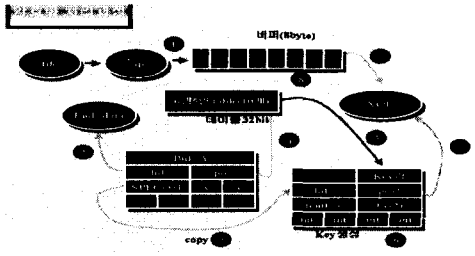
(7) change the end byte of contents of buffer A every 26 times

(8) store transfering data in buffer C

(9) buffer B and bufer C is computed using XOR and and rotate

(10) change the contents of table by random number generator every 40 times

암호화 알고리즘의 구체적인 내용은 [그림 2.]와 같다.



[그림 2. 암호화 알고리즘]

① 압축파일을 8바이트 단위로 data buffer에 저장한다.

② 파라미터를 별도마련 key 생성을 위한 head 부분 전송한다.

③ 저장될 data 형태를 변환시켜 다른 구조의 형태로 공동 이용하도록 버퍼내용 temp 로 복사한다.

④⑤ random number table의 32비트(unsigned int) data를 받는다

⑥ 암호화 key를 생성하기 위해 데이터와 key값과 rotato 시킨다.

⑦ xor 연산 data 생성한다.

⑧ 암호화된 data를 파일로 전송한다.

1) 난수(Random Number) 생성

key 생성을 위해 R·N 초기 값 123456으로 지정 6행5열 구성 10개 테이블 구성 R·N 암호화 key 참조 매 40회마다 다시 생성된다.

2) key생성 파라미터

암호화 key를 생성하기 위한 변수 값의 구성은 [표 1] 과 같다.

[표 1. key 생성 parameter 구조]

# ? *	table no	key 생성 array 값
3byte	1byte	4byte

: buffer A

3byte 는 수신자가 key 생성을 위한 parameter 값이 전송된 것이라는 것을 알기 위한 head 부분이다.

그 다음 1byte 는 random number 가 위치한 곳을 나타내는 것으로서 10개의 table 중 어느 하나를 뜻하는 table number 이다. 나머지 4 byte는 6행 5열의 table 에 순차적으로 위치한 random number 중 어느 하나를 참조하기 위한 array 값을 나타낸다. 이 parameter 는 26 회마다 변경시켜 key를 재생성 시킨다.

3) 난수참조

10개의 테이블에 저장되면 random number는 참조되며, 40회마다 재생성 된다.

4) key 생성

buffer A에서 파라미터 값으로 암호화 위한 key가 생성되는데 bufer A의 구조에서 상위 4byte를 2byte 씩 나눠 첫 번째 2byte는 오른쪽으로 2번, 두 번째 2byte는 오른쪽으로 4번 rotato 시켜 buffer의 앞쪽 4byte에 저장한다. 그리고 buffer A에서 구성한 table number 와 array 값에 의해 생성된 random number 값을 뒤 4byte에 넣는다. 이렇게 생성된 key는 [표 2.]와 같은 구조를 갖는다.

[표 2.. key의 구조]

상위 4byte rotato된 값	생성된 key 값	
4byte	4byte	:buffer B

key 값 생성을 위한 파라미터 값을 저장한 buffer A는 buffer B 의 내용 즉 key 생성과 동시 전송된다.

5) 데이타 암호화 연산

암호화 시켜 전송할 data를 8byte 단위로 buffer C 에 받아들인 수 buffer B에 구성된 key와 연산하여 암호화가 이루어진다. 전송된 data인 원래의 평문은 일정한 buffer에 위치시켜 key가 만들어짐과 동시에 암호화를 시키게 되는데 XOR과 rotate를 이용하여 암호화 key와 원래의 평문을 연산시킨다.

먼저 8byte의 데이터를 16bit 4개의 프레임으로 구성하여 data의 첫 번째 프레임은 2번 rotate 시키고 3번째 프레임은 4번 rotate시킨다. 그리고 2번째 4번째 프레임은 XOR 시킨다.

이렇게 변환시킨 data는 key와 다시 연산을 하게 되는데 key도 16bit 4개 프레임으로 나눈 후 수행한다

3-2-3 복호화

본 논문에서 제안하는 복호(DecryptionAlgorithm) 알고리즘 설계는 다음과 같다.

(1) generator random number by the random number generator

(2) get the parameter of key and inspect head

(3) generator key by the value of parameter

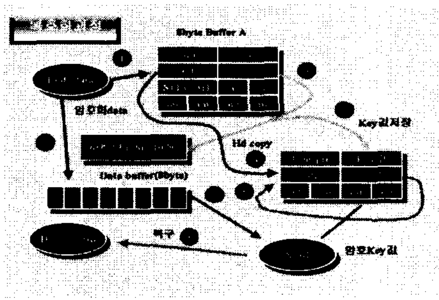
(4) reverse compute the generated key encrypted data

(5) decompress the decrypted data

복호화 과정은 다음과 같다.

복호화 과정은 암호화 과정에서 전송되어온 파라미터 head 부분을 읽기 위해 8byte를 버퍼에 저장한다. 버퍼에 내용은 암호화 key 생성 파라미터를 복구시키기 위해 자료구조가 변환되어 복사된다. 이때 만들어진 임시키를 이용해 테이블을 참조하여 그 값을 받아 key 값에 복사하여 rotato 시키고 key 생성 파라미터를 원래의 암호화 key로 복구시킨다. 그리고 암호화된 실제 data 8byte를 data 버퍼에 읽어들인다. 그리고 data 버퍼내용과 암호화 key를 XOR 하여 파일에 저장시킨다.

복호화 알고리즘의 구체적인 내용은 다음과 같다.



[그림 3. 복호화 알고리즘]

① 전송 파라미터의 head부분을 읽기 위해 버퍼에 8byte 씩 저장한다.

② 버퍼에 내용은 암호화키 생성을 위해 자료구조가 변환되어 head 부분을 복사 전송한다.

③④⑤ 자료구조가 변환된 temp key를 이용 R · N table참조 key 값에 복사 rotato 한 후 key 생성 파라미터 복구

⑥ 암호된 data 8byte를 read한다.

⑦ 버퍼 data와 암호화 key를 rotato 및 xor 연산 data 복구한다.

⑧ des-res. zip에 저장한다.

IV구현 및 평가

4-1 구현

파일 첫 부분에는 key 생성을 위한 parameter 값이 전송되었다는 것을 나타내는 head 부분이고 다음 8 byte 는 암호화 key에 의해 암호화된 부분이다. 이러한 암호화는 매 26회마다 다른 값이 head 부분을 전송하게 된다. 평문과 암호문은 [그림 4.]와 [그림 5.]과 같다.

(1) 평문

전 세계가 하나의 전자 시장으로 연결되어 있고 인터넷을 통해 쉽게 정보를 입수할 수 있다. 그러나 해킹으로 인한 위협 등 보안상의 위협으로 가상공간의 사기와 속임수가 발생할 가능성이 높다.

[그림 4. 평문]

(2) 암호문

#?* 鍍び7?ê ?낼? ?S70? ?370뛲Wu ;"t? 砥 ;z :?삗L잝?.?效;情뮣?둙??%i+ ?/旨? s S :臨3浚 2H?zg5亻눯쌨/ 뾜$H\?캉.쳄[?걷??찵?뫉<LB/3/智+M ?5 쀍n.轉늀? 漢? L?둙 ?? x/(W2W 佚eoT : w= >뛟 5#?* 뙖 ?+ " Ul 2ì 6(쿎 칔 ¢ ?5 3?(AK(? 相0 ¢ ?0 ¢

[그림 5. 암호문]

복호화는 수신된 key 생성을 위한 파라미터 값을

이용하여 암호화 Key를 생성한 후 수신된 암호문으로 복호화 루틴의 수행에 의하여 평문을 얻게 된다.

4-2 평가

본 논문에서 제안한 암호화 알고리즘을 인텔(r)셀러론(tm)Coprocessor, Memory 64MB, Windows ME 환경하에서 수행결과를 평가하였다. 본 논문에서는 암호화 key를 생성하기 위한 테이블을 난수참조 40회마다 재생성하여 암호화 강도를 향상시켰다.

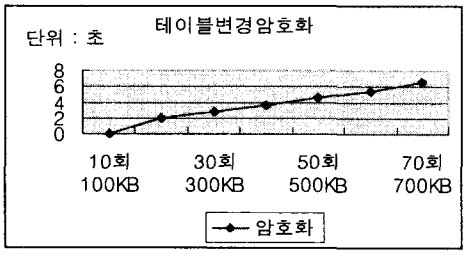
4-2-1 암·복호화 수행시간 평가

본 논문에서 제안 알고리즘을 인텔(r)셀러론(tm)Coprocessor, Memory 64MB, Windows ME 환경에서 수행시간을 평가하였다. 그 결과는 다음과 같다.

(1) 테이블 변경시 암호화 수행

테이블 변경시 암호화 수행시간은 [표 3.]과 같다.

[표 3. 데이타 양에 따른 테이블 변경 암호화 수행]

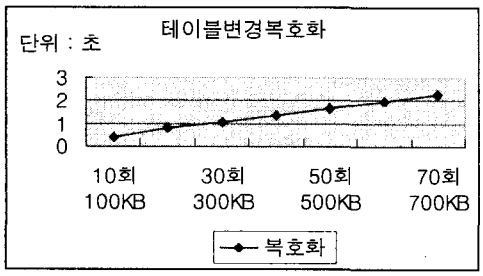


[표 3.] 에서 100kbyte의 데이터 량을 제안알고리즘 암호화에는 0.08/sec로 처리됨을 알 수 있었다.

(2) 테이블 변경시 복호화 수행

테이블 변경시 복호화 수행시간은 [표 4.]와 같다.

[표 4. 데이타 양에 따른 테이블 변경 복호화 수행]



[표 4.] 에서 100Kbyte 데이터 량을 제안알고리즘 복호화에는 0.38/sec로 처리됨을 알 수 있었다.

4-2-2 강도평가

암호알고리즘이 갖추어야할 특성은 여러 가지 있으나, 가장 중요한 것은 암호화 강도가 강해야 한다는 점이다. 암호화 시스템이 얼마나 안전한가를 측정하는 암호화 강도에는 shannon이 정의한 무조건 안전(unconditional secure) 과 계산적 안전(computational secure)이 있다. 무조건 안전은 암호해독자의 연산능력은 무한하다고 할지라도 암호해독에 이용할 수 있는 양은 불충분한 경우에 암호화 시스템이고, 계산적 안전은 암호해독자가 이용할 수 있는 정보의 양이 충분하여 언젠가는 풀 수 있지만 그 해독과정이 복잡하고 시간과 경비가 많이 요구되어 경제적으로 푸는 것이 부적합한 암호화 시스템을 말하는데 현재 대부분 암호화 방식은 계산적 안전을 중시하고 있다.[3,4,11]

본 논문에서는 정보를 찾기 위해 시행착오 식으로 모든 경우를 시행하여 사용된 key를 찾는 전수탐색에 대한 암호화 강도를 평가하였다.

64비트의 파라미터를 이용하여 64비트의 key를 생성하므로 2의 64승 개의 가능한 모든 key를 조합하여 사용된 key를 분석하게 된다.

매시 10의12승/sec 단위의 수행속도를 가진 고속 컴퓨터에 의해 해독한다면 그 파라미터를 찾아내는데 소요되는 평균시간은 식(1)에서와 같이 약 3.4개월이 소요된다.

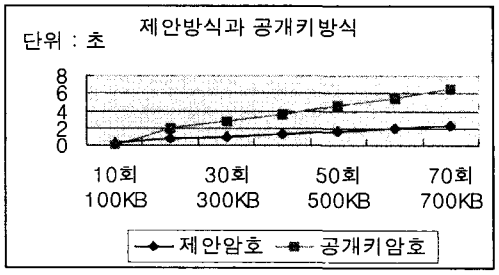
(9*10의 18승* 1/10의 12승)/ 3600*24*365 = 약 3.4 개월)

또한 파라미터 값이 208 바이트마다 변경되므로 데이터의 양에 따라 암호화 정도는 비례적으로 높아진다.

4-2-3 공개키 알고리즘(DES)와 비교

본 논문에서 제안한 알고리즘과 공개키 알고리즘(DES)과 수행시간을 평가하였다. 수행평가 결과는 [표 5.] 와 같다.

[표 5. 제안방식과 공개키 방식(DES) 수행비교]



[표 5.] 에서 공개키 알고리즘(DES)와 비교결과 본 논문에서 제안알고리즘은 초기값을 사용자가 입력하는 부분은 필요하지 않고 자동생성에 의한 방법으로 초기값 전송 루틴을 수행하게 된다. 또한 random number table에서 random number 참조 방법을 효율적으로 처리함으로서 보안 유지도를 높였다. 본 논문에서는 table 참조방식은 순차적이 아닌 매번 바뀌게 구성하였고 random number 참조 40회마다 table을 다시 작성하도록 하여 암호화 key 의 보안의 더욱 강화되었다. 단, 제안알고리즘의 단점으로써는 파일을 txt 파일형태로 만들어야 한다는 점과 압축 화일이 필요로 한다.

V. 결 론

개방형 통신망이 점차 확장되고 발달에 따라 정보의 누출과 조작이 용이하게 되었으며, 전자결재시스템 상에서 보안문제의 해결책은 암호화 기법이 가장 효율적임이 잘 알려져 있다.

본 논문에서는 개방형 통신망에서 안전한 전자결제기법으로 통신을 위한 효율적인 암호화 알고리즘을 제시하였다. 그 특징은 다음과 같다.

1. 암호 KEY 관리측면에서 KEY를 전송하지 않고 KEY생성을 위한 파라미터 값을 암호화하여 전송한다.

2. 그리고 파라미터 값은 난수에 의해 임의적으로 생성되고 난수는 주기적으로 바뀌도록 하여 데이터량에 따라 암호화 강도를 높였다.

3. 암호화 알고리즘의 효율성 측면에서 처리시간 단축을 위해 파일을 압축하였다.

4. 그리고 자료처리 및 데이터 저장 측면에서 비용절감 효과가 기대된다.

본 논문에서 제시한 알고리즘은 메시지가 100KB일 때 암호화 및 복호화에 소요된 시간은 0.0152/sec 소요되었고, 8 바이트 단위의 메세지를 나노초 속도의 컴퓨터로 해독하는데 약 3.4개월이 소요된다. 그리고 key를 생성하기 위한 파라미터 값이 주기적으로 변경되므로 데이터의 양에 따라 암호화의 강도는 더욱 향상되어 실무에서의 강력하고 효율적인 보안 알고리즘으로서의 활용이 가능하다고 판단되었다.

앞으로 보안의 강도를 강화하기 위한 보다 효율적이고 더욱 안전한 암호화 알고리즘을 위해 Key 생성을 위한 parameter를 별도로 유지하는 문제와 key값 생성 테이블 재생성에 따른 문제에 대한 지속적인 연구가 요구된다.

참고문헌

[1] 황희철, "전자서명과 법률문제", 정보법학 제2호

[2]HTTP;//kmh.yungnam-c.ac.kr/networkprog/sec/

[3] 김규성, "분산체제에서의 데이터 통신을 위한 보안 알고리즘의 설계 및 평가", 경남대학교 대학원, 1995.6

[4] 김영실, "데이타 통신에서의 보안을 위한 암호화 알고리즘 설계 및 구현", 경남대학교 대학원, 1995

[5] 임채훈, "VoIP 시스템에서의 보안기술" 정보처리학 제8권, 2001.3.[

[6] 강신각, 박정수, "월드 와이드 웹 보안기술", 정보처리학회 제7권2호, 2000.3.

[7] 염용섭, 강경희, 황미화, "KT-EDI 정보보호시스템", 98추계 학술발표 논문집 제5권 제2호,1998.10

[8] 신상욱, 이경현,"ALL-or-Nothing 성질을 지닌 해쉬함수", 98추계 학술발표 논문집 제5권2호 ,1998.10

[9] 최윤복, 김태연, 노봉남,"개방형 분산환경에서 에이젠트 기반접근제어", 98추계 학술발표 논문집, 제2권2호,1998.10

[10] 박윤식 "DES 암호화 과정에서 발생될수 있는 제어문자 처리를 위한 연구 " 경상대학교대학원, 1995.8

[11] 정진욱, 변옥환, " 데이터 통신과 컴퓨터 통신망에서 보안 기법", 정보과학회지 1권 5호, 1983.

[12] 유성진, 김성열, 정일용, "안전한 전송을 위한 RPC기반의 정보보안 시스템 설계", 98추계 학술발표 논문집 제5권제2호, 1998.10

[13] 전태건, 김창수," 멀티미디어 전자우편보안시스템 분석과 설계에 관한 연구", 98추계학술발표논문집,1998.10

[14] 이윤아, 장경선," PES 알고리즘의 FPGA구현", 98추계학술발표논문집 제5권2호, 1998.10

[15] CHARLES P. PELEEGER, "security in computing", preutive-hall International Editions.

[16] dorothy E.Denning, cryptography and data security", Adison Wesley publishing company, pp 101~ 147, 1982.

[17] bransted, Dennis K, "Consideration for Security in the osi architecture", IEEE network Magazine,1987