# P25 ENCRYPTION AND INTEROPERABILITY

## Introduction

Encryption in a P25 radio is an option feature to enable secure voice and data communication. A group of radios may be assigned a unique encryption key to allow users to communicate securely. Users of these radios can then send a message which is digitized and encrypted (locked) and can only be decrypted (unlocked) and received by those radio users with the same unique key.

Most P25 radio equipment is optionally available with the capability of storing and using multiple keys. That is, a unit could use one key for one group of users and use a separate key for another group of users.

The encryption keys also have the option of being re-keyed by digital data over the RF links. This is referred to as Over The Air Re-keying (OTAR). This capability allows the radio systems manager to change encryption keys without having the subscribers physically bring the radios back to a service shop.

The P25 vocoder produces a digital bit stream that is relatively easy to encrypt. Major advantages of the P25 encryption design are that encryption does not affect speech intelligibility nor does it affect the system's usable range. Both of these advantages are important improvements over encryption previously used in analog systems.

## Encryption Types

In the U.S. there are four general "types" of encryption algorithms:

Type 1 is for U.S classified material (national security)
Type 2 is for general U.S federal interagency security
Type 3 is interoperable interagency security between U.S. Federal, State and Local agencies
Type 4 is for proprietary solutions.

The P25 Common Air Interface (CAI) supports use of any of the four types of encryption algorithms. P25 documents currently standardize on two different Type 3 encryption processes. One encryption process is the U.S. Data Encryption Standard, or DES algorithm and the other encryption process is Advanced Encryption Standard (AES).

## Encryption Algorithms

AES Encryption

Advanced Encryption Standard (AES) is an encryption standard adopted by the U.S. government. The standard was announced by National Institute of Standards and Technology (NIST) laboratory as compliant with the security requirements of the Federal Information Processing Standard (FIPS) on November 26, 2001. It became effective as a Federal government standard on May 26, 2002 after approval by the Secretary of Commerce.

Algorithm Type: Type 3 is interoperable interagency security between U.S. Federal, State and Local agencies
Algorithm: AES
Key Length: 256 bit
Key Loading Method: KVL Programmer - A Motorola KVL is an expensive piece of equipment that is not readily available
Remarks:
FIPS 140-2 Certificate

Supported by OTAR (Over-The-Air-Rekeying)

DES Encryption

The Data Encryption Standard (DES) is an encryption that was selected by the National Bureau of Standards as an official Federal Information Processing Standard (FIPS) for the United States in 1976 and which has subsequently enjoyed widespread use internationally.

DES is now considered to be insecure for many applications. In recent years, the cipher has been superseded by the Advanced Encryption Standard (AES). Furthermore, DES has been withdrawn as a standard by the National Institute of Standards and Technology (formerly the National Bureau of Standards).

Algorithm Type: Type 3 is interoperable interagency security between U.S. Federal, State and Local agencies
Algorithm: DES
Key Length: 56 bit
Key Loading Method: KVL Programmer - A Motorola KVL is an expensive piece of equipment that is not readily available
Remarks:
No longer has a FIPS certificate
Supported by OTAR (Over-The-Air-Rekeying)

ADP Encryption

ADP is a Motorola patented and proprietary encryption standard. It is not a published federally certified encryption that any manufacturer could use. Therefore, it cannot be used to communicate securely with other brand of radios except Motorola. It is designed as a cheap implementation of encryption to prevent casual eves dropping. ADP software encryption isn't as secure as DES or AES.

ADP is loaded by the customer programming software so if a radio is stolen and the thief has the customer programming software they can read the system key. ADP is not supported by the P25 OTAR (Over-The-Air-Rekeying) so if the key does get out, there's no easy way to "fix" everything. All the radios must be returned to the shop to be rekeyed.

Algorithm Type: Type 4 is for proprietary solutions
Algorithm: RC4
Key Length: 40 bit
Key Loading Method: CPS (Customer Programming Software)
Remarks:
No FIPS certificate
Not supported by OTAR (Over-The-Air-Rekeying)

## Encryption Algorithms Supported by 700/800 MHz P25 Trunking Radio Manufacturers

| | Encryption algorithms supported by 700 MHz P25 trunking radio manufacturers | | | | | |
|---|---|---|---|---|---|---|
| Encryption Algorithms | **Motorola** | **EF Johnson** | **Harris** | **Tait** | **Kenwood** | **Thales** |
| AES (Federal government encryption standard) | *AES* | *AES* | *AES* | *AES* | *AES* | *AES* |
| DES (Former federal government encryption standard replaced by AES) | *DES* | *DES* | *DES* | *DES* | *DES* | *DES* |
| ADP (Motorola proprietary encryption) | *ADP* | | | | | |

## APCO Project 25 (P25) Standard Requires AES Encryption for Interoperability Purposes

"For interoperability purposes, all Project 25 equipment implementing Type 3 encryption shall utilize the Advanced Encryption S algorithm. Key length for the AES shall be 256 bits."

*APCO PROJECT 25, STATEMENT OF REQUIREMENTS, (P25 SoR), March 3, 2010, Section 4.1.1.1*

## AES Encryption Must be Used by the Federal Government

"5.1 Encryption Services - Several encryption algorithms are available for use with P25 systems. The oldest algorithm, for which there are P25 standards documents, is Data Encryption Standard (DES). This particular algorithm is no longer endorsed (after May 2005) by the Federal Government for secure communications. The most recently endorsed algorithm is Advanced Encryption Standard (AES) and must be used by all Federal agency communications systems beyond May 2007. The recommendation has been that State and local agencies also transition to AES to ensure interoperability."

*Project 25 Documents & Standards Reference, Public Safety Communications Research, U.S. Department of Commerce*
http://www.pscr.gov/outreach/p25dsr/menu_top/downloads/p25dsr.pdf

## National Emergency Communication Plan Recommends AES for State, Local, and Tribal Emergency Responders

"Initiative 4.4: Implement the Advanced Encryption Standard (AES) for Federal responders. A standard nationwide encryption method will diminish the interoperability challenges faced by Federal responders (who previously used different methods) and will provide guidance to local and State agencies when working with Federal agencies. "

*Recommended National Milestones:*
- Within 18 months, achieve encrypted interoperability between Federal departments and agencies using the AES.
- Within 18 months, publish a uniform standard for the AES for State, local, and tribal emergency responders who decide to use encryption.
- Within 24 months, Federal grant policies are modified to accommodate an AES-encrypted feature for radio equipment used by State, local, and tribal emergency responders.

*National Emergency Communications Plan – Homeland Security*
http://www.dhs.gov/xlibrary/assets/national_emergency_communications_plan.pdf

## FCC Amends Rules to replace DES Encryption with AES Encryption on the 700 MHz Interoperability Channels

"4. Encryption Standard – 56 - In the *Fourth R&O,* the Commission decided that encryption should be permitted on the 700 MHz interoperability channels and adopted the TIA/EIA IS 102 AAAAA Project 25 DES encryption standard as recommended by the Public Safety National Coordination Committee (NCC). The NCC states that this standard has been superceded by the Advanced Encryption Standard (AES) because the DES standard had been compromised and is no longer suitable for encrypting sensitive public safety information. The NCC recommends that the Commission amend the rules to reflect this new document: Project 25 Block Encryption Protocol, approved June 13, 2002, Telecommunications Industry Association, ANSI/TIA/EIA-102-AAAD-2002, Annex C-Advanced

Encryption Standard. We agree with the NCC that our rules should reflect the latest standard, therefore, we tentatively conclude to amend the Commission's rules to incorporate by reference the revised document."

FIFTH MEMORANDUM OPINION AND ORDER, SIXTH REPORT AND ORDER, AND SEVENTH NOTICE OF PROPOSED RULEMAKING
http://tsiec.region49.org/FCC-05-9A1.pdf

## Conclusion

For encrypted interoperability, AES encryption is the only encryption that meets the P25 type 3 encryption standards for interoperability communications. When selecting an encryption standard, always choose AES encryption for interoperability.

---

Compiled by Scott Grimmett, Consulting Engineer, Industrial Communications, Spokane Valley, WA 99037, 800-537-7047, contactus@twoway.net.