# Hytera DMR Conventional Series

## Encryption
## Application Notes

# Hytera DMR Conventional Series

# Encryption

## Application Notes

**Version 1.0**

*Date: January 28, 2011*
*Web: http://www.hytera.com*

# Revision History

| Version | Date | Description | Remarks |
|---|---|---|---|
| R1.0 | 01-28-2011 | Initial release | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

# Contents

# 1. Overview

## 1.1 Definition

This function provides end-to-end encryption for communication services (including voice and data) on digital channels, allowing the target terminal to receive the voice and data privately.

## 1.2 Principle

We provide two encryption mechanisms: Basic Encrypt and Full Encrypt, which employ a key accessible to the involved call parties only. These two mechanisms, based on Hytera exclusive technology and algorithm, can not work with the encryption function of other manufacturers.

### 1.2.1 Basic Encrypt

The Basic Encrypt function can protect your voice or data against unintentional eavesdropping. This mechanism has features below:

1) You can configure the key type (40 bits, 128 bits and 256 bits) and key value freely.

2) It transforms the voice or data using a simple mathematical algorithm.

Information encrypted with this mechanism can be decrypted easily by attackers who capture over-the-air voice or data packet. Since no encryption parameter is required to be sent, the system access time for encrypted and unencrypted voice is the same. See Figure 1.2.1-1 for the basic encryption flow.

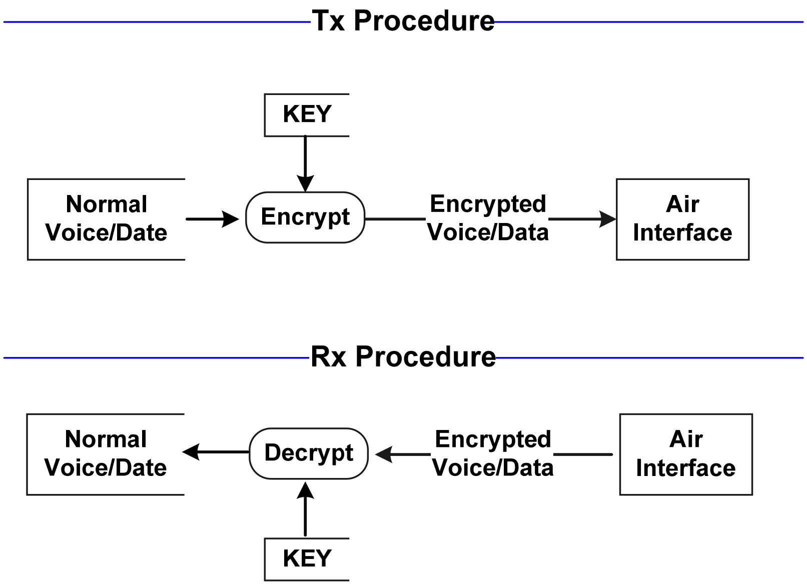


**Figure 1.2.1-1 Basic Encryption Work Flow**

**** The key plays an important role in encryption. It is recommended to configure a unique key, which has at least five different bits from other keys after converted into binary value; otherwise a warning will pop up.***

## 1.2.2 Full Encrypt

**The Full Encrypt function can provide enhanced protection for your communication privacy by using a secure algorithm. This mechanism has features below:**

**1) You can configure the key type (40 bits, 128 bits and 256 bits) and key value freely.**

**2) The 40-bit key adopts ARC4 to generate a key stream to convert the voice or data, while the 128-bit or 256-bit key uses AES to convert the voice or data. Such keys provide different key streams for each voice superframe or data packet, making it impossible for the attackers to decrypt by capturing over-the-air voice or data packet.**

**In this mechanism, an extra header is required for sending the encryption parameters, and it prolongs the system access time by approximately 60ms. Additionally, the system late entry time may also be prolonged due to**

encryption-related information embedded in the voice superframe. See Figure 1.2.2-1 for the Full encryption flow.

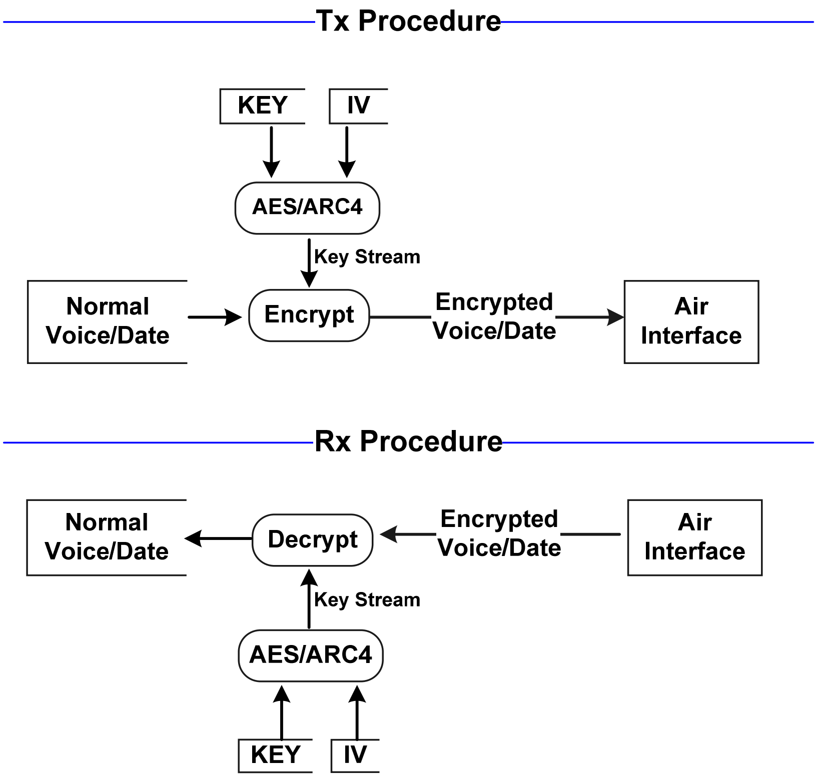


Figure 1.2.2-1 Full Encryption Work Flow

## 1.3 Version

1) DMR conventional series software R2.0: Basic Encrypt available;

2) DMR conventional series software R2.5: Basic Encrypt available;

3) DMR conventional series software R3.0: Basic Encrypt and Full Encrypt available (you can view key list and create new key in the menu).

## 1.4 Scope

These two mechanisms encrypt voice and data only, rather than other information involved in supplementary services (Radio enable/Radio disable, Remote monitor, Radio check and Alert call, etc).

# 2. Encryption and Communication

## 2.1 Application of Encryption

**The terminal that receives the encrypted voice or data, no matter whether the encryption function is enabled, always tries to decrypt the voice or data with the key and encryption type defined for the current channel. Decryption will be achieved if the key and encryption type match; however, if the voice or data is not encrypted, it will be output without decryption.**

**Decryption may fail in situations below:**

**1) Both parties adopt Basic Encrypt mechanism but different keys are employed. In this case, the data can not be transmitted and indistinct voice will be heard at the receiving party.**

**2) Both parties adopt Full Encrypt mechanism but different key IDs are employed. In this case, the data can not be transmitted and no voice will be heard at the receiving party.**

**3) Both parties adopt Full Encrypt mechanism and the same key ID, but different key values are employed (see Figure 4.1.1-1). In this case, the data can not be transmitted and indistinct voice will be heard at the receiving party.**

**4) Both parties adopt different encryption mechanisms. In this case, the data can not be transmitted and no voice will be heard at the receiving party.**

## 2.2 Transfer of Encrypted Data

**At present, there are three modes available for transferring encrypted data.**

**1) DM (Direct Mode)**

**Under this mode, the terminals communicate with each other directly over the air.**

**2) RM (Repeater Mode)**

Under this mode, the encrypted data is transferred to the receiving terminal via a repeater.

3) IP Multi-site Connect Mode

Under this mode, the encrypted data can be transferred via a repeater, an IP network or over the air. Note that only end-to-end data encryption/decryption is supported.

Under the IP Multi-site Connect mode, the repeater and IP network are dedicated to data transfer only. See Figure 2.2-1.

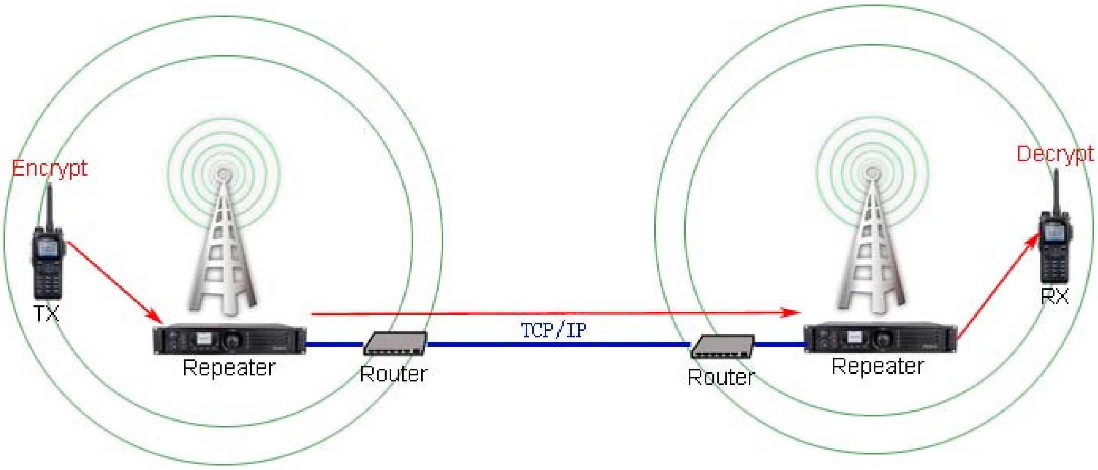


Figure 2.2-1 Encrypted Data Transfer under IP Multi-site Connect Mode

# 3. Equipment Requirements

**At present, the encryption function is realized through software, requiring no extra hardware.**

# 4. Configuration Guide

## 4.1 Terminal Configuration

**The encryption function can be enabled/disabled through the CPS (Customer Programming Software), menu or programmed key, but the encryption type can only be set via the CPS. If the terminal does not support such menu or programmed key, the encryption function on the current channel cannot be changed.**

### 4.1.1 Software Configuration

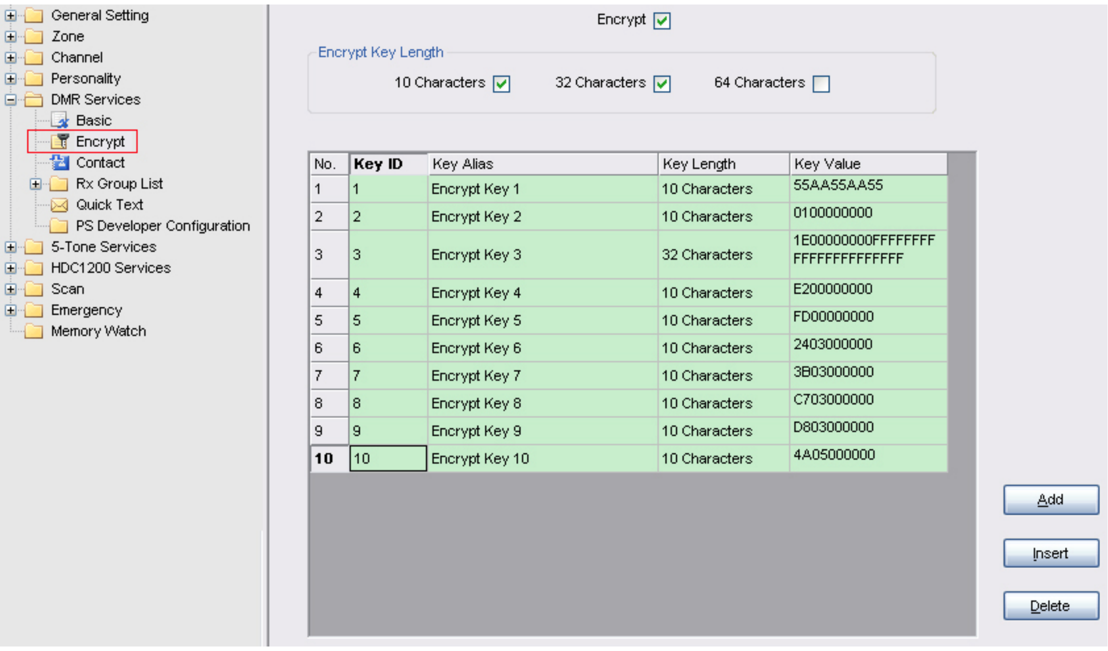
**Three steps are needed to configure the encryption function via CPS: Set the common encryption parameters, Set the digital channel and Set the programmed key and menu.**

**Step 1: Set the common encryption parameters**

**Run the CPS, and go to “DMR Services -> Encrypt”. See Figure 4.1.1-1.**

**1) Set Key Length: 10 characters (40 bits), 32 characters (128 bits) and 64 characters (256 bits)**

**2) Add a Key: one terminal can support 30 keys in all.**



Encrypt ☑

Encrypt Key Length

10 Characters ☑ 32 Characters ☑ 64 Characters □

| No. | Key ID | Key Alias | Key Length | Key Value |
|---|---|---|---|---|
| 1 | 1 | Encrypt Key 1 | 10 Characters | 55AA55AA55 |
| 2 | 2 | Encrypt Key 2 | 10 Characters | 0100000000 |
| 3 | 3 | Encrypt Key 3 | 32 Characters | 1E00000000FFFFFFFF<br>FFFFFFFFFFFFFF |
| 4 | 4 | Encrypt Key 4 | 10 Characters | E200000000 |
| 5 | 5 | Encrypt Key 5 | 10 Characters | FD00000000 |
| 6 | 6 | Encrypt Key 6 | 10 Characters | 2403000000 |
| 7 | 7 | Encrypt Key 7 | 10 Characters | 3B03000000 |
| 8 | 8 | Encrypt Key 8 | 10 Characters | C703000000 |
| 9 | 9 | Encrypt Key 9 | 10 Characters | D803000000 |
| 10 | 10 | Encrypt Key 10 | 10 Characters | 4A05000000 |

**Figure 4.1.1-1 Common Encryption Parameters**

Keys that are defined through CPS can not be read, edited or deleted through terminal operation. Once a key is employed for a terminal, it can only be overwritten by a new one. And it can not be programmed via the remote control or air interface.

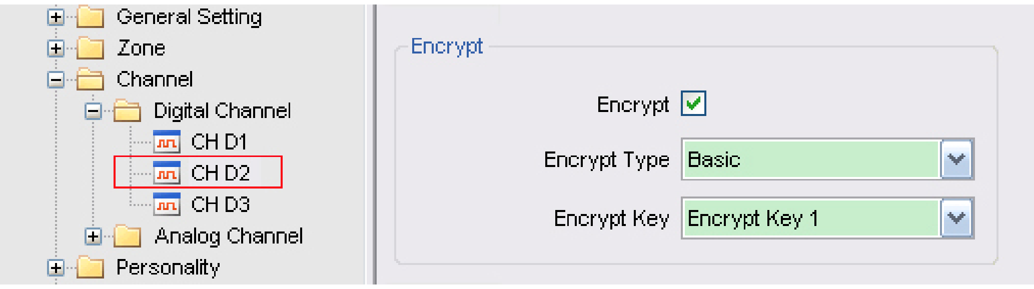
Step 2: Set the digital channel

Go to “Channel -> Digital Channel -> Encrypt”. See Figure 4.1.1-2.

1) Encrypt option: check it to enable encryption function; vice versa (for transmitting party only).

2) Encrypt Type: select a encryption type between Basic Encrypt and Full Encrypt.

3) Encrypt Key: assign a key for the current channel.



Encrypt

Encrypt ☑

Encrypt Type: Basic

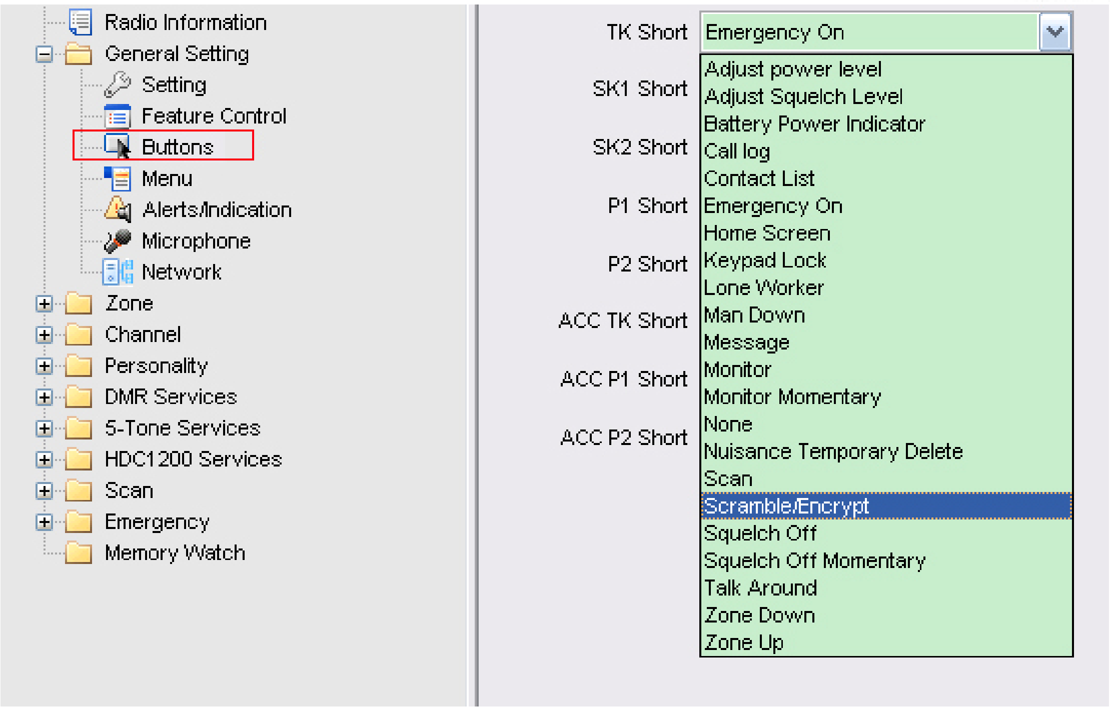
Encrypt Key: Encrypt Key 1

Figure 4.1.1-2 Encryption Parameter Settings

** These settings are set for a certain channel only. If they can also be edited through the menu or programmed key of a terminal, the modification will be applied to the current channel only. Even if the channel or zone is changed, these settings will be reserved. Please note that modification to a specific channel will not apply to other channels.*

Step 3: Set the programmed key and menu

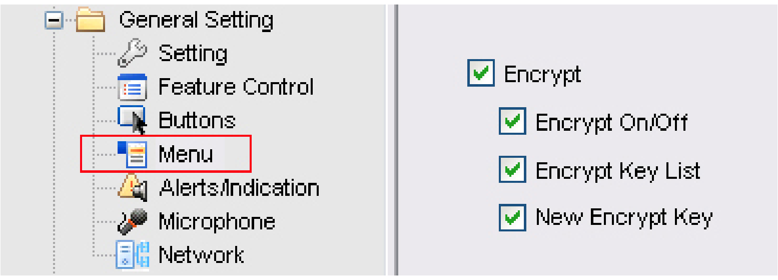
1) Go to “General Setting -> Buttons”, and assign a certain key with Scramble/Encrypt function. See Figure 4.1.1-3. After the encryption function is configured to a key, you can enable or disable it via the key directly.



TK Short: Emergency On

Figure 4.1.1-3 Button Programming

**2) Go to "General Setting -> Menu -> Encrypt", and check the parameters shown below. See Figure 4.1.1-4. And then you can edit these parameters via the menu directly.**



☑ Encrypt

☑ Encrypt On/Off

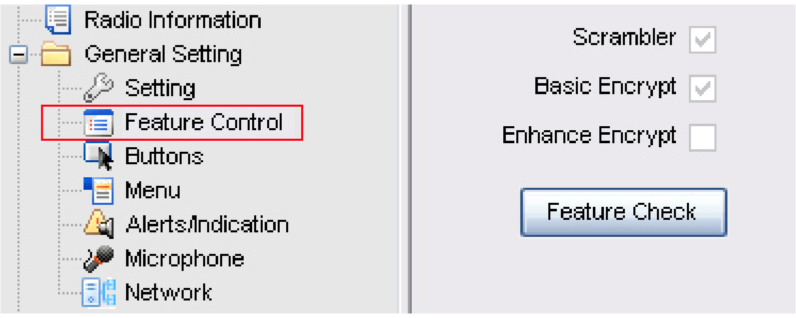
☑ Encrypt Key List

☑ New Encrypt Key

Figure 4.1.1-4 Menu Configuration

**** For security reason, the key information of a terminal can not be written into another terminal directly. However, there is a shortcut to apply a key to a number of desired terminals. First, program one terminal via CPS, and save the settings as the template for other terminals; then program other terminals according to this template.***

**** The Full Encrypt function is available for users authorized by Hytera only. To enable it, click the Feature Check button. See Figure 4.1.1-5.***



Scrambler ☑

Basic Encrypt ☑

Enhance Encrypt □

**Figure 4.1.1-5 Full Encrypt Access**

## 4.1.2 Terminal Menu Configuration

**If a key has been programmed for the current channel via CPS, you can**

**1) use the programmed key to enable or disable the encryption function;**

**2) use the menu to:**

**2.1) enable or disable the encryption function on the current channel;**

**2.2) change the key of the current channel;**

**2.3) add keys for the terminal. See Figure 4.1.2-1.**

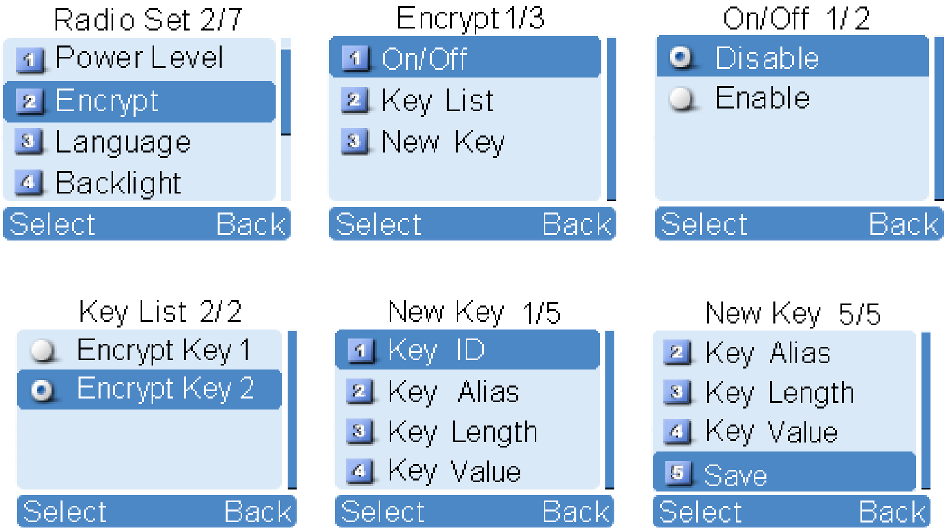


**Figure 4.1.2-1 Encryption Menu on Terminal**

**The settings made through the programmed key or menu will be saved.**

**In non-emergency status, the LCD displays an encryption icon for channels on which the encryption is enabled. See Figure 4.1.2-2. However, if this function is disabled, the icon will not appear.**

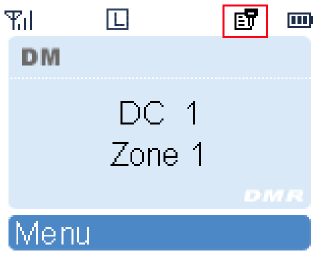


Figure 4.1.2-2 Encryption Icon on LCD

## 4.2 Repeater Configuration

At present, there is no such configuration required.

## 4.3 Hardware Configuration

At present, there is no such configuration required.

# 5. Instruction of Application

**As a tool for commanding and dispatching, the conventional wireless communication system plays an important role widely. However, its security and reliability encounter a great challenge due to poor privacy. Therefore, all kinds of important voice or data must be transferred securely. In response to the security issue, Hytera develops a unique digital encryption function, which can secure the privacy of voice and data in two levels: Basic Encrypt and Full Encrypt.**

**The Basic Encrypt function employs a simple algorithm for common information. However, in case of crucial information, we recommend you to choose the Full Encrypt function. By applying ARC4 and AES, it is an ideal solution for communication security in many areas such as government, public security, energy and transportation.**

# 6. FAQ

## 6.1 Can both encryption mechanisms apply to one terminal?

Yes, but each channel supports one mechanism only.

## 6.2 How many key-length options are available?

We provide three options: 40 bits, 128 bits and 256 bits.

## 6.3 Can we use our own encryption devices?

At present, the encryption function is embedded in the DMR terminal, requiring no extra device. In the future a port will be reserved for users to further develop such function.

## 6.4 What is the purpose of encryption?

This function provides end-to-end encryption for voice and data on digital channels, so as to enhance the communication security.

## 6.5 Will encryption affect the communication coverage and voice quality?

No at all.

## 6.6 Will the encryption settings work for both parties operating on the same channel?

Yes, but the Encrypt option applies to the transmitting party only, that is, if this option is checked, the data to be transferred will be encrypted; otherwise, the data will not be encrypted. See Figure 4.1.1-2.