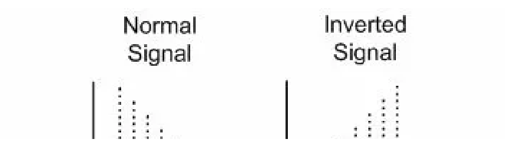
Two Way Radio Encryption Basics

How Does Radio Encryption Work?

Encryption is the process of encoding information (in this case audio signals) in such a way that eavesdroppers or hackers cannot understand it, but authorized parties can access it. In two-way radios, encryption modifies a voice signal using a coding algorithm. This algorithm is controlled by an encryption key. The encryption key is used by the transmit and receive radios to enable the voice signal to be coded and decoded for both radios. Therefore, all radios communicating must have matching encryption keys to receive transmissions.

There are several different methods for encrypting voice signals.

Fig. 1 - Simple Voice Inversion Encryption



Simple Inversion Encryption

Inversion scrambling inverts the frequencies and volume of the voice signal. In figure 1 on the left, all the voice signal frequencies at 300Hz are inverted to 3kHz. The volume level is also inverted. Most two-way radios with simple voice inversion have 32 different encryption keys to choose from. The keys are set in the radio through radio programming software. Only radios using the same frequency, with the same privacy code, the same encryption key, and within range of your signal, will be able to hear your transmissions. This type of encryption provides enough protection for most two-way radio users. Many entry-level and mid-tier radios have this type of encryption built-in.

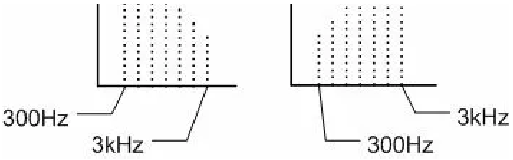


Fig. 2 - Frequency Hopping Encryption

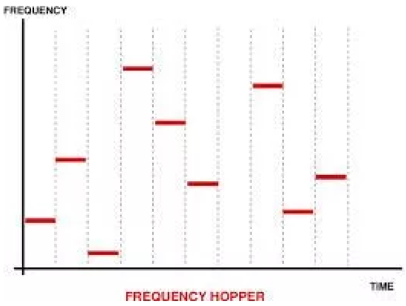
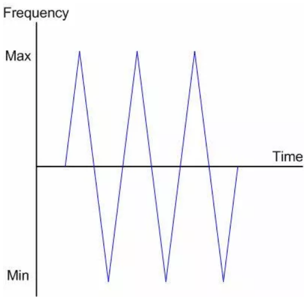


Fig. 3 - Rolling Code Encryption



Hopping Inversion Encryption

Frequency hopping encryption adds a greater degree of security than simple inversion. Using this method the frequencies and frequency rates change irregularly as seen in figure 2. This cause the voice signal to "hop" over a number of different frequencies and frequency rates. Some radios in the commercial market have used this technology in the 900MHz range, although most do not.

Rolling Code Inversion Encryption

Rolling code inversion uses a method where the voice signal is inverted at a constantly changing rate. As shown in figure 3 on the left, the signal starts at an upward inversion frequency direction and climbs to the upper limit.

Then, it reverses direction and inverts at lower frequencies until it reaches the lower limit. It is a more robust form of encryption than simple voice inversion. Most radios with *rolling code encryption* have 1020 encryption keys to choose from. The keys are set in the radio by programming software. As with simple inversion, only radios using the same frequency, with the same privacy code, the same encryption key, and within range of your signal, will be able to hear your transmissions. The difference with rolling code vs simple inversion is the number of codes (1020 for rolling) and the "rolling" inversion of the signal that make it more difficult to break. Rolling code is used for more sensitive applications. Some mid-tier radios and most advanced radios have rolling code encryption as an optional feature.

DES and AES Encryption

The most sensitive applications (such as FBI, military, some financial applications, etc.) use either AES (Advanced Encryption Standard), or it's former cousin DES (Data Encryption Standard). DES was developed in the 1970s but has been replaced by it's newer cousin AES in many applications. These encryption algorithms are quite advanced and take some understanding of encryption methods and mathematics to fully explain. They are the "gold standard" when it comes to encryption. However, just like real gold, there is a higher cost and complexity associated with implementing them.

How Encryption Keys Are Set in AES and DES Encryption

Since AES and DES are used for highly sensitive applications setting their encryption keys is also highly sensitive. Setting the codes requires a special device known as a "Keyloader", also called a KVL (Key Variable Loader). This device (looks similar to a radio) allows the operator to insert the keys into the encryption boards within the individual radios. The KVL attaches to the radio with a special cable and attaches to the interface port of the radio. The operator enters individual numbers and letters (depending on the protocol) into the KVL to produce a unique code to your radio traffic. The KVL transcribes your code of approximately 20 characters into the final key that is then loaded into each radio. Since access to the KVL constitutes access to the entire system, these devices are not available to the general public and are closely guarded at radio shops, or government agencies, where they reside.

Managing Encryption Keys in a Complex Environment

So, how do you manage to change encryption keys when you have large operations? OTAR (Over-The-Air-Rekeying) is the answer. In OTAR you have a dedicated computer, called a Key Management Controller (KMC), which centrally manages the encryption keys. OTAR allows radios to have new encryption keys loaded into them over the air, as the name suggests. Encryption keys can also be erased over the air. When a radio is lost or stolen all radios in the system, except the one that is lost, can be re-keyed over the air. Also, if you accidentally remove your radio battery, thus erasing the encryption key, the KMC can download the encryption key back into your radio over the air. The KMC can also download the encryption keys into KVLs, so that encryption keys can be transported. Should the radios be out of the range of the KMC, the KVL device can be used in its place.

Most radios can only hold one encryption key at a time. But some radios also have the ability to store multiple encryption keys (multi-key). If you have two separate groups using different encryption keys, multi-key allows designated users to have both encryption keys in their radios to communicate with both groups, while the rest of the group cannot monitor each other's conversations. Some multi-key radios can have up to 16 different encryption keys stored in them.

OTAR and multi-key are usually only available on more advanced radio models.

Compatibility of Encryption Between Different Brands

The question of compatibility between different radio brands and their encryption often comes up. The simple answer is, only AES and DES are standardized encryption methods. This means AES and DES are compatible between different two-way radio brands. However, there is no set of agreed-upon standards for simple inversion or rolling code inversion encryption. Each manufacturer can set their own codes and scrambling techniques for simple and rolling code inversion. So, simple inversion and rolling code inversion encryption are generally not compatible across brands.

MOST VIEWED

MOST VIEWED

Icom F3001 | F4001 Two-...
$138.95
★★★★★
(https://quality2wayradios.com/st ic-f3001-vhf-ic-f4001-uhf)

Icom F1000 | F2000 Two-...
$179.95
★★★★★
(https://quality2wayradios.com f1000-f2000)

About Us

Our Company

Privacy Policy

Terms of Use

Purchase Orders

Payment & Shipping

Customer Service

Contact Us

Cancellations & Returns

Site Map

My Account

My Account

Order History

Why Buy From Us?

- Authorized Dealer
- Unbeatable Prices
- 1,000s of Products / Many brands
- 30-Day Return Policy
- Fast Shipping
- Excellent Service (BBB A+ Rating)
- Secure Online Purchasing
- Knowledgeable Support
- FCC Licensing Services

VISA mastercard AMERICAN EXPRESS DISCOVER PayPal P