암호화를 이용한 전자결재 시스템의 설계 및 구현

장 용 철[†] · 오 태 석[††] · 오 무 송[†††]

요 약

컴퓨터를 이용한 정보처리가 일반화 되고 컴퓨터 통신망을 통한 문서양식의 통폐합 및 간소화는 되었지만 문서의 결재는 여전히 수작업으로 이루어지고, 컴퓨터의 역기능이 급증하면서 문서에 대한 보안 사항들의 부정 유출도 심해서 기업의 기밀이 타기업으로 넘어가 커다란 타격을 받는 경우가 발생하여 이를 개선하는 방안으로 문서를 효율적으로 이용하고 중요한 문서에 대한 보안유지와 문서결재의 신속성을 추구하며 보관된 문서는 변형된 Vernam의 암호화 기법을 이용하여 클라이언트/서버간에 기능을 분담할 수 있는 전자결재 시스템을 설계 및 구현한다.

Design and Implementation of Electronic Approval System using Encryption

Young-Chul Jang[†] · Teh-Sok Oh[††] · Moo-Song Oh[†††]

ABSTRACT

Information processing using computer is generalized in the office automation. In spite of to be integrate and concise form of document through computer network, signature of document with hand have processed as ever. The security on document flow out severely unjust by reason of increment inverse function of computr. Because of revelation secret of enterprise result from unjust outflow, lots of loss of self-enterprise is occured.

In this paper, we used efficiently document using the method, electronic approval system with encryption, for the resolving above problems. Also we pursue maintenance of security for the important document and process document signature rapidly. Finally, we design and implementation of electronic approval system that take one's share of function between server and client using to be transformed Vernam's encryption technique in stored document.

1. 서 론

최근 정보처리 기술이 급격히 진보되어 컴퓨터 통신 회선을 통해 서로 연결되고 수많은 단말기들이 근거리 또는 원거리에 부착됨에 따라 명실상부한 종합적 정보 시스템이 구축되고 있으며 이러한 정보 시스템의 보급 확대로 우리 사회는 고도의 정보화 사회로 진입되고 있다.

현업무가 갖고 있는 보안 사항들의 부정 유출이 심각한 문제들로 대두되면서 이를 보호하기 위한 적절한 보안 대책이 필요할 것으로 보인다[1]. 이러한 예

※이 논문은 1995년도 조선대학교 학술연구비의 지원을 받아 연구되었음.
† 정 회 원:목포전문대학 전산정보처리과 조교수
†† 정 회 원:목포전문대학 전자과 조교수
††† 정 회 원:조선대학교 컴퓨터공학과 교수
논문접수:1997년 1월 7일, 심사완료:1997년 7월 23일

기치 못한 컴퓨터의 역기능이 급증하는 이유는 기존의 사무처리가 주로 종이를 이용하여 이루어지던 것이 현재에는 컴퓨터의 보급으로 통신 회선을 통하여 서로 연결된 컴퓨터와 단말기를 통해 이루어짐에 따른 환경의 변화와 이에 따라 발생하는 보안상의 약점을 현행 정보시스템이 적절히 대처하지 못한데 그 근본 원인이 존재한다.

이러한 정보시스템은 과거의 문서 보안과는 다른 보안상의 특징을 가지며 전자결재 시스템에서 중요한 부분 중의 하나가 데이터의 보안이므로 보안상의 특징과 전자결재 시스템에서 암호화 방법에 대해서 연구한다.

전자결재가 이루어지는 부분은 컴퓨터를 이용하여 자료를 주고 받는 거의 모든 현업무에서 이용이 확산되리라 생각을 하고 본 연구에서는 사무 자동화의 일환으로 이제 까지 사람의 손으로 직접 문서의 결재를 받았던 것을 컴퓨터를 통해서 결재 할 수 있도록 구현하고 문서관리의 결재 데이터는 보안의 측면을 고려해서 클라이언트/서버 간에 기능을 분담하도록 데이터베이스를 설계한다.

2. 전자결재 시스템의 모델

2.1 전자결재 시스템의 출현배경

현대사회가 정보화 사회라는 점은 누구도 부정할 수 없으며 최근 몇 년 사이에 세계를 하나로 연결하는 인터넷등이 그 중의 일예라고 할 수 있다. 정보통신의 발달로 국내의 업체들은 거의 사무 자동화가 이루어지고 중소업체에서도 사무 자동화를 추진하고 있는 중이다.

그러나 이러한 사무 자동화가 되어 있는 현업무에서도 일부분만 사무 자동화가 이루어져 있어서 완벽한 사무 자동화 시스템을 구축하기 위해서는 많은 투자와 연구를 거듭해야 할 것이다. 이제 까지 일반 문서나 기밀 문서를 사람이 직접 작성했고 많은 문서를 좁은 공간에 보관해 왔을뿐 아니라 기밀 문서의 외부 유출이나 도난 등에 대해서는 안이하게 생각을 했었다.

따라서 문서 기안자는 컴퓨터를 이용해 문서를 작성하여 결재권자에게 컴퓨터를 통해서 결재를 받고 결재된 문서는 컴퓨터의 데이타베이스에 보관되도록 설계하여 문서결재를 빠르고 편리하게 하며 또한 기밀 문서 유출 등에 보안을 취할 수 있게하는 것이 전자결재 시스템의 출현 배경이라할 수 있다.

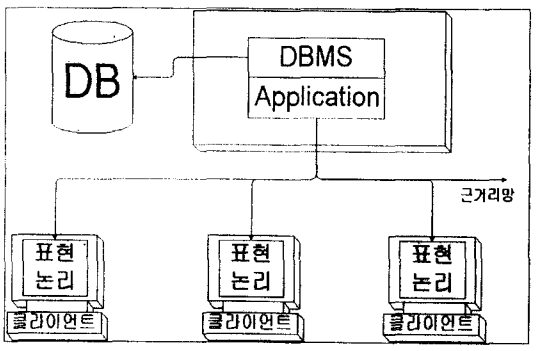
2.2 전자결재 시스템의 구성

전자결재 시스템 구성의 특징은 네트워크상에 트래픽을 줄이기 위해서 단위 부서별로 브리지/라우터 기능이 있는 LAN장비를 도입했으며 문서관리용 결재 서버를 단위부서별로 두는 클라이언트/서버간에 기능을 분담하도록 데이터베이스를 설계하였고, 사용자별 PC로 구성된 클라이언트에서는 안내 및 에러 화면과 같은 사용자 인터페이스기능, 기안문서 작성 기능, 결재처리 조회 등 관리기능을 담당하고 서버시스템에서는 결재 진행상태 관리, 부서별 문서관리의 기능을 담당한다 〈표 1〉.

〈표 1〉 Client/Server의 기능
〈Table 1〉 Function of client/server

클라이언트	서버
사용자 인터페이스 담당	결재경로 변경
기안문서 작성	결재진행상태 관리
문서결재	부서별 문서관리
문서조회	부서별 문서조회

시스템 하부 구조인 네트워크는 (그림 1)과 같이 PC(팬티엄)간에 통신기술을 활용하기 위해서 윈도우즈NT 3.51환경에서 윈도우즈 프로그래밍 언어인 Visual Basic을 이용하여 문자 도형등이 포함된 복합정보에



(그림 1) 전자결재 시스템의 Network 구성도
(Fig. 1) Network structure diagram of electronic approval system

대해서는 문서의 보관 및 전송이 쉽고 편리하게 하였고 결재권자가 문서의 반송을 위해 사용한 음성합성의 원리를 이용한 녹음기 기능은 사운드 카드를 사용하였으며 문서처리 기능에서는 윈도우즈 워드프로세스를 사용할 수 있게 구성하였다.

2.3. 전자결재 시스템의 패스워드 관리

정보에 대한 접근은 기본적으로 읽기, 쓰기, 실행 등의 유형이 있다. 각 사용자들이 각 파일에 대해서 읽기, 쓰기, 실행중 어떤 종류의 접근을 할 자격이 있는지 적절한 기준에 따라 명시하여야 하며 접근의 통제를 위해서는 사용자에 대한 3가지 통제의 개념이 필요하다[2].

(1) 식별(Identification): 입력된 패스워드가 정당한 패스워드인가를 체크 하고 패스워드의 주인을 식별한다.

(2) 인증(Authentication): 패스워드를 입력한 사람이 그 패스워드의 정당한 주인 인가를 인증한다.

(3) 허가(Authorization): 패스워드를 입력한 사람이 요구하는 작업이 그 패스워드의 주인에게 인가된 작업인가를 확인한다. 이는 각 부서원에 대해 각 파일에 대한 접근유형별 자격을 미리 컴퓨터에 입력 저장하여 둠으로서 수행된다.

이러한 세가지 통제를 수행하기 위해서 패스워드를 통한 통제법이 있는데 이는 매우 간단하여 사용자에게 큰 불편을 주지 않는다는 장점이 있는 반면에 인증기능에 대해서는 취약하다는 단점이 있다.

3. 전자결재 시스템의 설계 및 구현

이장에서는 전자결재 시스템의 개요에 대하여 설명을 하고 전자결재 시스템의 기본 설계에 대해서 살펴본다.

3.1 전자결재 시스템의 개요

문서 양식의 통폐합 및 간소화로 전산자료의 전송체제와 전자우편을 이용한 정보의 전달과 의사소통은 신속성과 간편성을 이룩해 왔으나 문서의 결재 과정은 여전히 인쇄된 문서에 서명을 하는 체제를 유지하고 있다. 이로 인한 기안자와 수신자의 결재과정은 공통적으로 인쇄기를 통해 출력된 문서에 서명을 하는 결재 과정을 유지하면서 문서를 별도로 보관하는 이중보관 체제를 가질 수 밖에 없었으며 특히 지점이 원거리에 있는 경우에 결재권자에게 결재를 위해서 우편발송이나 결재권자에게 직접 가야하는 소요시간 및 인적 낭비가 클 뿐만 아니라 보안의 여러 측면을 고려하여 사원들이 알고있는 정보를 교체하기 위해서 부서를 강제로 이동시키는 것은 당연한 것으로 생각했다.

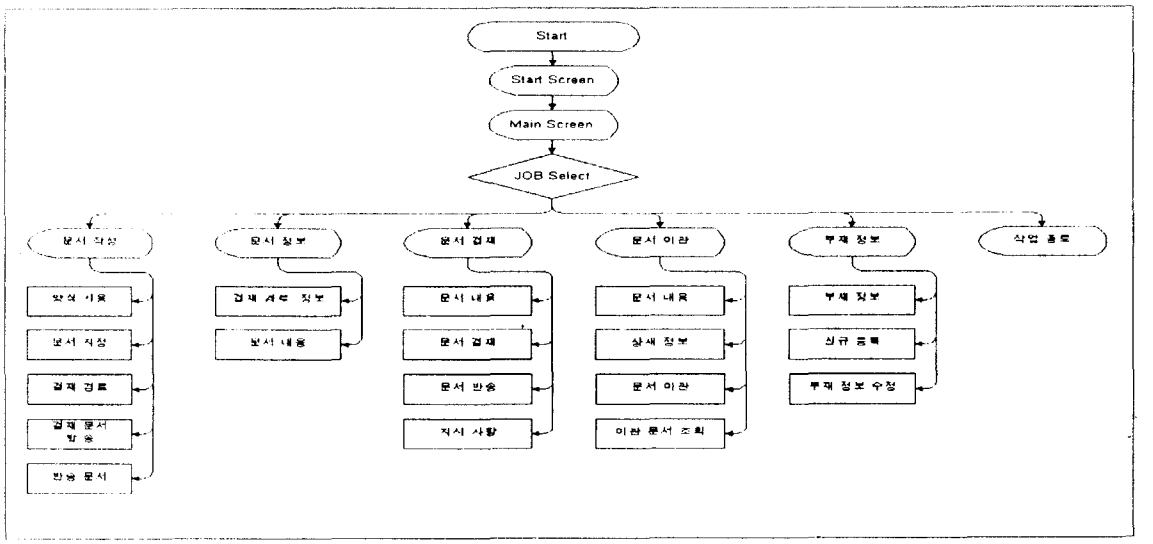
기존의 많은 기업들은 사원들간에 신뢰를 기본으로 중요한 결재 문서를 결재권자의 손으로 서명을 하면서 개인에 대한 프라이버시의 침해뿐만이 아니라 이미 결재된 보관 문서의 내용이 사원들에게 공개 되어서 기업의 기밀이나 보안유지가 되지 않아 쉽게 경쟁 기업으로 넘어가 자회사에 커다란 타격을 받는 경우가 발생했다. 이렇게 수작업으로 작성된 문서등을 보관 또는 이관하는 작업을 효율적으로 이용하고 기밀이나 보안유지의 해결방법으로 전자결재 시스템을 이용한다.

3.2 전자결재 시스템의 설계

전자결재 시스템의 기본기능은 〈표 2〉와 같고 문서작성, 문서결재, 문서정보, 부재정보, 문서보관등은 (그림 2)와 같이 설계한다.

〈표 2〉 전자결재 시스템의 기본기능
〈Table 2〉 Basic function of electronic approval system

기본설계	주요기능
문서작성	기안을 위한 양식사용, 문서지정, 결재경로의 지정, 문서의 발송등을 한다.
문서결재	결재권자의 미결문서에 대해 문서보기, 결재, 반송, 결재경로변경등의 작업관리를 한다.
문서정보	미결재 문서 및 이관전의 반송서류에 대한 정보를 가진다.
부재정보	사용자의 출장 등에 대비하여 자신의 부재를 등록, 결재권자의 부재정보를 참조할 수 있다.
문서이관	결재 문서에 대해 완결이 되고 참조가 완료된 후 기안자가 따로 보관하고자 할 경우의 해당 문서에 대한 이관작업을 한다.
작업종료	전자결재의 모든 작업을 종료한다.



(그림 2) 전자결재 시스템의 기본기능
(Fig. 2) Basic function of electronic approval system

3.3 전자결재 시스템의 보안 및 암호화

3.3.1 전자결재 시스템의 보안

자산과 자원이 침해받을 수 있는 가능성을 최소화하는 것을 보안이라 말하며[3] 전자결재로 업무를 처리하기 위해서 전자 문서의 송수신시 정당한 권리를 갖고 있지 않은 제3자가 관련 데이터를 변조, 훼손 또는 첨가하는 것을 방지하고 거래 당사자가 송수신 사실을 부인하지 못하게 하는 보안 대책이 매우 필요하다[3].

보안상의 위협요인들에는 제3자에 의한 불법적인 접근 및 이용, 전자문서의 분실 및 중간에서의 변경, 전자문서가 제3자에 의해서 읽혀지는것, 거래 당사자의 송수신 사실을 부인하지 못하게 한다는등의 요소가 있다[4].

보안을 하는데 고려사항을 보면 사용자의 인증확인(Authentication), 데이터가 불법으로 노출되는 것을 방지(Confidentiality), 데이터의 무결성을 점검(Integrity), 데이타 송수신 사실 부인(Non-repudiation), 데이터베이스로의 접근통제 및 정당성 확인(Access control) 등을 고려해야 한다[6]. 이러한 보안을 하기 위한 대책으로는 스마트 카드(Smart card)를 사용한다든지 사용자ID 및 Password를 정기적으로 변경 해주어야 하며 전자문서 통제 절차를 강화하고 전송된 데이터의 정확한 전달 여부 및 송신자 확인을 해야 한다[6].

기술적인 보안대책 으로는 다음과 같은 것이 있다[6][7].

(1) 운영체제 액세스 통제

액세스 통제가 운영체제의 중요한 기능이라 하지만 오늘날 사용되는 대부분의 운영체제는 액세스 통제 기능을 완벽히 하지 못하고 있는 현실이다.

운영체제가 통제를 강력하게 할 수록 컴퓨터 시스템은 더욱 안전 해지는데 운영체제가 얼마나 액세스 통제 능력을 갖고 있는지 평가하는 기준은 앞에서 언급된 식별, 인정, 허가 능력이다.

(2) DBMS 액세스 통제

데이타베이스는 대개 체계-하부체계의 구조로 구성되어 있는데 체계는 데이타베이스를 구성하는 모든 데이터를 총칭하는 것이고 하부체계는 특정한 프로그램이나 프로그램의 집합체의 수행시 요구되는 데이터들만 지칭하는 것이다. 하나의 체계 속에는 여러 개의 하부체계가 존재하는데 하부체계는 여러 개의 체계에 의해서 표현이 되어지고, 데이타베이스에서 하나의 View로 인식이 되어질 수 있다. 따라서 데이타베이스의 보안과 안전한 DBMS의 구축을 위해서는 데이타베이스 설계시 하부체계나 View에 대한 액세스 통제를 염두에 두어야 한다.

(3)네트워크 보안

네트워크는 개방 네트워크와 폐쇄 네트워크로 구분하는데 불법적인 액세스의 형태는 비슷하지만 개방 네트워크에서는 시스템의 외부인이 네트워크에 더 쉽게 접근할 수 있으므로 폐쇄 네트워크보다 그 취약성이 더욱 심각하다고 할 수 있다.

개방 네트워크에서 안전한 액세스 통제를 구축하기 위해서는 다음과 같은 방법이 있다.

①개방 네트워크의 액세스 통제

- 시스템에서 만들고 시스템에서 제어하는 패스워드 시스템
- 통신 위주의 암호화
- 보안의 특성을 보유하고 있는 통신 설비
- 적절한 서명 인정 시스템
- 안전한 DBMS의 설계

②폐쇄 네트워크의 액세스 통제

개방 네트워크에 비하여 폐쇄 네트워크의 액세스 통제의 특징은 사용자들의 엑세스가 파 악되기 쉽고 국부적으로 설치되어 있으며 다이알 시스템으로 액세스 되지 않는다는 점이다.

폐쇄 네트워크에서 안전한 액세스 통제를 구축하기 위해서는 다음과 같은 방법이 있다.

- 상호응답 기구
- 외부 통신 보호 위주의 액세스 통제 소프트웨어
- 불법적 정보 채널의 금지
- 통신을 위한 하드웨어, 소프트웨어 암호화 체계

폐쇄 네트워크내의 자원의 분리가 이루어지면 민감하지 않는 자원에 대해서는 사용자들에게 개방을 하고 민감한 자원에 대해서는 폐쇄를 시킴으로서 유용성을 증가시킬 수 있다.

(4)단말기 접속 통제

한 사용자가 공공 통신망을 통하여 단말기를 호스트 컴퓨터에 접속시키려 시도할 때 호스트 컴퓨터는 이 사용자가 정당한 사용자인가를 확인을 할 때 패스워드를 사용하는 방식, 최근에는 Callback 시스템, 발신측 신호를 확인하는 방식, 암호 방식을 이용한 디지털 서명 방식등이 확인 방법으로 이용된다.

3.3.2 전자결재 시스템의 암호화

암호화 기법은 비인가자가 알지 못하도록 보통문을 암호문으로 변형시키고 허가자로 하여금 필요시에 다시 암호문을 보통 문으로 복호화 시킬 수 있도록 하는 체계를 뜻하며 암호화 되지 않은 원래의 데이터인 평문(Plaintext)알고리즘에 사용되는 변수인 키(Key)와 암호화 알고리즘에 의해 변형된 데이터인 암호문으로 구성되어 있다[8]. 보통문을 암호문으로 되는 과정을 암호화 과정이라 하고 암호분을 보통문으로 만드는 과정을 복호화 과정이라 한다. 암호 시스템을 구성하는 요소는 (그림 3)과 같다[9][10].

(가)보통문 P

(나)암호문 C

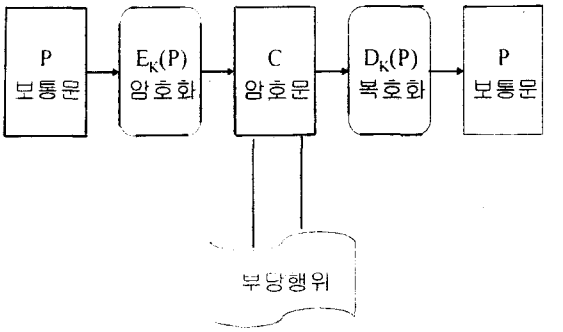
(다)키 K

(라)암호화 알고리즘 E_k

$E_k(P)=C$

(마)복호화 알고리즘 D_k

$D_k(C)=P$



(그림 3) 암호 시스템
(Fig. 3) Encryption system

(가) Vernam의 암호화

Vernam의 암호화 방식은 논리연산인 Exclusive-OR의 연산을 하며 BCD 표를 이용하여 보통문과 키를 이진수로 변환하여 암호화 문자로 대치한다[11].

〈표 3〉 Vernam 암호화의 예
〈Table 3〉 Example of Vernam encryption

보통문		C(010011)	O(100110)	D(010100)	E(010101)
키	⊕	N(100101)	A(010001)	M(100100)	E(010101)
		110110	110111	110000	000000

〈표 3〉에서의 결과는 "WX50"으로 암호화가 이루어짐을 알 수 있다.

(나) DES(Data Encryption Standard)알고리즘

DES의 암호화 알고리즘은 컴퓨터의 데이터를 보호하기 위한 수학적인 알고리즘으로서 위치교환법과 대치기법으로 TUCMAN, CARL MEYER의 연구를 포함해 IBM에서 개발한 기법이다.

이 알고리즘은 BCD 데이터를 사용하여 64비트의 정보를 암호화하기 위하여 64비트의 키를 사용하여 현재는 일반적으로 널리 알려져 있으므로 키 관리가 보안성의 성패를 좌우한다.

암호화된 데이터는 역순의 절차를 거쳐 평문의 데이터로 환원될 수 있으며 64비트의 키 중에서 56비트만 사용하고 나머지 8비트는 패리티 검사용으로 사용한다[11].

$$L_i = R_{i-1} \tag{1.1}$$

$$R_i = L_i - 1 \oplus f(R_i - 1, K_i) \tag{1.2}$$

(1.1)과 (1.2)를 간단히 변형하면 다음과 같다.

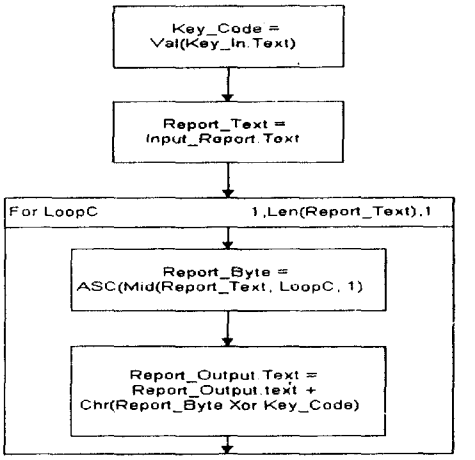
$$R_{i-1} = L_i \tag{1.3}$$

$$L_{i-1} = R_i \oplus f(R_{i-1}, K_i)$$
$$= R_i \oplus f(L_i, K_i) \tag{1.4}$$

따라서 식(1.3), (1.4)을 살펴보면 i 라운드의 결과로서 (i-1)라운드의 결과를 유도할 수 있다. 그러므로 복호화를 위해서 암호화시 사용된 키 K_1, K_2,..., K_{16}를 역순인 K_{16},..., K_2, K_1순으로 적용하여야 함을 알수 있고, 암복호화시 16라운드 후에는 좌우측을 반드시 교환해 주어야 동일한 순서로 올바른 암복호화가 가능하다.

(다) 변형된 Vernam의 암호화

본 전자결재 시스템에서 보안을 위한 암호화는 Vernam암호화 기법을 변형한 것으로 문서작성자에 의해서 작성된 문서를 다른 부서원이 볼수 없게 부서원 고유의 ID를 입력하여 부서 ID를 구분한 후 암호 Key 테이블과 XOR연산의 결과를 데이터 베이스에 암호화하여 저장 되므로 다른 부서에 있는 부서원들은 그 문서에 대한 내용을 볼수 없게 암호화 시켰으며 문서결재를 위한 결재권자만이 지정된 문서를 다시 복호화하여 볼수 있다. 입력된 문서를 암호화 하는 Flow chart는 (그림 4)와 같다.



(그림 4) 변형된 Vernam 암호화 flow chart
(Fig. 4) Transformation Vernam encryption flow chart

입력된 문서를 문자 단위로 절단한후 절단된 문자를 ASCII Code로 변환하고, 변환된 Code와 암호 Key인 부서 Code를 XOR연산을 수행하여 암호화된 문자들이 생성되며, 생성된 문자들을 순서에 맞추어 연결한 후 저장하면 암호화된 문서가 생성되며 그에 따른 알고리즘은 (그림 5)와 같이 구현된다.

```
Private Sub Convert()

    Dim Key_Code As Byte
    Dim Report_Byte
    Dim LoopC

    Key_Code = Val(Key_In.Text)
    Report_text = Input_Report.Text

    For LoopC = 1 To Len(Report_text)

        Report_Byte = Asc(Mid(Report_text, LoopC, 1))
        Report_Output.Text = Report_Output.Text + _
                Chr(Report_Byte Xor Key_Code)
    Next LoopC

End Sub
```

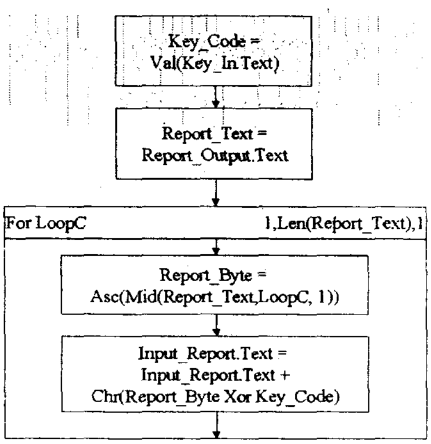
(그림 5) 변형된 Vernam 암호화 알고리즘
(Fig. 5) Transformation Vernam encryption algorithm

위의 알고리즘을 이용하여 입력된 문서를 처리한 결과는 (그림 6)과 같다.

[illegible]	朝鮮 대학교 Multimedia Lab.
부서 Code	암호화된 문서
01	條鳳!닳한괄!Ltmuhldeh`!M`c/
02	粟屑"닺할괏"Ownvkogfkc"Nc`,
03	檣楔#닻칠곕#Nvowjnfgjb#Oba
...	....
10	措詵•닮핸국•G[f~cgonck•Fkh$
11	揉跣+ 닯햏구+ F~g[bfnobj+ Gji%
12	旱選,당햄굟,Ay`xeaihem,@mn"
...	....
100	梯善D곷쿼그D) ◀ㅓ♪ ┌♪ ID(ㅓ-J
101	瀛嬋E곷쩡글E(ㅓ ◀ㅁ┌ㅇE)┘•K
102	祭宣F굜뮈균F+ ‼[0ㄴ0•F•┘H
...	....
123	諸署[큭퐄궐[6ㅐㅇㅣ┬▲▼l-[7→ㅏU
124	踊西₩퀵푼귄₩1 ┼ㅁ┴◀ㅓㅣ┴-₩0-▲R
125	酲犢}큌퓸귂}0■◀ ㅒ+ㅣㅒㄴ]1ㄴ▼S

(그림 6) 변형된 Vernam 암호화의 처리결과
(Fig. 6) Result of transformation Vernam encryption

암호화된 문서를 복호화 하기 위한 Flow chart는 (그림 7)과 같다.



(그림 7) 변형된 Vernam 복호화 flow chart
(Fig. 7) Transformation Vernam decipherment flow chart

암호화된 문서를 문자 단위로 다시 절단한 후 절단된 문자를 ASCII code로 변환하며 변환된 code와 암호화시 사용되었던 암호 Key인 부서 code를 XOR연산을 수행하면 보통문의 문자로 복호화되고 복호화된 보통문의 문자들을 순서에 맞추어 조합한 후 저장한다. 그에 따른 알고리즘은 (그림 8)과 같이 구현된다.

```
Private Sub UnConvert()

    Dim Key_Code As Byte
    Dim Report_Byte
    Dim LoopC

    Key_Code = Val(Key_In.Text)
    Report_text = Report_Output.Text

    For LoopC = 1 To Len(Report_text)

        Report_Byte = Asc(Mid(Report_text, LoopC, 1))
        Input_Report.Text = Input_Report.Text + _
                Chr(Report_Byte Xor Key_Code)
    Next LoopC

End Sub
```

(그림 8) 변형된 Vernam 복호화 알고리즘
(Fig. 8) transformation Vernam decipherment algorithm

위의 암호화 작업에서 생성되었던 결과를 다시 복호화 한 결과는 그림 9와 같다.

부서 Code	복호화된 문서
01	朝鮮 대학교 Multimedia Lab.
02	朝鮮 대학교 Multimedia Lab.
03	朝鮮 대학교 Multimedia Lab.
...	....
10	朝鮮 대학교 Multimedia Lab.
11	朝鮮 대학교 Multimedia Lab.
12	朝鮮 대학교 Multimedia Lab.
...	....
100	朝鮮 대학교 Multimedia Lab.
101	朝鮮 대학교 Multimedia Lab.
102	朝鮮 대학교 Multimedia Lab.
...	....
123	朝鮮 대학교 Multimedia Lab.
124	朝鮮 대학교 Multimedia Lab.
125	朝鮮 대학교 Multimedia Lab.

(그림 9) 변형된 Vernam 복호화의 처리결과
(Fig. 9) Result of transformation Vernam decipherment

3.5 전자결재 시스템의 구현

(그림 10)과 같이 전자결재 시스템 접속시 시스템 관리자가 사용자에게 계정된 ID 및 패스워드를 관리하고 사용자는 네트워크와 연결을 위하여 시스템 관리자에게 부여 받은 ID 및 패스워드를 입력하여야만이 전자결재 시스템의 사용권한을 허가 받는다.

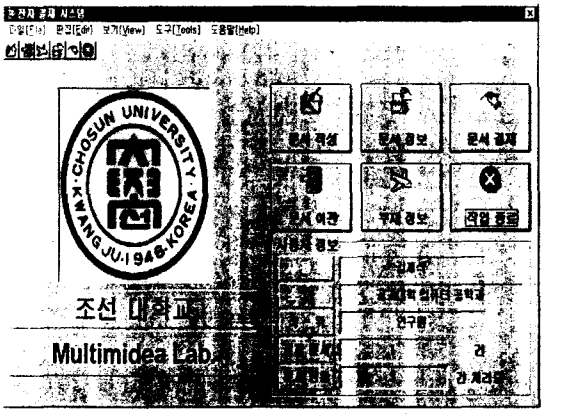
(그림 11)과 같이 전자결재 시스템 관리자는 사용자의 로그인 ID와 패스워드가 정당한가를 체크하고, 정당한 사용자인가 신분을 확인한 후 전자결재 시스템을 사용할 수 있게 구현한다. 문서 작성의 기능은

(그림 12)에서와 같이 문서를 작성하는 사람이 원하는 문서의 양식이 기안문서인지 첨부문서인가를 선택하여 사용할 수 있으며 문서 작성자는 문서를 지정 사용하고자 하는 문서를 지정하여 문서를 결재 받고자 하는 결재권자들을 차례로 지정하면 작성문서는 지정된 결재권자에게로 네트워크를 통해 전송이 이루어진다.

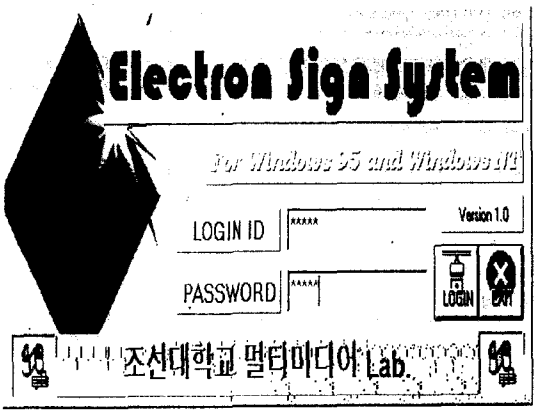
문서결재의 기능은 (그림 13)에서와 같이 문서 작성자에 의해 전송된 문서를 결재권자는 문서의 내용을 해당 워드프로세스를 통해서 확인한 후 문서에 대한 결재인가, 반송인가를 결정하게 된다. 반송된 문서에 대해서는 결재권자의 음성을 윈도우즈에 있는 녹음기 기능을 이용하여 전송하고 텍스트는 윈도우즈 환경의 해당 워드프로세스를 사용하여 지시사항을 반송함으로 문서작성자에게 지시사항을 쉽게 알 수 있도록 구현되었다. 결재된 문서를 보관하기 위해서는 변형된 Vernam의 암호화 방식을 이용해 데이터베이스에 저장되게 한다.

문서정보 기능은 아직 결재완료 되지 않은 문서나 이관되기 전까지의 완결된 문서에 대해서 문서작성자에게 문서에 대한 정보를 제공해 주고 문서에 대한 세부사항 정보들 뿐만이 아니라 결재권자에 의해서 반송된 문서에 대한 정보도 볼 수 있게 (그림 14)에 나타나 있다. 부재정보 기능은 결재권자의 출장 등에 대비하여 결재권자의 부재를 등록하여 문서작성자로 하여금 부재정보를 알수 있고 부재정보에 대한 등록은 결재권자만이 등록이 가능하고 문서작성자는 부재정보에 대한 참조만 할 수 있으므로 결재권자의 부재시에도 그 누구도 결재권자를 대신해서 결재를 할 수 없도록 (그림 15)에 나타나 있다.

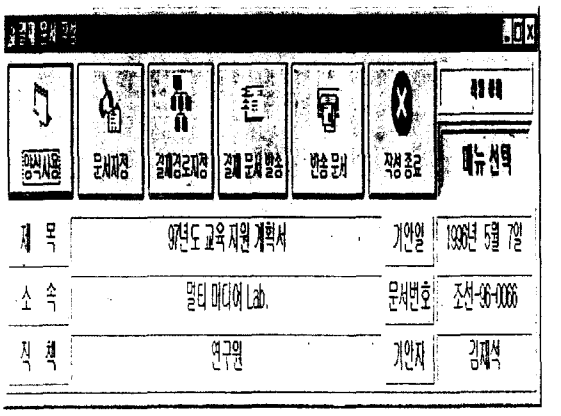
문서이관 기능은 결재를 올린 문서에 대해서 완결이 이루어 지고 참조가 완료된후 문서작성자가 문서를 보관하고자 할 경우에 해당문서에 대한 문서의 내용을 해당 워드프로세스를 통해서 볼 수 있으며 이관된 문서에 대해서는 상세한 정보도 검색할 수 있다.



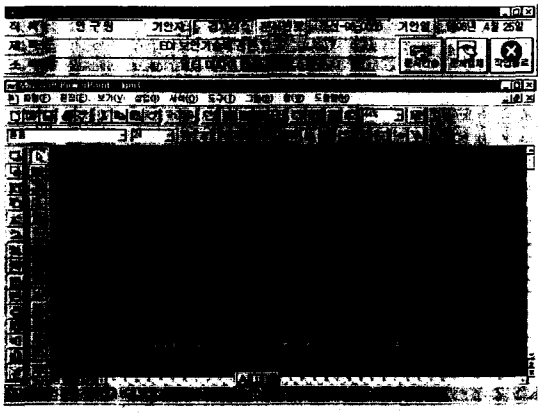
(그림 11) 전자결재 시스템의 주 화면
(Fig. 11) Main screen of electronic approval system



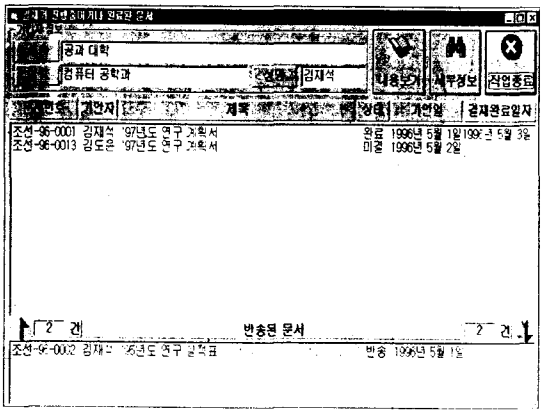
(그림 10) 전자결재 시스템의 LOGIN 화면
(Fig. 10) Login screen of electronic approval system



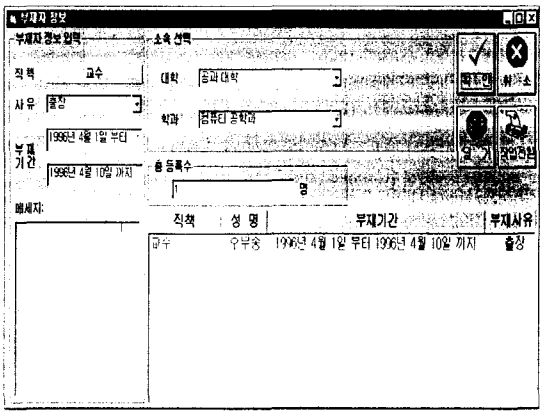
(그림 12) 결재 문서 작성 화면
(Fig. 12) Document description screen



(그림 13) 문서 결재 화면
(Fig. 13) Document approval screen



(그림 14) 문서 정보 화면
(Fig. 14) Document information screen



(그림 15) 부재 정보 화면
(Fig. 15) Absent information screen

4. 결 론

전자결재 시스템 구축에 따라 문서의 Life-Cycle 전 단계를 체계적으로 통합 관리함으로서 다양한 문서 처리 요구를 충족시킬 수 있으며 문서 보관의 중복성 배제, 저장된 문서의 공유, 문서검색의 신속화가 이루어졌으며 모든 공통양식의 데이터베이스화를 통한 양식관리의 용이성, 결재대기시간의 절약, 새로운 정보처리 기술의 습득에 따른 정보제공 시스템 구축의 기반이마련 되었다. 기존의 전자결재 시스템은 결재권자의 인장이나 서명을 미리 데이터베이스에 여러 개 만들어 놓고 필요할 때 마다 불러 사용함으로서 타인에게 서명이 노출될 확률이 많으므로 문서가 위조될 가능성도 높았다. 본 논문에서는 이런 제반 문제를 극복하기 위해서 문서를 검색할 수 있는 일반 사용자들에게 로그인ID에 보안의 등급을 주어 이관 문서나 저장된 문서에 대해서 쉽게 접근할 수 없게 함으로서 문서에 대한 유출은 없었다.

본 논문의 전자결재 시스템은 윈도우즈 환경하에서 사용할수 있도록 구현 되었으므로 초보자도 전자결재 시스템을 통하여 문서의 작성 및 결재를 쉽게 할 수 있었으며 전자결재 시스템은 기안자가 작성한 문서는 근거리 또는 원거리에 떨어져 있는 부서간에도 네트워크를 통해 결재권자에게 전송되므로 결재과정에서 부서원들이 직접방문해서 결재를 받을 경우보다 시간적인 절약과 결재의 번거로움이 사라지고 반송된 문서에 대한 결재권자의 지시사항을 문서 작성자는 쉽게 파악할 수 있으므로 업무의 신속성을 추구할 수 있었다.

문서의 보관적인 측면에서는 좁은 공간에 많은 양의 문서를 종이로 보관함으로 문서에 대한 분실 및 보안상의 문제들이 본 전자결재 시스템에서는 문서를 변형된 Vernam의 암호화 기법을 이용함으로서 문서에 대한 보안을 유지 하였으며 사무 자동화의 일환으로 종이없는 사무실(Paperless office)의 효과도 기대한다.

앞으로의 연구과제는 본 연구에서 이용한 변형된 Vernam의 암호화 기법은 암호화 테이블을 담당자 외에는 아무도 모르는 것으로 간주하기 때문에 암호문의 상태는 양호하지만 암호 테이블이 유출 되었을 경우에는 적절한 대비책이 없으므로 그에 따른 적절한

보안 기법의 개발이 필요하며 전자결재 시스템의 신원검증 방법과 문서에 대한 보안 유지를 위해서 결재권자가 결재를 하던 현행 방법을 음성인식이나 문자인식 등으로 할 수 있도록 설계 및 구현하는 방법을 연구하는 것이 좋을 것으로 생각된다.

참 고 문 헌

[1] Bonyun, D. A., "The Secure Relational Database Management System Kernel Three Years After", IEEE Computer Security and Privacy Processings, Oakland, Ca., April 14-16, 1980, pp 34-37.

[2] W.Differ and M.E.Hellman, "Privacy and Authentication", IEEE proc. Vol. 67 NO. 3 march 1979, pp. 398-400.

[3] B.W. lampson, "protection", Proceedings of 5th Princeton Conference on Information Science and systems, princeton, N.J., March 1971.

[4] Miranda, S.M., "Aspects of Data Security in General-Purpose Management Systems", IEEE Computer Security and Privacy Proceedings, Oakland, Ca April 14-16, 1980, pp. 46-58.

[5] "Password Usage Standards," NBS publication, National Bureau of Standards, Washington, D. C., 1984.

[6] J.P Anderson, "Computer Security Technology Planning Study", EDS-TR-73-51, prepared for Deputy for Command and Management Systems, HQ Electronic System Davissio(AFSc), L.G. Hanscom Field Bedford, Mass, October 1972, vols 1, 2.

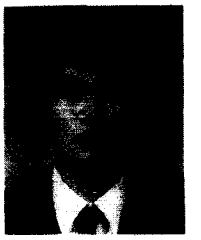
[7] "Working Draft for an Addendum to ISO 7498 on Security", International Standatds Organization, TC97/SC16, Secretariat, ANSI, October, 1984.

[8] NBS, Data encryption standard, FIPS PUB 46 By Federal Info. Processing standards Publication Jun. 15 1977.

[9] Dorothy E. Denninf cryptography and Data Security, Addison-Weseley, 1982, pp. 191-263.

[10] Charles P. Pfleeger, Security in Computing, Prentice-Hall 1989. 6. Data Encryption Standard, Federal Information processing Standard publication No. 46, National Bureau of Standards, U. S. Dept. of Commerce, Jan. 1977.

[11] Clay brook, Billy G., "Using views in a Multilevel Secure Database Management System", IEEE computer Security and Privacy Proceedings, Oakland, Ca., April 2-May 2, 1984, pp. 62-74.



장 용 철

1988년 조선대학교 공과대학 컴퓨터공학과 졸업(공학사)
1990년 조선대학교 대학원 컴퓨터공학과(공학석사)
1997년 조선대학교 대학원 컴퓨터공학과 박사과정 수료
1990년~현재 목포전문대학 전산정보처리과 조교수
관심분야:멀티미디어 시스템, 영상처리

오 태 석

1991년 조선대학교 대학원 컴퓨터공학과(공학석사)
1997년 조선대학교 대학원 컴퓨터공학과 박사과정
1992년~현재 목포전문대학 전자과 조교수
관심분야:마이크로프로세스,멀티미디어 시스템

오 무 송

1965년 조선대학교 공과대학 전기공학과 졸업(공학사)
1969년 조선대학교 대학원 전기공학과(공학석사)
1965년~1982년 조선대학교 공업전문대학 전기과 교수
1983년~현재 조선대학교 컴퓨터공학과 교수
관심분야:멀티미디어 시스템, 영상처리