Voice Crypt 1.0a

High security voice encryption for Tytera MD380/MD390 UHF version.

This software is based on MD380TOOLS by Travis GoodSpeed, thanks to him for all the work done. This software does not work on MD-UV380 and MD-UV390. It works on the MD380 UHF and MD390 UHF (with and without GPS). It does not work on VHF versions. Voice Crypt uses the new Vocoder, if your MD380 is not compatible with the new Vocoder then you will not be able to use it.

Motorola Basic Privacy mode belongs to Motorola, thanks to them for the work done. No patent exists for Basic Privacy mode.

Enhanced Privacy mode uses 128-bit AES encryption and belongs to Tytera, thanks to him for the work done. It is, however, a degraded mode of the AES and much less secure than the AES of Motorola.

The PC4 Cipher mode belongs to Alexander Pukall, thanks to him for the work done.

Voice Crypt does not contain ARC4 and AES Motorola encryption because a patent exists and prevents its legal use, which is why the PC4 Cipher mode was chosen because it is royalty-free.

This software is free, it is a Freeware.

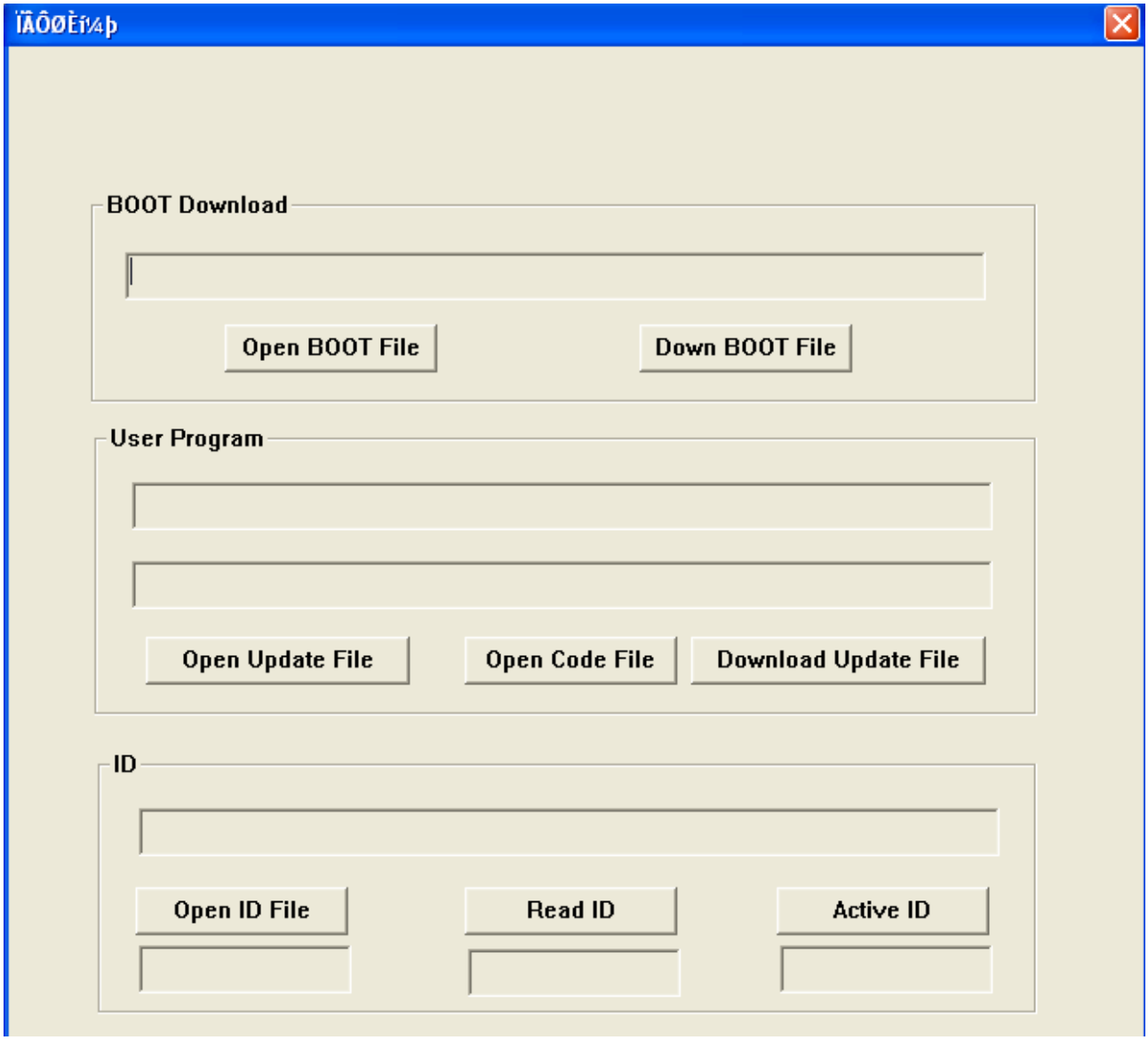
This manual is in RTF format so that you can translate it into your language if you want to distribute Voice Crypt with a translation into your own language.

How to Flash the Firmware:

Voice Crypt is based on firmware D013.020 (without GPS) and S013.020 (with GPS). If your MD380/390 does not turn on after flashing, it is not compatible with version 013.20. You will then need to reflash your original firmware.

To flash your MD380 launch the Upgrade.exe program:

On your MD380 turned off, press the 1 and PTT keys simultaneously (the top 2 keys on the left) and without letting go of the keys turn on the MD380 (by turning the volume knob). The screen does not display anything but the LED flashes red/green, the MD380 is ready to be flashed.


BOOT Download
Open BOOT File
Down BOOT File
User Program
Open Update File
Open Code File
Download Update File
ID
Open ID File
Read ID
Active ID


下载软件
BOOT Download
打开
查找范围(I):
Upgraded softare for scanni:
Upgraded software ...
文件名(N):
Upgraded software for scanning function
打开(O)
文件类型(T):
(*.bin)
取消
以只读方式打开(R)
Open ID File
Read ID
Active ID

Click **Open Update File**, choose Voice Crypt firmware for GPS or without GPS and click **Download Update File.**

Voice Crypt is flashed on the MD380. At the end turn off the MD380 and turn it back on.

It is recommended to do a Reset after flashing to make sure that Voice Crypt is working properly (see the **Reset** section at the very end of this manual).

How to get started quickly

Motorola Basic Privacy Mode with Password

This mode is compatible with a Motorola Basic Privacy radio in reception (RX). It can transmit in Basic Privacy but in the absence of a Pi Header frame, a Motorola radio will not be able to recognize that it is an encrypted broadcast in Basic Privacy. On the other hand, two MD380s will be able to transmit and receive in Basic Privacy.

To configure it go to:

Menu – Utilities – 4 Md380Tools – 8 Voice Crypt – 1 Crypt Mode – Basic Privacy

To go to:

3 Password

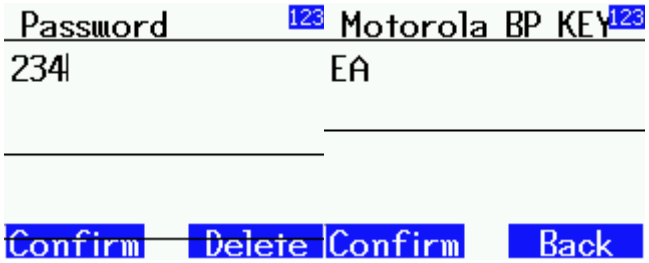
Enter the encryption key to use in decimal format (from 1 to 255). You can write 1, 01, or 001. Do not forget to switch to the numeric mode (123) to write the numbers otherwise you are in the alphabetical mode (EN). To switch from (EN) mode to (123) press the # key several times. Do not use Chinese mode as it is not supported.

Check if the encryption key is enabled in:

4 Show key

If it says Motorola BP KEY 01 it means that the encryption key is activated.

Try it out with the 234 encryption key in **3 Password**, then look in **4 Show Key**, the encryption key is written in hexadecimal: EA



It's the same encryption key but **Show Key** shows the encryption keys in hexadecimal.

You can then send and receive in Basic Privacy. The main screen tells you "Moto BP pas" for "Motorola Basic Privacy password" and "K:EA" for the active "EA" encryption key in hexadecimal.

You can talk with another MD380 using the same encryption key or listen to a Motorola radio with the same encryption key.

You can change the Moto BP encryption key without having to retype the password using the up and down arrows. To do this, you must first unlock these keys by pressing the * key 3 times in a row.

Once the arrows are unlocked you can increase the encryption key by +1 with the up arrow or decrease the encryption key by -1 with the bottom arrow.

In emission (TX) you cannot use the up and down arrows to change the encryption key. On the other hand in reception (RX) you can use the up and down arrows to change the encryption key. If you are listening to an encrypted channel in Basic Privacy and you do not know the encryption key, then you can use the up and down arrows to try the 255 possible encryption keys (from 1 to FF in hexadecimal). As soon as the encryption key is correct, you will hear the conversation in the clear. Once the conversation is over you will see which encryption key you stopped at.

PC4 Cipher Mode with Password

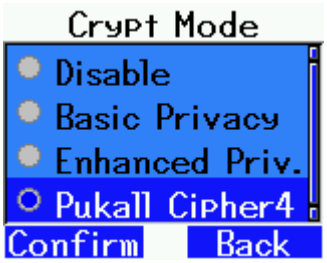
The PC4 Cipher developed by Alexander Pukall uses encryption keys ranging from 8 bits to 2212 bits depending on the length of the password or encryption key. It works in ECB mode, has been created specifically for DMR radio mode and is extremely secure.

Voice Crypt allows you to use encryption keys ranging from 112 bits to 420 bits simply because the MD380's screen does not display more characters correctly. As Voice Crypt does not allow the use of Chinese characters, English Ascii characters (letters, numbers, special characters) are used. An Ascii character is 7-bit.

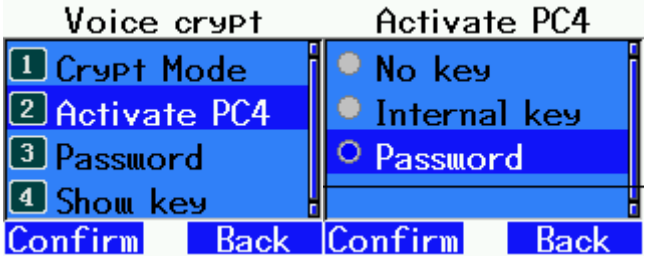
Voice Crypt allows passwords ranging from 16 characters to 60 characters. So we get encryption keys from 112 bits (16*7) to 420 bits (60*7). We believe that this is more than enough to counter all possible threats of unauthorized eavesdropping.

The PC4 Cipher is royalty-free and in the public domain, so it does not infringe any Motorola patent to use it in Voice Crypt.

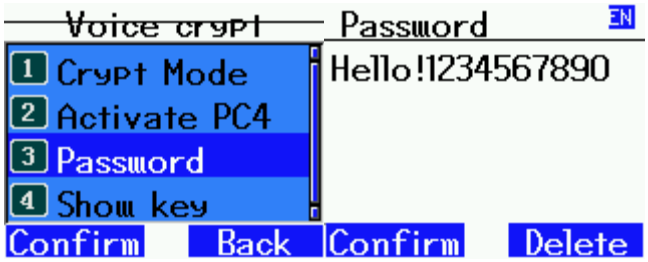
Go to **Menu – Utilities – 4 Md380Tools – 8 Voice Crypt – 1 Crypt Mode – Pukall Cipher 4**



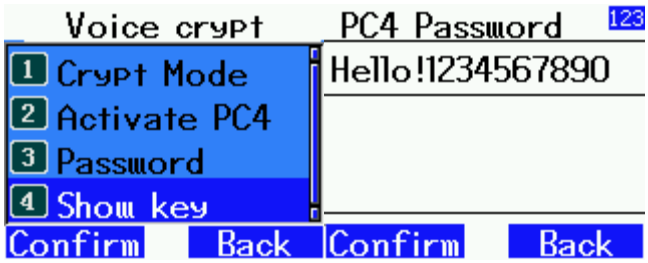
Then **2 Activate PC4** and choose **Password** :



Then go to **3 Password** and enter a password of at least 16 characters (up to 60 characters):



You can verify that PC4 is enabled by clicking on **4 Show key** and you should see the same password you entered, which means that PC4 is enabled:



On the main screen you should then see "PC4 password" it means that PC4 is activated in "password" mode (be careful you will only see it if the Display Mode is set to OFF).

You can then securely communicate with another MD380 that uses the same password.

Mode Display :

To see the activation of encryption on the main screen the MD380Tools Display Mode must be set to OFF otherwise you will not see it.

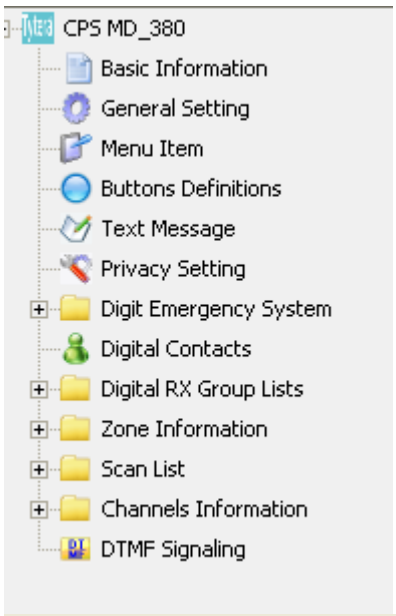
You can check this by going to **Menu Utilities – 4 MD380Tools – 1 Display - 4 Mode Display**


Menu
Zone
Messages
Call Log
Utilities
Confirm
Back
Utilities
1 Radio Settings
2 Radio Info
3 Program Radio
4 MD380Tools
Confirm
Back
MD380Tools 2.0
1 Display
2 Radio
3 DMR Setup
4 SMS Service
Confirm
Back
Display Setup
1 Backlight
2 Date/Status
3 Show Calls
4 Mode Display
Confirm
Back
Mode Display
Mode/CC Off
Mode/CC
Mode/CC/Mic
Mode compact
Confirm
Back

Modes with internal encryption keys

Tytera's programming software (CPS) allows you to enter encryption keys for DMR channels.

In the Tytera CPS, you can click on Privacy Settings to see the encryption keys:



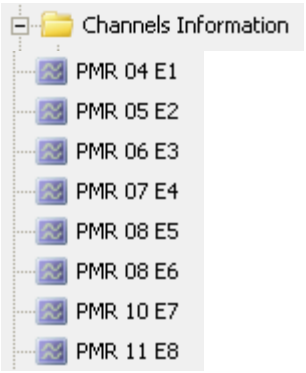
No.	Key Value(Basic)
1	FFFF
2	FFFF
3	FFFF
4	FFFF
5	FFFF
6	FFFF
7	FFFF
8	FFFF
9	FFFF
10	FFFF
11	FFFF
12	FFFF
13	FFFF
14	FFFF
15	FFFF
16	FFFF

No.	Key Value(Enhanced)
1	FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
2	FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
3	FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
4	FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
5	FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
6	FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
7	FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
8	FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF

Do not use the column (Basic), always use the column (Enhanced) to put 128-bit encryption keys (16 hexadecimal characters), you can create 8 encryption keys, such as:

No.	Key Value(Enhanced)
1	00000000000000000000000000000000
2	00000000000000000000000000000001
3	00000000000000000000000000000002
4	00000000000000000000000000000101
5	00000000000000000000000000000202
6	112233445566778899AABBCCDDEEFF11
7	74581225622174788112236655123336
8	ABCDEDCBABCDDBCABDBCABDABBABBDBE

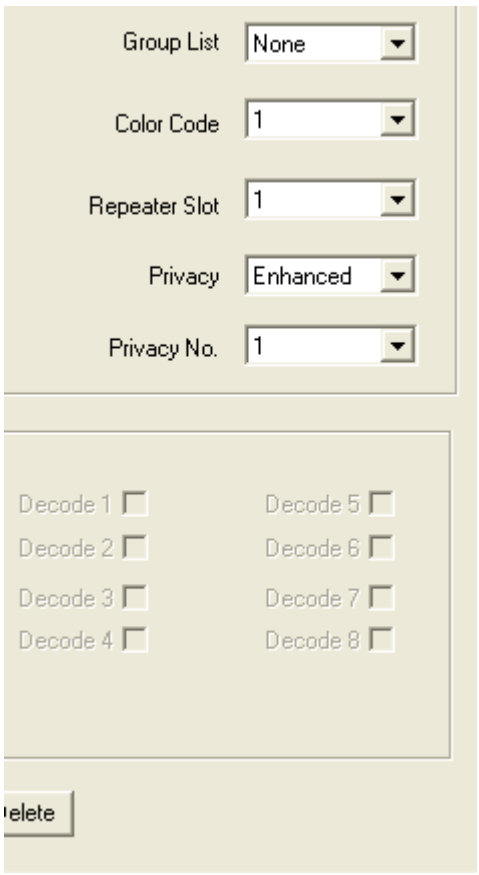
In the Channels Information section you can configure your channels:



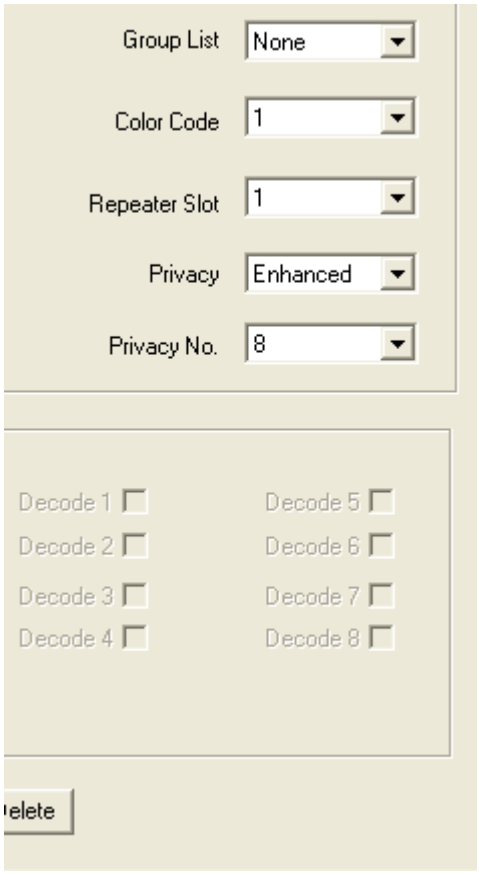
E1 stands for Enhanced Privacy Channel 1, E2 Enhanced Privacy Channel 2...

Opening channel E1 we see:

At the bottom right we observe Enhanced and the encryption key number, here Privacy Key No. 1.



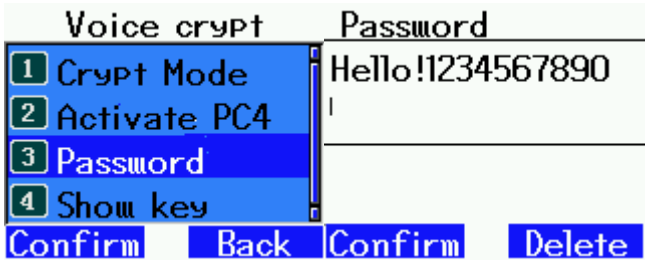
Another example with the E8 channel:



Motorola Basic Privacy Mode with Internal Encryption key

Menu – Utilities – 4 MD380Tools – 8 Voice Crypt – 1 Crypt Mode – Basic Privacy

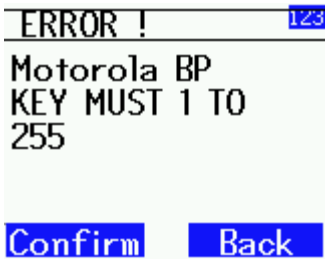
Go to **3 Password** and type a password longer than 4 characters (or no password at all):

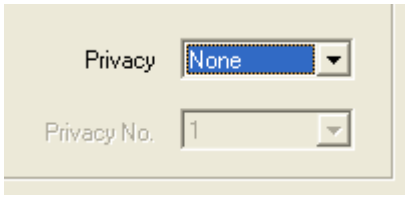


If the password consists of numbers from 1 to 255 then the password mode takes precedence over the internal encryption key mode and Basic Privacy uses the password as the encryption key. Otherwise it uses the internal encryption key programmed on the active channel.

Go to **4 Show Key** :

If you are on a channel without Enhanced mode being active then you will get this error message (because there is no active internal encryption key):

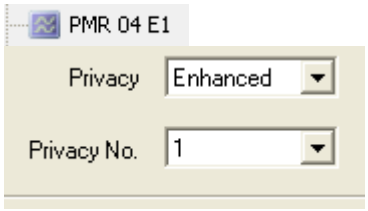




On the main screen there will be nothing, indicating that encryption is not active:

If a channel is enabled in Enhanced Mode, it depends on the contents of the rightmost byte of the encryption key:

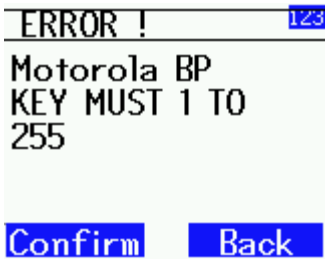
In the following example, channel E1 uses the Enhanced Privacy key No. 1:



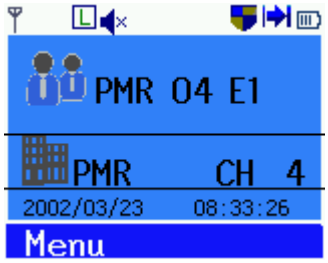
But the rightmost byte of encryption key 1 is at 0:

No.	Key Value(Enhanced)
1	00000000000000000000000000000000
2	00000000000000000000000000000001
3	00000000000000000000000000000002

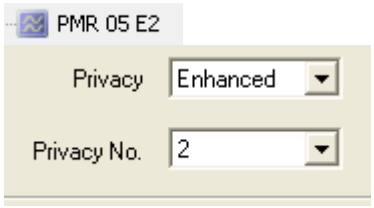
So you will get this error message in **4 Show key** :

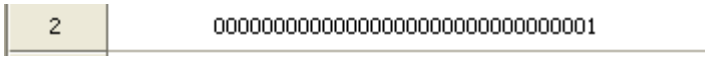


And nothing will be displayed on the main screen:

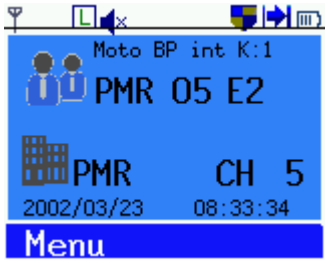


If we go to channel E2 that uses the Privacy Key No. 2:

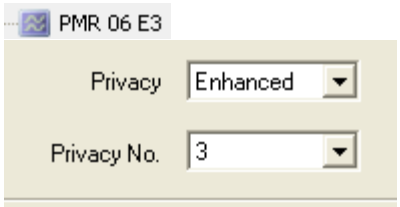




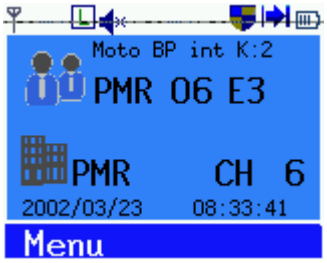
The rightmost byte being 01, the Basic Privacy 1 encryption key will be activated: "Moto BP int K:1" stands for "Motorola Basic Privacy internal key" and the K for the encryption key number (here 1).



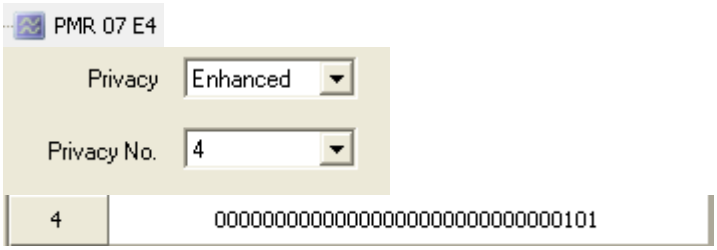
If we go to the E3 channel that uses the Privacy key No. 3:



The rightmost byte being 02, it is the Basic Privacy 2 encryption key that will be activated:

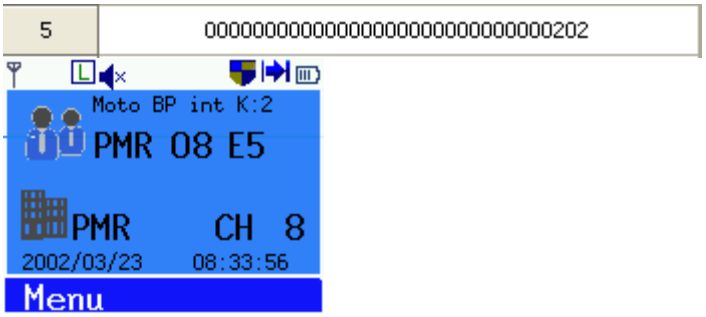


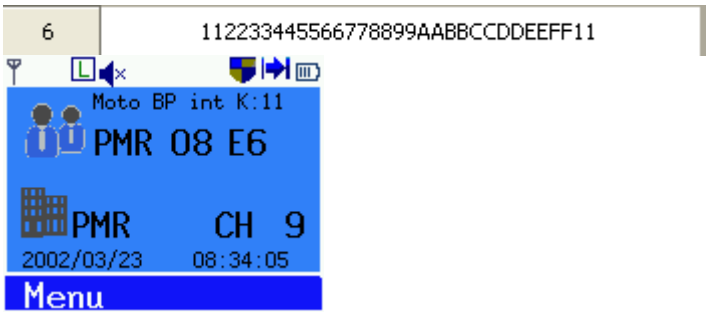
If we go to channel E4 that uses the Privacy key No. 4:



There are two bytes 01 but it is the rightmost byte that is used for Basic Privacy, so it is the Basic Privacy 1 encryption key that will be activated:

Here are examples of the remaining channels:





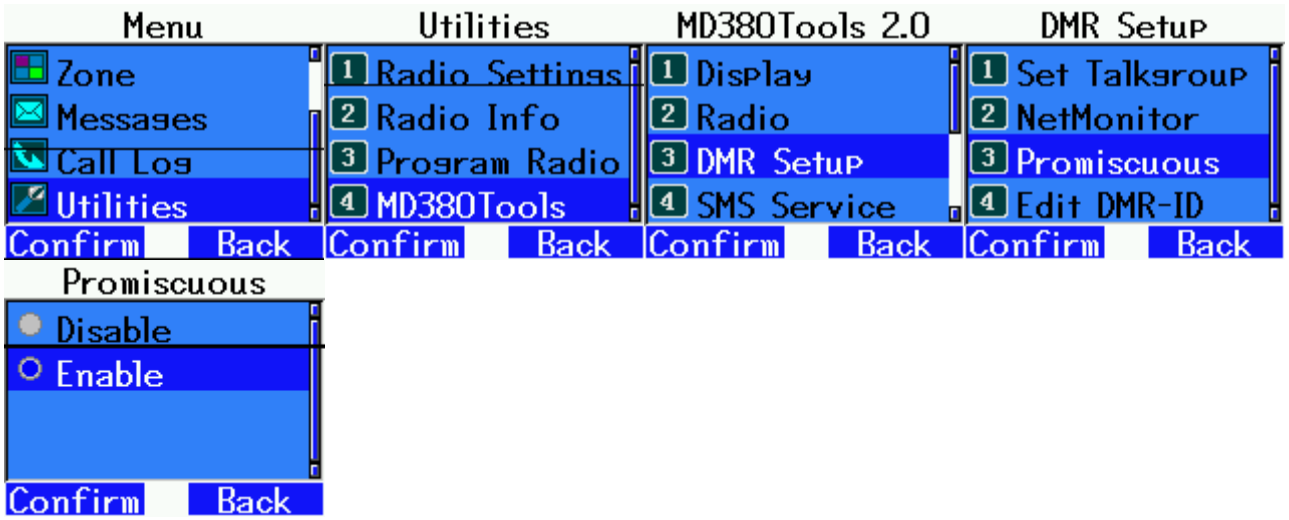
7	74581225622174788112236655123336

8	ABCDEDCBABCDDBCABDBCABDABBABBDBE

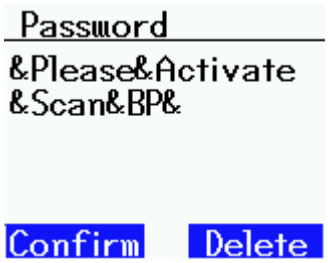
There's an additional hidden option: you can scan and automatically find a Motorola Basic Privacy key.

First you need to configure the MD380 to receive all communications, this is the Promiscuous mode.

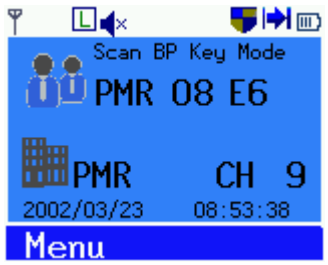
Go to :



Then go to **Password** and type in the secret password:



You will then enter the Motorola Basic Privacy Scanner mode:



Wait for an encrypted Motorola Basic Privacy communication to start, as soon as the encryption key is found you hear a beep and the communication is then heard in plain text.

Once the reception stops, you will see the key that was found:

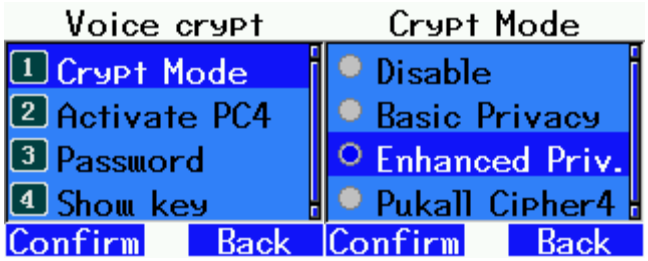
If you want to run a new scan, you can press the PTT button once or press the # key.

Be careful, this mode only works with an official Motorola device because Motorola has introduced a backdoor to scan encryption keys.
The backdoor isn't present in Voice Crypt, so you can't find the Basic Privacy key from another Voice Crypt.

To exit the Motorola Basic Privacy Scanner Mode, you can retype the same hidden password as above or turn the MD380 off and on again.

Tytera Enhanced Privacy mode with internal encryption key

In **Crypt Mode** choose **Enhanced Privacy**:



Then everything will depend on which channel you are on.

Go to **Show key :**

If you see the error message:

It's that you're not on an Enhanced Privacy channel. Sometimes you also have to switch to another channel and come back to it so that it is taken into account.

If you are on an Enhanced Privacy channel then the 128-bit encryption key used by the Tytera Enhanced Privacy algorithm appears.

In the example below it is Privacy No. 5:

5	00000000000000000000000000000202

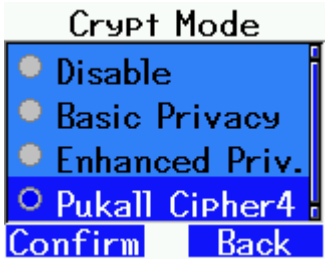
On the main screen appears "Tyt EP int K0:2": This means "Tytera Enhanced Privacy internal key" with K0 (rightmost zero byte:2).

The K0 encryption key is not the complete 128-bit encryption key (there is not enough room on the screen to display everything) but it allows the user to know the rightmost byte and therefore quickly check which encryption key is used. The full encryption key is displayed using **Show key**:

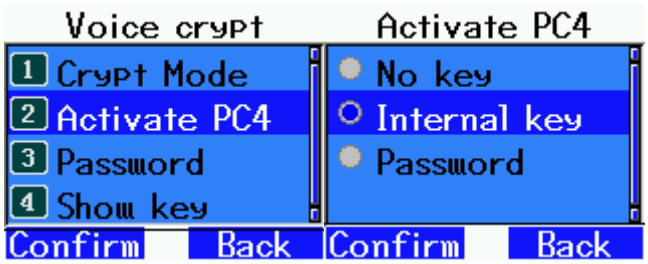
Example with other encryption keys:

PC4 Cipher mode with internal encryption key

In **Crypt Mode** choose **PC4 Cipher**:



Go to **2 Activate PC4** and choose **Internal key**:



As with Tyt Enhanced Privacy mode, the encryption key used will depend on the channel you are on.

Show Key shows you the active encryption key and the main screen shows you the rightmost byte of the active encryption key (re-read the Tyt Enhanced Privacy section if necessary for the explanation of the K0 byte).

PC4 Cipher Advanced part

PC4 Cipher is active in the most secure mode (253 rounds of encryption). However some MD380 may have a processor too slow (CPU) this would result in poor quality voice.

It is possible to reduce the number of encryption rounds if you have a CPU that is too slow. All MD380s must then be configured with the same number of rounds to be able to communicate with each other.

This is a hidden menu, to activate it you have to go to **8 Voice Crypt:**

Then **3 Password :**

You must then enter a special password with lowercase uppercase and special characters
: « **&Please&Activate&Round&Config&** » :

Get out of the menu and return to the menu, the hidden menu has appeared:

You can then reduce the number of rounds (this also reduces security and should only be done if the CPU is too slow and the voice is bad):

On the main screen you are warned that you are in a mode with reduced rounds and this is displayed for the PC4 with password or the PC4 with internal encryption key:

You can make this hidden menu disappear again by retyping the same special password a second time.

MI Config

PC4 Cipher is an ECB mode block cipher algorithm. This means that identical data in different voice frames will be encrypted in the same way if the same encryption key is used. This is the case, for example, with silence frames.

To avoid this, an additional option exists that adds random data so that identical silence frames are encrypted differently.

This increases security, but it decreases the voice quality because bits in voice frames are removed.

You can choose between 4 and 6 bits per voice frame. With 6 bits, the security is better than with 4 bits, but the sound is worse.

It's a hidden menu, to activate it you have to go to **8 Voice Crypt :**

Then **3 Password :**

You must then enter a special password with lowercase letters and special characters:
« **&Please&Activate&MI&Config&** » :

Exit the menu and return to the menu, the hidden menu is here:

On the main menu you will be notified by MI4 or MI6 if you are in MI Config mode.

Ideally, all participants in a discussion should use the same MI configuration, but this is not mandatory, decryption is possible even if not everyone uses the same MI configuration.

You can make this hidden menu disappear again by retyping the same special password a second time.

RC2 Encryption

Voice Crypt offers another encryption mode: RC2 in CFB mode.

This is an encryption cipher created by Ron Rivest and improved by Alexander Pukall (removal of reduced encryption key sizes and increase the internal state of the RC2 to 1024 bits).

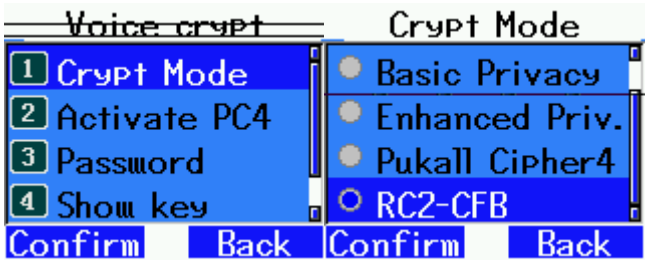
The encryption key size is 128 bits if you use the internal encryption keys or up to 420 bits if you use a 60-character password.
It also uses a 6-bit MI Config so this RC2 mode degrades the sound quality of the voice.

It's a hidden menu, to activate it you have to go to **8 Voice Crypt :**

Then **3 Password :**

You must then enter a special password with lowercase letters and special characters:
« **&Please&Activate&RC2&Encryption&** » :

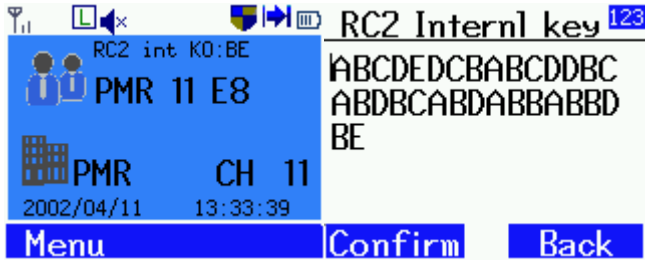
Exit the menu and return to the menu, the hidden menu is here:



You can make this hidden menu disappear again by retyping the same special password a second time.

To use the mode with a password, enable **Password** in **Activate PC4** (even if PC4 is not active but RC2).

You can also choose **Internal Key** :



Reset

In case of problem and if nothing works properly you can reset all options.

Go to **Utilities - 4 MD380 Tools- 7 Developer – 4 Config Reset**