데이타 보호용 모뎀 시스템

°백 기 진*, 이 창 순**, 문 상 재*
*경북대학교, **대구공업전문대학

A Secure Modem System

°Ki Jin BAEK*, Chang Soon LEE**, Sang Jae MOON*
*Kyungpook National Univ., **Daegu Technical Junior College

ABSTRACT

This paper presents the hardware development of a secure modem system for personal computers. This system consists of a data encryption system and an existing modem. The algorithm of LUCIFER-type with block size of 64-bit is used for data encryption and Diffie-Hellman method is also employed for generation of the encryption key. We implement the system in hardware using the DSP56001.

Ⅰ. 서 론

데이타 통신의 증가와 함께 공중 전화망 혹은 전용 회선망을 통한 퍼스널 컴퓨터간 데이타 통신에 모뎀을 이용한 비동기식 데이타 전송이 증가하고 있다. 이러한 비동기식 데이타 전송에 있어서 전송 데이타의 불법 유출, 삭제 및 수정 등에 대한 보호 조치는 중요하고도 필수적인 문제로 부각되고 있다. 정보 보호를 위한 대책으로는 설비면에서의 물리적 대책, 운영면에서의 인적 자원에 대한 대책 및 제도면에서의 대책 등이 있겠으나 보다 경제적이고 효율적인 방법은 기술면에서의 정보 보호 대책인 암호계(cryptosystem)를 이용하는 방법이다[1,2].

본 논문에서는 전송 데이타를 보호하기 위한 데이타 보호 장치를 개발하여 기존 모뎀에 인터페이스함으로써 secure modem 시스템을 구현하였다. 데이타 암호화 알고리듬은 관용 암호화 알고리듬인 LUCIFER[3]를 블록 크기 64비트로 변형한 것이며[4], 키

이 관리 방식으로는 Diffie - Hellman 방법[5]을 사용하였다. 데이타 보호 장치의 구현에는 고속의 디지탈 신호 처리 칩인 Motorola DSP56001[6]을 사용하였으며 본 장치를 수행할 수 있는 운용 소프트웨어도 개발하였다.

Ⅱ. Secure Modem의 구성 및 동작 원리

그림 1은 본 논문에서 구현한 secure modem의 블럭 선도를 나타낸 것이다. Secure modem의 구성은 크게 데이타 보호 전송 시스템과 기존의 모뎀으로 되어 있다. 데이타 보호 전송 시스템은 병렬 인터페이스부, 직렬 인터페이스부, 데이타 전송부, 키이 관리부 그리고 암호부로 크게 나누어진다. 이 시스템내의 전송부는 PC로부터 병렬로 전송된 데이타를 모뎀으로 직렬로 전송하고 그와 반대로 모뎀으로부터 직렬로 전송되어 온 데이타를 PC로 병렬 전송을 하는 부분이다. 키이 관리부는 공용 키이 암호 방식을 사용하여 세션(session) 키이를 생성하는 곳이며, 암호부에서는 관용 암호화 방식을 이용하여 데이타를 암호화 한다. 그리고 병렬 인터페이스부는 퍼스널 컴퓨터와 인터페이스하기 위해 사용된다.

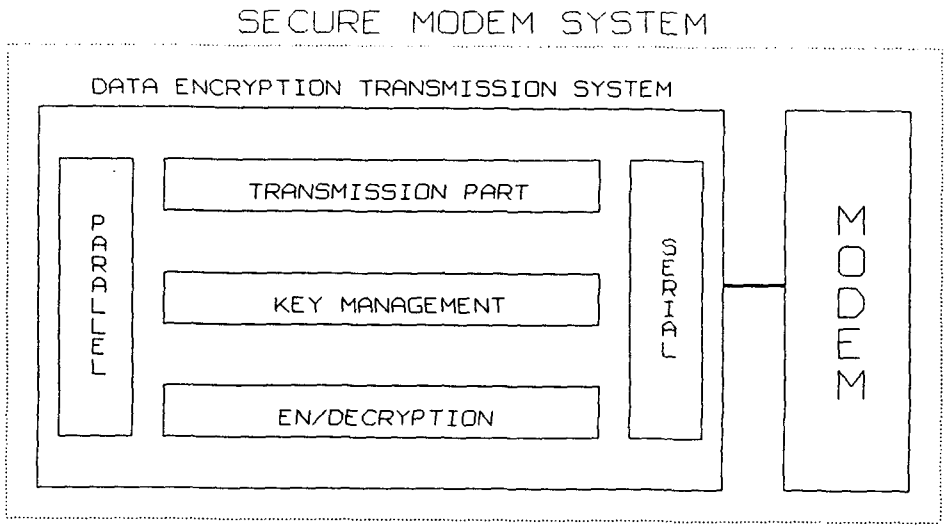

Fig. 1. Block diagram of the secure modem system

이 secure modem을 통해 데이타를 전송하고자 하면 먼저 모뎀제어 명령어(dialing)를 사용해서 송·수신자간 회선을 접속한다. 그리고 데이타를 암호화하여 전송하고자 할 때는 먼저 보호 전송 시스템내의 키이 관리부에서 공용 키이 암호 방식으로 세션 키이(session key)를 생성한다. 그런 다음 이 생성된 키이를 가지고 암호부에서 PC로부터 전송된 데이타를 암호하여 모뎀을 통해 공중 전화망으로 전송한다. 수신측에서는 송신측과 동일한 세션 키이로 복호한다. 따라서 송신측 모뎀과 수신측 모뎀사이의 공중 전화망에서는 암호화된 데이타가 전송된다.

Ⅲ. 데이타의 암호화

본 논문에서 채택한 데이타 암호화 알고리듬은 블럭 크기가 128 비트인 LUCIFER를 변형하여 DES나 FEAL-8과 같이 64 비트로 조정한 것이다[4]. 이 암호화 알고리듬에 입력되는 키이의 크기와 정보문 및 출력되는 암호문의 블럭 크기는 공히 64비트이다. 암호화는 그림 2와 동일한 형태의 과정을 8번 반복 수행하여 암호문을 형성한다.

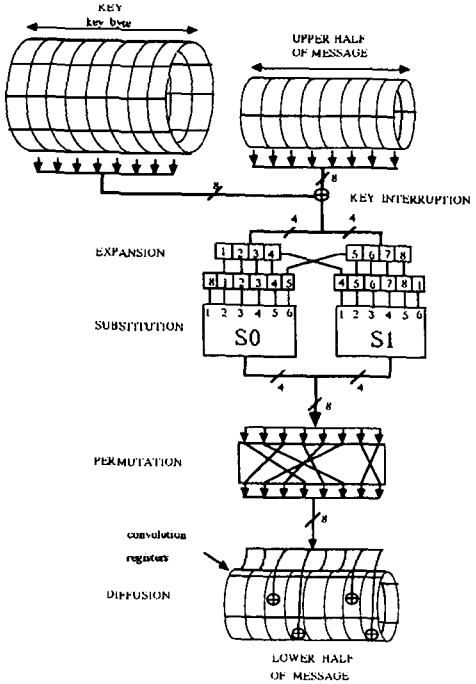

Fig. 2. The 64-bit Lucifer-type encryption algorithm

그림 2에서 입력 정보문의 64 비트는 32 비트씩 상반부와 하반부로 나누어진다. 한 라운드가 수행되는 과정에서 상반부 및 보조 키이의 영향을 받아서 새로운 32 비트의 하반부가 구성되고, 이 변형된 하반부는 최종 라운드를 제외하고는 다음 라운드로 넘어가기 전에 서로 교체되어진다. 그리고 매 라운드마다 두 개의 대체 상자와 하나의 치환 상자를 4번 반복 수행한다.

데이타 암호 또는 복호에 사용될 키이의 생성 및 분배를 보다 효과적으로 수행하기 위해서 공용 암호 키이 방식인 Diffie-Hellman 방법[5]을 적용하였다. D-H 방법은 유한체(finite field)에서의 멱승법으로 두 통신자간에 공통 키이를 생성할 수 있는 방법이다. D-H 방법에서 통신자 A는 자신의 비밀 키이 X_A와 공개 키이 Y_A($a^{X_A} \mod q$)를 가지며 통신자 B는 자신의 비밀 키이 X_B와 공개 키이 Y_B($a^{X_B} \mod q$)를 가지고 있다. 각 통신자는 통신하고자 하는 상대방의 공개 키이에 자신의 비밀 키이를 지수승함으로써 공통의 세션 키이 $K_{AB} = a^{X_A \cdot X_B} \mod q$ 를 생성할 수 있다. 본 논문에서는 가입자의 모든 공개 키이를 ROM에 저장하여 놓았으며 통신자간에 공통의 세션 키이를 생성하고자 할 때는 ROM에 저장된 상대방의 공개 키이에 자신의 비밀 키이를 지수승하도록 하였다.

Ⅳ. Secure modem 시스템의 구현

암호화 알고리듬을 하드웨어로 구현하기 위해서는 고속의 디지탈 신호 처리기가 필요하게 되었다. 따라서 본 논문에서 구현한 시스템에서는 디지탈 신호 처리기 제품중 처리 속도가 빠른 Motorola사의 56 비트 범용 디지탈 신호 처리기인 DSP56001 칩을 선택하였다. 이 DSP56001을 이용하여 데이타 보호 전송을 위한 암호화 알고리듬을 탑재한 회로 보드를 제작하였다.

Ⅳ.1 회로도

그림 3은 본 본문에서 사용한 보호 전송 시스템 하드웨어 회로도이다. 이 회로도의 주요 구성은 크게 암호화 알고리듬과 운용 소프트웨어 프로그램을 심을 32K × 24 비트 EPROM과 데이타 저장을 위한 8K × 24비트의 RAM, DSP56001 칩, RS-232C 보드, 병렬

인터페이스부, 그리고 20MHz 발진기 등으로 이루어져 있다.

EPROM 에는 직·병렬 인터페이스를 위한 소프트웨어, 암호화 알고리듬과 키이 관리를 위한 어셈블리 프로그램을 저장하였으며, RAM은 암·복호를 위해서 데이타를 일시 저장하는데 사용된다. DSP56001 칩은 고속 신호 처리기로서 암호 알고리듬을 빠른 속도로 수행할 수 있도록 해 준다. 그리고 이 전송 장치는 기존 모뎀과의 인터페이스를 위해서 RS-232C 보드가 필요하며, PC 와의 인터페이스를 위해서 병렬 인터페이스 장치가 사용되었다.

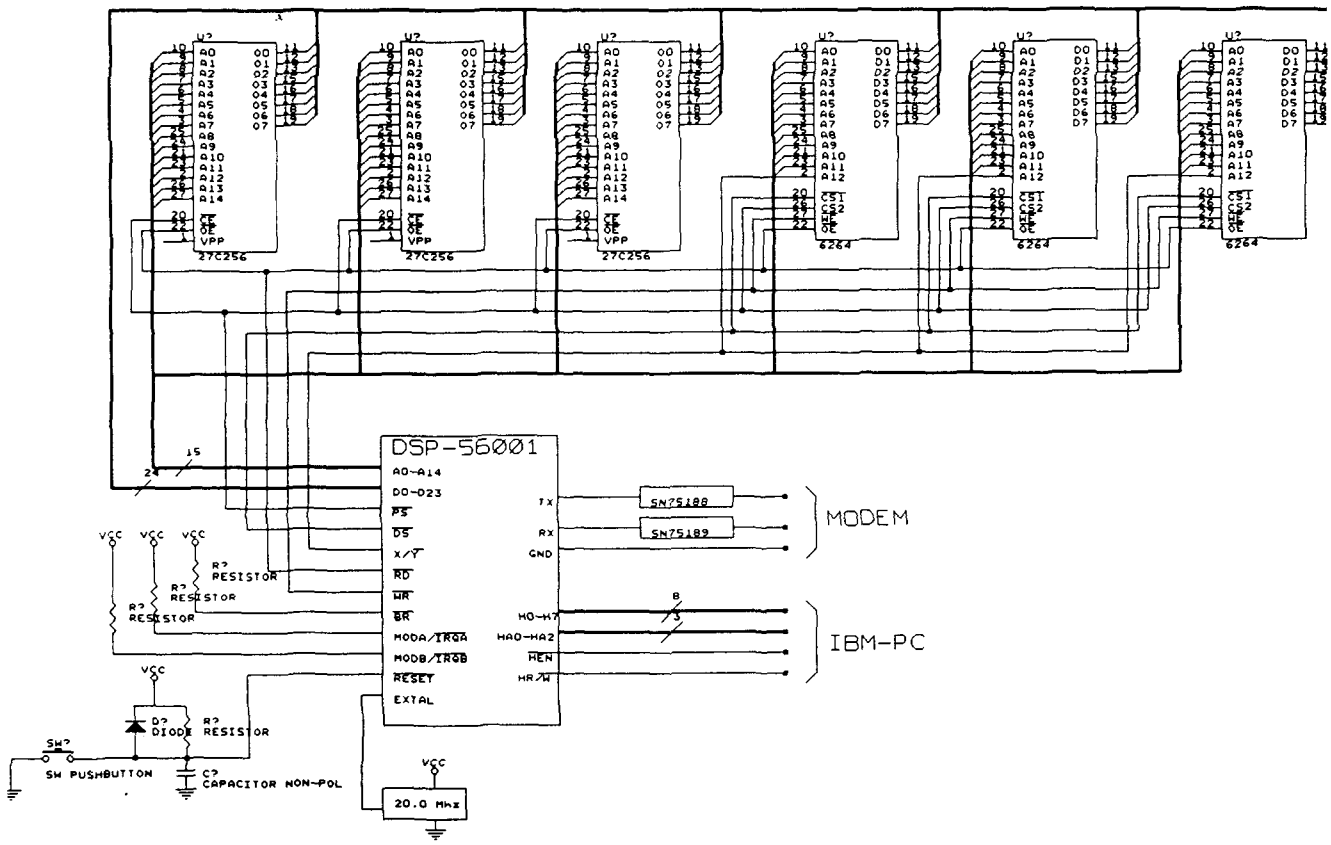

Fig. 3. The circuit of DSP56001 board in the secure modem

Ⅳ.2 디지탈 신호 처리 칩의 개요

그림 4는 본 연구에서 하드웨어 구현에 사용한 DSP56001의 구성도이며 주요 특성은 다음과 같다. DSP56001은 24/56 비트 고정 소수점의 범용 디지탈 신호 처리기로서 사용자가 프로그램할 수 있는 512 x 24비트의 RAM 영역이 있다. 이 칩의 처리 속도는 20.5 MHz 에서 10.25 MIPS이며 24 x 24 비트 승산을 단일 사이클에 수행할 수 있다. 칩상에는 두 개의 256 x 24 비트의 데이타 RAM, 두 개의 256 x 24 비트의 데이타 ROM, 그리고 512 x 24 비트의 프로그램 RAM 및 32 x 24 비트의 Bootstrap ROM이 있다. 또한 DSP56001의 총 메모리 공간은 192K word(24-bit)이고, 단일 5 볼트 전원을 사용하며, 88-pin grid array 패키지로 되어 있다. DSP56001의 주요 구성 부분은 데이타 버스, 주소 버스, 데이타 산술 논리기, 주소 발생기, X 데이타 메모리, Y 데이타 메모리, 프로그램 제어기, 프로그램 메모리, 부트스트랩 ROM, 그리고 입/출력 장치로 확장 포트, 범용 I/O, 호스트 인터페이스(HI), 직렬 통신 인터페이스(SCI) 그리고 동기 직렬 인터페이스(SSI)로 구성되어 있다.

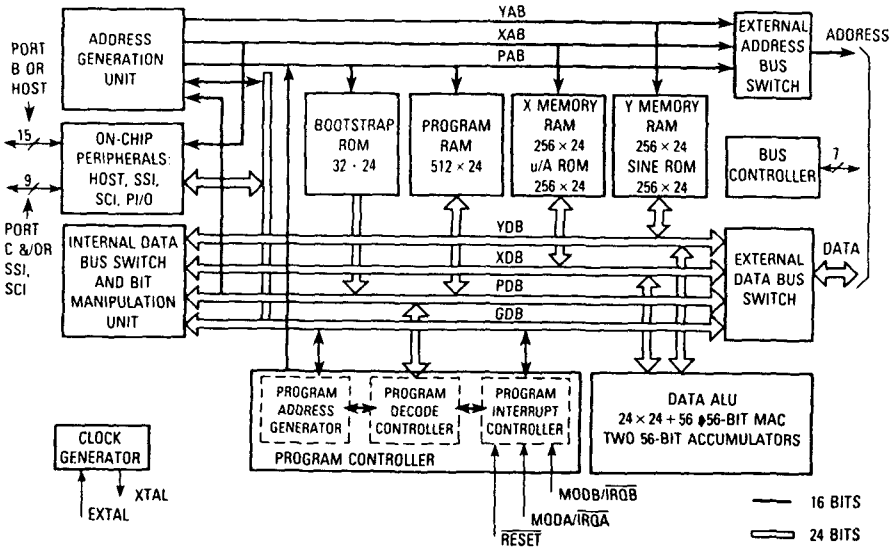

Fig. 4. DSP56001 block diagram

Ⅳ.3 인터페이스

본 논문에서 구현한 보호 전송 장치는 그림 5와 같이 기존 모뎀과 직렬로 인터페이스하고, PC와는 병렬로 인터페이스하였다.

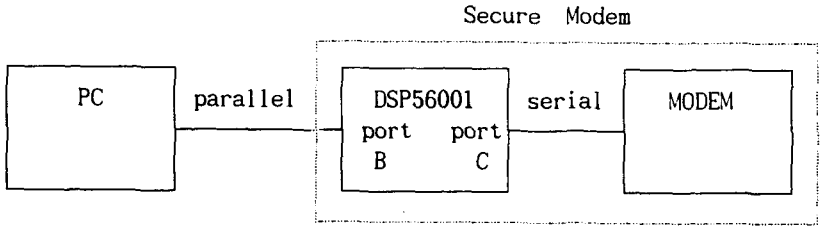

Fig. 5. Block diagram of PC - DSP56001 - MODEM interface

DSP56001의 직렬 포트(포트 C)와 모뎀의 인터페이스를 위해서는 RS-232C를 사용한 비동기 직렬 통신 방식을 사용하였다. RS-232C의 전기적 인터페이스를 위해서 DSP56001의 TXD와 RXD에 SN75188과 SN75189를 접속한 것을 그림 6의 점선내에 나타내었다. 또한 모뎀과의 직렬 인터페이스를 위해서 포트 C의 RXD와 TXD 그리고 GND의 3핀만을 사용해서 모뎀의 RS-232C 핀 2번과 3번 그리고 7번에 각각 연결하였으며, 나머지 핀들은 그림 6과 같이 연결했다.

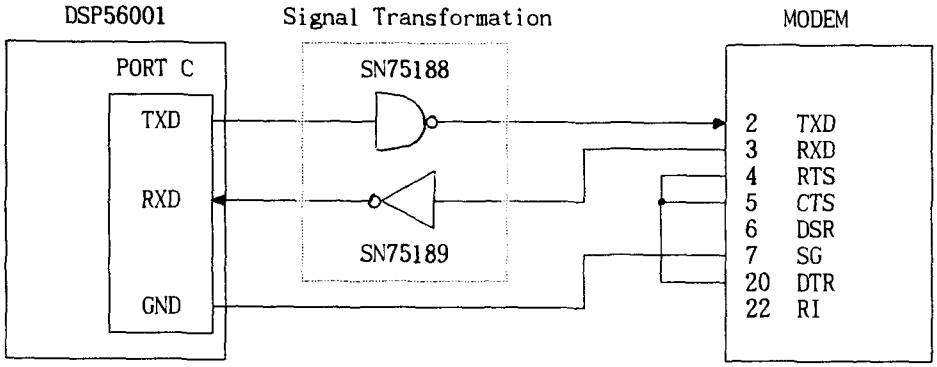

Fig. 6. RS-232C connection and circuit for the signal transformation

본 논문의 비동기 통신 방식에서는 1200 bps의 전송 속도, 8-bit의 데이타 길이, no-parity, 1 bit의 시작 및 정지 비트를 사용했다.

PC와 secure modem의 인터페이스는 DSP56001의 병렬 포트(포트 B)를 이용한 8 비

트 양방향 호스트 인터페이스(host interface)를 사용했다. 호스트인 PC에서의 인터페이스는 DSP56001의 HI(host interface)가 8개의 address를 가지므로 PC의 I/O 메모리를 8개 점유한다. 본 논문에서는 PC의 I/O 메모리 0x300 - 0x307의 번지에 DSP56001의 HI가 매핑되게 하였다.

V. 실험 및 고찰

개발한 secure modem을 운용할 소프트웨어는 퍼스널 컴퓨터에 이식시킬 소프트웨어와 DSP56001에 구현시킬 소프트웨어로 구별된다. 퍼스널 컴퓨터에서는 모뎀 제어 명령어, 화일의 입출력에 관련한 명령어 그리고 DSP56001 하드웨어와의 인터페이스를 처리하는 프로그램을 C-언어로 구성하였다. 또한 DSP56001의 EPROM에 구현된 소프트웨어는 데이타 암호화 알고리듬과 키이 관리 프로토콜, 그리고 퍼스널 컴퓨터 및 모뎀과의 인터페이스를 처리하는 프로그램이 어셈블리 언어로 되어 있다.

그림 7은 실험에 사용한 보호 전송 시스템 보드를 나타낸 것이다. 그리고 그림 8의 (a)는 전송하고자 하는 데이타를 나타낸 것이며, (b)는 공중 전화망을 통해 실제로 전송되는 암호화된 데이타를 나타낸 것이다.

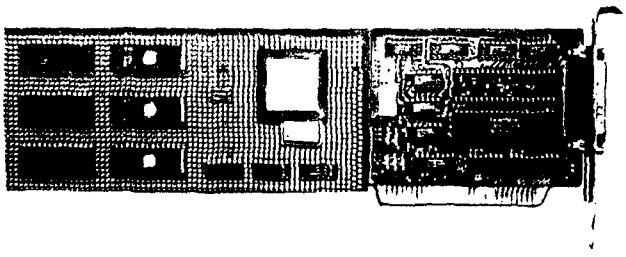

Fig. 7. The encrypted data transmission system board

```
Displacement ---------------- Hex codes------------------    ASCII value
 0000(0000)  53 65 63 75 72 65 20 4D 6F 64 65 6D 2E 0D 0A 45   Secure Modem.  E
 0016(0010)  6E 63 72 79 70 74 69 6F 6E 20 61 6E 64 20 64 65   ncryption and de
 0032(0020)  63 72 79 70 74 69 6F 6E 2E 0D 0A 52 65 73 65 61   cryption.  Resea
 0048(0030)  72 63 68 20 61 6E 64 20 64 65 76 65 6C 6F 70 6D   rch and developm
 0064(0040)  65 6E 74 2E 0D 0A 0D 0A 31 32 33 34 35 36 37 38   ent.    12345678
 0080(0050)  39 30 0D 0A 0D 0A 4D 79 20 66 61 76 6F 72 69 74   90    My favorit
 0096(0060)  65 20 73 6F 6E 67 20 69 73 20 27 73 61 69 6C 69   e song is 'saili
 0112(0070)  6E 67 27 2E 0D 0A 49 20 61 6D 20 73 61 69 6C 69   ng'.  I am saili
 0128(0080)  6E 67 2C 20 49 20 61 6D 20 73 61 69 6C 69 6E 67   ng, I am sailing
 0144(0090)  2C 20 68 6F 6D 65 20 61 67 61 69 6E 20 27 63 72   , home again 'cr
 0160(00A0)  6F 73 73 20 74 68 65 20 73 65 61 2E 0D 0A 49 20   oss the sea.  I
```

(a)

```
Displacement ---------------- Hex codes------------------    ASCII value
 0000(0000)  B3 2F 6D 49 BF 65 6E 6E 50 DF 96 72 3B 63 38 96   |/mI+ennP  r;c8
 0016(0010)  7D E9 24 41 85 7E D1 0F 89 22 AC F7 F9 CC E0 CE   } $A ~   "
 0032(0020)  B3 01 A7 D6 75 FE 2B 5A 7C 34 87 AB A5 7B 67 79   |   u +Z|4   {gy
 0048(0030)  3E 07 5F 28 AB EA 09 E4 A5 2E D9 23 42 C6 D2 DE   > _(      .+#B
 0064(0040)  FB 51 69 50 90 56 3F F6 C5 62 8F 7C 98 FD 22 67    QiP V?  b |  "g
 0080(0050)  42 26 08 0B AA CF 45 19 19 3C 32 29 17 20 18 C9   B&.   Evv<2)  ^=
 0096(0060)  F1 C4 31 2A 0A E3 F5 E4 1E 65 04 DC 50 56 8E E1    -1*     ^e  PV
 0112(0070)  D4 96 5B F9 7F FF 50 3A 74 64 C3 C9 EC C8 C4 6C     [ . P:td+= =-l
 0128(0080)  78 4E 3C 47 6C E8 50 E4 88 1E BC 3C F9 23 BA 6E   xN<Gl P  ^=< #"n
 0144(0090)  BF 4E FE D9 5F 7E 83 25 D8 C0 53 AE E9 22 94 A7   +N +_~ % +S  "
 0160(00A0)  9B 42 EA 9A AC AB CC F2 7B 8A 33 DF EC D0 F2 07    B       { 3
```

(b)

Fig. 8. (a) Original data (b) Encrypted data

Ⅵ. 결 론

본 논문에서는 전송 데이타를 보호하기 위한 데이타 보호 장치를 개발하여 기존 모뎀에 인터페이스함으로써 secure modem 시스템을 구현하였다. 데이타 암호화 알고리듬은 LUCIFER 알고리듬을 64 비트로 변형시킨 것을 사용하였으며, Diffie-Hellman 방식을 사용하여 키이 생성 및 분배에 관한 키이 관리 문제를 해결하였다. 그리고 하드웨어 제작을 위해서 고속의 디지탈 신호 처리기 칩인 DSP56001을 사용하였다.

이 시스템은 기존의 모뎀 회로를 수정하지 않고 그대로 사용할 수 있으며, PC의 입출력 포트에 장착할 수 있도록 인터페이스 회로와 더불어 plug-in board로 제작되었다. 또한 PC DOS상에서 수행되는 운영 시스템 소프트웨어는 C-언어로 개발하였고 DSP56001에서 수행되는 어셈블리 소프트웨어도 함께 개발하였다.

참 고 문 헌

[1] M.E.Hellman, "An Overview of Public Key Cryptography," IEEE Comm. Society Mag. vol.16, no.6, pp.24-32, Nov. 1978.

[2] D.B.Newman, Jr., J.K.Omura, and R.L.Pickholtz, "Public-key Management for Network Security," IEEE Network Mag., vol.1, no.2, pp.11-16. Apr. 1987.

[3] A.Sorkin, "Lucifer, a cryptographic algorithm," Cryptologia, vol.8, no.1, pp.22-35, Jan. 1984.

[4] 강해동,이창순,문상재, "Lucifer 형태의 암호화 알고리듬에 관한 연구," 전자 공학회 논문지, 제 26권, 제 3호, pp.339-346, 1989년.

[5] W.Diffie and M.E.Hellman, "New directions in cryptography," IEEE Trans. on Inform. Theory, vol.IT-22, pp.644-654, Nov. 1976.

[6] DSP56000/DSP56001 Digital Signal Processor User's Maual, Motorola Inc.

[7] CCITT Recommendation V.24, List of definitions for interchange circuits between data terminal equipment and data circuit-terminating equipment.

[8] Lewis C. Eggebrecht, *Interfacing to the IBM Personal Computer*, Howard W. Sams & Co., Inc., 1983.

[9] Joe Campbell, *C Programmer's Guide to Serial Communications*, Howard W. Sams & Co., Inc., 1987.