F3400/F5400 Series: High Level (DES/AES) Encryption

Introduction

The following procedures describe how to program DES/AES encryption into the F3400/F5400 Series digital radios. This document describes how to program DES (more than four keys) or AES , using the accessories and procedures listed below.

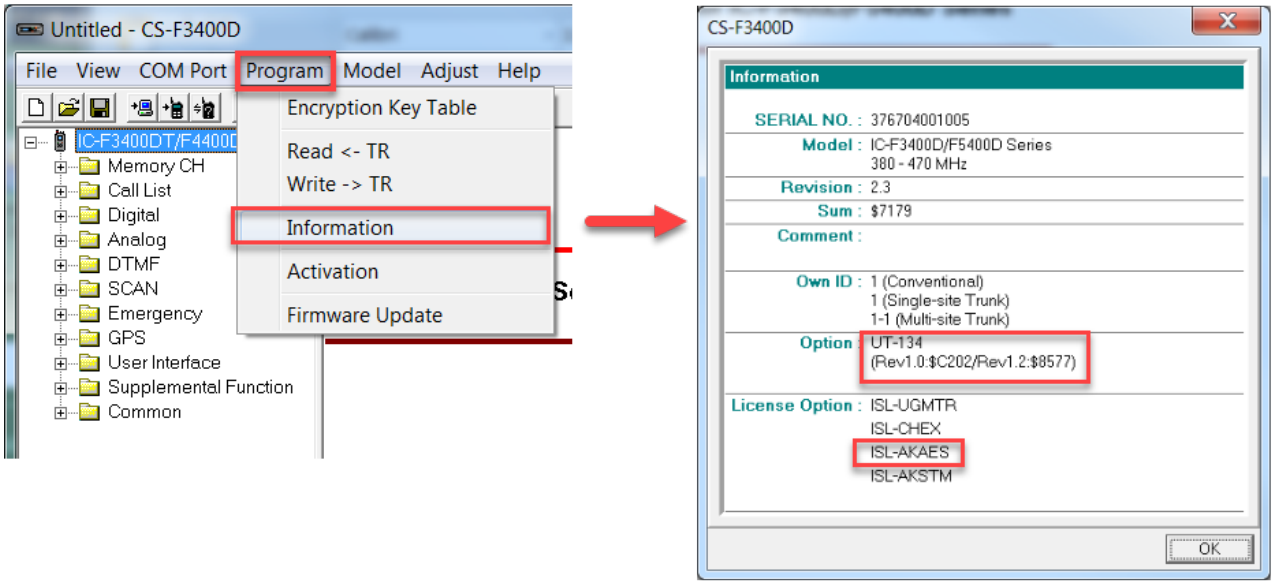
A maximum of 64 encryption codes, AES, DES or both, can be loaded into a given radio.

Note: The F3400/5400 series radios offer low level 15-bit encryption or limited DES (four keys maximum) built into each radio and do not require the CS-KLD2 software or the UT-134.

Note: High and Low Level encryption are for digital operation only.

Prerequisites

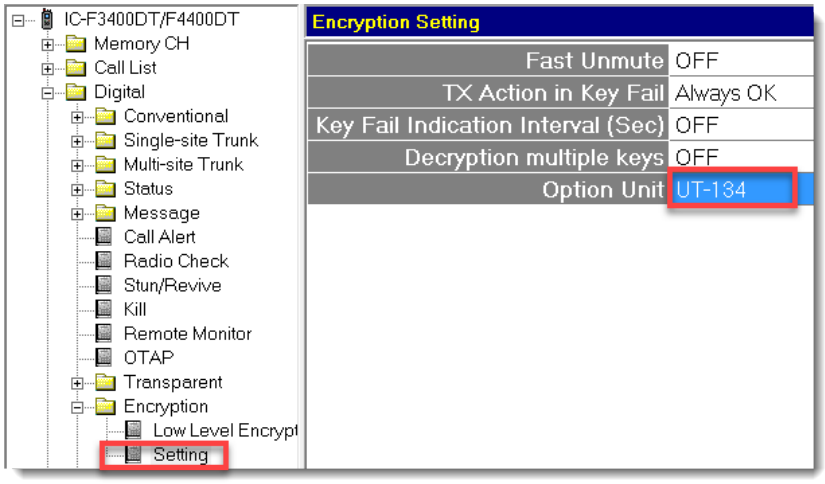
- UT-134 Option Board (Installed in each radio)
- Digital Channels only.
- CS-KLD2 keyloader Software
- USB Secure Key plugged into PC
- AES Activation Key (from Icom America Customer Service) loaded into all radios. Verify proper activation in the Program-Information window (below).



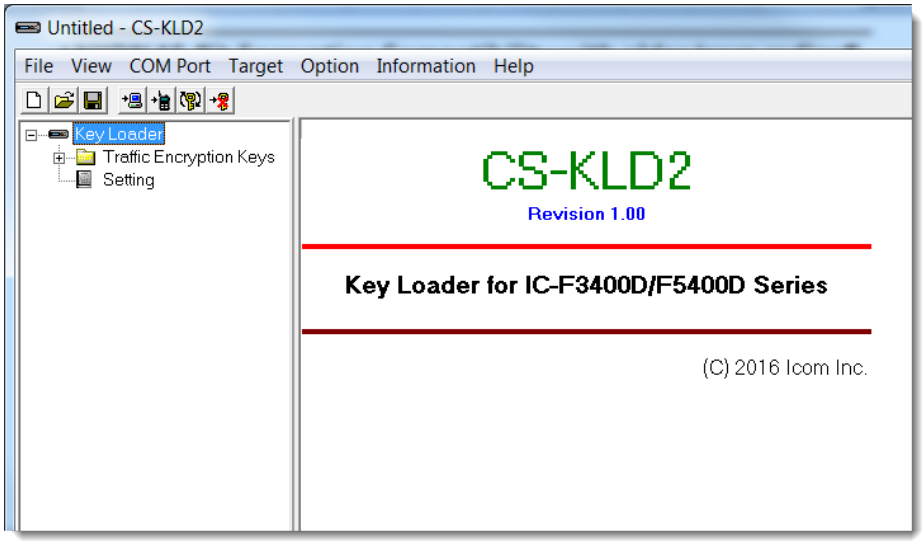
- USB A to micro B type, or OPC-1862 (portables) or OPC- 2363 (Mobiles) with matching drivers for icf and encryption file loading.
- Firmware and Software are updated to the latest version
- Windows® 7, 8.1, or 10 (32/64bit) operating system

CS-F3400 Preliminary Programming

1. Go to **Encryption**-> **Setting**-> **Option Unit**. Set to **UT-134**.



2. Open the **CS-KLD2** Software.

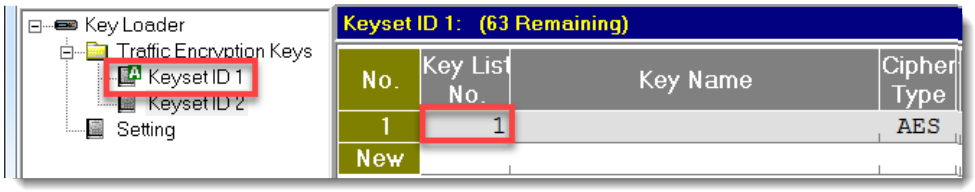


3. Go to **Setting**->**Active Keyset**-> **Traffic Encryption Keyset**. Set to **KeySet ID 1.** This specifies that the Keyset ID 1 list will be used for storage of all encryption keys for voice transmissions.

4. Go to **Traffic Encryption Keys**-> **Keyset ID 1**.

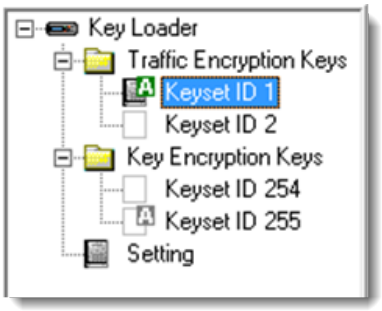
   The programming has 2 Keyset ID lists. For voice communications, use Keyset ID 1 for up to 64 Key List No's.

   Future updates will allow Keyset ID 2 to be used for OTAR functions.



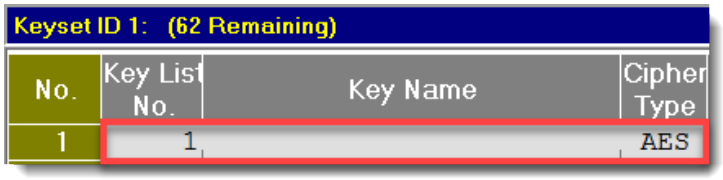
5. Go to **Traffic Encryption Keys** > **Keyset ID 1** > **Key List No**. Enter any number between 1 through 4095. Up to 64 Key List numbers s can be entered, but the assigned numbers can only be used once.

   The Key List No- a numerical label (between 1-4095) assigned to an encryption key by the administrator. This number is a reference to the actual AES or DES encryption code that is generated in the CS-KLD2 on this line.



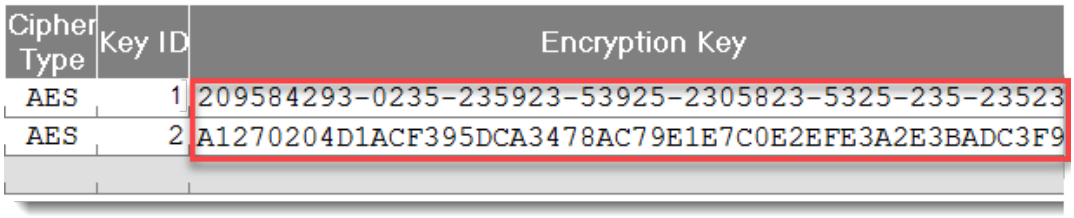
6. In **Key Name**, enter a descriptive text identifier for this specific encryption code.

7. In **Cipher Type**, select **AES** or **DES**.

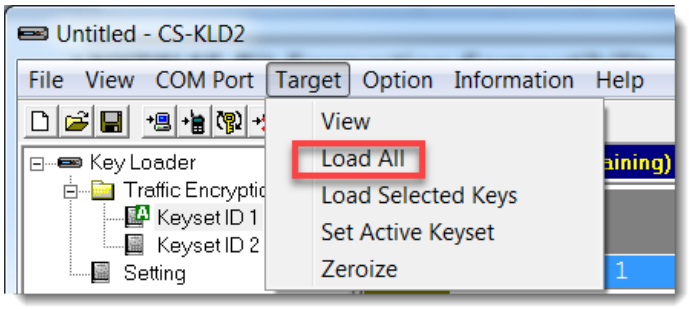


8. In **Key ID (Dec)**, enter a key ID (0-63). Key ID's can only be used one time in the table. The Key ID is a 2 digit numerical identifier that, when received by other radios with the identical encryption load, allows the receiving radio to refer to the correct encryption code for proper un-muting.

9. In **Encryption Key (Hex)**, enter an Encryption key by right clicking and selecting **Auto Generate**. DES keys are composed of 16 Hexadecimal characters; AES keys are composed of 64 Hexadecimal characters.



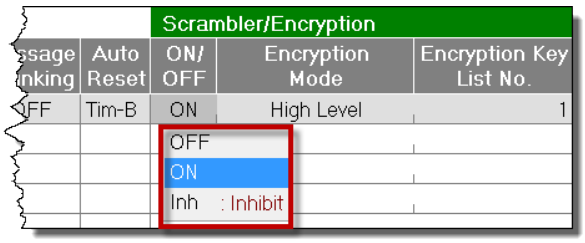
10. Once the key has been entered, go to **Target** and click **Load All**. These keys will be loaded into the radio through the USB cable.



CS-F3400 Preliminary Programming

Before you can use the keys generated and loaded as described above, you will need to set the CS-F3400D cloning software so that it is enabled for encryption.

1. Program the radio with all channels required.
2. Go to **Zone 1** > applicable Channel number > **Scrambler/Encryption** > **ON/OFF**. Set to **ON**. Encryption will be active on this channel by default. If this is set to **OFF**, encryption will be inactive on this channel by default. A Scrambler/Encryption key, assigned in Key and Display, allows the user to toggle the encryption state On and Off on a channel by channel basis.



3. Set the **Encryption Mode** to **High Level** for DES/AES encryption.

4. Set the **Encryption Key List No.** in the radio cloning software to the desired **Key List No**. (numbers ranging from 1-4095) in the **Keyset ID** 1 list of the CS-KLD2 software. This Key List No. directs the radio to one of the up-to 64 possible encryption codes previously loaded in the radio.
5. Repeat this for each radio channel that requires encryption.
6. Write this data to the radio.
7. Go **to Key Assign**, and assign a key as a Scrambler/Encryption key if you want to be able to toggle between On and Off.

Encryption Use Notes

For any 2 or more radios to encrypt and decrypt properly, the **Encryption Key**, **Key ID**, and **Cipher Type** must match on the operating channel.

Other Settings on CS-KLD2 software

- To make the encryption key visible in the CS-KLD2 software windows, go to **Option** in the Main Menu and select **Encryption Keys Visible**.
- To save a Key or a list of keys to your PC, click **Save Key**.
- To open a key that was saved previously, click **Open Key**.

Operation

- If all radios are set to the same encryption code they will decode each other correctly.
- If it is desired to turn on or off encryption on each channel, a Scrambler/Encryption key needs to be programmed into the radio (Menu -> Channel Scan -> Scrambler -> Encryption).
- If one radio is operating with encryption, other NON-encrypted radios will hear no audio when receiving that signal.