AN ILLUSION **OF SECRECY**

By: Larry Randall

President, **THE NRE™ GROUP**

NOTE TO READER: *This article is basically in the format that was required by Public Safety Communications Magazine, whose editor (at that time) mandated extreme emphasis on "key" points and words requiring definition. (It was published as a two-part series by that magazine.) I have removed some of the "shouting" (overuse of bolding, all caps, and italics), but not all of it, as I have not had time to fully edit it and/or rewrite it for a more nearly "generic" audience. Please also note that this article was written in 1994 – and that it both reflects the technologies of that time and accurately predicts several future changes.*

No other science seems to have attracted quite the number of "inventors" as has Cryptology -- the science of communication in "secret" codes or ciphers. The root word "Crypto-," (from Latin "Crypta" and Greek "kruptos" -- meaning "hidden") was often associated with the occult. Perhaps this explains some of the myths that persist to today. Encryption is not a "Black Art," it is a science. This article will present the pertinent issues of encryption in general, and relate these issues to the Communication Security of Public Safety telephone, fax, and data links over landline and radio channels.

Cryptology, in reality, encompasses two sciences. **Cryptography** is the largely theoretical science of system and device creation. Cryptography concerns itself with changing the original **"plaintext"** message into an unintelligible **"ciphertext,"** from which the intended recipient(s) who have the proper ***"KEY"*** may recover the original "plaintext**.**" **Cryptanalysis** is the applied science of "codebreaking," that is, the science of recovering the "plaintext" from the "ciphertext" *without* benefit of the key.

Cryptography and Cryptanalysis are really at opposing ends of the same field, and they constantly drive each other to advance the overall science of Cryptology. If Cryptography produces a new system, Cryptanalysis must find a way to attack it. If a "breakthrough" in Cryptanalysis renders a current system obsolete, Cryptography must develop a better system to counter the attack. Thus, an advance in either requires an advance in the other.

Cryptography is concerned with "Communication Security". In other words, Cryptography hides the *content*, but not the *existence* of communication. Another science, called **Steganography,** is concerned with "Transmission Security," which seeks to hide the *existence* of communication. There is a place for each, and some systems employ both Cryptography and Steganography.

"Traffic Flow Security" is a form of Steganography which is used on continuously available links which may also be continuously accessible to an attacker. Examples of such links are dedicated telephone lines and microwave channels. Traffic Flow Security seeks to prevent the attacker from determining if a valid call or message ("traffic") is in progress. It does this by maintaining a constant "noise" on the channel that does not change in any manner whether "traffic" is present or not. This prevents the attacker from detecting how much (or little) "traffic" is being sent, preventing "Traffic Analysis."

In **"Traffic Analysis"** the *existence* of communication, and the *number of "pieces" (traffic count)* is analyzed. Over time, this intelligence can very accurately detect an impending operation. Normally, last-minute details generate "traffic" in the form of messages, faxes, telephone calls, or radio "chatter", but either a sudden "peak" or a sudden "valley" can suggest that something is happening. "Special Operations" Units should be especially aware of this, and should carefully control their communications activities to prevent losing the Tactical advantage of surprise *even if ALL of their communications are encrypted!*

5709 Kettering Court, Richardson, Texas, 75082 g 214-536-0325 g www.nregroup.net

PRACTICAL APPLICATION OF ENCRYPTION DEVICES

TIME VALUE OF INFORMATION

The concept of "Time Value" of information is the single most important principle that must be considered to determine the **level of security** needed to secure information against attack. There are three basic levels of security. In ascending order, they are: **"Privacy," "Tactical,"** and **"Strategic."** The word **"Privacy"** is also used when referring to encryption devices which are "non-Government Crypto." In that context, "privacy" does not address the level of security, it merely differentiates the device from "Crypto." In government and defense industry circles in the United States, "CRYPTO" is used exclusively to refer to National Security Agency (NSA) Approved Government Crypto devices.

"Privacy" level information is defined as information that may either have limited impact, or that may have very short "time value." "Privacy" information *might* be the meeting of a task force before a raid, *if and only if* undercover agents/sources are not mentioned or otherwise identified. The information has short "time value" because the "bad guys" **know** a raid is happening after the door is knocked down.

Tactical level information is defined as information that must be protected from a well-equipped adversary for an absolute *minimum* of 18 months. Obviously, the force make-up of an undercover operation in progress, and even the *existence* of the operation is of this level.

Strategic level information is defined as information that must be protected from a well-equipped adversary for a *minimum* of a few decades. A "subset" of "Strategic," called "Diplomatic" extends the minimum to multiple decades of governmental attack with "ultimate" technology.

DETERMINING THE SECURITY LEVEL OF A DEVICE

The security level a device is capable of is determined by a combination of the "goodness" of the **"Key Generator" (KG)** and the "balance" of the **cipher**. The *"Key Generator"* (KG) is the device which accepts a ***"Key"*** and produces an output data stream which is used to encrypt the information to be transmitted. The *"Key"* is a very long number. Normally, the length of the *"Key"* is expressed in either "bits" (180 bits = 2^{180}) or in powers of ten (1.53×10^{54}). Each time a transmission is begun, a new **"Message Key"** is used. The purpose of the *"Message Key"* is to prevent the *Key Generator* from producing *the same output* on each transmission. The *minimum* number of *"Message Keys"* for a secure device is 2^{25} ($= 3.3 \times 10^{7)}$, and several devices use 2^{33} ($= 8.5 \times 10^{10}$) or higher. The number of message keys has a direct impact on the required key change interval.

While a discussion of *Key Generator* indicators of "goodness" is beyond the scope of this article, the critical requirements of a *Key Generator* are: 1) that it produce an output which does not reveal the *Key*, 2) that a one bit change in the *Key* produce a large change in the output stream, 3) that its output appear to be *random*, 4) that the length of the output *cycle* be very long, and 5) that no "mini-cycles" exist within the cycle.

The "balance" of the *Cipher* is critical to effective encryption. *Data* streams may be enciphered by the *perfectly balanced* "Exclusive OR" method. *Asynchronous data* may require *character* encryption. *Character* encryption becomes *language sensitive* if the output must be restricted to allow it to pass over a network, such as Telex®. A network message system is normally balanced for only one language and *should not* be used to protect information in another language!

5709 Kettering Court, Richardson, Texas, 75082 g 214-536-0325 g www.nregroup.net

SELECTION OF DEVICE LEVEL

Public Safety users are principally concerned with "Privacy" and "Tactical" levels of information. As the difference in cost between **good** "Privacy" devices and "Tactical" devices is small; and as "Tactical" devices eliminate the need for two kinds of devices in inventory, the best choice for all Public Safety communications is a "Tactical" device.

SELECTION OF DEVICE TYPE

The selection of the **type** of encryption device for a given application requires consideration of the expected communication system(s) (telephone, radio, or a combination) to be used, the type of information (voice, data, or other) to be transmitted, the technical constraints imposed by the device, and the operational impact of adding the device to the system. To properly evaluate these factors, it is necessary to understand both the technical and the operational consequences of attaching a particular device to a communication system.

VOICE: WHAT IS IT?

As all common communication systems are primarily designed to carry the human voice, it is useful to understand the nature of voice. The human voice is highly "redundant," meaning that parts of a spoken word may be missed without affecting our ability to understand the word.

Human speech consists of both "voiced" and "unvoiced" sounds. These sounds cover a range of 80 to over 8000 Hertz, and are "individualized" primarily by the basic (or "fundamental") frequency and by the shaping of the five cavities in the vocal tract. Individual **resonances** of each of these five cavities combine to enhance (build up) some frequencies and to suppress (reduce) others. As the shape of any of the cavities is changed, by "pursing" the lips, for instance, the resonance of that cavity is changed, which changes the "sound" of the voice.

The "*voiced*" sounds contain most of the *power* (loudness) of speech. The *vowel* sounds(a,e,i,o,u) are the greatest contributors to this power, as they represent the longest duration sounds. Unfortunately, the greatest contributors to *intelligibility* ("understandability") are the *consonant* sounds, which are primarily "unvoiced" and contain *much lower power* than the vowel sounds. Because of this, words such as "give" and "live," "set" and "get," and even "nine" and "five" may be confused in noisy environments.

If we can see the speaker's mouth, we subconsciously associate the shape of the mouth with the missing sound, allowing us to "hear" without receiving the sound. Without the mouth shape reference, we must resort to other clues, such as *context*. (Context is the "background" of the rest of the message or conversation.) If no unmistakable clue is available otherwise, we may ask the person to *spell* the word in question. Unfortunately, many letters of our alphabet sound very much alike. For this reason, we must resort to *phonetic* alphabets for precise transmission of letters in names and vehicle tag numbers. In a phonetic alphabet, each letter is represented by a word that begins with that letter, and that cannot be confused with the word representing any other letter.
(A = Alpha, B = Bravo, ... P = Papa, Q = Quebec, ... X = X-ray, Y = Yankee, Z = Zulu)

5709 Kettering Court, Richardson, Texas, 75082 g 214-536-0325 g www.nregroup.net

COMMON FACTORS OF VOICE COMMUNICATION SYSTEMS

All "Voice Communication Systems" (such as telephone and radio systems) limit communication to a "Voice Frequency" range that begins at approximately 300 Hertz and extends to approximately 3000 Hertz. This range only partially accommodates the first three "*Formants*" of human speech, meaning the first three resonances of the human vocal cavity. Note that the "fundamental" frequency of the voice, which lies between 80 and 200 Hertz in males and 100 to 250 Hertz in females is not transmitted. The lowest frequencies are primarily *vowel* sounds, and are not critical to intelligibility. The higher frequencies are primarily *consonant* sounds, however, which are *essential* to intelligibility.

The "magic" which allows voice communication systems to limit the high frequency to only 3000 Hertz is the human brain. The redundancy of speech provides "clues" to sounds that are above the 3000 Hertz limit. Humans subconsciously "hear" sounds such as the /s/ in "sit," even though the frequency of this sound lies between 5000 and 8000 Hertz, and *is not* passed by a voice communication system. Obviously, sounds above 3000 Hertz are not absolutely required for intelligibility, as the human brain can "supply" missing sounds.

DATA COMMUNICATION OVER VOICE SYSTEMS

Remember that voice communication systems limit the highest frequency that may be transmitted to 3000 Hertz. This means *any* signal must fall below 3000 Hertz. If *data* at 9,600 bits per second (bps) is applied to these systems, it *cannot* be passed, as it is above the 3000 Hertz limit. This has a profound effect on the transmission of data over voice communication systems. In the case of 9600 bps data, the system would have to be able to pass 9,600 Hertz (actually, more -- but let's keep it simple) to allow this data to pass.

In other words, a voice communication system *cannot* support 9,600 *Baud*, because it cannot pass a *frequency* high enough to allow the data to be transmitted. *But*, you say, personal computer modems operate at 56,000 Baud. No, they don't. A56,000 bps (56 kbps) modem operates at 2,400 *Baud*, and sends multiple bits in each *symbol*. (One *Baud* is, by definition, one *symbol* per second.) The *Bit rate* is 56,000 bps. The *Baud rate* is 2,400 *Baud*. This sounds really "picky," but it gets *very* important when we consider radio links.

THE GOOD: TELEPHONE SYSTEMS

The telephone system normally provides a relatively "*clean*" environment with little or no noise and a very "smooth" or *"Linear"* frequency response -- meaning that all frequencies are treated relatively equally. In this environment, very *complex* modulation methods may be used. The 56,000 bps modem in the example above uses a complex combination amplitude and phase modulation which produces a "signal constellation" of a few hundred possible points.

If either *amplitude* (how "big" the signal is) or *phase* (how the signal is "rotated," or shifted in time) is sufficiently distorted, an error occurs. *One error* produces multiple erroneous bits, as a *single point* (a "symbol") represents multiple bits. An extra bit is added to "Trellis code" the pattern to provide a measure of *symbol error detection and correction*. This limited error correction improves the performance of the modem over marginal links.

5709 Kettering Court, Richardson, Texas, 75082 g 214-536-0325 g www.nregroup.net

THE BAD: VHF/UHF RADIO SYSTEMS

VHF/UHF radios, "trunked" systems, and "Cellular" systems use *Frequency Modulation (FM)*. An FM system is composed of a transmitter, with a *modulator*; and a receiver, with a *demodulator*. Between, there is a distance that must be traversed, with attenuation that (typically) lowers the signal level at the demodulator to a few millionths of a volt. There are also many sources of noise and distortion that are added to the signal appearing at the demodulator. If a "*Repeater*" is used, an additional Demodulator and Modulator appear in the "chain." Each signal path, each Demodulator, and each Modulator is a source of noise and distortion, *adding* to the total *system* noise and distortion.

Modulation systems that depend upon extremely precise phase and amplitude positions are not well suited to transmission over these systems *unless* "perfect" links may be assured. In a "perfect" link, the modulator of the transmitter is *linear*, and the *noise-free, undistorted received signal* is applied to a demodulator that is also *linear*. Perfect links do not exist, though their characteristics may sometimes be approached. In many radios, modulators and demodulators are far from linear.

THE WORSE: MOBILE VHF/UHF RADIO SYSTEMS

If *either* the transmitter *or* the receiver is moving, the change in relative time of reception caused by reflections from buildings, mountains, etc., represents a change (distortion) in the *phase* of the signal, and "fades" may distort the *amplitude*. Clearly, the mobile environment is not perfect.

By reducing the complexity of the signal, better performance may be achieved. Unfortunately, reducing complexity means reducing the maximum *bit rate* that may be transmitted at a given *Baud rate*. Recall that the (approximate) maximum *Baud rate* that may be transmitted on a "normal voice communication system" is *2400 baud*.

Reducing the bit rate from 14,400 bps to 9600 bps, while maintaining a Baud rate of 2400, reduces the "constellation" from 128 points to 16 points. Clearly, this means the *symbol* points are farther apart, and the *probability* of a correct decision is improved. Even this complexity is too much for many radio systems to handle, so commonly used data rates are 1200 to 4800 bits per second, at Baud rates of 1200 to 2400.

At 1200 bps, both the Baud Rate and the BIT rate are 1200. This means *one symbol equals one bit*, and the modulation is simple Frequency Shift Keying (FSK). This simple modulation is the most "robust" in its ability to be correctly detected, as (audio) phase errors have no effect and amplitude errors are relatively insignificant.

THE UGLY: HF RADIO

Voice communication over High Frequency (HF) Radio is possible under very adverse conditions. The HF radio system normally uses Single SideBand (SSB) modulation. Normal AM modulation (like "CB") *wastes* 50 percent of the transmitter's power in the "carrier," and *wastes* another 25 percent in one of two *identical* sidebands. Thus, *only 25 percent of the transmitter's power is actually used to transmit the information* that is the *reason* for the transmission to exist. SSB places all of the transmitter power in the information to be transmitted. An AM transmitter needs an *output* power of almost 800 Watts to provide the *same* range as a 100 Watt transmitter using SSB, *given the same antennas and the same frequency*.

5709 Kettering Court, Richardson, Texas, 75082 g 214-536-0325 g www.nregroup.net

If you can imagine attempting to vocally convey a series of numbers to another person across a crowded room while the cannons of "The 1812 Overture" are booming, you have a picture of the problem faced by the HF data modem during a thunderstorm. With the proper modem, however, data communication is *completely error free*! To achieve this perfect communication, both the *complexity of the modulation* and the *speed of the data* are greatly reduced. *Reliable* communication is of greater benefit than *fast* communication. Relatively fast data communication over HF **is** possible, however, the cost is usually not justifiable.

SPECIAL CONCERNS FOR CELLULAR SYSTEMS

The Cellular network occasionally "drops" a few hundredths of a second of audio. This is devastating to data. Normal "PC" data communication uses various methods of "ARQ" (Automatic Repeat reQuest) to correct errors. This is *not* adequate for Cellular, because of the modulator *linearity* problem, discussed earlier. For successful data transmission over Cellular, the modem *and* software *must* support a special protocol called MNP-10®. This protocol allows the program to automatically adjust the modem *transmit level* for minimum errors.

Even this is not adequate for "PC" based facsimile, as *none* of the "PC FAX" modems support *error correction* for facsimile transmission. For this reason, it is *virtually impossible* to successfully transmit or receive a fax over a Cellular system using a "PC" at *either* end of the link. *"REAL"* fax machines employ CCITT Standard Error Correction, which allows them to operate *error free* over the Cellular system.

I have talked with many of the "designers" of "PC" modems, to inquire about their reasons for not offering facsimile error correction. Not one manufacturer was even aware that error correction was included in facsimile transmission. One Product Manager even told me that there *was no error correction method* for facsimile, and there was *no reason* to have error correction on facsimile, as the user could simply *re-send* the page until it was received.

The inescapable conclusion is that "PC" modem manufacturers do not understand facsimile, and do not *wish* to understand facsimile. Until users *demand* that "PC" modems properly support the CCITT Standard for facsimile transmission, they will remain *unusable* over Cellular.

SO, WHAT DOES THIS HAVE TO DO WITH ENCRYPTION?

Every encryption device has limitations in the form of the information it can encrypt and in the type of communication system required to support it. An understanding of the limitations of the technical issues relating to each type of communication system is needed if one is to select a device that will perform properly in a given environment. Good management dictates that we look not only at today, but that we also plan for the future.

TELEPHONE SYSTEMS: THE FUTURE

Politics and rhetoric about *"The Information Highway"* aside, the telephone system will not *appreciably* change over the next five years, and *probably* for the next ten years. The reasons behind this are economics, logistics, and telephone company "foot dragging."

5709 Kettering Court, Richardson, Texas, 75082 g 214-536-0325 g www.nregroup.net

In Richardson, Texas, we have the largest concentration of telecommunications companies in North America in the "Telecom Corridor." Even here, only one telephone company central office supports the "standard" 56kpbs/64kbps "Integrated Services Digital Network (ISDN)," and only a total of three central offices in the entire Dallas area support it. This situation has not changed in the past five years.

Private microwave and SATCOM facilities pave our information "pathways," while the "streets" necessary to reach both businesses and homes are merely pictures on a drawing board. There they will remain until the "TELCO's" are either forced to *provide* them, or are prohibited from continuing to *inhibit* them.

RADIO SYSTEMS: THE FUTURE

Because of the problem of "crowding," the FCC has mandated that channel widths be reduced. Voice may be transmitted in much less "bandwidth" by using more efficient modulation methods. Despite the reluctance of manufacturers to adopt more efficient methods in which they do not have a proprietary interest, more efficient modulation methods MUST appear in future radios.

CANDIDATES

ACSB (**A**mplitude **C**ompandered **S**ide-**B**and) is available now. ACSB makes it possible to transmit the same quality voice now available to Public Safety in a bandwidth of 3000 Hertz, or less. Range tested as equal to (or better than) FM for identical power levels and antenna heights. Testing of this method was vigorously opposed by at least one powerful radio manufacturer with a vested interest in the "status-quo". The segregation of ACSB to a band completely removed from the Public Safety allocations is a testament to the power of this manufacturer.

"NARROW FM" is possible. By reducing the maximum deviation from ±5,000 Hertz to ±2,500 Hertz, the channel may be "split" to a total width of 5,000 Hertz. This effectively doubles the number of available channels, while maintaining a "migration" path for current equipment. Frequency stability would require relatively tight control, but all radios now being offered on the commercial market meet or exceed the required stability. The effect on *RANGE* is a theoretical increase, although it is barely perceptible in practice.

"FREQUENCY SHIFT" modulation is also possible. Using this method, the frequency is allowed to vary on only ONE side of the carrier. This method is currently used in video recorders. Essentially FM, this method further reduces the bandwidth by a factor of two.

"FREQUENCY COMPANDERING" may be applied to the voice before it is applied to any of the above, reducing the highest voice frequency to be transmitted. This method takes advantage of the "holes" in the voice spectrum, and shifts the upper frequencies downward to eliminate them. The receiver restores the "holes" and outputs the original voice spectrum. Higher fidelity audio is possible in a given bandwidth with this method. Alternatively, the same fidelity is possible in a *smaller* bandwidth. Excellent intelligibility has been obtained in a bandwidth as low as 1,600 Hertz!

VERY LOW BIT-RATE DIGITAL VOICE is a long-term goal, not a short-term reality. While it is *theoretically* possible to transmit voice at 300 bits-per-second (bps), the results of all attempts to date have been very poor. At 1200 bps, the channel width required would equal that required for "normal" voice.

5709 Kettering Court, Richardson, Texas, 75082 g 214-536-0325 g www.nregroup.net

TYPES OF DEVICES AND THEIR APPLICATION

Let's address the spoken word first. *Voice* information may be secured by either *Analog* ("Scrambling") or *Digital* ("Encryption") means. There is no *Security* advantage to either, at the Tactical level. There may, however, be significant complexity and cost *disadvantages* to one of them, as we shall discover later.

Data links obviously require Digital encryption devices. These devices must match the *form* of the data from the "terminal." Yes, Alice, there are two types of data in Dataland. The data from Personal Computers is *Asynchronous*, meaning it uses archaic "Start/Stop" communication. The data of Facsimile transceivers, as well as that of all high-level computer links is *Synchronous*. Synchronous data transmits information in less time, assuming identical information and identical Asynchronous and Synchronous bit rates.

VOICE: SCRAMBLING FOR SECURITY

It is unfortunate that many law enforcement agencies, as well as private companies, turn to low-cost "scramblers" of the type advertised in airline magazines and radio industry publications. Each manufacturer of these devices claims "millions," "billions," or "trillions" of possible "key"("code") combinations. Unfortunately, the number of "keys" is not an indicator of the security level of a device. It should, however, be pointed out that "trillions" (10^{12}) of possible keys *is an extremely small number* for a Tactical Level device, which *should* have at least 10^{20} key combinations. (A Strategic Level device *should* have at least 10^{50} key combinations.)

The security level of a scrambler is, *first and foremost*, a function of the relative complexity of the scrambling method used. *IF* the scrambling method is good, then the "worth" of the "key generator" is a factor. If the scrambling method is poor, the *best* key generator cannot help!

The *REAL* question is "How good is the *device* at protecting information?" Unfortunately, many of the *so-called* "scramblers" on the Police market *will not* protect information long enough for a strike team to drive from headquarters to the "Bad Guy's" house, even if that house is only *ten minutes* from headquarters!

Ten minutes is the *longest* time needed to attack three well-known "scramblers" before three persons, each in independent tests, could read *100 percent of the content* and *86% to 95%of actual words* in "real-time." The "expensive and complicated system" used to attack these so-called "scramblers" consists of a normal "police scanner" and *TEN dollars' worth of parts!* No, not "in addition to a computer," just ten dollars' worth of parts, period.

It is critical to note that *no attack was made on the "millions" or "billions" or "trillions" of "key" combinations* each manufacturer touts as "evidence" of security. This attack is not necessary, as the scrambling algorithm yields to unsophisticated attack. Because the "scrambler" *output* is easily "broken," *any* system using the same "scrambling" technique is worthless.

5709 Kettering Court, Richardson, Texas, 75082 g 214-536-0325 g www.nregroup.net

These *so-called* "scramblers" are **dangerous** in the extreme, because they **falsely** lead the user to feel secure. The technique used to decipher them dates to September 1941. It was used by the Germans to listen to conversations between President Franklin Delano Roosevelt and Prime Minister Winston Churchill (among others).[1]

The problem with these so-called "scramblers" is their simplicity. They are basically a form of *"Frequency Inversion"* device. This type of device simply changes the *frequency* of the voice, turning lows to highs, and vice-versa. All of the tested (and easily broken) devices expand on this basic technique by splitting the speech into "bands" and changing the inversion frequency every few tenths of a second. The result is a constantly changing sound similar to a tape played too fast, *except* that the *"cadence"* of the words remains.

In order to effectively "scramble" speech, the nature of speech must be understood. In human speech, the long *vowel* sounds (a,e,i,o,u) represent both the greatest time and the greatest power, but the smallest portion of intelligibility. The *consonant* sounds, which are both short in time and low in power, are essential to intelligibility.

The vowel sounds, which are preserved in their *time* relationship by "inversion" devices, not only allow the *cadence* of speech to be heard, but also provide a *pitch reference* for decoding. Once a relatively understandable *pitch* is found, the consonant sounds are in their proper place, and the "scrambling" is effectively undone.

True scramblers do not permit this attack because their designers recognize the redundancy of speech. True scramblers change frequency **and** time relationships in a constantly changing pattern determined by a voice encryption "algorithm" (method) designed to produce a high level of unintelligibility. The algorithm is, in turn, driven by a well-designed *key generator*, which constantly changes the sequencing of the voice "taps" in a highly non-linear fashion.

True scramblers are in current use by United States forces and agencies for many types of *Tactical* communications. The reason a scrambler can never be considered to be a Strategic Level device is that elements of voice appear in the output. No matter how well disguised these may be, they can be *eventually* reassembled into the original message. With a *"real"* scrambler, however, information loses its value before any reasonable chance of recovery. Further, with a *"real"* scrambler, recovery of one "message" *does not* permit recovery of any other message, *including* the reply.

Real scramblers may be used on *any* voice communication system. They may be used with any radio system, including HF, *without* reducing the range of the system. They have even been successfully used with "phone patches," both manual and automatic, in a number of systems.

---

[1]The primitive "A3" scrambler used on the circuit was replaced in 1944 with a "Two-Dimensional" scrambler. Voice scrambling was then quickly abandoned for all but the most innocuous conversations. (Strategic Level communications in the last months of the war made use of a "Telekrypton" teletype cipher device. It is speculated that these messages were sent with "one-time" tapes.)

5709 Kettering Court, Richardson, Texas, 75082 g 214-536-0325 g www.nregroup.net

VOICE: THE DIGITAL "SOLUTION"

"Digital Voice" is really not "voice". It is a digital ***representation*** of voice in one of several forms. "Digital Voice" may be used in radio systems, but the required bandwidth for intelligibility merely ***equal*** to FM systems ***doubles*** the present FM bandwidth. This increase in bandwidth is contrary to spectrum efficiency. Worse, it ***decreases range by a factor of two*** (or more), compared to an identical system using standard FM!

Digital voice is most often added as *"secure voice"*, and used on limited frequencies. This may, in some instances, be an acceptable compromise. In many cases the digital voice "solution" was implemented only because a salesman of a radio manufacturer said it was the ***only*** secure voice system which was technically compatible with their radios. Such salesmen may be charitably described as "unknowledgeable" in communications security applications.

The ***costly changes*** to existing radio systems which are required to permit even reasonably good quality digital voice to be used ***today*** make this a "future" technology for most practical systems. "Reasonably good quality" should be taken to mean digital voice which roughly approaches ***minimum*** telephone quality in speaker recognition and intelligibility. Today, the required bit rate is at least 8,000 bps for the "medium complexity" digitization methods (CELP, etc.), and 16,000 bps for a relatively simple digitization method (CVSD).

DATA

The most "common" data encryption device is a ***Link Encryptor***. These are devices which automatically encrypt any data appearing at their input, and automatically decrypt data as it is received. The better devices employ *"Traffic Flow Security"* to counter Traffic Analysis. These devices are *"Transparent"* to the operator, as they do not change normal operational procedure. Link encryptors may be employed on either "dial-up" or "dedicated" circuits.

The *"STU-III"*, *"SECTEL®"*, and *AT&T®* "NSA Type I and Type II" secure telephones used by some U.S. Government agencies and state police agencies, as well as the commercial counterparts of these devices, may be used to encrypt the data from personal computers. The modem of the secure telephone device (not the "PC") is used on the line.

Data may be ***either*** Asynchronous or Synchronous. If one has both Asynchronous and Synchronous terminals, it may be desirable to secure them with a single encryption device. This is made possible by the use of an "Async-Sync Convertor."

Asynchronous data should be converted to Synchronous for encryption and transmission, then reconverted to Asynchronous after decryption. Synchronous data produces ***fewer errors*** than Asynchronous for the ***same*** link noise level. Additionally, Synchronous devices ***DO NOT*** require the link speed (the "bit rate") to be known, as they automatically adapt to any speed within their operational range. Their operational range is typically from 10 bps to ***at least*** 20,000 bps.

5709 Kettering Court, Richardson, Texas, 75082 g 214-536-0325 g www.nregroup.net

FACSIMILE

The facsimile machine is simply a different form of data device. Thus, its encryption may be treated as a data encryption need. There are also some *special* encryption devices for facsimile transceivers, which require only a *telephone line* connection to the fax. These *facsimile only* encryptors permit the operational procedure of the fax to remain unchanged. These devices represent the ultimate in operational simplicity, as the operator does not require re-training. They allow communication between fax machines of differing manufacturers, and some (*NOT* all) allow all "Non Standard Features" to pass. These "Non Standard Features" include "400 dpi" or "High Resolution" modes which are available *only* between essentially *identical* fax machines of the *same* manufacturer!

In the "traditional" encryption arena, some fax machines may be (optionally) equipped with *two* "RS-232" ports, allowing a normal *synchronous* data "link" encryption device to be used. The operation of each type and manufacturer of fax machine is different in this scenario. With some fax machines, the operation is unchanged and "transparent" to the operator. With others, many steps are added to the procedure, and extensive re-training may be necessary to prevent accidental "CLEAR" (unencrypted) transmission of sensitive documents.

Some, but *not* all, fax machines used with "link" encryptors *must* communicate with machines of the *same brand*, and some must even communicate with the exactly identical *model*! The "Model Specific" scenario, especially, should be avoided. A failure will cause you to incur high maintenance costs on *obsolete* equipment to preserve your *now unexpandable* network. *Combination* data and fax applications are possible when "link" encryptors are employed.

Finally, the *"STU-III"*, *"SECTEL®"*, and *AT&T®* devices require a fax capable of operation with one "RS-232" port. The author has adapted several commercial fax transceivers to these devices and to "special" power sources. We now build a system that is used by the United States Air Force to operate the STU-III and MFAX® from 10 - 30 Volt vehicular power.

THE FAX FACTS

Most facsimile manufacturers and vendors are unable to offer advice, or even answer questions concerning operation of their machines with encryption devices of any type. As the designer of the first operational "encryption interface" to a commercial "Group 3" (Digital) fax machine, the author normally receives several telephone calls per year regarding fax encryption applications from manufacturers, vendors, and end users. Because most encryption devices and fax machines are available to us, we often have an answer available. In other cases, specific models are made available to us for testing and evaluation.

The best advice one can offer is common sense. Regardless of the opinions of the vendor(s), manufacturer(s), Chiefs, Indians, Purchasing, or others -- the *most* important opinions are the opinions of the persons who must make a system work! Select the **Security** of the device for the **Time Value** of the information. Select the **Type** of device, and the facsimile machine with which it will be used, (in the cases in which the fax machine operation may change between "CLEAR" and "ENCRYPTED"), according to the "comfort level" of the operators. Just because a system *technically* meets operational specifications, that does *not* mean the system works. If the operator cannot successfully operate the system, the *SYSTEM* doesn't work!

5709 Kettering Court, Richardson, Texas, 75082 g 214-536-0325 g www.nregroup.net

All decisions must, of course, be consistent with network **compatibility** and quality. This is especially important both **AFIS** (**A**utomatic **F**ingerprint **I**dentification **S**ystem) applications. Only *ONE* manufacturer is *totally compatible* with this system, using specific *MODEL NUMBERS* and *SPECIAL* firmware revisions.

"DES": THE "DATA ENCRYPTION STANDARD"

There is a common misconception in security and Law enforcement circles that the "magic word" which ensures security is "DES". Some even believe "DES" to be a "Government" communication security algorithm, and thus, highly secure.

The truth is that "DES" was developed under contract to the National Bureau of Standards as a "standard" for data encryption. It is *relatively* secure **IF** properly implemented. There was **ONE** version of "DES" which was approved by the National Security Agency (NSA) for use by some "soft agencies" and government contractors ***for NON-CLASSIFIED INFORMATION*. ONLY** that one version was *ever* "approved" for any government use.

"DES" is, at best a ***"Tactical"*** level system. If improperly implemented, as *many* devices were, it is barely "*Privacy"* level! The reason for the drastic drop is the tendency of the algorithm to "short-cycle" in certain implementations. This allows an attacker an easy "break" of the system.

SOFTWARE BASED ENCRYPTION

The U.S. Government allows **only hardware** devices to be used to encrypt the transmission of *any* form of *"CLASSIFIED"* material. The reason is simple. It is **impossible** to develop a method of software encryption which is truly secure. An attacker need only to access the file in which the "*KEY"* is stored in order to access all information encrypted with that key. This is almost trivially easy for a person with computer knowledge. The **only defense** is total round-the-clock **physical security** of the computer.

In the same vein, **"passwords"** are absolutely the *worst* form of **false** protection of data ever imagined. If they are *short* enough to be remembered, they are *simple* enough to guess (spouse's name, birth/anniversary date, social security/phone numbers, address, etc.). If they are *long enough to be effective,* they **are** written somewhere in the work area. (I once found **fifteen** passwords in **one** department, just by opening desk drawers!)

Hardware devices must be opened, drilled, or tampered to access the *"KEY(s)"* (and any stored messages). For an acceptable device, any of these actions **must** cause the *"KEY(s)"* of the device and any stored messages, to be both *erased* and *overwritten by random data*, foiling the attacker by *hardware "Self-Defense"*.

Software based encryption is dangerous in another aspect. Most of the algorithms are based either on "DES" or on some form of "Public Key". If "DES," poor implementation *will* cause the "short-cycle" problem mentioned earlier. If "public key" based, the strength of the algorithm must be known. Evaluation of ***EITHER*** method requires intimate knowledge of Cryptology, as well as access to the algorithm. If a vendor tells you that "the government" "prohibits" disclosure of the algorithm, **RUN!** This is the "snake-oil" of someone with something to hide.

Software encryption is **dangerous***, but usable,* given proper caution. As with any other security measure, it must be *properly* used.

5709 Kettering Court, Richardson, Texas, 75082 g 214-536-0325 g www.nregroup.net

THE "SECURITY" OF CELLULAR TELEPHONES

Many departments and agencies have become large users of Cellular "Telephones." It has been observed that some of these agencies and departments are using the Cellular telephone as a "private channel" for discussions they do not wish to hold on their radio channel.

Folks, the Cellular "telephone" **is** a radio channel! It **is** monitored by news personnel, the controversial "Cellular Privacy Act" notwithstanding. Near Waco, Texas, during the "Branch Dividian" problem, officials of the Texas Department of Public Safety suspected that the media was illegally monitoring their Cellular conversations. They contacted me for my recommendations.

I recommended that a specific preplanned conversation take place between two specific persons, covering fictitious information of a type likely to be of interest to the media, but to be spoken of **only** over Cellular, and **only** when not in the presence others. These steps were designed to detect **IF** the news media were monitoring Cellular conversations. **They were**. They were "spoofed" by the fictitious event, and even interrupted normal programming to show the buses that were supposed to come to carry away the Dividians - but never arrived. Needless to say, much less law enforcement information was transmitted by Cellular after this proof that the media was monitoring.

It is extremely easy to monitor Cellular and Trunked conversations, and to follow a conversation from cell to cell and channel to channel. It is possible with simple equipment. It is incredibly easy with moderately sophisticated equipment.

We have secured voice, data, and fax transmissions over fixed and mobile Cellular telephones with several different devices. The point, however, is this: If you choose **not** to secure your Cellular telephones, just **be aware** that your conversation **is** being heard by others. Don't say anything you would not say in a quiet restaurant. **IF** you need more security than that, talk to someone who totally understands *BOTH* Cellular *AND* Encryption *of the type of information YOU will be sending*.

FOLLOWING SECTION TO BE PERHAPS REVISED - A “Clipper like” proposal was “re-flown” by the FBI in January, 2003, and a similar one is in play again in 2013.

A CRUISE TO DANGER ON A "CLIPPER" CHIP

In early 1993, President Clinton quietly signed an Executive Order with profound impact on the lives of every American. This Executive Order establishes a new system of cryptography for all private citizens and organizations, including Law Enforcement. Under this system, a new chip, codenamed "Clipper" will be established as an encryption "standard" under NIST (Not NSA!).

The **"catch"**, and it is a **big** one, is that the device has **two** sets of crypto variables ("keys") -- one for you and one "for the government, in case a wiretap is authorized on your telephone." Hey! Sounds great! We can be assured of tapping any telephone we need to, and being able to listen to the conversation! Well,...not quite. Let's carefully examine the realities before deciding whether "Clipper" is a friend or a dangerous enemy.

First, consider the effects on the ***security*** of *your* information. The primary tenet of modern Cryptology states that the security of a system must reside in the "crypto variables" -- the **"keys"**. Stated another way, if your worst enemy possesses an *identical* device, has *full knowledge* of the internal operation of the device, but *lacks* your "keys", it should afford this enemy ***no advantage*** in attacking your messages.

5709 Kettering Court, Richardson, Texas, 75082 g 214-536-0325 g www.nregroup.net

"Clipper" violates this tenet in an extremely dangerous manner. "Clipper" requires each device to have TWO sets of "keys" -- one for your use, the other for use by "the government" in the event a wire tap is authorized on your line. These "keys" will reside in "Key Depositories", which will be administered by "agencies to be determined at a later date."

"Joe" is a $20,000.00 per year clerk with access to these keys. These keys have **no** National Security implications, as **no** "Classified" material will be allowed to be sent with these devices. Without the emotional penalty of "selling out my country", will "Joe" listen to what may seem to be a very generous offer to "copy" (of course not "steal") certain keys? Will a fake "under cover man" from "an Agency" be able to convince "Joe" to give him "John Jones'" keys and "help nail this guy" for implied but unspecified crimes?

The most chillingly dangerous threat of the "Clipper" key depository system is *the threat to the political process itself*. Will a sitting Administration of the "X" Party be able to resist the temptation to obtain the keys to the secret communications of the "Y" Party? And, **IF** it does, will the "Y" Party be as honest when it takes power? When some in power in *BOTH* major parties have been shown to define **"RIGHT"** to mean "helps someone who thinks like me", and **"WRONG"** to mean "helps someone who doesn't think like me", **IS IT LIKELY?**

SOME QUESTIONS

Q. What is the magnitude of the problem, in other words, how many times have *LEGAL* wiretaps encountered any form of encryption device?

A. Only approximately 280 times. How many actually *thwarted* the wiretap is not known. (This accurate number is from a confidential Washington source.)

Q. Will "Clipper" allow criminals and terrorists to be wiretapped?

A. NO! These individuals are capable, both financially and physically, of smuggling large quantities of drugs and weapons into this country. An encryption device is much smaller than either, and dogs won't "sniff out" a piece of electronic equipment -- *IF* that is what is used.

Q. Can encryption devices be bought by criminals and terrorists outside of the United States?

A. YES. Encryption devices are manufactured in at least four other countries, in addition to the United States. These countries exercise at least some measure of sale and export control, although not as stringently as the United States.

Q. Do these other countries require "keys"?

A. *NONE* of these "less free" countries require keys to encryption devices.

Q. Won't the availability of "keys" help Law Enforcement?

A. A drug or arms dealer who is SMART enough to know an encryption device is needed is probably not DUMB enough to purchase a device using a "Clipper" chip and then register keys with the Depository. If not, Law Enforcement is in exactly the same position as now.

5709 Kettering Court, Richardson, Texas, 75082 g 214-536-0325 g www.nregroup.net

Q. Is an electronic device the only "secure" form of encryption for the criminal or terrorist?

A. NO. A ***truly*** "unbreakable code" has been in existence since 1918, when the future U.S. Army Chief Signal Officer, (then) Maj. Joseph O. Mauborgne, invented it. The **"ONE TIME PAD"** may take (and has taken) the form of a pad of paper, a rolled cigarette paper, a teletype tape, or a computer chip. Each "sheet" is used *ONCE*, and *ONLY* once to encipher or decipher a single message, which must be shorter than the length of the "key." This makes the system both *theoretically and actually* unbreakable.

Q. Is the "One Time Pad" well suited for use by criminals and terrorists?

A. Ideally. Many of the smugglers use radio, with short messages (to thwart Direction Finding) in various forms of code.

Q. What controls *NOW* exist to prevent the criminal or terrorist from exporting an encryption device to an "associate", or from importing one?

A. The import or export of an encryption device requires a *United States Department of State Munitions Control License*. Even a device owned by an individual or company and transported by that individual or company to another country for use by that individual or company must have a *Specific* State Department Export License Issued for **that specific country** and **specific end user** *before* it Can Be Exported. It must be taken to U.S. Customs at the time of export, along with the license. When it re-enters the United States, it must be declared to U.S. Customs, and the license must again accompany it. Failure to adhere to **any** of these provisions may result in confiscation of the device, a fine of $25.000.00, and up to 10 years in Federal prison!

Q. What additional penalties does the Executive Order impose?

A. *NONE*.

Q. What are the dangers to Law Enforcement?

A. Criminals and terrorists have large amounts of money at their disposal. If one of these outstanding citizens "obtains" a copy of **your** "keys", all of your operations are compromised. You have **no** way of controlling access to **your** "keys", and **no** way of knowing of a security breach until several operations are "blown", if then! The ultimate cost may be measured in lives.

Q. If the law is so bad, how did it pass Congress?

A. IT DIDN'T! An Executive Order is a "Proclamation" by the President, not a bill which has survived the legislative process.

5709 Kettering Court, Richardson, Texas, 75082 g 214-536-0325 g www.nregroup.net

THE ULTIMATE QUESTION

Even **IF** some benefit to Law Enforcement could be proven, would the loss of the Constitutional right of privacy and the serious risks to the *precious and delicate balance* of the American political process be justified? Possession of the keys to any person's or organization's secret communications device is possession of **absolute power** over that person or organization. According to the wisdom of one Mr. Benjamin Franklin, "***All Power corrupts. Absolute power corrupts absolutely!***"

The "necessity" of security against terrorism, drugs, and arms dealers is cited as the reason behind the Executive Order. The words of William Pitt, the Younger, in the House of Commons on 18 Nov, 1783 are somewhat chilling, regardless of your politics: "***Necessity is the plea for every infringement of human freedom. It is the argument of tyrants; it is the creed of slaves.***"

SUMMARY

Communications Security, as with all security efforts, encompasses threat evaluation and selection of a means to counter the threat. In Communications Security, however, proper evaluation of both threats and "counters" requires a high level of technical and operational knowledge in telephone systems, radio systems, and Cryptology.

The Public Safety sector has been very slow to embrace Communications Security. Many feel that the "threat" is minimal. In some towns, this may be true. In cities, and in towns in the path of drug and arms smuggling, the threat is only too real. If you cannot positively state that a lack of Communications Security has **never** endangered an officer or agent, your department or agency needs **effective** Communications Security.

ABOUT THE AUTHOR

Larry Randall was the Senior Field Engineer and was jointly responsible for Product Concept and Development at a respected manufacturer of Communications Security devices for a number of years. He founded The NRE™ Group in 1988. He has traveled to 39 countries to solve Tactical and Strategic Communications Security problems in military, government, and civilian communications systems; has managed international projects, and has designed and built unique systems for government agencies and companies. Mr. Randall has successfully designed and implemented encrypted communications networks using HF, VHF, UHF, and trunked radio; landline and Cellular telephone systems; microwave systems; and satellite systems.

NOTE TO READER: *This article is basically in the format that was required by Public Safety Communications Magazine, whose editor (at that time) mandated extreme emphasis on "key" points and words requiring definition. (It was published as a two-part series by that magazine.) I have removed some of the "shouting" (overuse of bolding, all caps, and italics), but not all of it, as I have not had time to fully edit it and/or rewrite it for a more nearly "generic" audience. Please also note that this article was written in 1994 – and that it both reflects the technologies of that time and accurately predicts several future changes.*

5709 Kettering Court, Richardson, Texas, 75082 g 214-536-0325 g www.nregroup.net