Voice Crypt 1.0a
Cripta de voz 1.0a

Cifrado de voz de alta seguridad para la versión UHF de Tytera MD380/MD390.

Este software está basado en MD380TOOLS por Travis GoodSpeed, gracias a él por todo el trabajo realizado. Este software no funciona en MD-UV380 y MD-UV390. Funciona en el MD380 UHF y MD390 UHF (con y sin GPS). No funciona en versiones VHF. Voice Crypt utiliza el nuevo Vocoder, si su MD380 no es compatible con el nuevo Vocoder, no podrá utilizarlo.

El modo de privacidad básico de Motorola pertenece a Motorola, gracias a ellos por el trabajo realizado. No existe ninguna patente para el modo de privacidad básica.

El modo de privacidad mejorada utiliza cifrado AES de 128 bits y pertenece a Tytera, gracias a él por el trabajo realizado. Sin embargo, es un modo degradado del AES y mucho menos seguro que el AES de Motorola.

El modo de cifrado PC4 pertenece a Alexander Pukall, gracias a él por el trabajo realizado.

Voice Crypt no contiene encriptación ARC4 y AES Motorola porque existe una patente e impide su uso legal, por lo que se eligió el modo de cifrado PC4 porque está libre de regalías.

Este software es gratuito, es un Freeware.

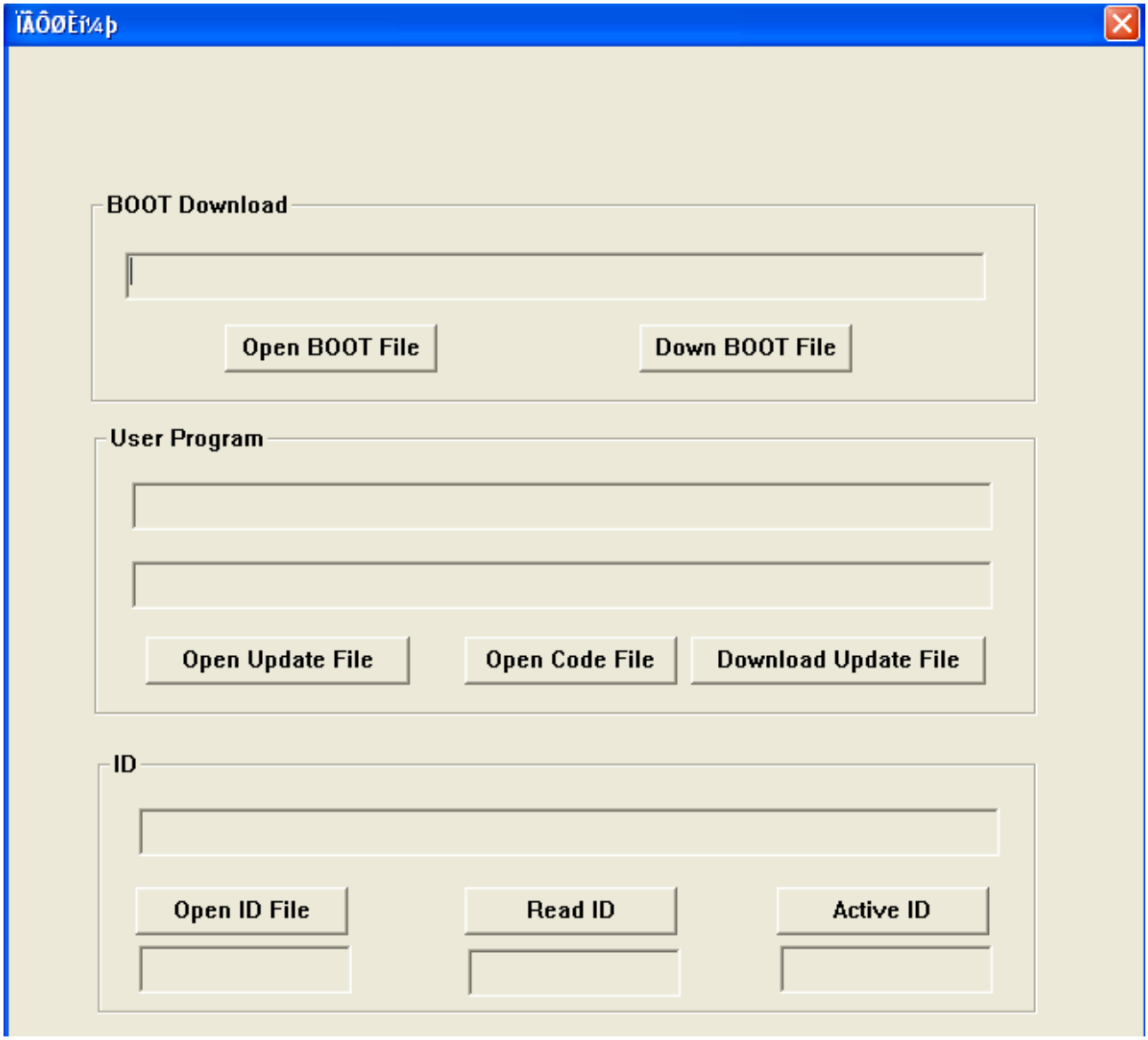
Este manual está en formato RTF para que puedas traducirlo a tu idioma si quieres distribuir Voice Crypt con una traducción a tu propio idioma.

Cómo actualizar el firmware:

Voice Crypt se basa en los firmware D013.020 (sin GPS) y S013.020 (con GPS). Si su MD380/390 no se enciende después de flashear, no es compatible con la versión 013.20. A continuación, deberá volver a actualizar el firmware original.

Para actualizar el archivo MD380, inicie el programa Upgrade.exe:

En su MD380 apagado, presione las teclas 1 y PTT simultáneamente (las 2 teclas superiores a la izquierda) y, sin soltar las teclas, encienda el MD380 (girando la perilla de volumen). La pantalla no muestra nada, pero el LED parpadea en rojo/verde, el MD380 está listo para parpadear.


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

Clic **Open Update File**, elija el firmware de Voice Crypt para GPS o sin GPS y haga clic en
Download Update File.

Voice Crypt se muestra en el MD380. Al final, apague el MD380 y vuelva a encenderlo.

Se recomienda hacer un reinicio después de flashear para asegurarse de que Voice Crypt funciona correctamente (consulte la sección **Restablecimiento** al final de este manual).

Cómo empezar rápidamente

Modo de privacidad básico de Motorola con contraseña

Este modo es compatible con una radio Motorola Basic Privacy en recepción (RX). Puede transmitir en Privacidad Básica, pero en ausencia de una trama Pi Header, una radio Motorola no podrá reconocer que se trata de una transmisión cifrada en Privacidad Básica. Por otro lado, dos MD380 podrán transmitir y recibir en Basic Privacy.

Para configurarlo vaya a:

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

A continuación, vaya a:

3 Password

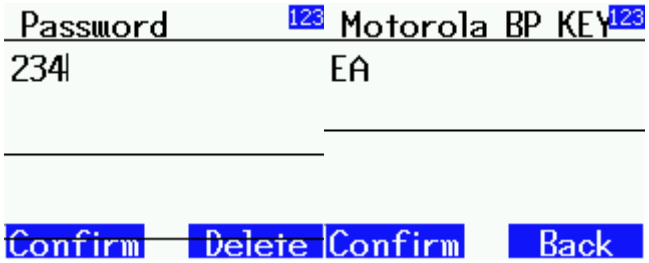
Introduzca la clave de cifrado que desea utilizar en formato decimal (de 1 a 255). Puede escribir 1, 01 o 001. No olvide cambiar al modo numérico (123) para escribir los números, de lo contrario estará en el modo alfabético (EN). Para cambiar del modo (EN) al modo (123), pulse la tecla # varias veces. No utilice el modo chino ya que no es compatible.

Compruebe si la clave de cifrado está habilitada en:

4 Show key

Si dice Motorola BP KEY 01 significa que la clave de cifrado está activada.

Pruébelo con la clave de cifrado 234 en "3 Password", luego busque en "4 Show Key", la clave de cifrado está escrita en hexadecimal: EA



Es la misma clave de cifrado, pero **Show Key** muestra las claves de cifrado en hexadecimal.

A continuación, puede enviar y recibir en Privacidad básica. La pantalla principal le indica "Moto BP pas" para la "Motorola Basic Privacy password" y "K:EA" para la clave de cifrado "EA" activa en hexadecimal.

Puede hablar con otro MD380 utilizando la misma clave de cifrado o escuchar una radio Motorola con la misma clave de cifrado.

Puede cambiar la clave de cifrado Moto BP sin tener que volver a escribir la contraseña usando las flechas hacia arriba y hacia abajo. Para hacer esto, primero debe desbloquear estas teclas presionando la tecla * 3 veces seguidas.

Una vez que las flechas estén desbloqueadas, puede aumentar la clave de cifrado en +1 con la flecha hacia arriba o disminuir la clave de cifrado en -1 con la flecha inferior.

En la emisión (TX) no se pueden utilizar las flechas hacia arriba y hacia abajo para cambiar la clave de cifrado. Por otro lado, en recepción (RX) puedes usar las flechas hacia arriba y hacia abajo para cambiar la clave de cifrado. Si está escuchando un canal cifrado en Privacidad básica y no conoce la clave de cifrado, puede usar las flechas hacia arriba y hacia abajo para probar las 255 claves de cifrado posibles (de 1 a FF en hexadecimal). Tan pronto como la clave de cifrado sea correcta, escuchará la conversación sin cifrar. Una vez que termine la conversación, verá en qué clave de cifrado se detuvo.

Modo de cifrado PC4 con contraseña

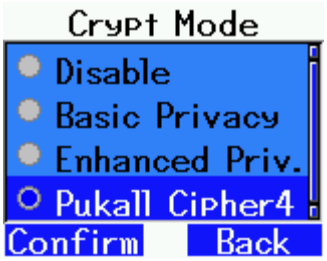
El cifrado PC4 desarrollado por Alexander Pukall utiliza claves de cifrado que van desde los 8 bits hasta los 2212 bits, dependiendo de la longitud de la contraseña o clave de cifrado. Funciona en modo ECB, ha sido creado específicamente para el modo de radio DMR y es extremadamente seguro.

Voice Crypt le permite utilizar claves de cifrado que van desde los 112 bits hasta los 420 bits simplemente porque la pantalla del MD380 no muestra más caracteres correctamente. Como Voice Crypt no permite el uso de caracteres chinos, se utilizan caracteres ASCII en inglés (letras, números, caracteres especiales). Un carácter Ascii es de 7 bits.

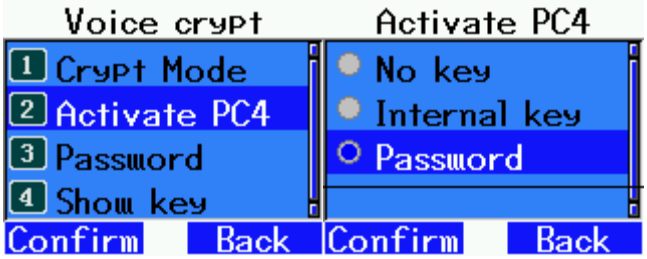
Voice Crypt permite contraseñas que van desde 16 caracteres hasta 60 caracteres. Así que obtenemos claves de cifrado de 112 bits (16*7) a 420 bits (60*7). Creemos que esto es más que suficiente para contrarrestar todas las posibles amenazas de espionaje no autorizado.

El cifrado PC4 está libre de regalías y es de dominio público, por lo que no infringe ninguna patente de Motorola para usarlo en Voice Crypt.

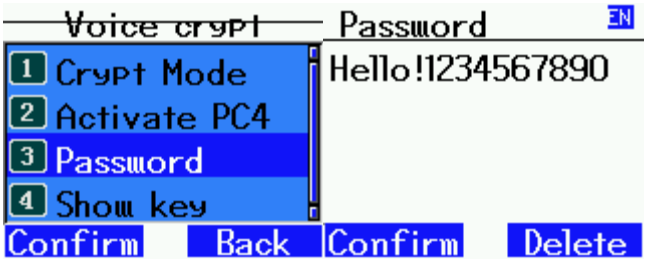
Vete a **Menu – Utilities – 4 Md380Tools – 8 Voice Crypt – 1 Crypt Mode – Pukall Cipher 4**



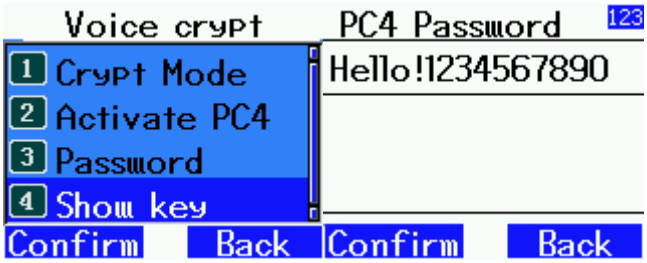
Entonces **2 Activate PC4** y elige **Password** :



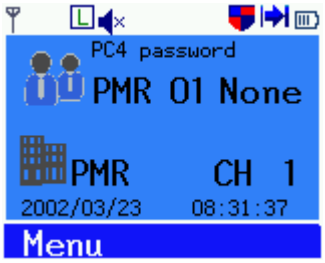
A continuación, vaya a **3 Password** e introduzca una contraseña de al menos 16 caracteres (hasta 60 caracteres):



Puede verificar que PC4 esté habilitado haciendo clic en **4 Show key** y debería ver la misma contraseña que ingresó, lo que significa que PC4 está habilitado:



En la pantalla principal, debería ver "PC4 password", significa que PC4 está activado en modo "password" (tenga cuidado, solo lo verá si el modo de visualización está desactivado).



A continuación, puede comunicarse de forma segura con otro MD380 que utilice la misma contraseña.

Visualización del modo:

Para ver la activación del cifrado en la pantalla principal, el modo de visualización MD380Tools debe estar desactivado, de lo contrario no lo verá.

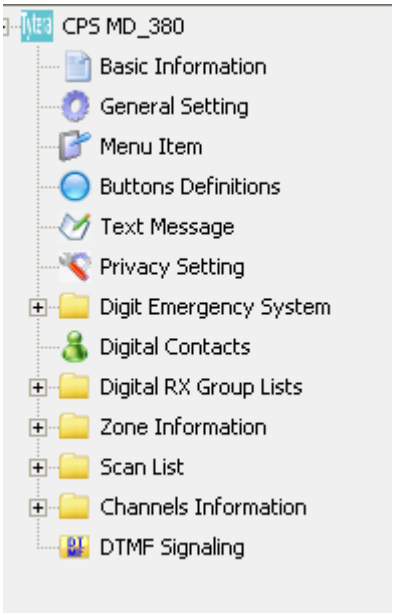
Puedes comprobarlo en **Menu Utilities – 4 MD380Tools – 1 Display -4 Mode Display**


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

Modos con claves de cifrado internas

El software de programación de Tytera (CPS) le permite ingresar claves de cifrado para canales DMR.

En Tytera CPS, puede hacer clic en Configuración de privacidad para ver las claves de cifrado:



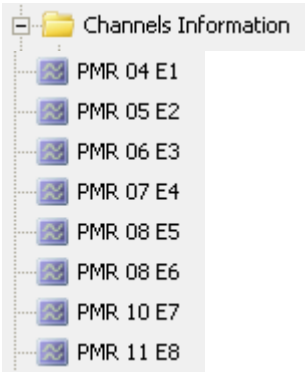
No.	Key Value(Basic)
1	FFFF
2	FFFF
3	FFFF
4	FFFF
5	FFFF
6	FFFF
7	FFFF
8	FFFF
9	FFFF
10	FFFF
11	FFFF
12	FFFF
13	FFFF
14	FFFF
15	FFFF
16	FFFF

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

No use la columna (Basic), siempre use la columna (Enhanced) para poner claves de cifrado de 128 bits (16 caracteres hexadecimales), puede crear 8 claves de cifrado, como:

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

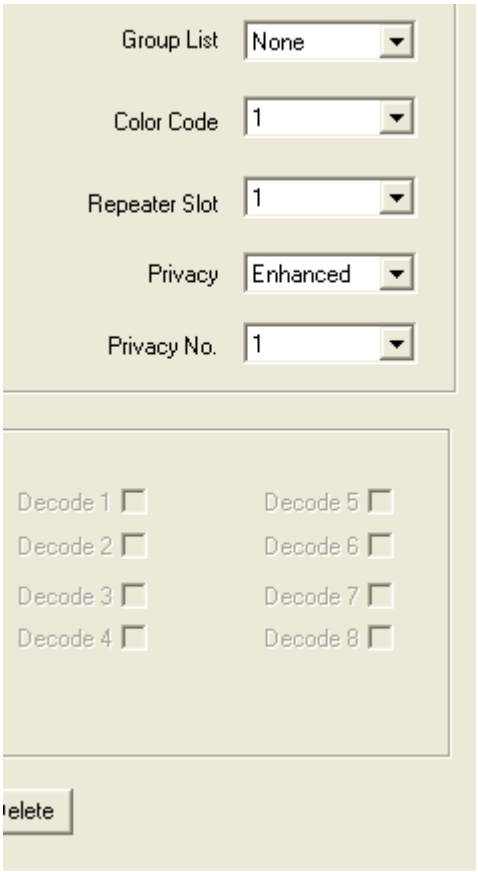
En la sección Channels Information puedes configurar tus canales:



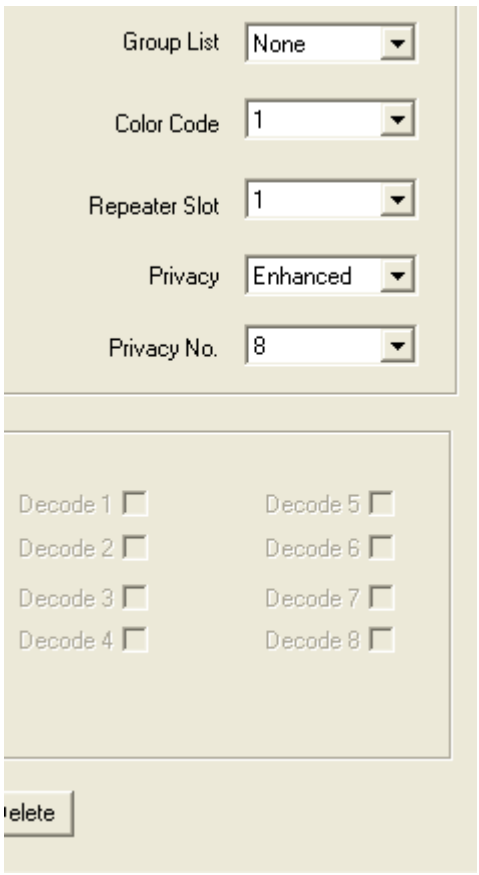
E1 son las siglas de Enhanced Privacy Channel 1, E2 Enhanced Privacy Channel 2...

Abriendo el canal E1 vemos:

En la parte inferior derecha observamos Mejorado y el número de clave de cifrado, aquí Clave de privacidad nº 1.



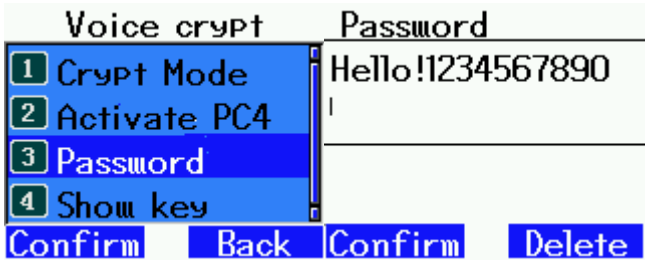
Otro ejemplo con el canal E8:


Group List
None
Color Code
1
Repeater Slot
1
Privacy
Enhanced
Privacy No.
8
Decode 1
Decode 2
Decode 3
Decode 4
Decode 5
Decode 6
Decode 7
Decode 8
elete

Modo de privacidad básico de Motorola con clave de cifrado interno

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

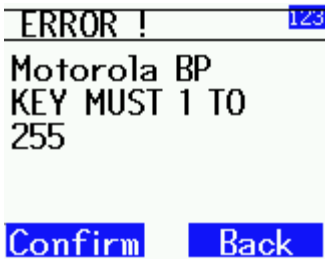
Vete a **3 Password** y escriba una contraseña de más de 4 caracteres (o ninguna contraseña):

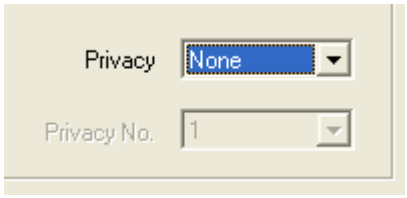


Si la contraseña consta de números del 1 al 255, el modo de contraseña tiene prioridad sobre el modo de clave de cifrado interno y Basic Privacy utiliza la contraseña como clave de cifrado. De lo contrario, utiliza la clave de cifrado interna programada en el canal activo.

Vete a **4 Show Key** :

Si está en un canal sin que el modo mejorado esté activo, recibirá este mensaje de error (porque no hay ninguna clave de cifrado interna activa):

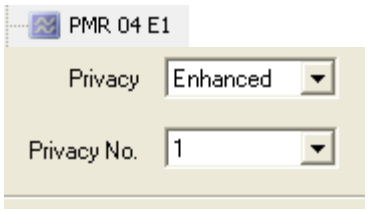




En la pantalla principal no habrá nada, lo que indica que el cifrado no está activo:

Si un canal está habilitado en modo mejorado, depende del contenido del byte situado más a la derecha de la clave de cifrado:

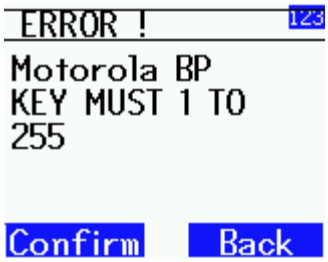
En el siguiente ejemplo, el canal E1 utiliza la clave de privacidad mejorada n.º 1:



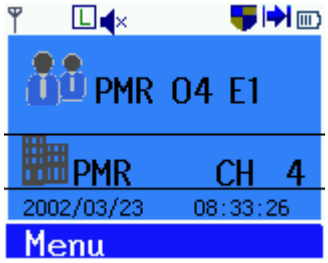
Pero el byte más a la derecha de la clave de cifrado 1 está en 0:

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

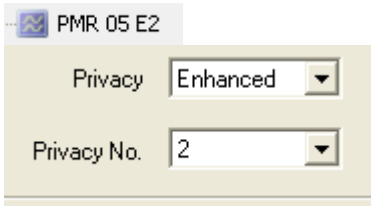
Por lo tanto, recibirá este mensaje de error en **4 Show key** :

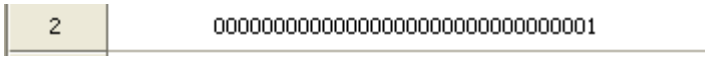


Y no se mostrará nada en la pantalla principal:

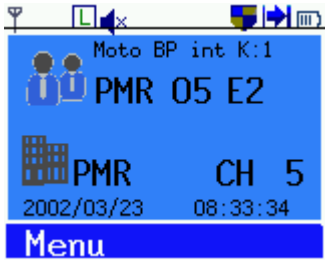


Si vamos al canal E2 que utiliza la Clave de Privacidad Nº 2:

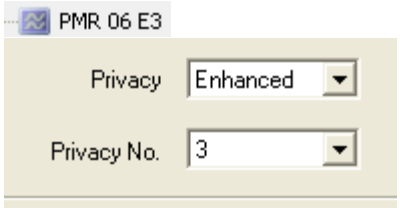




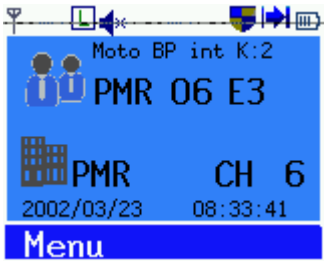
El byte más a la derecha es 01, se activará la clave de cifrado Basic Privacy 1: "Moto BP int K:1" significa "Motorola Basic Privacy internal key" y la K para el número de clave de cifrado (aquí 1).



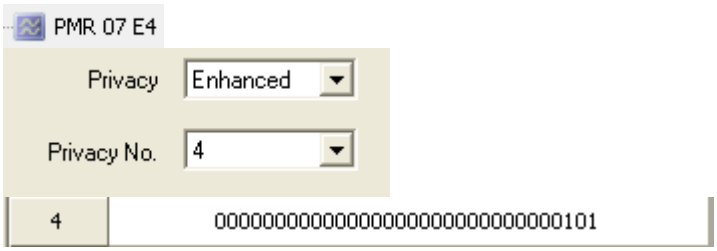
Si vamos al canal E3 que utiliza la clave de privacidad nº 3:



El byte más a la derecha es 02, es la clave de cifrado Basic Privacy 2 la que se activará:

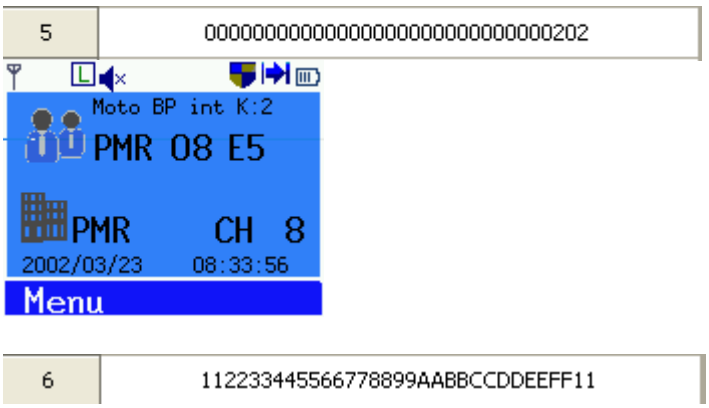


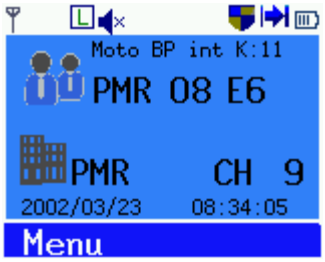
Si vamos al canal E4 que utiliza la clave de privacidad nº 4:



Hay dos bytes 01 pero es el byte más a la derecha que se utiliza para la privacidad básica, por lo que es la clave de cifrado de privacidad básica 1 la que se activará:

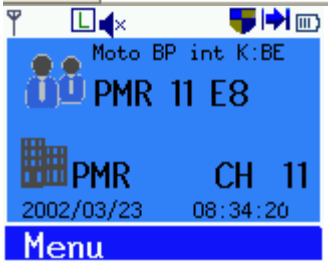
Estos son algunos ejemplos de los canales restantes:





7	74581225622174788112236655123336

8	ABCDEDCBABCDDBCABDBCABDABBABBDBE

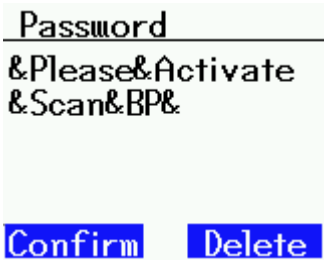


Hay una opción oculta adicional: puedes escanear y encontrar automáticamente una clave de privacidad básica de Motorola.

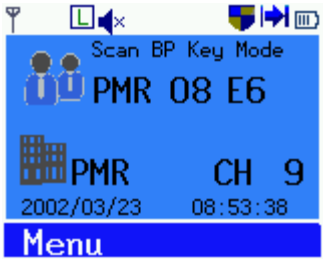
Primero debe configurar el MD380 para recibir todas las comunicaciones, este es el modo promiscuo.

Vete a:

A continuación, ve a Password y escribe la contraseña secreta:



A continuación, entrará en el modo Motorola Basic Privacy Scanner:



Espere a que comience una comunicación cifrada de privacidad básica de Motorola, tan pronto como se encuentre la clave, escuchará un pitido y la comunicación se escuchará en texto sin formato.

Una vez que se detenga la recepción, verá la llave que se encontró:

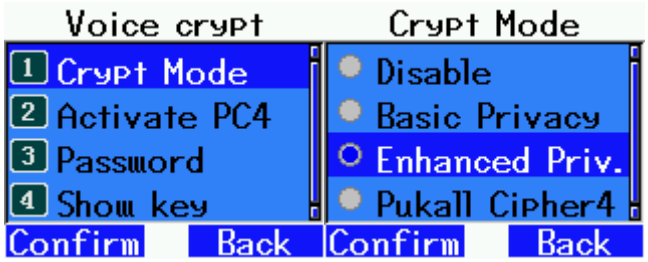
Si desea ejecutar un nuevo escaneo, puede presionar el botón PTT una vez o presionar la tecla #.

Tenga cuidado, este modo solo funciona con un dispositivo oficial de Motorola porque Motorola ha introducido una puerta trasera para escanear teclas. La puerta trasera no está presente en Voice Crypt, por lo que no puede encontrar la clave de privacidad básica de otro Voice Crypt.

Para salir del modo básico del escáner de privacidad de Motorola, puede volver a escribir la misma contraseña oculta que la anterior o apagar y volver a encender el MD380.

Modo de privacidad mejorada de Tytera con clave de cifrado interna

En **Crypt Mode** elegir **Enhanced Privacy**:



Entonces todo dependerá del canal en el que te encuentres.

Vete a **Show key :**

Si ves el mensaje de error:

Es que no estás en un canal de privacidad mejorada. A veces también hay que cambiar a otro canal y volver a él para que se tenga en cuenta.

Si se encuentra en un canal de privacidad mejorada, aparecerá la clave de cifrado de 128 bits utilizada por el algoritmo de privacidad mejorada de Tytera.

En el siguiente ejemplo es la Privacidad Nº 5:

5	00000000000000000000000000000202

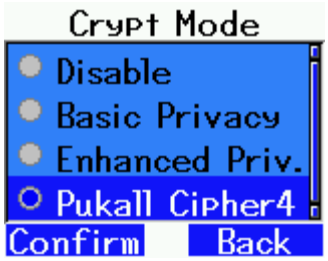
En la pantalla principal aparece "Tyt EP int K0:2": Esto significa "Tytera Enhanced Privacy internal key" con K0 (byte cero más a la derecha:2).

La clave de cifrado K0 no es la clave de cifrado completa de 128 bits (no hay suficiente espacio en la pantalla para mostrar todo), pero permite al usuario conocer el byte más a la derecha y, por lo tanto, verificar rápidamente qué clave de cifrado se utiliza. La clave de cifrado completa se muestra mediante **Show key**:

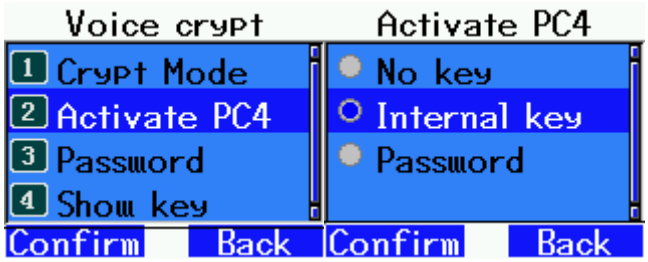
Ejemplo con otras claves de cifrado:

Modo de cifrado PC4 con clave de cifrado interna

En **Crypt Mode** elegir **PC4 Cipher**:



Vete a **2 Activate PC4** y elige **Internal key**:



Al igual que con el modo de privacidad mejorada de Tyt, la clave de cifrado utilizada dependerá del canal en el que se encuentre.

Show Key le muestra la clave de cifrado activa y la pantalla principal le muestra el byte más a la derecha de la clave de cifrado activa (vuelva a leer la sección Privacidad mejorada de Tyt si es necesario para la explicación del byte K0).

Parte avanzada de cifrado PC4

El cifrado PC4 está activo en el modo más seguro (253 rondas de cifrado). Sin embargo, algunos MD380 pueden tener un procesador demasiado lento (CPU), lo que daría como resultado una voz de mala calidad.

Es posible reducir el número de rondas de cifrado si tiene una CPU demasiado lenta. Todos los MD380 deben configurarse con el mismo número de rondas para poder comunicarse entre sí.

Este es un menú oculto, para activarlo tienes que ir a **8 Voice Crypt:**

Entonces **3 Password :**

A continuación, debe introducir una contraseña especial con minúsculas, mayúsculas y caracteres especiales : « **&Please&Activate&Round&Config&** » :

Sal del menú y vuelve al menú, ha aparecido el menú oculto:

A continuación, puede reducir el número de rondas (esto también reduce la seguridad y solo debe hacerse si la CPU es demasiado lenta y la voz es mala):

En la pantalla principal se le avisa de que está en un modo con rondas reducidas y esto se muestra para el PC4 con contraseña o el PC4 con clave de cifrado interna:

Puede hacer que este menú oculto desaparezca de nuevo volviendo a escribir la misma contraseña especial por segunda vez.

Configuración de MI

PC4 Cipher es un algoritmo de cifrado de bloques en modo ECB. Esto significa que los datos idénticos en diferentes tramas de voz se cifrarán de la misma manera si se utiliza la misma clave de cifrado. Este es el caso, por ejemplo, de los marcos de silencio.

Para evitar esto, existe una opción adicional que agrega datos aleatorios para que los fotogramas de silencio idénticos se cifren de manera diferente.

Esto aumenta la seguridad, pero disminuye la calidad de la voz porque se eliminan los bits de los fotogramas de voz.

Puede elegir entre 4 y 6 bits por trama de voz. Con 6 bits, la seguridad es mejor que con 4 bits, pero el sonido es peor.

Es un menú oculto, para activarlo tienes que ir a **8 Voice Crypt :**

Entonces **3 Password :**

A continuación, debe introducir una contraseña especial con letras minúsculas y caracteres especiales: « **&Please&Activate&MI&Config&** » :

Salga del menú y regrese al menú, el menú oculto está aquí:

En el menú principal, el MI4 o el MI6 le notificarán si está en modo MI Config.

Idealmente, todos los participantes en una discusión deberían usar la misma configuración de MI, pero esto no es obligatorio, el descifrado es posible incluso si no todos usan la misma configuración de MI.

Puede hacer que este menú oculto desaparezca de nuevo volviendo a escribir la misma contraseña especial por segunda vez.

Cifrado RC2

Voice Crypt ofrece otro modo de encriptación: RC2 en modo CFB.

Se trata de un cifrado de cifrado creado por Ron Rivest y mejorado por Alexander Pukall (eliminación de tamaños reducidos de claves de cifrado y aumento del estado interno del RC2 a 1024 bits).

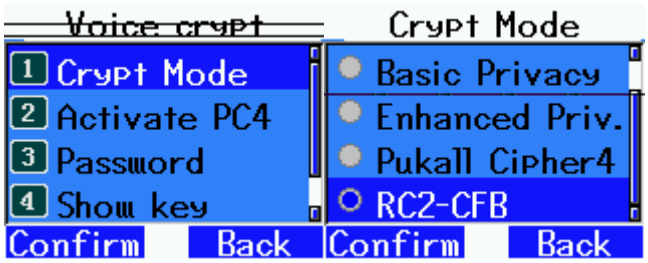
El tamaño de la clave de cifrado es de 128 bits si utiliza las claves de cifrado internas o de hasta 420 bits si utiliza una contraseña de 60 caracteres.
También utiliza una configuración MI de 6 bits, por lo que este modo RC2 degrada la calidad del sonido de la voz.

Es un menú oculto, para activarlo tienes que ir a **8 Voice Crypt :**

Entonces **3 Password :**

A continuación, debe introducir una contraseña especial con letras minúsculas y caracteres especiales: « **&Please&Activate&RC2&Encryption&** » :

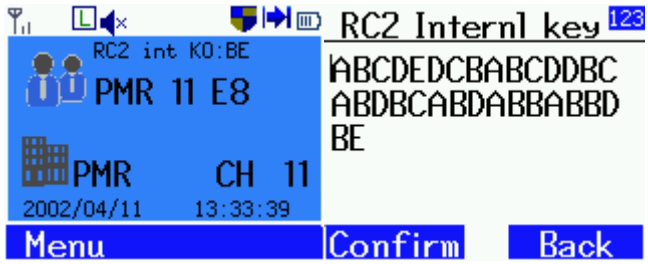
Salga del menú y regrese al menú, el menú oculto está aquí:



Puede hacer que este menú oculto desaparezca de nuevo volviendo a escribir la misma contraseña especial por segunda vez.

Para usar el modo con una contraseña, habilite **Password** en **Activate PC4** (incluso si PC4 no está activo sino RC2).

También puedes elegir **Internal Key** :



Restablecimiento

En caso de problema y si nada funciona correctamente, puede restablecer todas las opciones.

Vete a **Utilities - 4 MD380 Tools- 7 Developer – 4 Config Reset**