

# Voice Crypt 1.0a

Hochsichere Sprachverschlüsselung für die UHF-Version Tytera MD380/MD390.

Diese Software basiert auf MD380TOOLS von Travis GoodSpeed, vielen Dank an ihn für die geleistete Arbeit. Diese Software funktioniert nicht auf MD-UV380 und MD-UV390. Es funktioniert auf dem MD380 UHF und MD390 UHF (mit und ohne GPS). Es funktioniert nicht auf VHF-Versionen. Voice Crypt verwendet den neuen Vocoder, wenn Ihr MD380 nicht mit dem neuen Vocoder kompatibel ist, können Sie ihn nicht verwenden.

Der Motorola Basic Privacy-Modus gehört zu Motorola, vielen Dank an sie für die geleistete Arbeit. Für den Basic Privacy-Modus gibt es kein Patent.

Der erweiterte Datenschutzmodus verwendet eine 128-Bit-AES-Verschlüsselung und gehört Tytera, danke ihm für die geleistete Arbeit. Es ist jedoch ein verschlechterter Modus des AES und viel weniger sicher als das AES von Motorola.

Der PC4 Cipher-Modus gehört Alexander Pukall, vielen Dank an ihn für die geleistete Arbeit.

Voice Crypt enthält keine ARC4- und AES-Verschlüsselung von Motorola, da ein Patent existiert und die legale Nutzung verhindert, weshalb der PC4-Verschlüsselungsmodus gewählt wurde, da er lizenzfrei ist.

Diese Software ist kostenlos, es ist eine Freeware.

Dieses Handbuch ist im RTF-Format, so dass Sie es in Ihre Sprache übersetzen können, wenn Sie Voice Crypt mit einer Übersetzung in Ihre eigene Sprache vertreiben möchten.

## **So flashen Sie die Firmware**

Voice Crypt basiert auf den Firmware D013.020 (ohne GPS) und S013.020 (mit GPS). Wenn sich Ihr MD380/390 nach dem Flashen nicht einschalten lässt, ist es nicht mit Version 013.20 kompatibel. Sie müssen dann Ihre ursprüngliche Firmware neu flashen.

Um Ihren MD380 zu flashen, starten Sie das Programm Upgrade.exe:

Drücken Sie bei ausgeschaltetem MD380 gleichzeitig die Tasten 1 und PTT (die oberen 2 Tasten links) und schalten Sie den MD380 ein, ohne die Tasten loszulassen (durch Drehen des Lautstärkereglers). Der Bildschirm zeigt nichts an, aber die LED blinkt rot/grün, das MD380 ist bereit zum Blinken.

IAÖØÊ¼þ

BOOT Download

Open BOOT FileDown BOOT File

User Program

Open Update FileOpen Code FileDownload Update File

ID

Open ID FileRead IDActive ID



正在升级软件.....

BOOT Download

User Program

ID

Klicken **Open Update File**, wählen Sie die Voice Crypt-Firmware für GPS oder ohne GPS und klicken Sie auf **Download Update File**.

Voice Crypt ist auf dem MD380 geflasht. Schalten Sie den MD380 am Ende aus und wieder ein.

Es wird empfohlen, nach dem Flashen einen Reset durchzuführen, um sicherzustellen, dass Voice Crypt ordnungsgemäß funktioniert (siehe Abschnitt **Zurücksetzen** ganz am Ende dieser Anleitung).

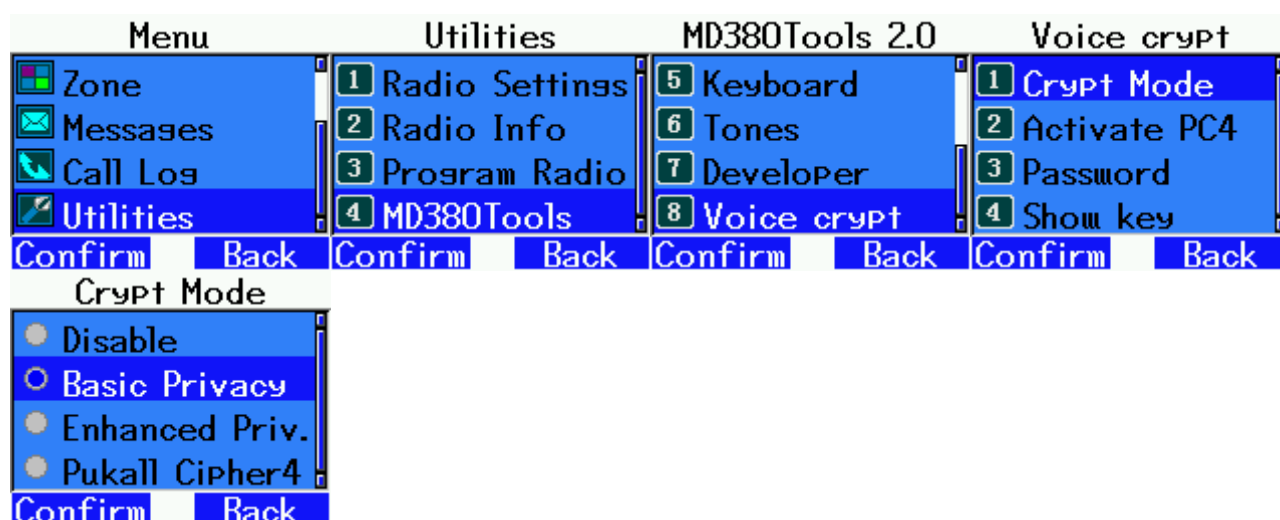
## So legen Sie schnell los

### Motorola Basic Privacy Mode mit Passwort

Dieser Modus ist mit einem Motorola Basic Privacy Radio im Empfang (RX) kompatibel. Es kann in Basic Privacy senden, aber ohne einen Pi-Header-Frame kann ein Motorola-Radio nicht erkennen, dass es sich um eine verschlüsselte Sendung in Basic Privacy handelt. Auf der anderen Seite werden zwei MD380 in der Lage sein, in Basic Privacy zu senden und zu empfangen.

Um es zu konfigurieren, gehen Sie zu:

**Menu - Utilities - 4 Md380Tools - 8 Voice Crypt - 1 Crypt Mode - Basic Privacy**



Dann gehen Sie zu:

### **3 Password**



Geben Sie den Verschlüsselungsschlüssel, den Sie verwenden möchten, im Dezimalformat (von 1 bis 255) ein. Sie können 1, 01 oder 001 schreiben. Vergessen Sie nicht, in den numerischen Modus (123) zu wechseln, um die Zahlen zu schreiben, sonst befinden Sie sich im alphabetischen Modus (EN). Um vom (EN)-Modus in den (123) Modus zu wechseln, drücken Sie mehrmals die #-Taste. Verwenden Sie nicht den chinesischen Modus, da er nicht unterstützt wird.

Passw0rd	EN	Passw0rd	123
234mjml		01	
Confirm	Delete	Confirm	Delete

Überprüfen Sie, ob der Verschlüsselungsschlüssel aktiviert ist in:

#### 4 Show key

Voice crypt	
1	Crypt Mode
2	Activate PC4
3	Passw0rd
4	Show key
Confirm	Back

Wenn Motorola BP KEY 01 angezeigt wird, bedeutet dies, dass der Verschlüsselungsschlüssel aktiviert ist.

Probieren Sie es mit dem Verschlüsselungsschlüssel 234 aus **3 Password**, dann schau rein **4 Show Key** klicken, wird der Verschlüsselungsschlüssel hexadezimal geschrieben: EA

Passw0rd	123	Motorola BP KEY	123
234		EA	
Confirm	Delete	Confirm	Back

Es ist derselbe Verschlüsselungsschlüssel, aber **Show Key** zeigt die Verschlüsselungsschlüssel in hexadezimaler Form an.

Sie können dann in Basic Privacy senden und empfangen. Auf dem Hauptbildschirm werden "Moto BP pas" für "Motorola Basic Privacy password" und "K:EA" für den aktiven "EA"-Verschlüsselungsschlüssel in hexadezimaler Form angezeigt.

Sie können mit demselben Verschlüsselungsschlüssel mit einem anderen MD380 kommunizieren oder ein Motorola-Radio hören.



Sie können den Moto BP-Verschlüsselungsschlüssel ändern, ohne das Passwort mit den Pfeiltasten nach oben und unten erneut eingeben zu müssen. Dazu müssen Sie diese Tasten zunächst entsperren, indem Sie die Taste \* 3 Mal hintereinander drücken.

Sobald die Pfeile entsperrt sind, können Sie den Verschlüsselungsschlüssel mit dem Pfeil nach oben um +1 erhöhen oder mit dem unteren Pfeil um -1 verringern.

In der Ausgabe (TX) können Sie den Verschlüsselungsschlüssel nicht mit den Pfeiltasten nach oben und unten ändern. Auf der anderen Seite können Sie beim Empfang (RX) die Pfeile nach oben und unten verwenden, um den Verschlüsselungsschlüssel zu ändern. Wenn Sie einen verschlüsselten Kanal in Basic Privacy hören und den Verschlüsselungsschlüssel nicht kennen, können Sie die Pfeile nach oben und unten verwenden, um die 255 möglichen Verschlüsselungsschlüssel (von 1 bis FF in hexadezimaler Form) auszuprobieren. Sobald der Verschlüsselungsschlüssel korrekt ist, hören Sie das Gespräch deutlich. Sobald die Konversation beendet ist, sehen Sie auf dem Verschlüsselungsschlüssel, den Sie gestoppt haben.

## PC4-Chiffriermodus mit Passwort

Die von Alexander Pukall entwickelte PC4-Chiffre verwendet Verschlüsselungsschlüssel von 8 Bit bis 2212 Bit, je nach Länge des Passworts oder des Verschlüsselungsschlüssels. Es arbeitet im ECB-Modus, wurde speziell für den DMR-Funkmodus entwickelt und ist extrem sicher.

Mit Voice Crypt können Sie Verschlüsselungsschlüssel von 112 Bit bis 420 Bit verwenden, da der Bildschirm des MD380 nicht mehr Zeichen korrekt anzeigt. Da Voice Crypt die Verwendung chinesischer Schriftzeichen nicht zulässt, werden englische Ascii-Zeichen (Buchstaben, Zahlen, Sonderzeichen) verwendet. Ein ASCII-Zeichen ist 7-Bit.

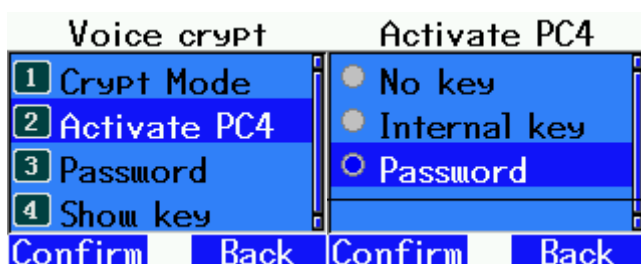
Voice Crypt erlaubt Passwörter mit einer Länge von 16 bis 60 Zeichen. Wir erhalten also Verschlüsselungsschlüssel von 112 Bit ( $16 \cdot 7$ ) bis 420 Bit ( $60 \cdot 7$ ). Wir glauben, dass dies mehr als genug ist, um allen möglichen Bedrohungen durch unbefugtes Abhören zu begegnen.

Die PC4-Verschlüsselung ist lizenzfrei und gemeinfrei, so dass sie kein Motorola-Patent verletzt, um sie in Voice Crypt zu verwenden.

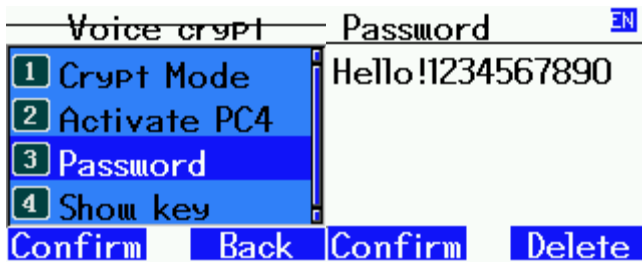
Gehe zu **Menu - Utilities - 4 Md380Tools - 8 Voice Crypt - 1 Crypt Mode - Pukall Cipher 4**



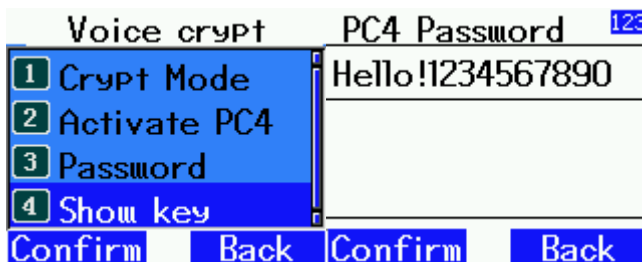
Dann **2 Activate PC4** und wählen Sie **Password** :



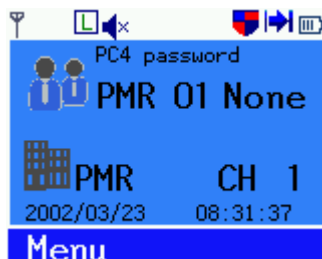
Gehen Sie dann zu **3 Password** und geben Sie ein Passwort mit mindestens 16 Zeichen (bis zu 60 Zeichen) ein:



Sie können überprüfen, ob PC4 aktiviert ist, indem Sie auf **4 Show key** und Sie sollten dasselbe Passwort sehen, das Sie eingegeben haben, was bedeutet, dass PC4 aktiviert ist:



Auf dem Hauptbildschirm sollten Sie dann sehen "PC4 password". Dies bedeutet, dass PC4 im "Passwort"-Modus aktiviert ist (Achtung, Sie sehen es nur, wenn der Anzeigemodus auf AUS eingestellt ist).





Sie können dann sicher mit einem anderen MD380 kommunizieren, der dasselbe Kennwort verwendet.

### **Modus-Anzeige:**

Um die Aktivierung der Verschlüsselung auf dem Hauptbildschirm zu sehen, muss der MD380Tools-Anzeigemodus auf OFF gestellt sein, sonst wird er nicht angezeigt.

Sie können dies überprüfen, indem Sie zu **Menu Utilities - 4 MD380Tools - 1 Display -4 Mode Display**

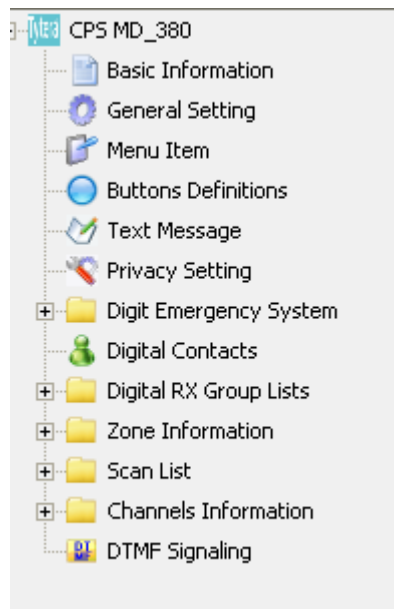


Menu	Utilities	MD380Tools 2.0	Display Setup
 Zone  Messages  Call Log  Utilities	1 Radio Settings 2 Radio Info 3 Program Radio 4 MD380Tools	1 Display 2 Radio 3 DMR Setup 4 SMS Service	1 Backlight 2 Date/Status 3 Show Calls 4 Mode Display
Confirm Back	Confirm Back	Confirm Back	Confirm Back
Mode Display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

## Modi mit internen Verschlüsselungsschlüsseln

Mit der Programmiersoftware (CPS) von Tytera können Sie Verschlüsselungsschlüssel für DMR-Kanäle eingeben.

Im Tytera CPS können Sie auf "Privacy Settings" klicken, um die Verschlüsselungsschlüssel anzuzeigen:



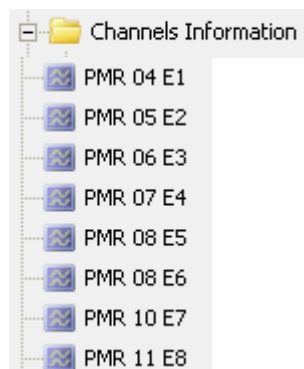
No.	Key Value(Basic)
1	FFFF
2	FFFF
3	FFFF
4	FFFF
5	FFFF
6	FFFF
7	FFFF
8	FFFF
9	FFFF
10	FFFF
11	FFFF
12	FFFF
13	FFFF
14	FFFF
15	FFFF
16	FFFF

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

Verwenden Sie nicht die Spalte (Basic), Verwenden Sie immer die Spalte (Enhanced) um 128-Bit-Verschlüsselungsschlüssel (16 Hexadezimalzeichen) einzufügen, können Sie 8 Verschlüsselungsschlüssel erstellen, z. B.:

No.	Key Value(Enhanced)
1	00000000000000000000000000000000
2	00000000000000000000000000000001
3	00000000000000000000000000000002
4	000000000000000000000000000000101
5	000000000000000000000000000000202
6	112233445566778899AABBCCDDEEFF11
7	74581225622174788112236655123336
8	ABCDEDCBABCDDBCABDBCABDABBABDBE

Im Abschnitt "Channels information" können Sie Ihre Kanäle konfigurieren:



E1 steht für Enhanced Privacy Channel 1, E2 Enhanced Privacy Channel 2...

Wenn wir Kanal E1 öffnen, sehen wir:

Unten rechts sehen wir Enhanced und die Schlüsselnummer, hier Privacy Key No. 1.

Group List

Color Code

Repeater Slot

Privacy

Privacy No.

Decode 1 ☐ Decode 5 ☐

Decode 2 ☐ Decode 6 ☐

Decode 3 ☐ Decode 7 ☐

Decode 4 ☐ Decode 8 ☐

Ein weiteres Beispiel mit dem E8-Kanal:

Group List

Color Code

Repeater Slot

Privacy

Privacy No.

Decode 1 ☐ Decode 5 ☐

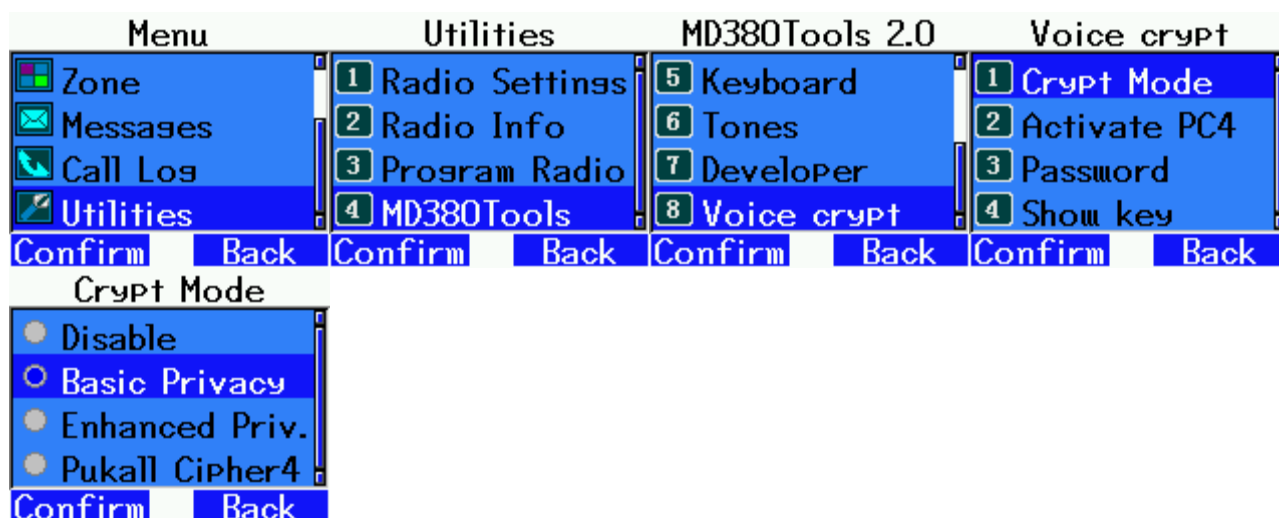
Decode 2 ☐ Decode 6 ☐

Decode 3 ☐ Decode 7 ☐

Decode 4 ☐ Decode 8 ☐

## Motorola Basic Privacy Mode mit internem Verschlüsselungsschlüssel

**Menu - Utilities - 4 MD380Tools - 8 Voice Crypt - 1 Crypt Mode - Basic Privacy**

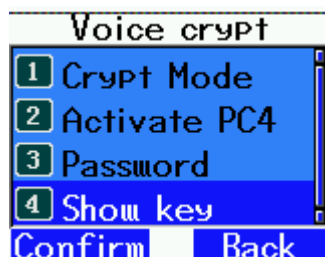


Gehe zu **3 Password** und geben Sie ein Passwort ein, das länger als 4 Zeichen ist (oder gar kein Passwort):

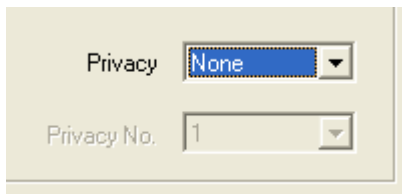
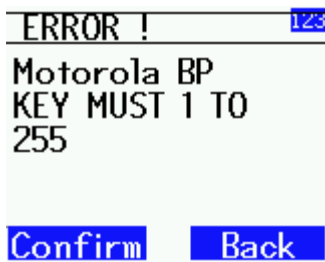


Wenn das Passwort aus Zahlen von 1 bis 255 besteht, hat der Passwortmodus Vorrang vor dem internen Schlüsselmodus und Basic Privacy verwendet das Passwort als Verschlüsselungsschlüssel. Andernfalls wird der interne Verschlüsselungsschlüssel verwendet, der auf dem aktiven Kanal programmiert ist.

Gehe zu **4 Show Key** :



Wenn Sie sich auf einem Kanal befinden, auf dem der erweiterte Modus nicht aktiv ist, erhalten Sie diese Fehlermeldung (da kein aktiver interner Verschlüsselungsschlüssel vorhanden ist):

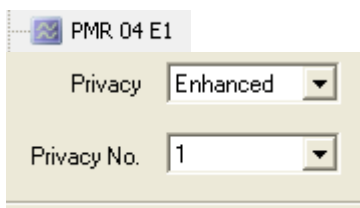


Auf dem Hauptbildschirm wird nichts angezeigt, was darauf hinweist, dass die Verschlüsselung nicht aktiv ist:



Wenn ein Kanal im erweiterten Modus aktiviert ist (Enhanced Key), hängt dies vom Inhalt des Bytes ganz rechts des Verschlüsselungsschlüssels ab:

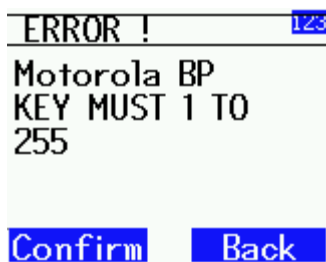
Im folgenden Beispiel verwendet Kanal E1 den erweiterten Datenschutzschlüssel Nr. 1:



Das rechte Byte des Verschlüsselungsschlüssels 1 befindet sich jedoch bei 0:

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

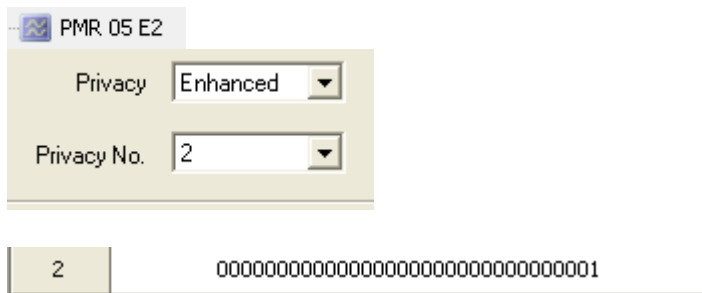
Sie erhalten also diese Fehlermeldung in **4 Show key** :



Und auf dem Hauptbildschirm wird nichts angezeigt:



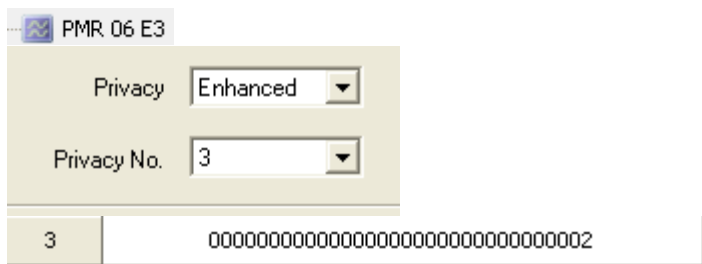
Wenn wir zu Kanal E2 gehen, der den Datenschutzschlüssel Nr. 2 verwendet:




Da das Byte ganz rechts 01 ist, wird der Basic Privacy 1 Verschlüsselungsschlüssel aktiviert: "Moto BP int K:1" steht für "Motorola Basic Privacy internal key" und das K mit der Nummer des Verschlüsselungsschlüssels (hier 1).



Wenn wir zum E3-Kanal gehen, der den Datenschutzschlüssel Nr. 3 verwendet:



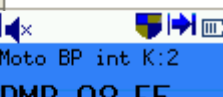
Moto BP int K:2  
PMR 06 E3  
PMR CH 6  
2002/03/23 08:33:41  
Menu

 PMR 07 E4

Privacy

Privacy No.

Moto BP int K:1  
PMR 07 E4  
PMR CH 7  
2002/03/23 08:33:48  
Menu

5	0000000000000000000000000000000202
	
6	112233445566778899AABBCCDDEEFF11





7	74581225622174788112236655123336
---	----------------------------------



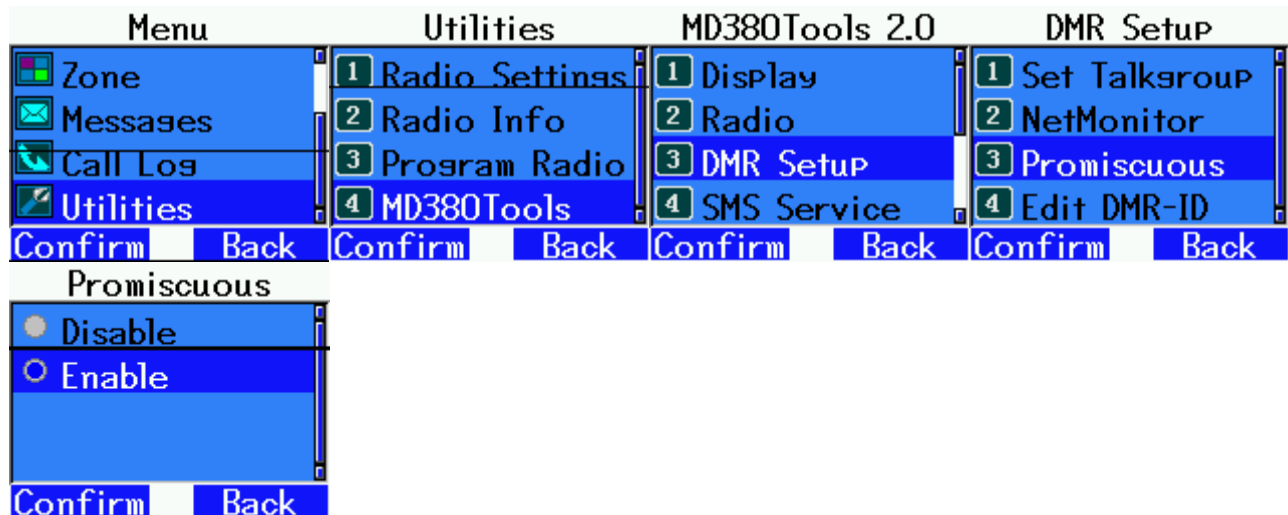
8	ABCDEDCBABCDDBCABDBCABDABBABBDDE
---	----------------------------------



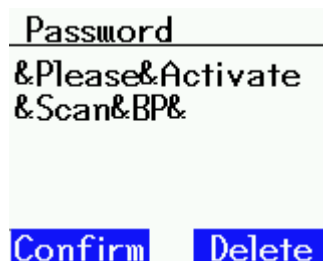
Es gibt eine zusätzliche versteckte Option: Sie können einen Verschlüsselungsschlüssel von Motorola Basic Privacy scannen und automatisch finden.

Zuerst müssen Sie den MD380 so konfigurieren, dass er alle Mitteilungen empfängt, dies ist der Promiscuous-Modus.

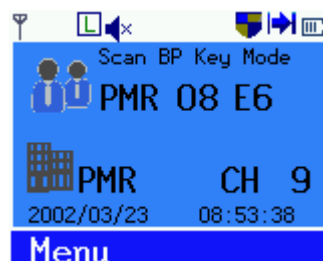
Gehe zu :



Gehen Sie dann zu Password und geben Sie das geheime Passwort ein:



Sie gelangen dann in den Motorola Basic Privacy Scanner-Modus:



Warten Sie, bis eine verschlüsselte Motorola Basic Privacy-Kommunikation gestartet wird, sobald der Verschlüsselungsschlüssel gefunden wurde, hören Sie einen Piepton und die Kommunikation wird dann entschlüsselt.

Sobald der Empfang stoppt, sehen Sie den gefundenen Verschlüsselungsschlüssel:



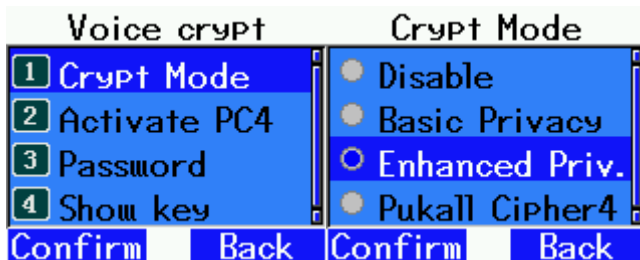
Wenn Sie einen neuen Scan ausführen möchten, können Sie die PTT-Taste einmal drücken oder die #-Taste drücken.

Seien Sie vorsichtig, dieser Modus funktioniert nur mit einem offiziellen Motorola-Gerät, da Motorola eine Hintertür zum Scannen von Verschlüsselungsschlüsseln eingeführt hat. Die Hintertür ist in Voice Crypt nicht vorhanden, sodass Sie den Basic Privacy-Verschlüsselungsschlüssel von einem anderen Voice Crypt nicht finden können.

Um den Motorola Basic Privacy Scanner-Modus zu beenden, können Sie dasselbe versteckte Passwort wie oben erneut eingeben oder das MD380 aus- und wieder einschalten.

## Tytera Erweiterter Datenschutzmodus mit internem Verschlüsselungsschlüssel

In **Crypt Mode** wählen **Enhanced Privacy**:



Dann hängt alles davon ab, auf welchem Kanal Sie sich befinden.

Gehe zu **Show key** :



Wenn die Fehlermeldung angezeigt wird:



Es geht darum, dass Sie sich nicht auf einem erweiterten Datenschutzkanal befinden. Manchmal muss man auch auf einen anderen Kanal umschalten und zu diesem zurückkehren, damit er berücksichtigt wird.

Wenn Sie sich in einem Enhanced Privacy-Kanal befinden, wird der 128-Bit-Verschlüsselungsschlüssel angezeigt, der vom Tytera Enhanced Privacy-Algorithmus verwendet wird.

Im folgenden Beispiel ist es Privacy Key Nr. 5:

[illegible]

Tyt EP int K0:2  
PMR 08 E5  
PMR CH 8  
2002/03/23 08:37:16  
Menu

TYT EP KEY 123

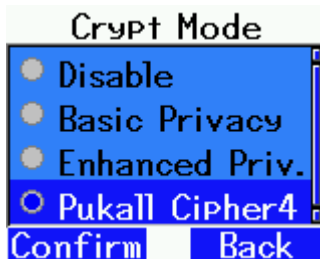
0000000000000000  
0000000000000000  
000202

Confirm Back

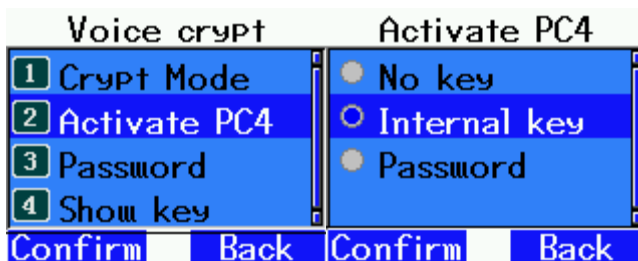
The screenshot shows the 'TYT EP KEY' menu. At the top, there are three buttons: 'Confirm', 'Back', and 'Menu'. Below the buttons, the text 'TYT EP KEY' is displayed. The main content area shows the frequency 'PMR 11 E8' and the channel 'CH 11'. The date and time are also displayed: '2002/03/23' and '08:38:03'. There are also some status icons at the top right, including a signal strength indicator and a battery level indicator.

## PC4-Verschlüsselungsmodus mit internem Verschlüsselungsschlüssel

In **Crypt Mode** wählen **PC4 Cipher**:



Gehe zu **2 Activate PC4** und wählen Sie **Internal key**:



Wie beim erweiterten Datenschutzmodus von Tyt hängt der verwendete Verschlüsselungsschlüssel von dem Kanal ab, auf dem Sie sich befinden.

**Show Key** zeigt Ihnen den aktiven Verschlüsselungsschlüssel und der Hauptbildschirm zeigt Ihnen das rechte Byte des aktiven Verschlüsselungsschlüssels (lesen Sie den Abschnitt "Erweiterter Datenschutz" von Tyt noch einmal, falls erforderlich, um das K0-Byte zu erklären).



## PC4 Cipher Advanced Teil

PC4 Cipher ist im sichersten Modus aktiv (253 Verschlüsselungsrunden). Einige MD380 haben jedoch möglicherweise einen zu langsamen Prozessor (CPU), was zu einer schlechten Sprachqualität führen würde.

Es ist möglich, die Anzahl der Verschlüsselungsrunden zu reduzieren, wenn Sie eine zu langsame CPU haben. Alle MD380 müssen dann mit der gleichen Anzahl von Runden konfiguriert werden, um miteinander kommunizieren zu können.

Dies ist ein verstecktes Menü, um es zu aktivieren, müssen Sie auf **8 Voice Crypt**:



Dann **3 Password** :

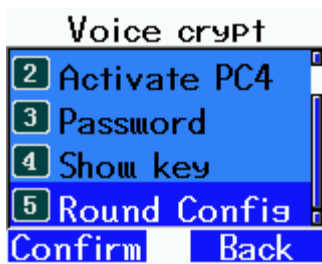


Anschließend müssen Sie ein spezielles Passwort mit Kleinbuchstaben, Großbuchstaben und Sonderzeichen eingeben :  
« **&Please&Activate&Round&Config&** » :



Verlassen Sie das Menü und kehren Sie zum Menü zurück, das ausgeblendete Menü ist erschienen:





Sie können dann die Anzahl der Runden reduzieren (dies verringert auch die Sicherheit und sollte nur durchgeführt werden, wenn die CPU zu langsam und die Stimme schlecht ist):



Auf dem Hauptbildschirm werden Sie gewarnt, dass Sie sich in einem Modus mit reduzierten Runden befinden, und dies wird für den PC4 mit Passwort oder den PC4 mit internem Verschlüsselungsschlüssel angezeigt:



Sie können dieses versteckte Menü wieder verschwinden lassen, indem Sie dasselbe spezielle Passwort ein zweites Mal eingeben.

## MI-Konfiguration

PC4 Cipher ist ein Blockchiffrealgorithmus im ECB-Modus. Das bedeutet, dass identische Daten in verschiedenen Voice-Frames auf die gleiche Weise verschlüsselt werden, wenn derselbe Verschlüsselungsschlüssel verwendet wird. Dies ist z.B. bei Silence Frames der Fall.

Um dies zu vermeiden, gibt es eine zusätzliche Option, die zufällige Daten hinzufügt, so dass identische Stille-Frames unterschiedlich verschlüsselt werden.

Dies erhöht die Sicherheit, verringert jedoch die Sprachqualität, da Bits in Voice-Frames entfernt werden.

Sie können zwischen 4 und 6 Bit pro Voice-Frame wählen. Mit 6 Bit ist die Sicherheit besser als mit 4 Bit, aber der Klang ist schlechter.

Es ist ein verstecktes Menü, um es zu aktivieren, müssen Sie zu **8 Voice Crypt** :



Dann **3 Password** :



Anschließend müssen Sie ein spezielles Passwort mit Kleinbuchstaben und Sonderzeichen eingeben: « **&Please&Activate&MI&Config&** » :



Verlassen Sie das Menü und kehren Sie zum Menü zurück, das versteckte Menü befindet sich hier:



Im Hauptmenü werden Sie vom MI4 oder MI6 benachrichtigt, wenn Sie sich im MI Config-Modus befinden.

Am besten sollten alle Teilnehmer an einer Diskussion die gleiche MI-Konfiguration verwenden, aber dies ist nicht zwingend erforderlich, die Entschlüsselung ist auch dann möglich, wenn nicht jeder die gleiche MI-Konfiguration verwendet.



Sie können dieses versteckte Menü wieder verschwinden lassen, indem Sie dasselbe spezielle Passwort ein zweites Mal eingeben.

## RC2-Verschlüsselung

Voice Crypt bietet einen weiteren Verschlüsselungsmodus: RC2 im CFB-Modus.

Dies ist eine Verschlüsselungsschiffre, die von Ron Rivest entwickelt und von Alexander Pukall verbessert wurde (Entfernung der reduzierten Verschlüsselungsschlüsselgrößen und Erhöhung des internen Zustands des RC2 auf 1024 Bit).

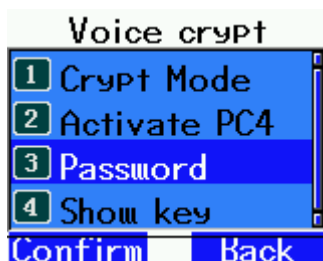
Die Größe des Verschlüsselungsschlüssels beträgt 128 Bit, wenn Sie die internen Verschlüsselungsschlüssel verwenden, oder bis zu 420 Bit, wenn Sie ein 60-stelliges Kennwort verwenden.

Es verwendet auch eine 6-Bit-MI-Konfiguration, so dass dieser RC2-Modus die Klangqualität der Stimme verschlechtert.

Es ist ein verstecktes Menü, um es zu aktivieren, müssen Sie auf 8 gehen  
**Voice Crypt :**



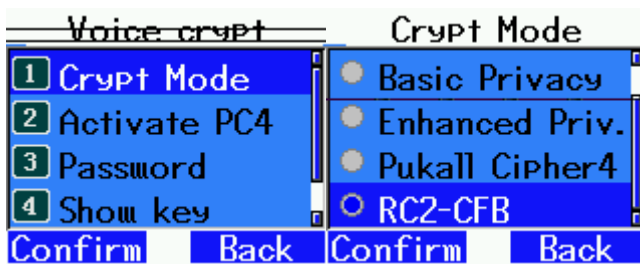
Dann **3 Password :**



Anschließend müssen Sie ein spezielles Passwort mit Kleinbuchstaben und Sonderzeichen eingeben: « **&Please&Activate&RC2&Encryption&** » :



Verlassen Sie das Menü und kehren Sie zum Menü zurück, das versteckte Menü befindet sich hier:



Sie können dieses versteckte Menü wieder verschwinden lassen, indem Sie dasselbe spezielle Passwort ein zweites Mal eingeben.

Um den Modus mit einem Passwort zu verwenden, aktivieren Sie **Password** unter **Activate PC4** (auch wenn PC4 nicht aktiv ist, sondern RC2).



Sie können auch wählen **Internal Key** :



## Zurücksetzen

Im Falle eines Problems und wenn nichts richtig funktioniert, können Sie alle Optionen zurücksetzen.

Gehe zu **Utilities - 4 MD380 Tools- 7 Developer - 4 Config Reset**

