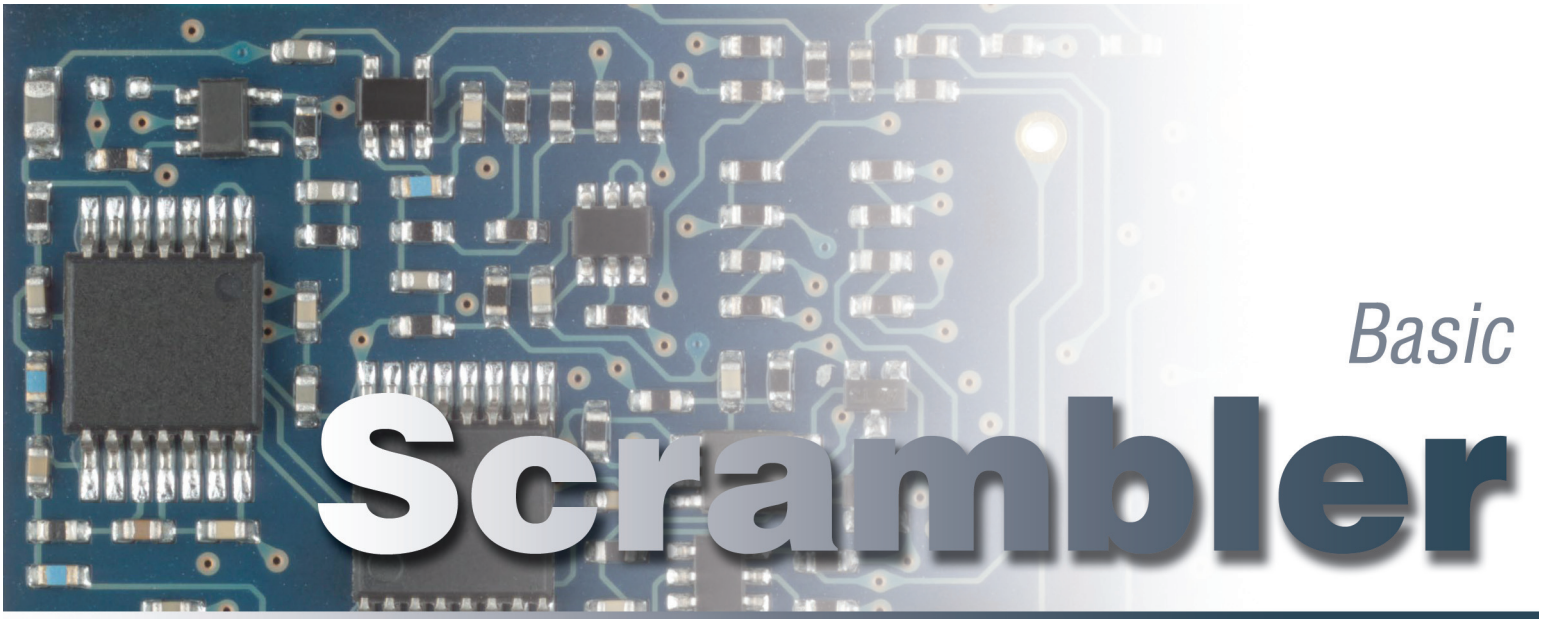

Basic Scrambler Information

By Jeanen France
Account Manager, North America
Transcrypt International

GETTING STARTED

Questions we will ask:

- What type of radio system — conventional, voted, simulcast, etc. — do you want to secure?
- What type of information will you be transmitting, and how determined will the eavesdroppers be to break the code?
- What types of radios are being used in your system?
- Are there already scramblers in the radio system that you need to communicate with?
- If ANI or emergency — such as MDC or G-Star signaling — is being used in the radios, is it pre- or post-ANI signaling?

Levels of LMR Radio Security

400 Series: Basic fixed inversion scrambler, factory programmable to any inversion frequency. The SC20-400-12 is our generic module and can be factory modified for just about any radio. We do have some radio-specific modules available for some of the Motorola portables and mobiles. This scrambler is the easiest to use and has the best recovered audio quality; however, it is a low level security scrambler. It would be conceivable for someone to break the code of this scrambler if they were very determined to do so.

Transcrypt has three levels of hopping code scramblers. The difference between the three levels is how rapidly the inversion frequency changes – the faster it changes, the higher the level of security. In order to communicate, the scramble code and master code of these scramblers has to match. These codes are factory programmed and can be changed in the field using our modem (TR30-3060) and dumb terminal (hyper-terminal) using Over-the-Air-Reprogramming (OTAR).

With hopping code scramblers, an initial data burst is transmitted to synchronize all the scramblers. The hopping code scramblers have automatic decode (the receiving radio will automatically decode the incoming secure transmission even if the scrambler is not turned on). These scramblers have ANI (Automatic Number Identification) and emergency functions available using Transcrypt's proprietary FlashCall™ format.

410 Series: CVP™ I - Level one hopping code; inversion frequency changes about one time per second.

416 Series: CVP I - Level one hopping code; the difference between this scrambler and the 410 is that the 416 series can be upgraded to a higher level of security.

430 Series: CVP II - Level two hybrid sweep / hopping code; inversion frequency changes on an average of 250 times per second.

460 Series: CVP III - Level three hybrid sweep / hopping code; inversion frequency changes an average of 650 times per second.

DES Series: DES — our highest level of security — is a continuous synchronization scrambler (rapid re-entry). The audio is secured to the Data Encryption Standard, although our final output is analog. With the purchase of the DES scrambler, the TR30-3060 modem and TR99-DES software is also required. This allows OTAR re-keying if desired; the modem / software also allows OTAR to optimize the scrambler's operation through a radio system. Either on-site or factory training is highly recommended when considering DES.

TRANSCRYPT INTERNATIONAL

Notes

For all radios with scramblers installed, there will be a means to turn the scrambler on / off using either an existing switch on the radio or adding an external toggle switch. It is recommended to not use the scrambler 100 percent of the time. Activate the scrambler as needed when the information transmitted needs to be kept confidential.

FREQUENTLY ASKED QUESTIONS

What is analog scrambling?

There are several methods of analog scrambling; Transcrypt modules modify speech using analog techniques in the frequency domain. With this method, frequencies in the original speech are converted into alternative frequencies. Transcrypt achieves this conversion by introducing a "mixing frequency" into the original voice before the signal is modulated. This process "inverts" the original voice spectrum around this mixing frequency. The receiver uses the same mixing frequency to invert this spectrum back to its original position. By itself, this complex process provides some level of security, but when the mixing frequency is allowed to change quickly with time in an unpredictable pattern, the original signal becomes extremely difficult to reconstruct without the corresponding descrambler. By utilizing sophisticated audio synchronization techniques, Transcrypt's proprietary Crypto-Voice-Plus™ (CVP) scrambling modules incorporate this method of shifting frequencies to provide several levels of voice privacy.

What's the difference between analog scrambling and digital encryption?

A digital encryption device converts the original voice waveform into a long sequence of 1s and 0s – a process called voice coding – and then uses a known algorithm to "encrypt" those 1s and 0s. This digital ciphertext is then modulated and transmitted. The receiving device demodulates, decrypts and converts this signal back into a plain text voice signal.

There are advantages to both digital and analog scrambling. For example, analog scrambling can provide a more natural sounding voice and simple key management. Digital encryption can use a highly complex cipher, and can employ sophisticated techniques to reduce noise in weak signal areas.

Is scrambling hard to use?

Not at all. The method for turning the scrambler on and off when transmitting varies by radio, but is usually no harder than flipping a switch or pressing a button. Receiving coded transmissions is even easier. Transcrypt scramblers monitor the incoming signal and automatically enter the coded mode when a synchronization signal is received. This means that someone who usually only monitors their radio doesn't have to continually switch the radio back and forth between clear and coded modes to understand incoming transmissions.

Will a scrambling module fit in my radio?

Transcrypt performs thousands of installations every year. Every time a module is installed into a radio, a set of instructions – known as an application note – is developed. Over 2,700 application notes exist today. This document supplements the generic module installation manual and provides explicit details for installing a given scrambler into a specific radio. As full-featured radios get smaller, customized miniaturized scramblers are required. Transcrypt is committed to continued advances in miniaturization and customization to meet this technological challenge. Therefore, custom scrambling modules have been developed for many of the most popular radios.

How hard is it to install a scrambling module?

As all radios are different, so is the effort required to install scrambling. The great majority of scramblers can be installed easily by an experienced professional radio or electronics technician. Very few installations are considered "factory only." If you tell us the model of radio in which the scrambler will be installed, we'll send additional instructions for installation into that radio. If we haven't scrambled your particular model of radio, you may want to send in a sample radio, along with the radio service manual, for our service technicians to evaluate the radio for scrambler installation. If possible, for a small fee we will perform the installation for you and generate the necessary application notes for future installs. We maintain a full-time staff of technicians whose responsibilities include installing scramblers in customers' radios.

What is Over-the-Air-Reprogramming and what can it do for me?

Over-the-Air-Reprogramming (OTAR) is a feature that allows you to change the operating parameters of a scrambler without removing if from the radio. This capability provides significant logistic and cost savings to the user and differentiates the less sophisticated competitive products. Using a PC, our special TR30-3060 modem controller, and a normal radio (without a scrambler installed), you can use OTAR to change scrambling codes in a single radio, or a whole fleet of radios, one radio at a time using the ESN (electronic serial number) of the scrambler. If a radio comes up missing, you can go looking for it from your operations console, and if it is turned on, remove its scramble codes or disable the radio from sending or receiving any transmissions. OTAR brings new levels of flexibility and control to the management of your system.

What types of radio systems can scrambling be used in?

Transcrypt has scrambling solutions for both conventional and nonconventional systems. Transcrypt has installed scramblers in over 10,000 systems in over 120 countries around the world. The complexity of these applications ranges from simple "talk around" unit-to-unit operation up to complex dispatch system installations such as repeated, voted, trunked, and wide area. The type of scrambler used is very much a function of the application. Transcrypt scrambling is also fully compatible with systems using CTCSS / DCS, DPL and other signaling formats in conjunction with Transcrypt's T-CAD software.