Voice Crypt 1.0a

高安全性语音加密，Tytera MD380/MD390 UHF 版本。

该软件基于 Travis GoodSpeed 的 MD380TOOLS，感谢他所做的所有工作。此软件不适用于 MD-UV380 和 MD-UV390。它适用于 MD380 UHF 和 MD390 UHF（带和不带 GPS）。它不适用于 VHF 版本。语音密码使用新的声码器，如果您的 MD380 与新的声码器不兼容，那么您将无法使用它。

摩托罗拉基本隐私模式属于摩托罗拉，感谢他们所做的工作。基本隐私模式没有专利。

(Enhanced Privacy) 增强隐私模式使用 128 位 AES 加密，属于 Tytera 的工作。但是，它是 AES 的降级模式，而摩托罗拉的 AES 更安全。

PC4 密码模式属于 Alexander Pukall，感谢他所做的工作。

语音加密不包含 ARC4 和 AES 摩托罗拉加密，因为存在专利并阻止其合法使用，这就是为什么选择 PC4 密码模式的原因，因为它是免版税的。

该软件是免费的，它是一个免费软件。

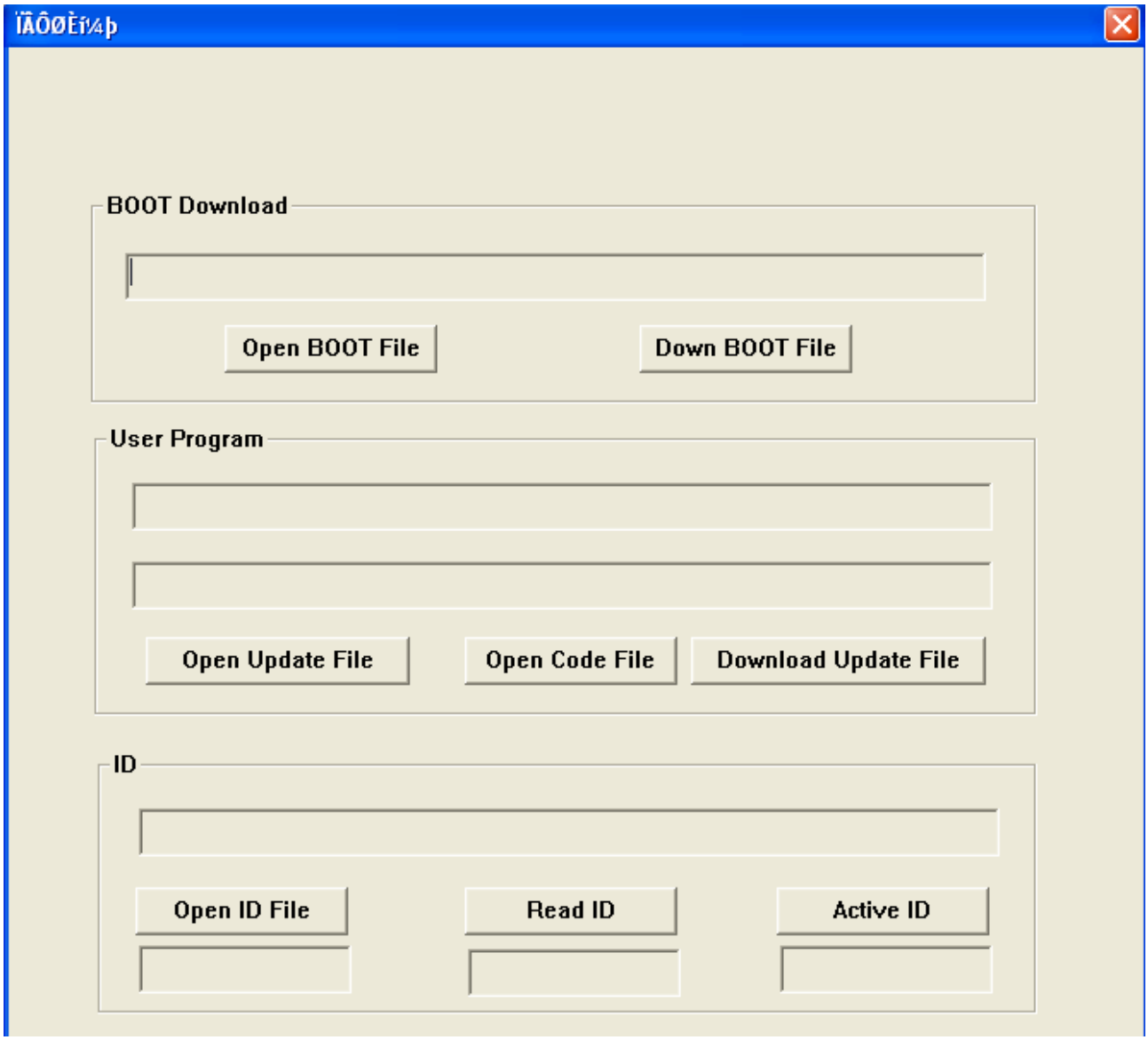
本手册采用 RTF 格式，因此如果您想分发带有翻译成您自己的语言的语音地穴，您可以将其翻译成您的语言。

如何刷新固件

语音加密基于固件 D013.020（无 GPS）和 S013.020（带 GPS）。如果 MD380/390 闪烁后未打开，则表示它与版本 013.20 不兼容。然后，您需要重新刷新原始固件。

要刷新 MD380，请启动升级.exe 程序 (Upgrade.exe)：

在关闭 MD380 时，同时按下 1 和 PTT 键（左侧顶部的 2 个键），并且不松开键打开 MD380（通过转动音量旋钮）。屏幕不显示任何内容，但指示灯呈红/绿闪烁，MD380 已准备好闪烁。


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

点击 **Open Update File**, 选择 GPS 的语音加密固件或不带 GPS，然后单击 **Download Update File.**

语音加密在 MD380 上闪烁。最后关闭 MD380 并重新打开。

建议在闪烁后进行重置，以确保 Voice Crypt 正常工作（请参阅本手册末尾的重置部分）。

如何快速入门

带密码的摩托罗拉基本隐私模式

此模式与接收中的摩托罗拉基本隐私无线电（RX）兼容。它可以在基本隐私中传输，但是如果没有 Pi 标头帧，摩托罗拉电台将无法识别它是基本隐私中的加密广播。另一方面，两个 MD380 都将能够在基本隐私下发送和接收。

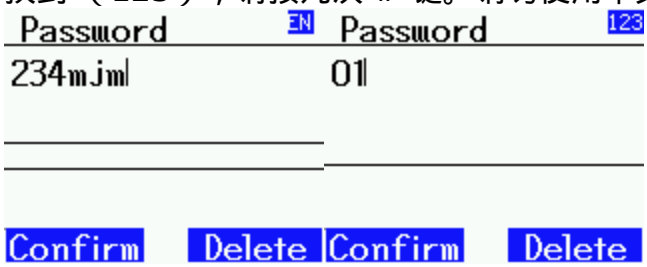
要对其进行配置，请转到：

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

然后转到：

3 Password

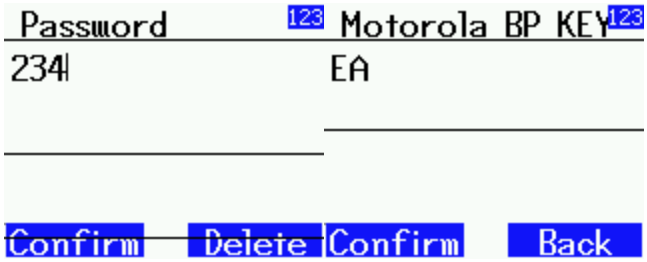
以十进制格式（从 1 到 255）输入要使用的加密密钥。您可以写 1、01 或 001。不要忘记切换到数字模式（123）来写数字，否则您将处于字母模式（EN）。要从 （EN） 模式切换到 （123），请按几次 # 键。请勿使用中文模式，因为它不受支持。



检查是否在以下位置启用了加密密钥：

4 Show key

如果显示摩托罗拉 BP KEY 01，则表示加密密钥已激活。
尝试使用 234 加密密钥 **3 Password**, 然后看 **4 Show Key**, 加密密钥以十六进制书写：EA



这是相同的加密密钥，但 **Show Key** 以十六进制显示加密密钥。

然后，您可以在基本隐私中发送和接收。主屏幕告诉你 "Moto BP pas"为 "Motorola Basic Privacy password"和 "K:EA" 加密密钥"EA"n 十六进制格式。

您可以使用相同的加密密钥与另一个 MD380 通信，也可以使用相同的加密密钥收听摩托罗拉收音机。

您可以更改 Moto BP 加密密钥，而无需使用向上和向下箭头重新键入密码。为此，您必须首先通过连续按 * 键 3 次来解锁这些键。

解锁箭头后，可以使用向上箭头将加密密钥增加 +1，或使用底部箭头将加密密钥减少 -1。

在传输过程中，不能使用向上和向下箭头更改加密密钥。另一方面，在接待处，您可以使用向上和向下箭头更改钥匙。如果您正在"基本隐私"中收听加密频道，但不知道加密密钥，则可以使用向上和向下箭头尝试 255 个可能的加密密钥（从 1 到 FF 的十六进制）。加密密钥正确后，您将清楚地听到对话。对话结束时，您将看到已停止的加密密钥。

带密码的 PC4 密码模式

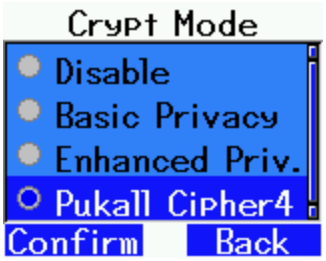
Alexander Pukall 开发的 PC4 密码使用从 8 位到 2212 位的加密密钥，具体取决于密码或加密密钥的长度。它在专门为 DMR 无线电模式创建的 ECB 模式下工作，并且非常安全。

语音加密允许您使用从 112 位到 420 位的加密密钥，仅仅是因为 MD380 的屏幕无法正确显示更多字符。由于 VOICE CRYPT 不允许使用中文字符，因此使用英语 ASCII 字符（字母，数字，特殊字符）。ASCII 字符为 7 位。

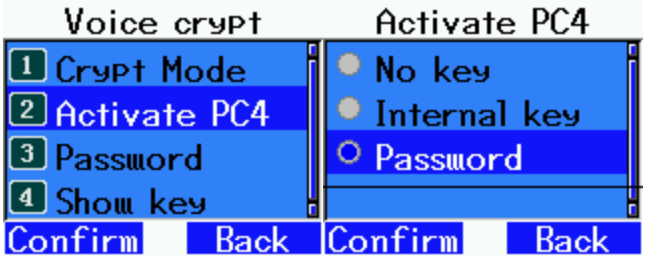
语音密码允许密码的范围从 16 个字符到 60 个字符。因此，我们获得从 112 位 （16*7）到 420 位 （60*7） 的加密密钥。我们相信这足以应对所有可能的未经授权窃听的威胁。

PC4 密码是免版税的，属于公共领域，因此在 Voice Crypt 中使用它不会侵犯任何摩托罗拉专利。

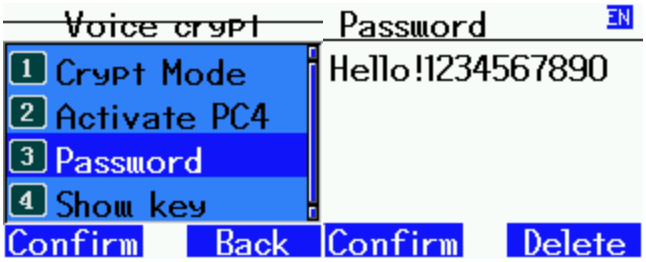
转到
Menu – Utilities – 4 Md380Tools – 8 Voice Crypt – 1 Crypt Mode – Pukall Cipher 4



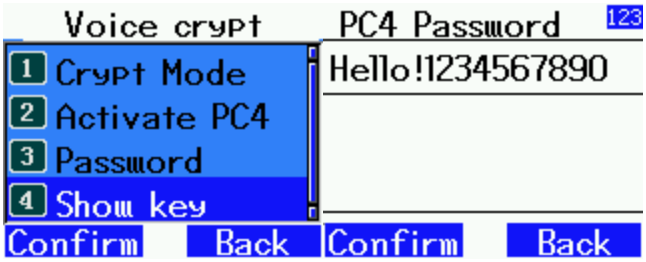
然后 **2 Activate PC4** ，然后选择 **Password**：



然后转到 **3 Password**，然后输入至少 16 个字符（最多 60 个字符）的密码：



您可以通过单击 **4 Show key** 您应该会看到您输入的相同密码，这意味着 PC4 已启用：



在主屏幕上，您应该会看到 "PC4 password" 这意味着 PC4 在"密码"模式下激活（请注意，只有当显示模式设置为 OFF 时，您才会看到它）。

然后，您可以安全地与使用相同密码的另一台 MD380 通信。

模式显示 ：

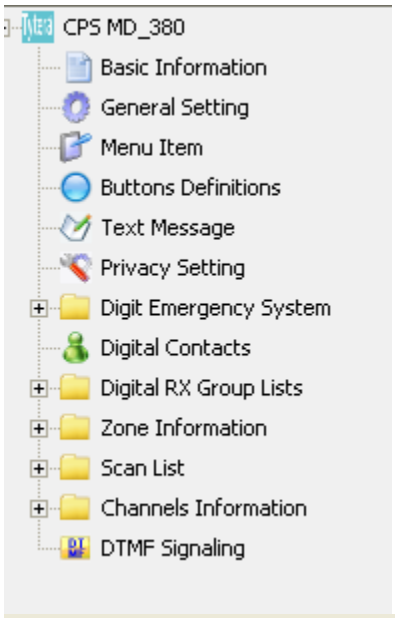
要在主屏幕上查看加密激活情况，MD380Tools 显示模式必须设置为 OFF，否则您将看不到它。

您可以通过转到 **Menu Utilities – 4 MD380Tools – 1 Display -4 Mode Display**

使用内部加密密钥的加密模式

Tytera 的编程软件（CPS）允许您输入 DMR 通道的加密密钥。

在 Tytera CPS 中，您可以单击隐私设置以查看加密密钥：



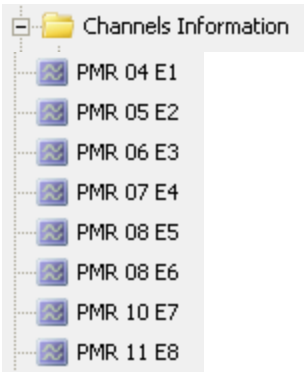
No.	Key Value(Basic)
1	FFFF
2	FFFF
3	FFFF
4	FFFF
5	FFFF
6	FFFF
7	FFFF
8	FFFF
9	FFFF
10	FFFF
11	FFFF
12	FFFF
13	FFFF
14	FFFF
15	FFFF
16	FFFF

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

不要使用该列 (Basic), 始终使用该列 (Enhanced) 放置 128 位加密密钥（16 个十六进制字符），例如，您可以创建 8 个加密密钥：

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

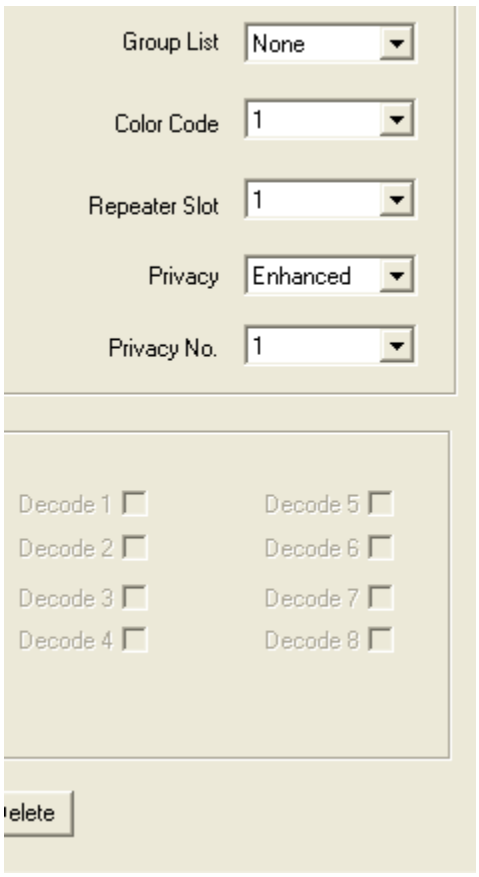
在"频道信息"部分中，您可以配置频道：



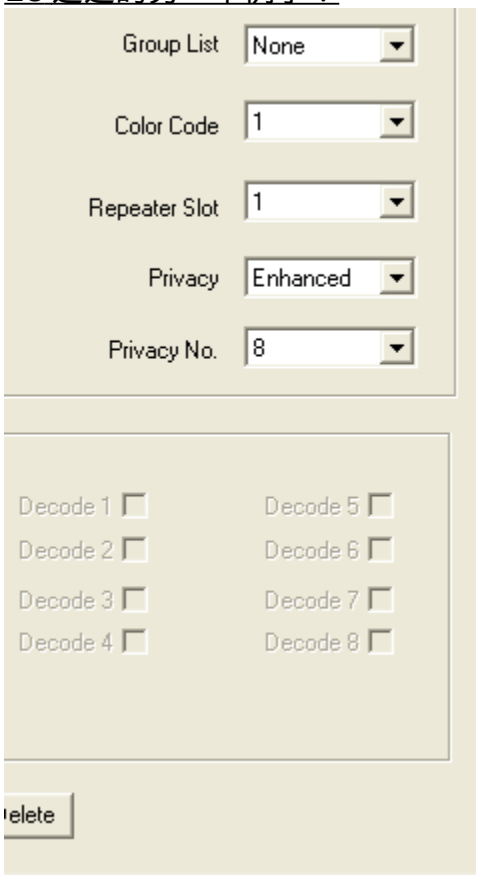
E1 代表增强型隐私通道 1，E2 增强型隐私通道 2...

打开通道 E1，我们看到：

在右下角，我们观察到 Enhanced 和加密密钥编号，在这里 Privacy Key No. 1.


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

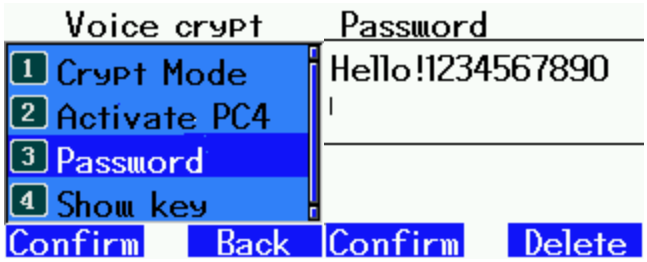
E8 通道的另一个例子：


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

带内部加密密钥的摩托罗拉基本隐私模式

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

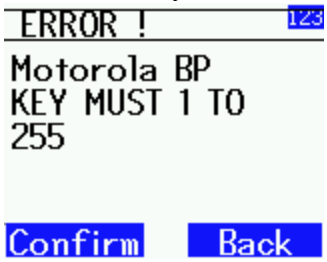
转到 **3 Password** 并键入超过 4 个字符的密码（或根本没有密码）：

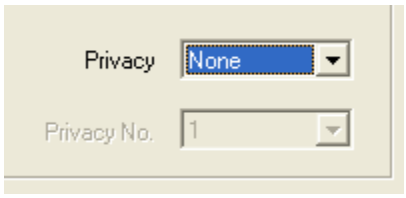


如果密码由 1 到 255 之间的数字组成，则密码模式优先于内部加密密钥模式，基本隐私使用密码作为密钥。否则，它使用在活动通道上编程的内部密钥。

转到 **4 Show Key**：

如果您在增强模式下未处于活动状态的通道上，则会收到以下错误消息（因为没有活动的内部加密密钥）：

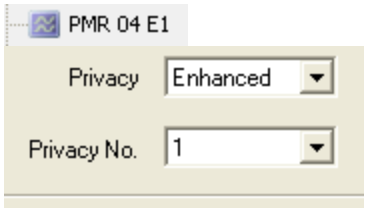




在主屏幕上将没有任何内容，表明加密未处于活动状态：

如果在增强模式下启用了通道，则取决于密钥最右侧字节的内容：

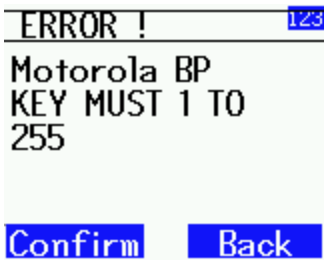
在以下示例中，通道 E1 使用增强型隐私密钥 1：



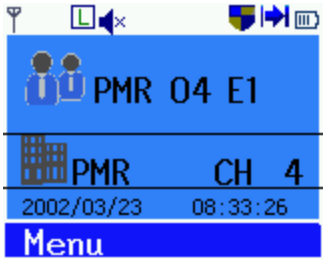
但键 1 的最右边字节为 0：

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

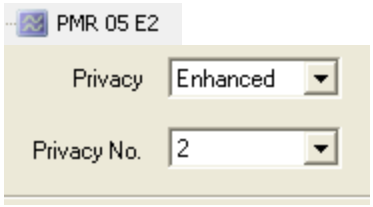
因此，您会收到一条错误消息 **Show Key**：

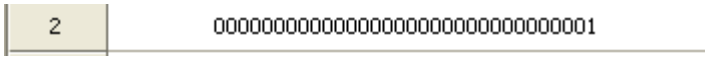


主屏幕上不会显示任何内容：

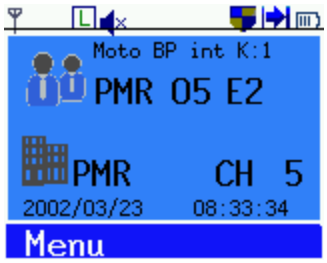


如果我们转到使用隐私密钥 2 的频道 E2：

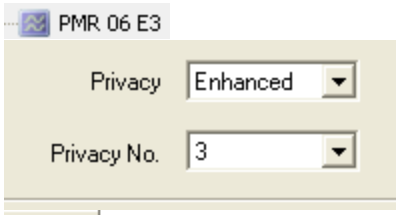




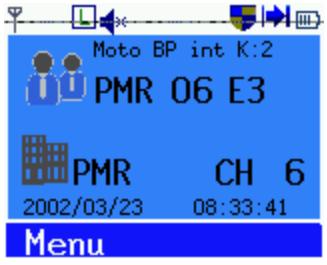
最右边的字节是 01，基本隐私 1 加密密钥将被激活："Moto BP int K：1 代表"摩托罗拉基本隐私内部密钥"，K 代表加密密钥号（此处为 1）。



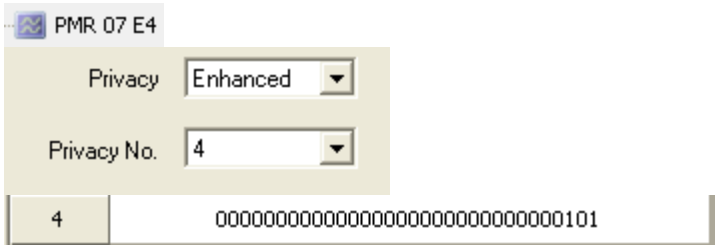
如果我们转到使用 3 号隐私密钥的 E3 通道：



最右边的字节是 02，这是将被激活的基本隐私 2 加密密钥：

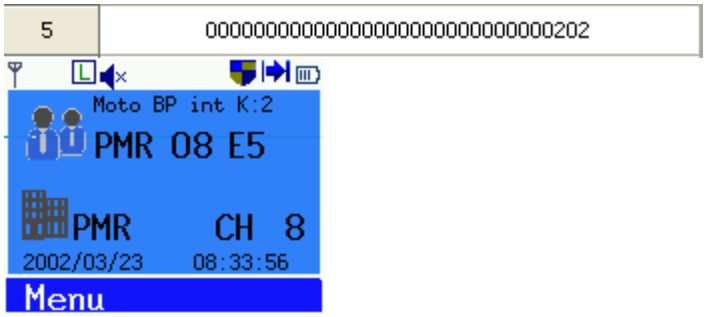


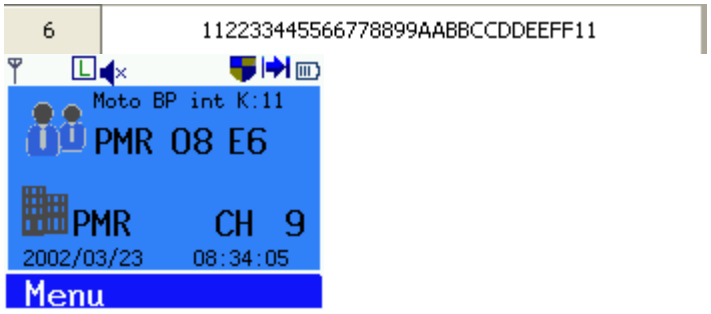
如果我们转到使用 4 号隐私密钥的频道 E4：

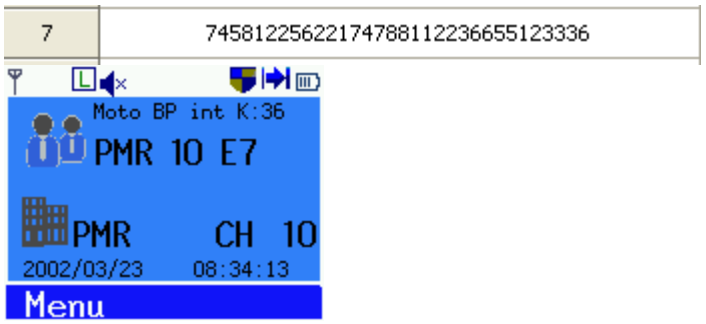


有两个字节 01，但它是用于基本隐私的最右边字节，因此激活了基本隐私 1 加密密钥：

以下是其余渠道的示例：







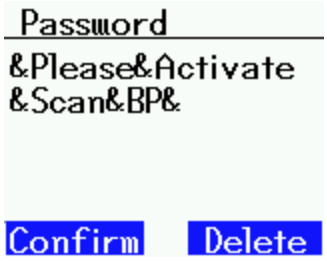

Moto BP int K:BE
PMR 11 E8
PMR
CH 11
2002/03/23
08:34:20
Menu

还有一个额外的隐藏选项：您可以扫描并自动找到摩托罗拉基本隐私密钥。

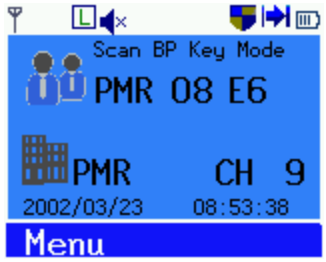
您必须首先配置 MD380，以便它接收所有通信，这就是混杂模式。

转到：

然后转到密码并输入秘密密码：



然后切换到摩托罗拉基本隐私扫描程序模式：



等待加密的摩托罗拉基本隐私通信开始，一旦软件找到加密密钥，您将听到哔哔声，然后清楚地听到通信。

接收停止后，您将看到找到的加密密钥：

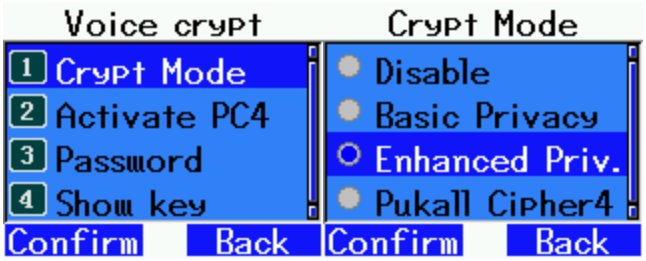
如果要重新启动新扫描，可以按一次 PTT 键或按 # 键。

请注意，此模式仅在扫描摩托罗拉官方设备时可用，因为摩托罗拉引入了后门来扫描加密密钥。此 MD380 固件中没有后门，因此找不到其他 MD380 基本隐私密钥。

要退出摩托罗拉基本隐私扫描仪模式，您可以重新键入与上述相同的隐藏密码或关闭 MD380 并重新打开。

Tytera 具有内部加密密钥的增强隐私模式

转到 **Crypt Mode** 选择 **Enhanced Privacy**:



然后一切都取决于您所在的频道。

转到 **Show key :**

如果您看到错误消息：

这是因为您不在增强型隐私频道上。有时您还必须切换到另一个频道并返回该频道，以便将其考虑在内。

如果您使用的是增强型隐私通道，则会显示 Tytera 增强型隐私算法使用的 128 位加密密钥。

在下面的示例中，它是隐私 5：

5	00000000000000000000000000000202

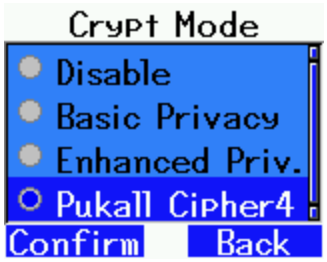
在主屏幕上出现 "Tyt EP int K0:2": 这意味着增强的隐私 内部加密密钥具有 K0（最右边的零字节：2）。

K0 字节不是一个完整的 128 位加密密钥（屏幕上没有足够的空间来显示所有内容），但它允许用户知道最右边的字节，允许快速检查使用了哪个加密密钥。对显示密钥使用完全加密的密钥：**Show key**:

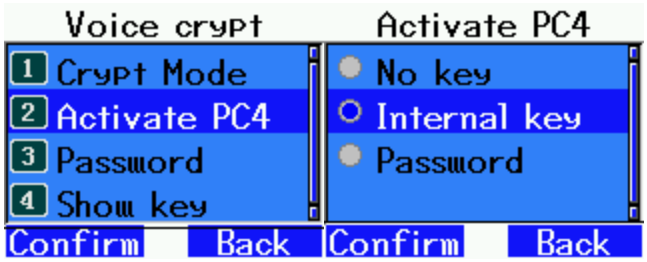
其他键示例：

具有内部加密密钥的 **PC4** 密码模式

转到 **Crypt Mode** 选择 **PC4 Cipher**:



转到 **2 Activate PC4**，然后选择 **Internal key**:



与 Tytera 增强型隐私模式一样，使用的加密密钥将取决于您所在的频道。

Show Key 将显示活动加密密钥，主屏幕显示活动加密密钥的最右侧字节（如有必要，请重新阅读 Tyt 增强隐私部分以解释 K0 字节）。

PC4 密码高级部分

PC4 密码在最安全的模式下处于活动状态（253 轮加密）。但是，某些 MD380 的处理器（CPU）可能太慢，这会导致语音质量差。

如果您的 CPU 速度太慢，您可以减少加密轮数。然后，所有 MD380 必须配置相同的轮数才能相互通信。

这是一个隐藏的菜单，要激活它，您必须转到 **8 Voice Crypt:**

转到 **3 Password :**

然后，您必须输入包含小写大写和特殊字符的特殊密码：
« **&Please&Activate&Round&Config&** »：

退出菜单并返回菜单，隐藏的菜单已经出现：

然后，您可以减少回合数（这也降低了安全性，并且只有在 CPU 太慢且声音不好时才应这样做）：

在主屏幕上，系统会警告您处于缩小回合模式，对于带有密码的 PC4 或带有内部加密密钥的 PC4，将显示该模式：

您可以通过再次重新键入相同的特殊密码来使此隐藏菜单再次消失。

MI 配置

PC4 密码是一种 ECB 模式分组密码算法。这意味着，如果使用相同的加密密钥，则不同语音帧中的相同数据将以相同的方式进行加密。例如，静音帧就是这种情况。

为了避免这种情况，存在一个附加选项，用于添加随机数据，以便以不同的方式加密相同的静默帧。

这提高了安全性，但会降低语音质量，因为语音帧中的位被删除了。

您可以选择每个语音帧的 4 到 6 位。使用 6 位，安全性比 4 位更好，但声音更差。

这是一个隐藏的菜单，要激活它，您必须转到 **8 Voice Crypt :**

然后 **3 Password :**

然后，您必须输入一个包含小写字母和特殊字符的特殊密码：
« **&Please&Activate&MI&Config&** » :

退出菜单并返回菜单，隐藏菜单在这里：

在主菜单上，如果您处于 MI 配置模式，您将收到 MI4 或 MI6 的通知。

理想情况下，讨论中的所有参与者都应使用相同的 MI 配置，但这不是强制性的，即使不是每个人都使用相同的 MI 配置，也可以解密。

您可以通过再次重新键入相同的特殊密码来使此隐藏菜单再次消失。

RC2 加密

Voice Crypt 提供了另一种加密模式：CFB 模式下的 RC2。

这是由 Ron Rivest 创建并由 Alexander Pukall 改进的加密密码（删除了减小的加密密钥大小并将 RC2 的内部状态增加到 1024 位）。

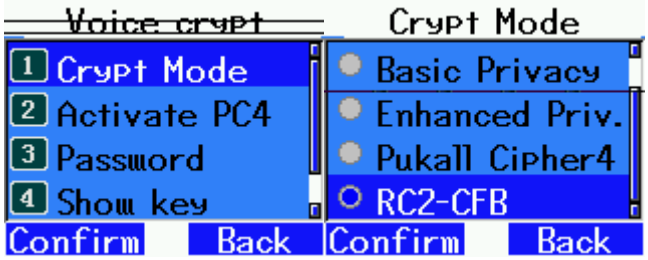
如果使用内部加密密钥，则加密密钥大小为 128 位，如果使用 60 个字符的密码，则最大为 420 位。
它还使用 6 位 MI 配置，因此此 RC2 模式会降低语音的音质。

这是一个隐藏的菜单，要激活它，您必须转到 **8 Voice Crypt :**

然后 **3 Password :**

然后，您必须输入一个包含小写字母和特殊字符的特殊密码：
« **&Please&Activate&RC2&Encryption&** »：

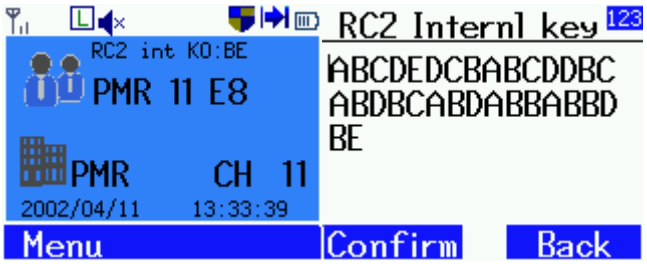
退出菜单并返回菜单，隐藏菜单在这里：



您可以通过再次重新键入相同的特殊密码来使此隐藏菜单再次消失。

要使用带密码的模式，请在激活 PC4 中启用"密码"（即使 PC4 未处于活动状态，但 RC2 处于活动状态）。

您也可以选择 **Internal Key**：



重置

如果出现问题并且没有任何工作正常，您可以重置所有选项。

转到 **Utilities - 4 MD380 Tools- 7 Developer – 4 Config Reset**