通信情報保護學會誌
第2卷 第4號, 1992. 12

영상회의에 대한 통신보안 대책

Communicatin Security for Video-Teleconferencing System

김 광 영*

요 약

정보화 사회를 선도하는 Compunication(컴퓨터 + 커뮤니케이션)의 최근 경향은 V.I.P로 요약될 수 있다. 즉 가시화(Visualized), 지능화(Intelligent) 및 개인화(Personalized)이다.

예를들어 1986년 세종로-과천 정부청사간의 국내영상회의 시스템을 효시로 하고 1992년 1월 30일 새로 개통한 국제영상회의 시스템을 보면 V.I.P. 중 V는 Video를 52인치 스크린을 통해 원격상대방을 볼 수 있는 경우이고 I는 첨단고도 압축기술로 적어도 1/60의 전송로(T-1 : 전화 24회선급)로 축소되는 경제적인 지능을 발휘하고 있으나 마지막 P의 경우 Privacy냐 Security냐 하는 정도차이는 있으나 이용자에 따라 정보누수를 우려하고 있어 적절한 Encryption 대책을 수립 검토하여야 할 것이다. 우리나라에 도입된 미국(CLI)과 영국(GPT)의 영상 Codec에 Option으로 채택된 Encryption 운용 Mode를 조사했고 관련 암호학 개념을 소개하였음.

1. 서 론

지구촌을 더욱 친밀감을 갖고 가깝게 할 수 있는 국제영상회의 시스템은 약칭 Video Conference 서비스로 역사는 짧지만 이용빈도는 일취월장 추세다. 현재 국제적으로 30여 국가에서 약 700개의 공중 또는 사설영상 스튜디오를 운용중에 있으며 우리 국내에도 10수개의 영상시설을 운용하고 있다.

Real-time, Real understanding, Face-to-Face meeting의 성격으로 거리개념을 초월하고 출장시간 절약과 생산성 제고 때문에 이용동기가 되고 있다.

특히 CODEC 발달로 표준 TV(NTSC)의 광대역보다 수십 또는 수백분의 1로 좁혀진 T-1 (1.544 Mbps), E-1 (2.048Mbps)은 물론 DSO (64Kbps 또는 56Kbps) 전송망으로도 동화상 (Motion-Picture)을 보낼 수 있는 매우 경제적인 점에서 매력 상품화가 되고 있다.

국내는 대기업체, 종교단체, 연구소 등이 이용하고 있으며 특히 한국통신은 국제 영상회의 고정스튜디오(92년 1월 개설) 외에도 지방영역 확대를 위한 고객중심의 가반형 CODEC 확보를 검토중이다.

CODEC 국내 도입선은 삼성과 금성측이 각각 CLI(Rambrandt), GPT(GVS)의 모델을 독점 공급하고 있는 실정이다.

* 한국통신 국제망운용국 국장

문제는 통신보안인데 고객에 따라 Privacy 또는 Security를 요구하고 있으나 Option의 DES 같은 Encryption key는 수출국 정책상 극히 도입이 어려운 실정이다. 현재 운용의 묘를 기하여 가급적 전송로 선택은 무선의 위성통신 보다 유선의 국제해저 광케이블로 이용하여 전송로상 통신보안 취약점을 줄이고 무선의 경우에도 위성의 안테나 카버리지가 Global, Hemi, Zone, Spot Beam 등으로 좁혀지므로 상황에 따라 좁은 카버빔을 선택한다. 전적으로 전송상 데이터 자체에 Encryption key가 동원된다면 더욱 금상첨화격이라 할 수 있다.

본론에서는 통신보안과 Encryption의 일반관계를 고찰하고 현재 국내에서 운용중인 Rembrandt와 GVS의 영상회의용 Codec 각각에 대한 대표적 Encryption 시스템 개념과 운용모드를 고찰해 본다.

2. 통신보안개념과 관련암호학

전기통신보안이란 각종 서비스를 제공하는 모든 전기통신시스템으로부터 이용자들의 음성정보를 부당하게 도청 당하거나 영상과 같은 비음성 정보를 도시 당하지 않도록 사전예방을 강구하는 것이다. 그러나 그 통신의 내용에 따라 비화장치는 경제성, 운용유지보수 난이정도가 달라질 수 있으므로 그 보호받을 정보의 개념을 냉철히 이해한 후 장비의 선택과 여기에 담겨져 있는 소프트웨어 Key를 관리 운용할 충직한 정보기술요원의 고용여부를 판단 결정해야 할 것이다. 본론에서는 국내 또는 국제적으로 각광받고 있는 원격 영상회의에 대한 관련암호학 기본 개념등을 설명하고 영상 Codec에 따른 2가지 대표적인 Encryption을 후술한다.

2.1. Encoding 시스템

Code(부호)는 Symbo(기호)에 의하여 말하거나 적을 수 있는 수단이 된다. 즉 Code는 송신자와 약정된 수신자간에만 약속해서 알려진 심볼로 사용될때 비밀로 취급받을 수 있다. 이러한 상황이 계속 유지되는한 완벽한 비밀이 되지만 이러한 심볼의 의미들이 사용자의 부주의로 함부로 이용하거나 시설상 통신 보안의 취약성 때문에 쉽게 노출될 수도 있다. Code 그 자체만으로는 적용한계(Limited Flexibility)가 있고 한편 Off-Line으로서 실시간에 직결되지 않고 있는 사유로 총체적 통신을 보호한다고는 말할 수 없다.

그렇지만 정보의 특징적이거나 비반복적인 내용물을 보호하기 위한 수단으로는 경제적이고 간이한 비화수단으로 응용될 수 있다.

예를들어 만약 특정조직의 모험적인 사업이 매우 민감한 것이라면 사업의 성공과 실패여부 내용을 보통 통신 시스템을 통해서도 당사자들만이 알 수 있는 사전 약정된 단어나 문구를 배열시켜 통보 내용을 받을 수 있을 것이다.

2.2. Encipherment 시스템

Cipher(암호) 시스템은 평문 또는 음성을 이해할 수 없는 형태로 바꿔 보낸후 원격수신단에서 지각할 수 있는 형태로 복원하는 방식이다. 암호시스템은 당초에는 모두가 애너로구였었다. 메세지안에 있는 알파벳 문자를 치환하는 것도 일종의 기초 암호방법이었다.

음성통신에 대한 Cipher system은 주파수, 진폭 또는 시간영역등에서 실제 신호파형을 변형시키는 것이었다. 소위 Scrambled Waveform으로 송신되고 수신단에서는 Unscrambled 상태로 복원하는 것이다. 만약 가용대역폭이나 다른 고려사항 때문에 신호를 애너로구상태로 전송시켜야만 할 경우 그때는 반드시 애너로구식 암호시스템이 도입되어야 한다. Digital Cipher 시스템은 최근 대부분의 통신에서 널리 적용되어 애너로구 경우는 사라지고 있다.

디지틀 암호시스템은 개념상으로는 매우 단순하다. 신호자체가 애너로구에서 디지틀로 변환된 후 Random bits의 Digital key system이 전송상에 합산되어 암호문으로 변형시킨다. 원격수신단에서는 그 Key가 다시 암호문을 평문으로 복원할 수 있도록 합산처리되는데 재사용된다.

시스템에 대한 보안수준은 Key 스트림을 구성하고 있는 bit의 Randomness의 함수에 관계된다. 다시 말하면 Key를 생산하는 알고리즘의 복잡성의 함수에

관계된다. 사실 디지틀 앤크립션 장치는 특수목적으로 설계된 컴퓨터라고 해도 과언은 아니다.

디지틀 앤크립션 장치는 디지틀화 할 수 있는 신호만을 취급하여 메세지, 데이타, 음성트래픽에 적용된다. 따라서 그 장치의 설계상 제한은 최대용량의 Data Rate에 의해서만 정해질 뿐이다.

대부분의 장치는 최대용량한도 이내에서 시간당 데이타량을 변경하면서 사용할 수 있다. 이러한 시스템의 출력은 디지틀신호이기 때문에 보통망 또는 패킷스위칭 데이타 통신망을 통하여 어려움없이 전송된다.

Data Encryption Standard(DES) Key 생성 알고리즘은 1976년 미국 국립표준국에 의해서 공인되었다. 그 알고리즘은 10^{17} Random bits의 System key를 생성한다. 미국의 디지틀 암호장치는 대부분이 알고리즘을 채용하고 있다.

DES는 다년간 국가 안보에 관련됐으나 비밀로 미분류된 사항의 보안을 위한 미정부의 공인된 유일한 알고리즘으로 유지되어 왔다. 이와 같은 독점형태는 새로운 기술진화로 변경될법도 하지만 DES는 아직도 경제적이면서 좋은 소기의 성과를 거양하고 있어 암호학에서 독보적 존재로 유지되고 있다. 따라서 미국의 비밀정보 전달에 관한 정부 계약자들은 특별히 공인된 암호시스템을 사용해야만 한다. 그러한 장치들은 요즘 상업적으로 거래되고 있다. KG-84 Key Generater 수준의 제품들이 수개의 경쟁사에 의거 시판되고 있다. 이러한 시스템은 여하한 비밀급수를 막론하고 음성, 데이타, 기록트래픽을 안전하게 전달하고 있다.

DES 경우 2^{64}개의 Key가 이론적으로 생산될 수 있으므로 Key를 모르면 최악의 경우 $2^{64}/2\mu sec \fallingdotseq$ 292년이 소요될 수도 있다.

2.3. Encryption System 선택

Encryption System은 자물쇠 (Padlock)와 같은 이치이기 때문에 침입을 절대적으로 보장하는 것이 아니고 시간상 지연을 유도하는 것이다. 정보의 비밀보장 유효기간의 장단 기준에 따라 선택을 정하는 것이 주요한 관건이다. 예를들어 적략성격의 정보는 순찰경비차에 출동지시 같은 것인데 그 정보비밀 유효기간은 수분이내로 짧은 것이다. 따라서 암호시스템 선택은 예상시간의 기간만 커버될 정도면 충분한 시스템이라 할 수 있다.

암호시스템은 매우 비싸기 때문에 이용할 정보성격을 충분히 이해하고 경제성을 고려한다면 과도한 것을 구입할 필요가 없다. 간단한 주파수 인버터가 300불정도 값싼것으로부터 디지틀 음성 암호 장비는 모뎀을 포함하여 7,500불을 홋가하는 것도 있다.

2.4. Communication Security 계획

통신보안 계획은 우선 주의깊은 우선순위 결정과 신중한 비밀분류 작업이 선행되어야 한다. 통신보안 장비는 구매가격 이외에 부가적인 안전조치 설비가 필요하고 운용할 비밀취급 요원의 인적사항도 고려되어야 한다. 미국 같은 선진국도 암호관련 예산이 막대하다는 것을 알고 비밀급수 이외에 대외비 정도는 완벽을 요구하는 "Protecting"이라는 방어개념을 배제해 두고 있다. 통신보안 계획은 모든 보안예산이 낭비성이 아니고 최상의 효과를 거양하는데 목표를 두고 있다. 특히 대용량의 무선시스템을 소유하고 있는 통신책임자는 항상 도청의 공격대상이 되고 있는 목표임을 명심하여야 한다. 하나 하나의 채널 암호시스템 조치는 비경제적이므로 일괄암호화(Bulk Encryption)하면 저렴한 단가로 수행이 가능할 것이다. 결국 통신보안 책임직은 계획방침, 예산이 어떻든간에 조직내부 구성직원의 훈련을 통하여 정보개념을 인식시켜서 안보효과를 상승적으로 향상시켜야 할 것이다.

암호이거나 부호이거나간에 굳게 다문 입보다 더 나을 것이 없다. "There is no Cipher or Code half so effective as a tightly closed mouth" 말하자면 Physical and Personal Security 양자간의 상승대책과 노력으로 소기의 성과를 거양할 수 있다는 의미를 신봉할 수 있도록 종사원들에게 꾸준한 훈련과정을 수행해야 한다. 만일 통신보안 책임직이 인적보안 단속을 소홀히 하고 시스템에만 의존한다면 마치 앞문과 창문을 개방한채 도적을 지키기 위하여 뒷문의 시건장치에만 급급하는 꼴이 될수도 있다.

2.5. Cryptology 과학

Cryptology는 그리스어의 Kryptos (Hidden)과 Logos (Word)의 합성어로 위장된 암호소통을 취급하는 관련 과학분야이다. 언어뿐만 아니라 Cryptography도 메세지 또는 기록물을 이해할 수 없는 형태로한 암호 전보문을 다루는 분야이다. 여기서 Graphy는 Graphein이라는 그리스어의 "Write" 의 미가 합성된 단어이다. 이 밖에도 통신서비스별로 암호화될 경우 해당 용어는 다음과 같다.

전보 (Telegram)은 Cryptogram이고, 전화 (Telephone)는 Ciphony, 팩시밀리 (Faximile)은 Cifax, 텔레비젼 (Television)은 Civision. 컴퓨터 Data에 대한 것은 DES(Data Encryption System)이라는 이름이 쓰여지고 있다. 이러한 암호화 수준은 그 깊이의 정도에 따라 Privacy 시스템과 Security 시스템으로 대별된다.

Privacy 시스템은 직접도청(Direct listening)이나 직접시청(Direct viewing)을 방어하는 정도의 Minimal 방어이고, Security 시스템은 절대적인 방어 차원으로 Maximum 수준이다.
영상회의 경우 Video는 광대역이므로 Privacy 시스템의 Speech나 Faximile에 비해 디지틀화된 광대역 스펙트럼을 전송해야 하므로 Key를 고속으로 생성해야 하는 점이 다를 것이다.

3. Rembrandt Codec Encryption 운용

영상회의실에 설치된 CLI사의 Rembrandt의 비화장치는 Encryption key가 있으며 CODEC(Codec-Decoder)의 전송비화에 대하여 Enable, Disable 2가지의 명령을 선택 운용할 수 있도록 되어 있다. Rembrandt codec은 애너로구 Video, 애너로구 Audio 및 Digital user data를 부호화 한 후 이용자가 지정한 전송로 매개체로 전송하기 위하여 동기비트 스트림 안으로 모든 데이타를 입력, 중첩한다. T1, NTT T1, G732, RS-449등의 통신망에 동기비트 스트림을 주고 받을 수 있도록 디자인 되어 있다.

여기서 VIDEO 압축은 애너로구 Audio와 Video 신호 및 이용자의 디지틀 Data 모두를 협대역 데이타 채널에 전송할 수 있도록 압축한 디지틀 데이타 스트림으로 변화시킨다(그림 1.a, 1.b, 참조).

전송대역폭은 384Kbps에서 2.048Mbps까지이며 64Kbps 단위로 증감이 가능하다. Codec 전면판넬에 부착된 Key pad에서 2가지의 Encryption 모드를 선택하여 전송상 보안을 유지할 수 있다.

PROM 캐트리치를 삽입하면 시스템 S/W는 Codec만으로 입력된다. Codec은 단지 PROM으로부터의 S/W를 Read 하거나 Load 하는 것뿐이다. 그 다음에 사용자가 프로그래밍을 하여 쓴다. Encryption Key 발생은 12 Decimal Digit Key와 16 Hexadecimal Characters Encryption Key가 있다.

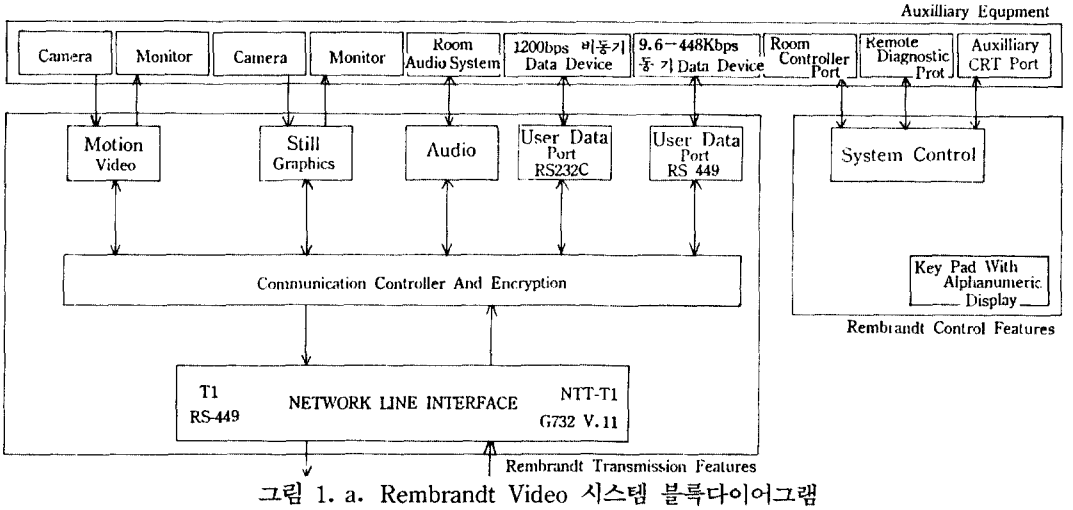


그림 1. a. Rembrandt Video 시스템 블록다이어그램

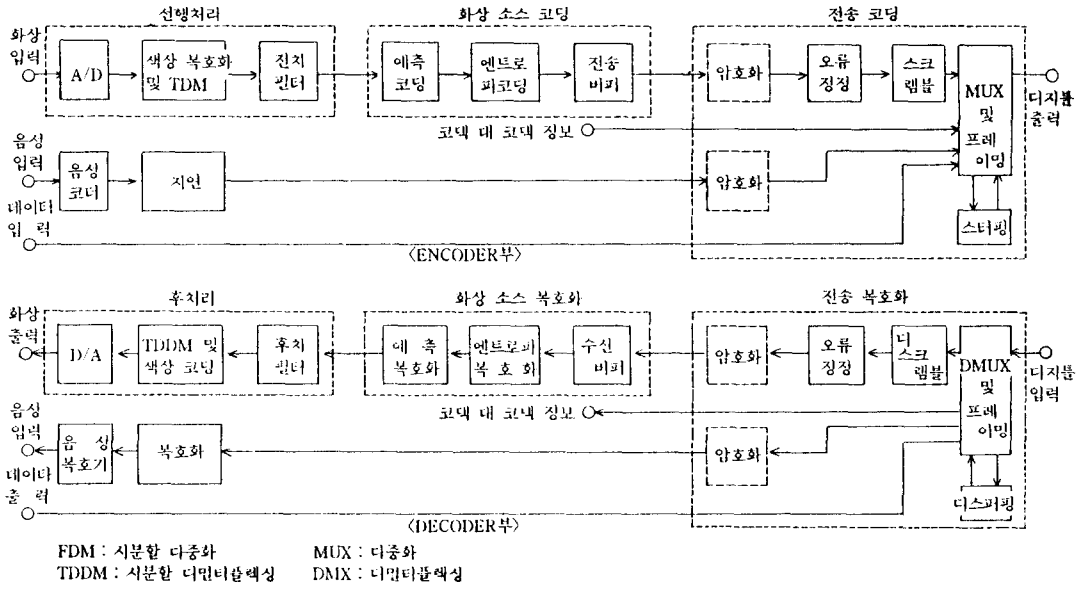


그림 1. b. CCITT-H120 표준 영상 코덱 계통 도면

3.1. Encryption Command

Codec의 Key pad 판넬에서 Encryption key를 선택하여 누르면 Codec의 전송신호가 비화된다. 비화전송신호가 수신되고 Display 되기 위하여 수신측은 송신측에서 선택한 Key를 틀림없이 사용해야 한다. 암호키는 2가지 모드 중 한개를 선택 암호를 발생시킨다.

QUICK 암호모드에서는 시스템 Default Encryption Key가 가동되거나 아니면 Default Key 대신에 1에서 12개 십진법 디지트의 Encryption Key로 사용된다.

시스템 Default Encryption Key는 사용자에 의해서 변경될 수 있다. 그러나 그 수정 내용은 전원 정전시 또는 Warmstart시에 망실된다. 전원이 인가될 동안 또는 윔업시작 상태에서 Command가 유효할 수 있을 때는 QUICK 모드 Default Key는 EEPROM (전기적으로 소거와 기록이 가능한 ROM)이 0 상태일 때이다.

VTS 암호모드에서는 Encryption Key는 16개의 16진법으로 구성되고 Odd Parity로 시동된다.

QUICK 암호는 Default Key 전량 또는 부분을 이용하면서 시동이 가능하나 VTS 암호는 완전한 Key가 구성되어야 유효이다.

Network Command (Internetwork Mode)	Line Command (Communication Mode)	(Transimission Mode)
ON	T1	Scrambled
ON	G732	Scrambled
OFF	T1	Scrambled
OFF	G732	Clear

Scramblcd는 T-1 통신 인터페이스에 대해서 Pre-set Default 상태이다.

만약 EEPROM안에 0 상태라면 ROM에는 공장에서 정의한 Default가 실장된 것이다. Encryption OFF (disable) 상태일때에는 Codec Transmission 모드는 Network command와 Line command에 좌우된다.

3.2. System Hardware Errors

만약 하드웨어가 QUICK 또는 VTS 모드 Encryption Key를 입력시켰을 때 오류가 발생하면 해당 오류관련 상세 내용 설명이 CRT에 나타난다. 스크린에 나타내는 메세지는 다음과 같다.

XMT Key Verification Error
RCV Key Verification Error
XMT Parity Error
RCV Parity Error
XMT Command-Pending Error
RCV Command-Pending Error

여기서 Command-Pending Error일 경우 비화장치가 모든 8bytes를 수신하지 않았다는 암시이다.

3.3. Consol Format

명령어 Encryption은 약호 E로 하며 QUICK (Q) 시에는 Encryption Enabled이고 OFF (OF)시에는 Disabled 상태를 의미한다. 콘솔 이외에도 영상회의 스튜디오 실내 통제반에서의 Format이 따로 있으나 생략한다. 또한 영상회의 기계실에 있는 코덱랙크 전면에 있는 Keypad에도 Format이 있다.

Function Key에서 Encryp를 누르면 Display에는 OFF, QUICK, VTS, DFLT가 나타난다.

3.4. Creating A Quick Encryption Key

Quick Encryption 모드 사용으로 4가지 방법의 암호화가 가능하다.

1) Key를 만들기 위하여 여하한 Decimal digits도 입력시키지 말고 Encryption Quick을 시행(Execute)하라. 그러면 이때는 시스템의 Quick 모드 Default Encryption Key는 EEPROM에서 Block 0 상태에 내장된 key이다.

이것은 전원인가 또는 Reset시에 시스템에 실장되어진 것이다. 만약 Block 0 상태가 비어있는 상태이던가 또는 Error가 발생하던가, Default 암호키가 포함되어 있지 않은 상태라면 그때는 Factory에서 설정한 내용의 ROM이 Default 암호 key로 사용되는 것이다.

2) 시스템의 Default 암호 key의 일부분을 대치하기 위하여 1에서 11개까지의 Decimal digits을 입력하는 동안 Encryption Quick을 시행하라. 예를 들면 1, 2, 3등을 부분대치로서 입력시킨다.

3) 완벽한 Default Encryption Key를 대치하기 위하여 12개 Decimal digits를 입력시키는 동안 Encryption Quick을 시행하라.

예를들면 1, 2, 3, 0, 9, 2, 5, 6, 3, 4, 7, 1와 같이 12개를 모두 입력시킨다.

4) Quick 모드 암호키를 포함한 EEPROM으로부터 Block 배열을 실장하기 위하여는 Load 명령을 사용하라. 그때 Encryption Quick을 시행하라. 그리고 물론 여러분은 Quick 모드 암호키를 포함한 EEPROM으로부터 Block 배열을 항상 실장(Load)할 수 있다. 이 때 Encryption Quick을 시행하기 전에 해당 Encryption key를 수정하는 것이다.

3.5. Creating VTS Encryption key

VTS 암호모드를 이용한 암호화 시도는 3단계 수행사항이 있다.

1) 첫번째 암호 소프트웨어 명령모드로서 Encryption VTS를 선택한다.

이것은 영상기계실의 Keypad, 영상회의실내 Room Controller, 또는 CRT 통제실 중 어느곳을 경유하여 명령을 입력시켰는가에 따라 변동된다.

Encryption VTS 모드를 선택하면 그 시스템은 VTS 암호키의 입력을 기다리게 될 것이다.

2) 16개 Hexadecimal (0-9, A-F) 문자나 숫자를 입력하라. 그 16개 캐랙터 암호키는 8개의 Pairs 캐랙터로 구성되었다. 각 Pairs는 Odd Parity를 지니고 있다.

VTS 암호키는 비밀을 유지하기 위하여 입력시켰

을때도 display 되지 않게 되어 있다.

3) Key가 입력된후 사용자를 위하여 체섬(Checksum)은 Dispaly된다.

그 시스템은 체섬이 맞는 것인지 확인할 수 있도록 기다린다. 체섬은 16진법 캐랙터의 각쌍의 합(Addition)이며 그들 합산(Sum)의 Binary 변환이고 총합(Total)의 2(Two)의 Complement이다.

디스플레이된 체섬은 사용자의 키를 위한 계산된 체섬과 일치되어야 한다. 그 체섬은 동일한 키를 Link의 양편과 같이 사용할 때 공인된다.

Checksum 간단히 확인될 수 있으며 16 캐랙터 키를 구두로 반복할 필요는 배제되고 있다. 사용자의 Code Book 또는 Encryption key Book에는 반드시 각 key에 대한 Checksum을 가지고 있어야만 된다. 이것이 확인되면 Encryption VTS를 시행하라. 이제 암호화는 시동되는 것이다.

3.6. Odd v.s Even Parity

Encryption key는 반드시 Odd Parity이어야 한다.

그 Key에 사용된 16진법 캐랙터의 각 쌍에 대한 대응하는 2진법비트는 Binary 1(one)의 Odd(기수) 넘버를 반드시 포함해야 한다.

기수와 우수 패리티는 캐랙터의 각 쌍에 대한 대응되는 Binary 1(one)을 합하여서 결정된다. 예를 들면 AB의 16진법 캐랙터 쌍의 구성은

A = 1010 (Binary) 1010에는 2개의 "1"을 포함하므로 우수 (EVEN)

B = 1010 (Binary) 1011에는 3개의 "1"을 포함하므로 기수 (ODD)

다시 총합(Total)은 1이 5개가 존재하므로 결국 A와 B라는 2개의 캐랙터(Characters)의 합 (Addition)이 5개의 1을 생성하니까 ODD(기수) SUM값이 된다. 따라서 AB는 Odd Parity Pair 값을 지닌다고 판정된다.

한편 무효인 경우를 예를들어 보면 A와 C의 경우이다.

A = 1010과 C = 1100에서 4개의 "1"이 존재하므로 EVEN SUM값이 되어 입력은 무효가 된다.

Odd Parity Hexadecimal Characters
= 1, 2, 4, 7, 8, B, D, E

Even Parity Hexadecimal Characters
= 0, 3, 5, 6, 9, A, C, F

따라서 각 암호키는 Odd와 Even Parity에서 동수개를 선정하여 구성되어야만 Total parity가 Odd로 보장된다.

VTS 암호키의 2가지 예를 들면 아래와 같다.

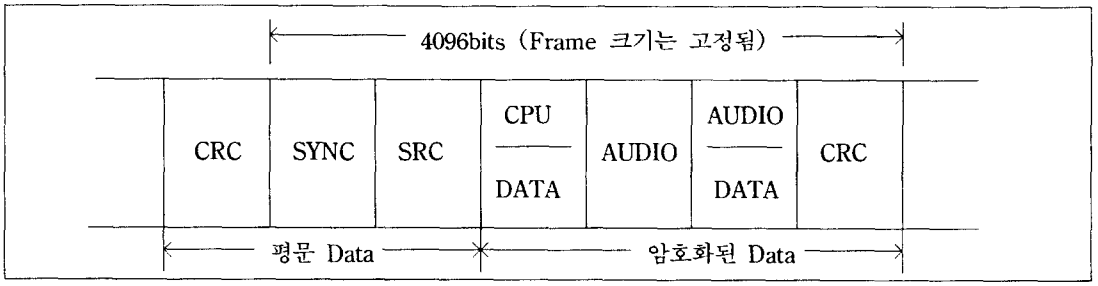
AB AB AB AB AB AB AB AB (8쌍 : 16개)

32 CD AB 51 37 9B F1 0E (8쌍 : 16개)

3.7. Encryption Data

Rembrandt 코덱은 애너로구 Audio, Video와 Digital 사용자의 Data 입력을 받아들인 후 Encode하고 연결된 통신 전송로에 해당 정보를 전송하기 직전에 모든 Data를 편집하여 소정의 통신후레임(Communication frame) 시스템동기와 데이타 관리를 마련하도록 Field를 마련하는 것이다. 만약 영상, 음향, 기타 데이타 모두를 Encryption key를 사용하여 비화시킬 경우 다음과 같은 Field가 편성된다.

SYNC(동기) 신호는 각 Frame 시작에 있고 CRC



는 Frame 안에 있는 Error를 지시한다. SRC는 한 Field에 있는 Video와 다른 Field에 있는 CPU 또는 사용자의 Data를 지시한다.

4. GVS3A Codec Encryption 운용

앞서 미국 CLI사의 Rembrandt Codec에 대한 Encryption을 살펴 보았으며 다음에서는 영국 GPT사의 GVS3A Codec에 대한 Encryption을 언급한다. CCITT H120 규격이 제정되기 이전 이미 개발된 영상회의 코덱 장비를 운용하고 있는 외국 국가나 국내 기업등은 구구각각이므로 통신주관청인 한국통신은 이러한 기존제품을 갖춘 고객과의 인터페이스를 위하여 영·미 제품을 모두 설치 운용중이다.

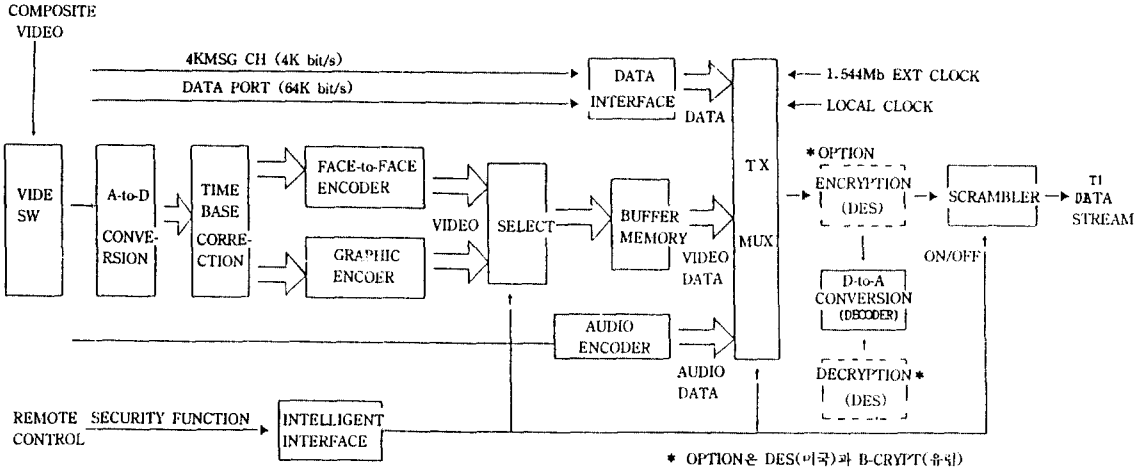


그림 2. GVS3A-CODEC 기능 블록다이어그램과 ENCRYPTION 위치도면

GVS 경우 그림 2에서와 같이 Encryption은 미국의 DES와 영국의 B-Crypt를 Option으로 선택할 수 있도록 설계되어 있다.

Composite Video인 NTSC 신호냐 R.G.B냐에 따라 Face-to-Face 또는 Graphic Video Coding Mode가 선택된 후에 4KHz Message 채널과 Data Port 및 Audio와 함께 송신 MUX에서 중첩된 후 T1의 스트림으로 만들어 송출되는 과정에서 Encryption 유니트를 경유하여 스크램블된 후 위성이나 해저케이블 전송매체를 통해 외국으로 전송한다.

Remote Control에 의해 Intelligent Interface 유니트를 통해 접속된 스크램블은 ON/OFF될 수 있으며 통신 Security 기능을 갖는다. Unauthorised 인터페이스는 차단된다. 사용자는 Codec 내장번호와 맷칭되는 Code 번호를 입력시켜야 한다. Encryption 명령은 지능망을 비화 조정 모드 스위치에 접속시킨다. Codec Number 명령은 Security Code 번호를 입력하게 된다. Code 번호는 컴퓨터에서 Password와 같은 기능을 갖는다.

0에서 4, 294, 967, 295에 이르는 지능망 작동 RAM 메모리에 있는 십진법의 보안 코드 수이다. 주의사항은 Comma 또는 Stop 없이 입력해야 하고 숫자에서 Zero로 시작할 수 있는 것은 선택권이다.

입력 Code 번호가 저장된 RAM 메모리 번호수와 비교해서 일치될 때 Ok, Use of Secure Commands Now Permitted라는 메세지가 CRT에 나타난다. 불일치 숫자가 입력되면 Incorrect Security Code-Secure Commands Now Inhibited Automatic Key Calculation라는 메세지가 화면에 나타난다.

Code Number New-Number 명령은 운용 RAM 메모리에 있는 Security Code 번호의 값을 수정변경하는데 유효하다. 새로운 번호값은 0에서 4, 294, 967, 295까지 영역내와 Code 번호 명령으로 입력된 새로 필요한 코드번호의 십진수 값이다.

두 수보다 더 큰수는 Invalid Command 메세지가 출현된다. 끝으로 Code off 명령어를 치면 이전에

사용했던 Security 명령어는 모두 무력화되므로 특별한 보안방안을 강구할 때 이런 명령을 입력하는 것이다.

4.1. Automatic Key Calculation

비화 메뉴에서 1번(기능번호)은 DES 또는 B-Crypt Key를 자동적으로 시동시킨다. 이 조정은 3단계로 진행되며 약 5분 소요된다. 각 단계는 일련의 링크를 통하여 출력된 메세지 지시에 의거 동작되며 Codec의 비디오 출력단에도 나타내 보인다.

Key 조정의 제 1 단계에서는 수학적 응용은 하드웨어 발생기에 나온 난수로 수행된다. 이 조정시간은 약 2분 소요되지만 과거 컴퓨터가 성공했던 어떤 방법을 동원해도 수년간 걸려야 밝혀낼 수 있을 것 같다. 이때 Key Calculation in Progress라는 메세지가 비디오에 나타난다.

제 2 단계에서는 조정의 결과가 디지틀 데이타 스트림의 Time Slot 2를 통해서 Remote Codec으로 전송된다. 비화시스템은 Remote Codec에서 나온 대응하는 조정결과를 수신하도록 기다리게 된다. 이때 Awaiting Number Exchange라는 메세지가 비디오 출력단에 나타난다.

제 3 단계에서는 Local과 Remote의 양 Codec은 그들 각각의 난수를 사용하고 동일한 DES 또는 B-Crypt 비화 Key를 조정하기 위해 Remote Codec으로부터 나온 조정 Key를 동시에 사용한다. 이 과정은 약 2분 소요된다.

마지막 조정단계에서 각 Codec은 새로운 DES나 B-Crypt Key를 사용하여 전송된 데이타를 비화하고 수신된 데이타를 해독하기 시작한다. Key Calculation in progress 메세지가 비디오에 나타난다.

조정중에 기능번호 2번이 비디오에 나오면 새로운 DES 또는 B-Crypt Key가 선택되면 Transmission Now Encryption이라는 메세지가 New Key in Use라는 메세지와 함께 나타난다. 이들 메세지는 20초 후에 사라지며 전송되는 데이타가 비화될 동안에는 비디오 상단 화면에 "E" 즉 Encryption이라는 약호가 계속 보여 확인 가능토록 돕는다.

4.2. Manual Key Entry

비화 메뉴에서 2번을 누르면 DES나 B-Crypt Key를 수동입력할 수 있게 된다. 이 Key는 56bits 2진수이고 17자리의 십진수로 입력된다. 따라서 모든 17자리수의 Key 값이 입력되어야 한다. 17개 숫자는 DES 또는 B-Crypt Key를 만들어 비화 하드웨어로 옮겨가서 전송될 데이터를 비화하고 수신된 데이터를 해독하는데 사용된다.

Transmission Now Encryption라는 메세지가 약 20초 동안 화면에 나타내 보인다. 역시 문자 "E"가 지속되어 기능 확인을 해준다. 이때 Key 값은 0에서 72, 057, 594, 927, 935까지의 영역내의 값이어야 한다. 만일 더 큰값이 입력되면 도움말이 출력되어 지시에 따르면 된다. 또 작업중 Escape 키를 치면 그 기능은 소실되고 기존의 Key가 사용될 수 있다. 도중 숫자가 틀렸을 때 지우려면 Backspace키를 누른다.

비화메뉴에서 3번을 누르면 문자 "E"가 화면에서 사라지면서 데이터 비화수행이 정지된다. 수신측 데이터의 Tiem Slot 2에 있는 신호는 비화 여부를 지시해주고 필요할 경우 Codec은 해독을 한다. 비화가 사라지면 Transmission Not Encryption 메세지가 약 20초동안 화면에 나타난다.

5. 결 론

우리나라에 도입 운용중인 Video Conferencing system(영상회의 서비스)에 대한 Encryption의 이모저모를 살펴보았다. Option으로 선택되는 DES 또는 B-Crypt Key의 핵심인 일련의 SBS(Standard Building Block) 도입이 보유 해당국가로부터 방출제한을 받고 있어 실제 운용에 애로가 많은 것이 현재 실정이다.

상술한 바와같이 현대인의 통신이용자 욕구는 소위 V.I.P(Visualized, Intelligent, Personalized) 3가지 요소를 기대하는 것인데 특히 이중 P의 개인화는 Privacy 또는 Security와 같은 개념으로서 암호학회 종사원 여러분들이 관심을 갖고 통신보안의 자체 개발을 상호 협력해서 수행해야 할 과제라고 사료

됩니다.

비단 본론에서 언급한 영상서비스 뿐만 아니라 국제산업경쟁기업체들의 주종인 국제 전용데이타통신회선에도 쉽게 도입할 수 있는 경제적인 Encryption System이 우리 연구팀에 의거 속히 개발되어야 하겠습니다.

수 많은 암호학관련 논문이 넘쳐 나오고 있으나 실제 운용요령등에 대한 글이 없던 것을 고려해서 여기서 개념적인 운용실재를 소개한 것임을 밝혀둡니다.

참 고 문 헌

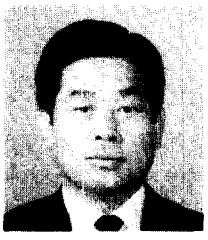
1. "Rembrandt Video Teleconferencing System", CLI, 1986.

2. "Rembrandt Video Codec", CLI, 1991.

3. "GVS3A Video Compression Codec", GPT, 1987.

4. "Making Your Communications System Secure", Datapro Research Corporation, Delran, USA 1987, June.

□ 著者紹介



김 광 영(정회원)

1938년 11월생
1966년 한양대학교 공과대학 학사
1989년 한양대학교 산업대학원 석사
1992년 한양대학교 대학원 전자통신 박사과정
1993년 한국통신 국제망운용국 국장

됩니다.

비단 본론에서 언급한 영상서비스 뿐만 아니라 국제산업경쟁기업체들의 주종인 국제 전용데이타통신회선에도 쉽게 도입할 수 있는 경제적인 Encryption System이 우리 연구팀에 의거 속히 개발되어야 하겠습니다.

수 많은 암호학관련 논문이 넘쳐 나오고 있으나 실제 운용요령등에 대한 글이 없던 것을 고려해서 여기서 개념적인 운용실재를 소개한 것임을 밝혀둡니다.

참 고 문 헌

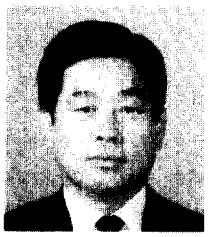
1. "Rembrandt Video Teleconferencing System", CLI, 1986.

2. "Rembrandt Video Codec", CLI, 1991.

3. "GVS3A Video Compression Codec", GPT, 1987.

4. "Making Your Communications System Secure", Datapro Research Corporation, Delran, USA 1987, June.

□ 著者紹介



김 광 영(정회원)

1938년 11월생
1966년 한양대학교 공과대학 학사
1989년 한양대학교 산업대학원 석사
1992년 한양대학교 대학원 전자통신 박사과정
1993년 한국통신 국제망운용국 국장