ENCRYPTION: A CABLE TV PRIMER

Anthony Wechselberger
Director, Advanced Engineering
Oak Communications Inc.

The use of encryption technology in the delivery of premium television is the center of much attention today. It is also an area of misinformation where misunderstood terminology and technology are being discussed. This paper defines the principal requirements, characteristics and benefits of encryption technology as it can be applied to pay TV. Particular attention is paid to differentiating the essentials of what constitutes "cryptographic security" from less complex techniques employing simple time varying characteristics or multiple scrambling modes. The fundamentals of encryption, principal approaches to its utilization and some associated technical jargon will be explained. The concept of the cryptographic "key" and the importance of secure key distribution will also be defined.

One major area of confusion lies in the technical differences between encryption and scrambling and, particularly, hybrid utilizations of the two. In understanding some basics about cryptography, one can better appreciate these differences, and differentiate buzz words from substance in the expanding selection of products utilizing encryption.

OAK Communications Inc.

CATV SYSTEM SECURITY — ITS TIME HAS COME

Whenever there's a need in the marketplace, any marketplace, responses to that need will be garnered from the market suppliers. The attribute approach to product demand theory tells us that demand can be influenced by need, price, competition and budget, as well as a whole set of attributes connected to the products perceived value or need. This can be hyped one way or another by advertising, the "bandwagon effect" and the like, which affects the consumer's perceptions and tastes.

And so it is in our marketplace, the CATV market, where specmanship and buzzwords change each year in the scramble for market share. This is not a negative thing. Consumer features in converters and decoders, for example, is an area where much innovation has taken place. When the consumer gives up the remote control for his $800 console TV, system suppliers are now able to give back some of those remote conveniences with newer CATV equipment.

The demands we cable equipment suppliers react to must be responsive to both the end user and our immediate consumer, the MSO. The MSO in turn creates needs, but also responds to the palpitations of his own market, for which he purchases equipment, runs a business, and distributes programming. *He must control* the consumption of his product (programming) for both short term and long term gains and market stability.

The process of controlling that product brings us to security and the newest contemporary market response: encryption technology. The industry has responded to a need for better security already, although not directly. The evolution of products into the baseband arena is being aided primarily by two attributes, one real, one perceived. The "real" attribute is increased utility as a result of baseband processing. Examples are user features (such as volume control), and the freedom to do novel kinds of signal processing. The "perceived" attribute is security. In reality, being at baseband has little to do with the ability of a system to resist compromise.

An understanding of the value of encryption when properly applied is the goal of this paper. It is intended that the skeptical reader be swayed by discussions and explanations contained herein by looking at a system's security from a global standpoint. By understanding some of the buzzwords, and asking a few critical questions about how the system you are evaluating is put together, *you* can tear down the rhetoric and make the tradeoffs. We first look at the main facets of a contemporary cable system.

THE ADDRESSABLE SYSTEM — WHAT'S IMPORTANT, WHAT'S NOT

A CATV system is a communications system. In a modern addressable system there are four basic kinds of information sent: Program video; Program audio; Control information; Data Services; **(Figure 1)**.

Under data services is lumped a variety of additive types of digital information such as teletext, videotext, downloaded software such as games or computer programs, and any interactive communications. While the need for security of these service will certainly become evident in time, the lack of standardization in format or modulation/transmission techniques causes us to set this category aside for the moment.

In securing premium television delivery, the methods of handling the first three information types are within the confines of a specific addressable pay TV system. Program audio and video are generally, though not always, associated with each other. For simplicity we consider them two constituents of a premium broadcast, as is usually the case. They are counted separately above, however, for two reasons: their broadcast formats are different and independent (VSB AM versus FM), and the associated channel bandwidths required for each are an order of magnitude different. The relevance of these differences will be explained, but we note that premium programming has no entertainment value without both.

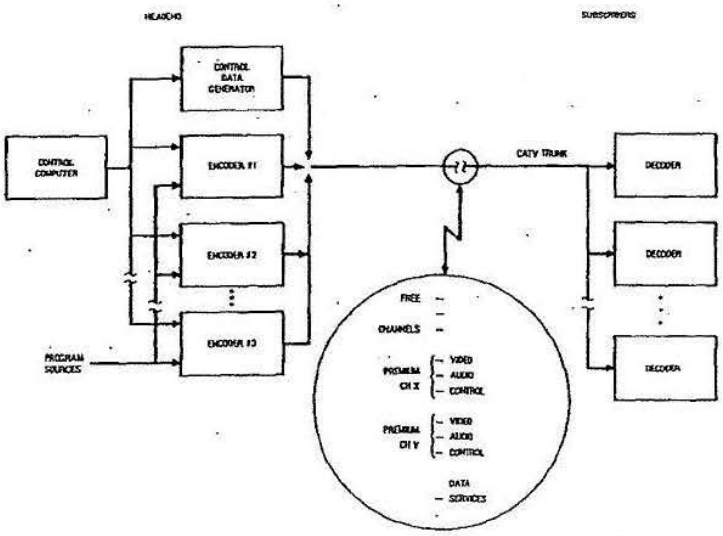

Figure 1. Contemporary CATV Network

The third information type, "control" is whatever is used by the manufacturer (assuming an addressable system) for network control and authorization purposes. Note that the control channel or channels have no direct relation to the entertainment being purchased. One of the first questions to ask then about a scrambling system is what is the function of the control/authorization channel? Secondly, how is it related to the scrambling approach if at all? In most systems the control channel(s) direct the decoder to decode or not to decode as a function of channel tuned to, or the "tier" of a given program. Critical to the issue is whether any information contained in the control channel is used in the decoding process. If not, the control channel can be ignored when attempting illicit program access. Likewise, if the scrambling technique or decoder circuitry easily succumbs to one-time defeats, the control channel content is of no interest. Such is the case when descrambling can be accomplished by observation of the scrambled signal alone.

What about "time varying scrambling"? Time varying scrambling adds a dimension of change to the scrambling process such that the decoder will not properly decode at all times unless it appropriately follows the change. Is this better security? To a degree, yes. But consider the pirate entrepreneur who wishes to build the "universal decoder." Most positive scrambling systems use one of several techniques of suppressing the horizontal synch pulse. ("Positive" systems are those which actively scramble the premium signal, and thus require a decoder. "Negative" systems remove the signal from the unauthorized viewer through filters or signal path switching.) Whether the systems' scrambling is at RF or baseband the pirate's universal decoder, if built to operate at baseband, can quite easily re-construct the synch pulse completely ignoring all control channel information, time varying or not.

Figure 2 illustrates several avenues where system attacks can take place. While simple wire changes/clipping/shorts, etc. are the deadly fears of operators, in fact there are many ways to attempt piracy. Jamming tones can be filtered, notch filters which trap out pay channels can be removed, addressing data can be synthesized locally, and add-on hardware in the decoder can be employed.

What is desired is a scrambling technique which 1) renders the entertainment value of scrambled programming useless, 2) does not lend itself prey to one-time defeats (implies some sort of time-dependence), 3) cannot be undone by observation of the scrambled waveform, and 4) requires information continually downloaded from the headend, forcing contact through the control channel between headend and decoder to be maintained.

The last criterion has an important implication: in order to effect proper decoding, it's necessary for the decoder to be instructed *how* to decode, not just simply when to decode. In an addressable system, the control channel is the link between headend and decoder over which decoding instructions can be sent.

The previous discussion is gearing us toward the theme of this paper. Principally that in CATV distribution "security" is a systems issue. The simplest method of defeat will be the path followed by the would be pirate. The system must therefore be viewed from several angles and an adequate threshold against compromise developed for each. How much added security is afforded by random video inversion of the picture, for example, if a simple-to-detect "flag" exists in the vertical interval indicating polarity? Is any security afforded in an addressable system simply because it's addressable? Not if it's easier to address (authorize) the box yourself than it is to open the box up and tamper with circuitry. At one time such arguments would have been considered too far out to worry about. But premium TV is big business these days and getting bigger. The motivations for the program thief and the MSO demand attention to these details as never before.

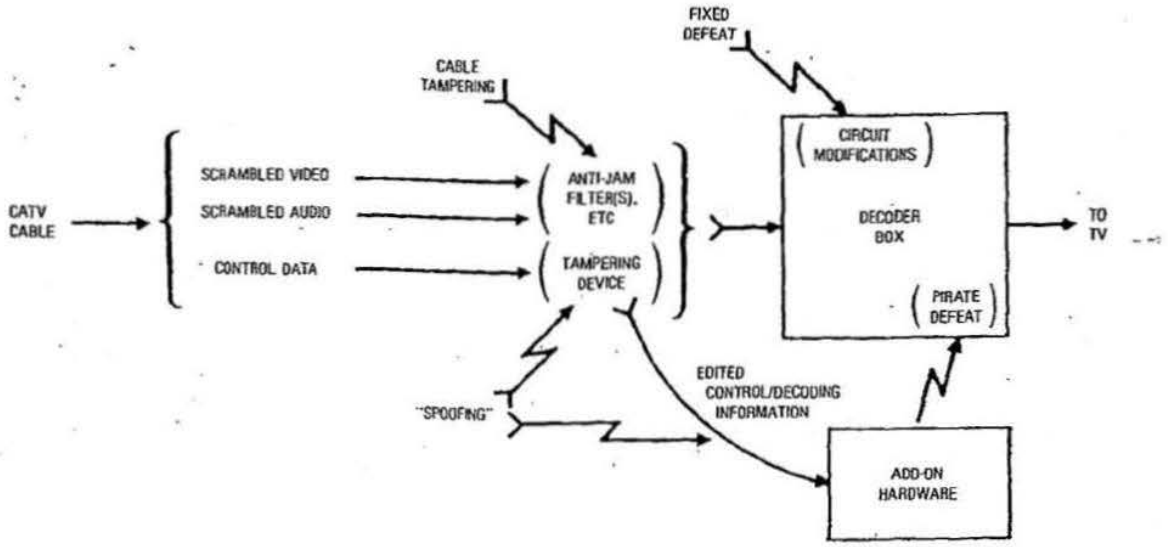

Figure 2. Network Attack Scenarios

ENCRYPTION IMPLIES DIGITAL

Now that we have defined what is desired, the value of encryption will be less mystifying. For encryption simply enables a complex security problem, in which many variables (audio, video, control) must be secured, to be bottled up into just protecting a few digital words. How this is brought about requires an appreciation for the difference between analog and digital transmission.

Standard television transmission, including all current scrambled pay TV techniques, is analog. That is, irrespective of whatever pre-processing or post processing techniques are used, the signal is analog during its transmission phase. Even newer systems claiming to employ "digital video" are in fact transmitted analog. The fact that they are processed digitally at the headend or receiver is purely an implementation convenience (and as yet an expensive one). The reason true digital video transmission techniques are not used in a matter of cost, both in terms of dollars and bandwidth. To digitize a color video picture requires a data rate between approximately 20 MBs and 80 MBs, depending on the coding technique and degree of compression applied. Efforts to reduce this bit stream appreciably are possible, but at extreme penalties of cost or picture fidelity.

The audio portion of a television program is less prohibitively handled digitally. A bit rate between 200 KBs and 700 KBs is necessary for digital audio, and this data can be readily transmitted within the confines of a standard 6 MHz video channel (along with the video, of course). Digital audio processing is no easy trick, however, this sort of technology requires a very sophisticated degree of systems engineering capability.

Once we have prepared the information itself for digital transmission, the door is open for the application of encryption. The control channel is inherently digital so it too can be "cryptographically" protected.

BOXING IT UP — THE ENCRYPTION OVERLAY

There are two main categories of modern encryption approaches: the "classical" or "conventional" approach and the "public-key" approach. The public key crypto system is, in theory, capable of performing all of the functions of the classical technique, but has a few special qualities in that fewer secret variables need to be passed around in the system. It also has implementational difficulties which make it less than attractive for many applications. For purposes of this paper, we consider only the classical system.

In the conventional encryption process (**Figure 3**) a digital bit stream (the information) is passed through an algorithm which transforms the input into a seemingly unrelated output bit stream. The transformation which is performed is a function of the "key variable," and in a conventional system the same key is used at both the transmit side where encryption is performed, and the receive side where decryption is performed. Since the key is a digital word of many bits, many different transformations are possible by varying the key. In a "good" algorithm, all keys are equally strong (i.e.: resistant to "cracking"), and no detectable relationship exists between the input data, output data, or key variable.

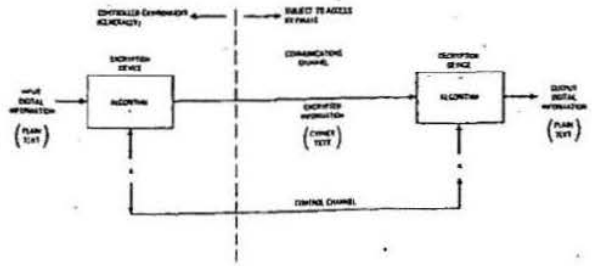

Figure 3. Classical Cryptographic System

The process of encryption must, of course, be reversible. That is, applying the same key at the receiver must yield back the original message. The original, non-encrypted data is called clear or plain text, the encrypted data is called cypher text. So during transmission, i.e., between headend and decoder, only non-intelligible cypher text is available to the would be tamperer. If the decoder doesn't have the proper key, no message or clear text will be obtainable, even if the pirate has the hardware. Further, in a properly designed system based on cryptographic security principles, we can give the pirate just about anything he desires: hardware, access to, and knowledge about the control channel, schematics, any firmware, even the crypto algorithm itself. The only doorway to information access, or in our case programming, is through the key variable. Controlling access to the key variables is thus essential. This is called "key distribution," and is the basis for what ultimately makes or breaks the security of a cryptographically-based system. The cryptographic or encryption algorithm, therefore, can be thought of as a lockbox. The message is encrypted or locked by the algorithm, and can only be unlocked by the same algorithm, which means the identical digital key must be used for decryption (we have yet to define exactly what is being encrypted).

KEY DISTRIBUTION

In a broadcast scenario, the problems of key variable distribution are not easy to solve. It probably has occurred to the reader by now that if access to working hardware is given to the pirate, it is little trouble to determine what digital key is being used for decryption. Recall, we said earlier that one-time defeats will not be allowed. Therefore, the message encryption/decryption keys (referred to as "service keys," since they are used in encrypting the service which in our case is programming) must be changed from time to time. The interval depends on the key length, the ability of the encryption algorithm to resist analysis by computer, the expected accessibility of the key, and the motivation of the system's enemy. Changing the key itself, if performed as part of the communications system network control protocol, is really very easy once the method is derived. (Alternate methods might be by courier, mail, etc.)

In an addressable system the CATV control channel is the obvious choice for a key distribution path. But one can't just go broadcasting the new keys throughout the network. They must remain secret to all but authorized decoders. The solution for controlling key access is to encrypt the keys for transmission. In fact, several types of information passing through the control channel are candidates for encryption. Authorization or tiering data, for example should also be considered "sensitive" information as, as pointed out earlier, it can easily be synthesized and fed to the decoder by simple digital hardware or any home computer. Such control channel manipulation by other than the legitimate network controller is called tampering. Attempts to subvert the system by tampering is called "spoofing."

So, we see that encryption alone will not secure the information exchange. Integrated within the system must be a totally planned out methodology for key distribution and protection against spoofing.

BACK TO BASICS

Armed with some encryption fundamentals, we look at the CATV distribution problem. Emphasized earlier was the notion that encryption is a digital process, that digital video transmission is not yet feasible, but that digital audio is. By recognizing that a time varying analog scrambling process can be developed in which the descrambling process is *controlled* digitally, we have a solid basis for an acceptibly secure entertainment delivery system. The other components are digital, encrypted audio, and an encrypted control channel for network control, key distribution and authorization of all program distribution and user features *from the headend*. In this system the information in the control channel must be employed to gain access to the services, because the services themselves are locked by the encryption overlay.

Time for another definition: Video "scrambling" refers to processes that are inherently analog. Line swapping, segment swapping, or other such time shuffling techniques operate to destroy the picture, and are quite effective. But they do not represent examples of encrypted video, for encryption requires a digital information source. Rather, these examples represent time varying analog scrambling controlled by an encryption process. Essentially any analog scrambling approach can be used with digital encryption of the audio and control channels, provided it adequately destroys the picture *and* is tied into the decryption process. This tie-in must be such that information necessary for proper descrambling is secured (and not self-evident by observation of the video) by the requirement for proper decryption.

In such a system "medium" security of the video exists and "hard" security on the audio is achieved. These phrases relate to the relative difficulty of pirating the resulting system. While analog scrambling is known to be less secure than encryption-based protection, with hard audio the entertainment value of the programming is, in fact, secured. In almost all current CATV systems, the audio channel is in the clear, or at best located on an easily defeated aural subcarrier. This leaves the only barrier to piracy the video scrambling. In the system described above, the video scrambling is very difficult to defeat and the audio is unrecoverable to the extent that the encryption cannot be broken.

Additional remarks are due in the area of key distribution. By transmitting service keys in an encrypted fashion throughout the system, we have not really solved the key distribution problem because to encrypt the service keys requires yet another key. Such is the notion of multilevel key distribution (**Figure 4**). Various information exchange networks (local area networks, electronic funds transfer, military communications, etc.) require different implementations of a multilevel approach. In the CATV environment the requirements dictate that 1) when the service keys are updated (changed), all decoders (and the encoder) must do so at the same time, 2) the system operation must insure that all decoders have had the new keys properly delivered, decrypted and prepared prior engaging them, and 3) only authorized decoders are able to perform (1) and (2).

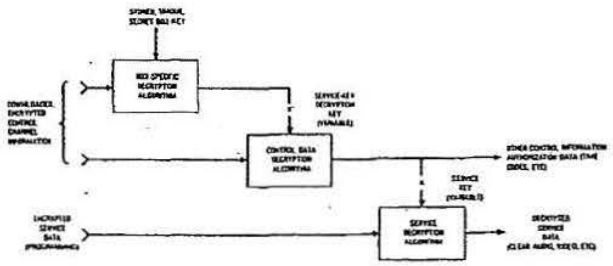

Figure 4. Multilevel Key Distribution (Decoder End)

Additional problems having to do with error control/error propagation must be addressed when dealing with encryption. Encryption algorithms generally have the characteristic that bit errors occurring in the receiving/detection process avalanche during decryption. Poor attention to detail in the systems design phase of a network employing encryption can have catastrophic results.

THE ADVERTISEMENT

Having given the reader enough background in the meaning of "cryptographically" protected CATV delivery system, the following is a brief description of Oak's new Cable Sigma system.

Scrambled video is employed, wherein complete horizontal and vertical synch pulse removal (as opposed to synch pulse suppression) is performed. Two channels of audio are digitized, encrypted and imbedded in the video. The standard aural carrier is not used, but is available. Two separate control channels are employed; the first, a global, FSK-modulated channel which all decoders continuously monitor; the other, an in-channel VBI (vertical blanking interval) data path which is channel-specific. The former contains general authorization and system oriented control data. The latter contains program-specific data relevant to a given channel and time. Separate service keys are utilized for each channel and the keys are varied continuously. A multi-level key distribution system is employed in which three key variables are used. These include a box-specific key which is secret and unique to each box (unknown, even to the MSO), a variable second-level key common to all legitimate subscribers, and the service keys. Solid state non-volatile memory is used in the decoder to store key and authorization information (encrypted while stored). Each box also has a non-secret box address which is its addressing ID used by the headend computer to communicate to the box.

A 64 bit field structured data-packet-based communications protocol has been designed around the FSK data channel. These packets deliver a continuous stream of data to decoders both globally and box-specific for purposes of encryption key delivery, special event programming, box installation and downloading of system parameters and box features. Special provisions exist to guard against spoofing and box swapping between systems. Protection for time-dependent variables and error control is also provided.

CONCLUSION

Oak is proud to present Sigma. With the information contained in this paper, it is our hope that the reader is better equipped to appreciate the security features available to him in this exciting new product line. The technology behind Sigma has been in development at Oak for the past four years. Extensive experience in digital audio and application of cryptographic principles has been accrued through Oak's ORION satellite security system and STV Sigma operations. Custom LSI circuits developed and used on those programs have been applied to Cable Sigma, and represent a major technology advantage toward reliability and manufacturability. We invite you to inquire for more detailed information, and encourage a comparison between Sigma and any CATV product on the market. With Sigma, program distribution is yours to control.

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.