Voice Crypt 1.0a

Голосовая крипта 1.0a

Шифрование голоса с высоким уровнем безопасности для версии Tytera MD380/MD390 UHF.

Это программное обеспечение основано на MD380TOOLS Трэвиса ГудСпида, спасибо ему за всю проделанную работу. Это программное обеспечение не работает на MD-UV380 и MD-UV390. Он работает на MD380 UHF и MD390 UHF (с GPS и без него). Он не работает на УКВ версиях. Voice Crypt использует новый вокодер, если ваш MD380 несовместим с новым вокодером, вы не сможете его использовать.

Режим Motorola Basic Privacy принадлежит компании Motorola, спасибо им за проделанную работу. Патента на базовый режим конфиденциальности не существует.

Расширенный режим конфиденциальности использует 128-битное шифрование AES и принадлежит Tytera, спасибо ему за проделанную работу. Однако это деградированный режим AES и гораздо менее безопасный, чем AES Motorola.

Режим PC4 Cipher принадлежит Александру Пукаллу, спасибо ему за проделанную работу.

Voice Crypt не содержит шифрования ARC4 и AES Motorola, потому что патент существует и препятствует его легальному использованию, поэтому был выбран режим шифрования PC4, потому что он не требует лицензионных отчислений.

Это программное обеспечение бесплатное, это бесплатное программное обеспечение.

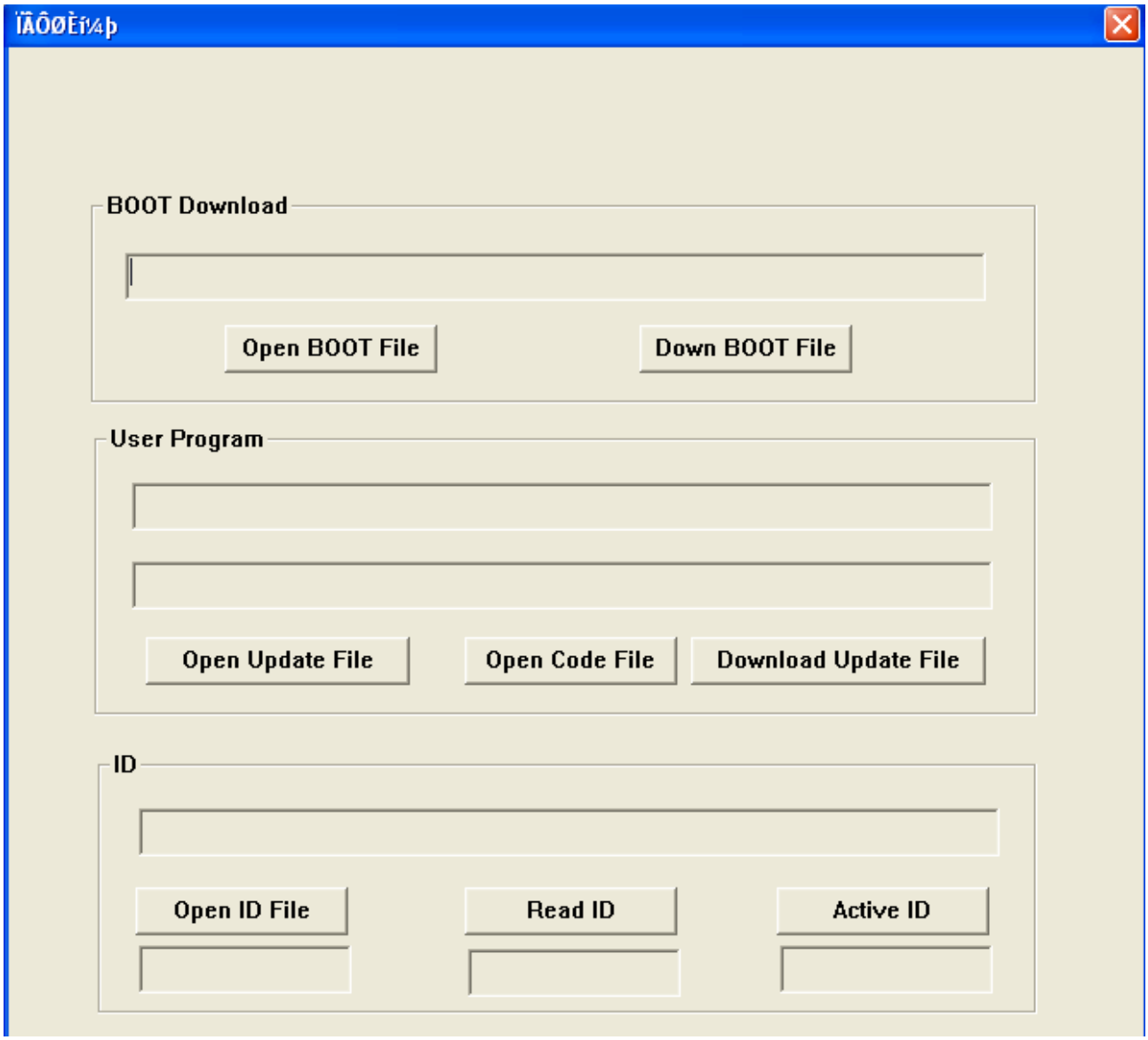
Это руководство в формате RTF, чтобы вы могли перевести его на свой язык, если хотите распространять Voice Crypt с переводом на свой родной язык.

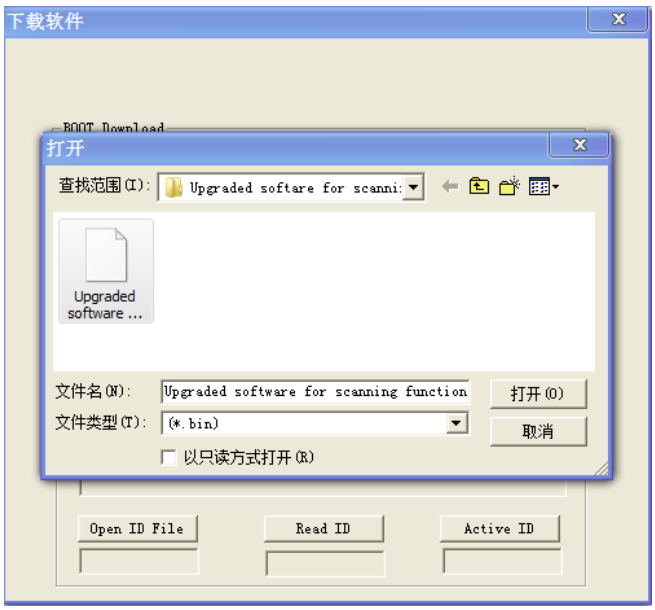
Как прошить прошивку

Voice Crypt основан на прошивках D013.020 (без GPS) и S013.020 (с GPS). Если ваш MD380/390 не включается после перепрошивки, он несовместим с версией 013.20. Затем вам нужно будет перепрошить оригинальную прошивку.

Чтобы прошить MD380, запустите программу Upgrade.exe:

На выключенном MD380 одновременно нажмите клавиши 1 и PTT (верхние 2 клавиши слева) и, не отпуская клавиши, включите MD380 (повернув ручку регулировки громкости). На экране ничего не отображается, но светодиод мигает красным/зеленым, MD380 готов к миганию.




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

Щелчок **Open Update File**, выберите прошивку Voice Crypt для GPS или без GPS и нажмите
Download Update File.

Voice Crypt прошивается на MD380. В конце выключите MD380 и снова включите его.

Рекомендуется выполнить сброс после перепрошивки, чтобы убедиться, что Voice Crypt работает правильно (см. раздел «**Сброс**» в самом конце этого руководства).

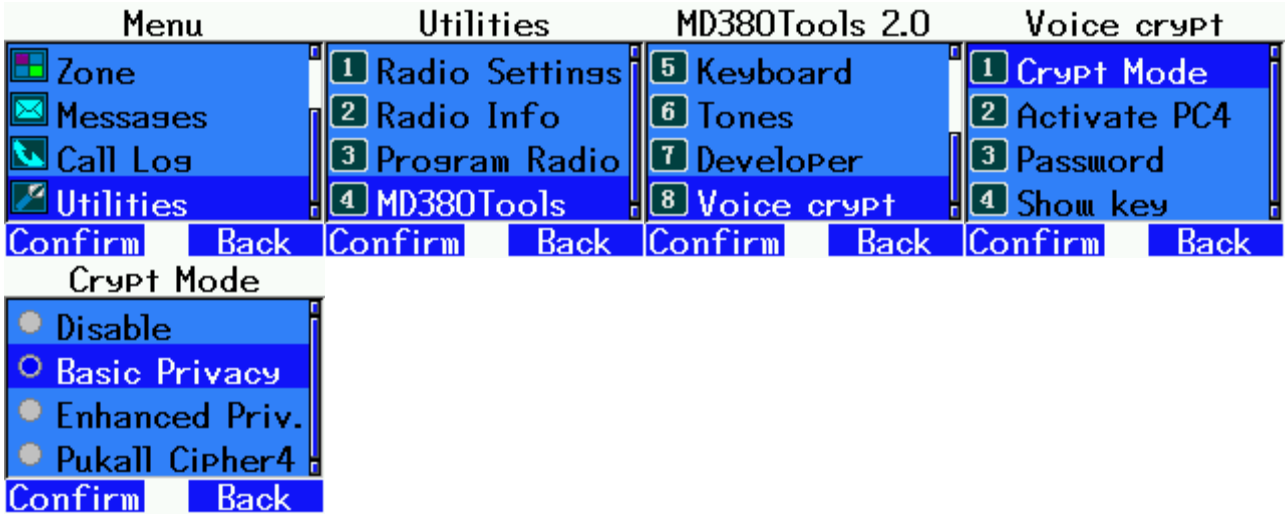
Как быстро начать работу

Базовый режим конфиденциальности Motorola с паролем

Этот режим совместим с радиостанцией Motorola Basic Privacy Reception (RX). Он может передавать в базовой конфиденциальности, но при отсутствии кадра Pi Header радиостанция Motorola не сможет распознать, что это зашифрованная передача в базовой конфиденциальности. С другой стороны, два MD380 смогут отправлять и получать данные в режиме базовой конфиденциальности.

Чтобы настроить его, перейдите по ссылке:

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



Затем перейдите по ссылке:

3 Password

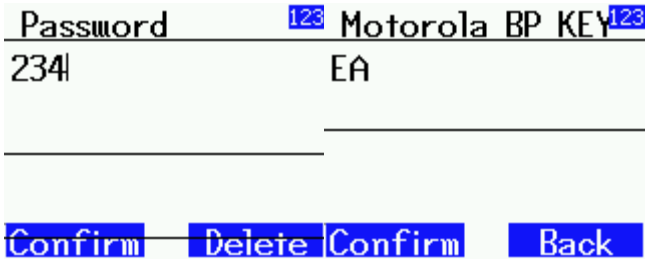
Введите ключ шифрования в десятичном формате (от 1 до 255). Можно написать 1, 01 или 001. Не забудьте переключиться в режим чисел (123), чтобы записать числа, иначе вы окажетесь в режиме алфавита. Чтобы переключиться из режима (EN) в режим (123), нажмите клавишу # несколько раз. Не используйте китайский режим, так как он не поддерживается.

Проверьте, включен ли ключ шифрования в :

4 Show key

Если на нем написано Motorola BP KEY 01, это означает, что ключ шифрования был активирован.

Попробуйте с ключом шифрования 234, Тогда загляните внутрь **Show Key**, ключ шифрования записывается в шестнадцатеричном формате: EA



Это тот же ключ шифрования, но Show Key отображает ключи шифрования в шестнадцатеричном формате.

После этого вы можете отправлять и получать в разделе "Базовая конфиденциальность". Главный экран покажет вам "Moto BP pas" " для "Motorola Basic Privacy password" и "K:EA" для активного ключа шифрования "EA" в шестнадцатеричном формате.

Вы можете разговаривать с другим MD380 с тем же ключом шифрования или слушать радиоприемник Motorola с тем же ключом шифрования.

Вы можете изменить ключ шифрования Moto BP без повторного ввода пароля с помощью стрелок вверх и вниз. Для этого необходимо сначала разблокировать эти клавиши, нажав клавишу * 3 раза подряд.

После разблокировки стрелок вы можете увеличить ключ на +1 с помощью стрелки вверх или уменьшить клавишу на -1 с помощью стрелки вниз. В режиме передачи (TX) вы не можете использовать стрелки вверх и вниз для изменения клавиш. С другой стороны, в режиме приема (RX) вы можете использовать стрелки вверх и вниз для изменения ключа шифрования. Если вы прослушиваете зашифрованный канал в базовой конфиденциальности и не знаете ключ шифрования, вы можете использовать стрелки вверх и вниз, чтобы попробовать 255 возможных ключей шифрования (от 1 до FF в шестнадцатеричном формате). Как только ключ шифрования будет выбран правильно, вы будете правильно слышать разговор. После завершения вызова вы увидите, какой ключ шифрования вы выбрали.

Режим шифрования PC4 с паролем

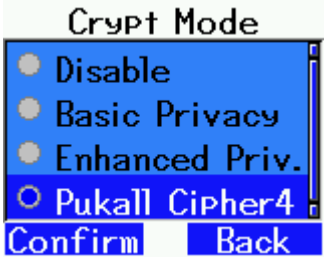
Шифр PC4, разработанный Александром Пукаллом, использует ключи шифрования длиной от 8 до 2212 бит в зависимости от длины пароля или ключа шифрования. Он работает в режиме ECB, был создан специально для радиорежима DMR и предельно безопасен.

Voice Crypt позволяет использовать ключи шифрования в диапазоне от 112 до 420 бит просто потому, что экран MD380 неправильно отображает больше символов. Так как Voice Crypt не позволяет использовать китайские иероглифы, используются английские символы Ascii (буквы, цифры, специальные символы). Символ Ascii является 7-битным.

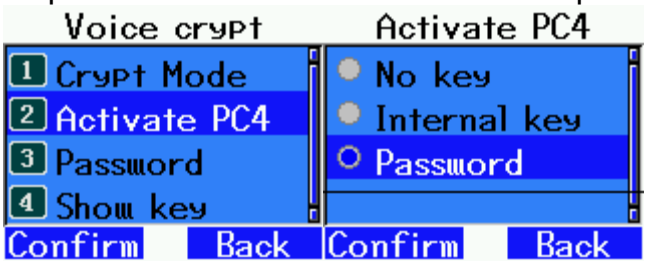
Voice Crypt позволяет использовать пароли длиной от 16 до 60 символов. Таким образом, мы получаем ключи шифрования от 112 бит (16*7) до 420 бит (60*7). Мы считаем, что этого более чем достаточно для противодействия всем возможным угрозам несанкционированного прослушивания.

Шифр PC4 не требует лицензионных отчислений и находится в общественном достоянии, поэтому он не нарушает патент Motorola на его использование в Voice Crypt.

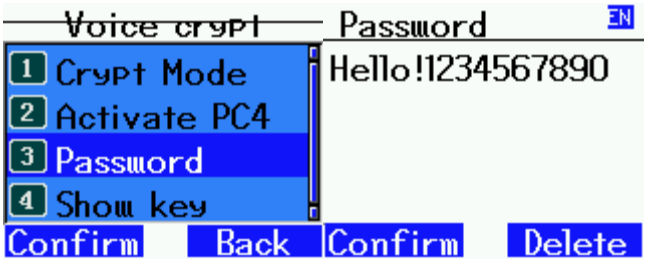
Перейти к **Menu – Utilities – 4 Md380Tools – 8 Voice Crypt – 1 Crypt Mode – Pukall Cipher 4**



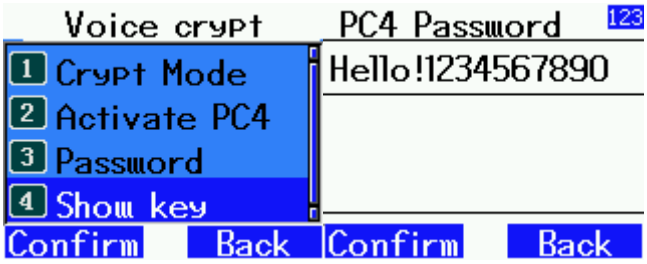
Перейти к **2 Activate PC4** и выберите **Password** :



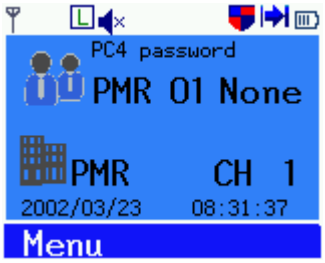
Затем перейдите в раздел **3 Password** и введите пароль длиной не менее 16 символов (до 60 символов):



Вы можете убедиться, что PC4 включен, нажав на **4 Show key** и вы должны увидеть тот же пароль, который вы ввели, что означает, что PC4 включен:



На главном экране вы должны увидеть "PC4 password" это означает, что PC4 активирован в режиме "пароль" (будьте осторожны, вы увидите его только в том случае, если для режима отображения установлено значение ВЫКЛ).



После этого вы сможете безопасно взаимодействовать с другим MD380, использующим тот же пароль.

Дисплей режима:

Чтобы увидеть активацию шифрования на главном экране, режим отображения MD380Tools должен быть установлен в положение OFF, иначе вы его не увидите.

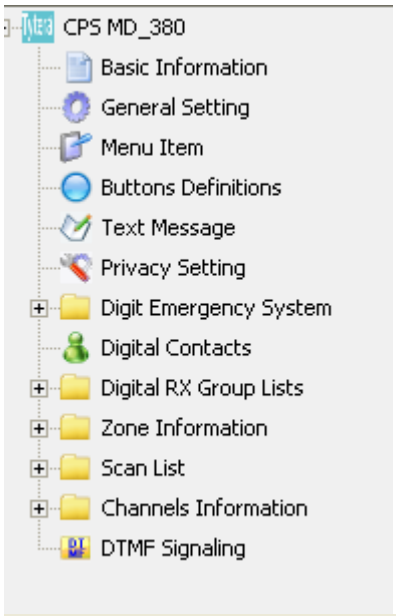
Вы можете проверить это, перейдя по ссылке **Menu Utilities – 4 MD380Tools – 1 Display -4 Mode Display**


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

Режимы с внутренними ключами шифрования

Программное обеспечение Tytera Programming Software (CPS) позволяет вводить ключи шифрования для каналов DMR.

В Tytera CPS вы можете нажать на «Privacy Setting», чтобы увидеть ключи шифрования:

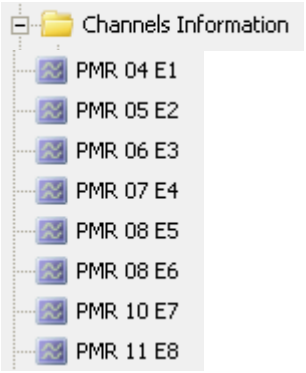


No.	Key Value(Basic)
1	FFFF
2	FFFF
3	FFFF
4	FFFF
5	FFFF
6	FFFF
7	FFFF
8	FFFF
9	FFFF
10	FFFF
11	FFFF
12	FFFF
13	FFFF
14	FFFF
15	FFFF
16	FFFF

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

Не используйте столбец (Basic), Всегда используйте столбец (Enhanced) Чтобы поставить 128-битные ключи шифрования (16 шестнадцатеричных символов), можно создать 8 ключей шифрования, например:

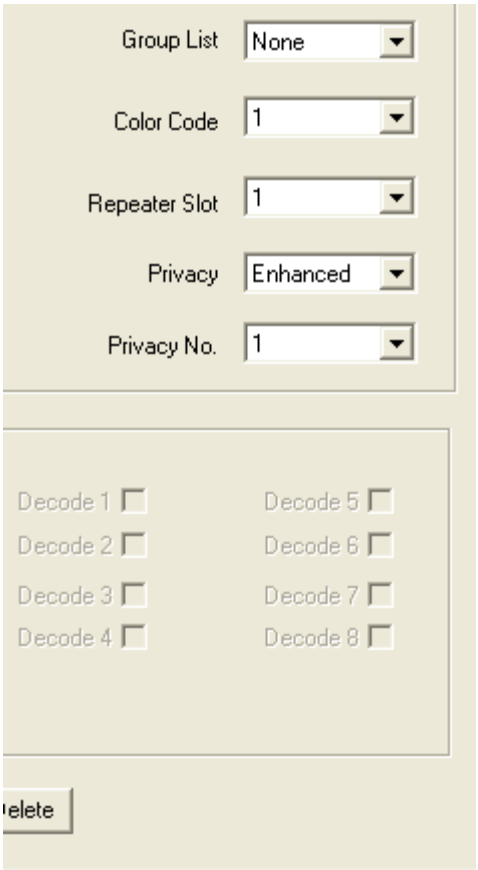
В разделе «Channels Information» вы можете настроить свои каналы:



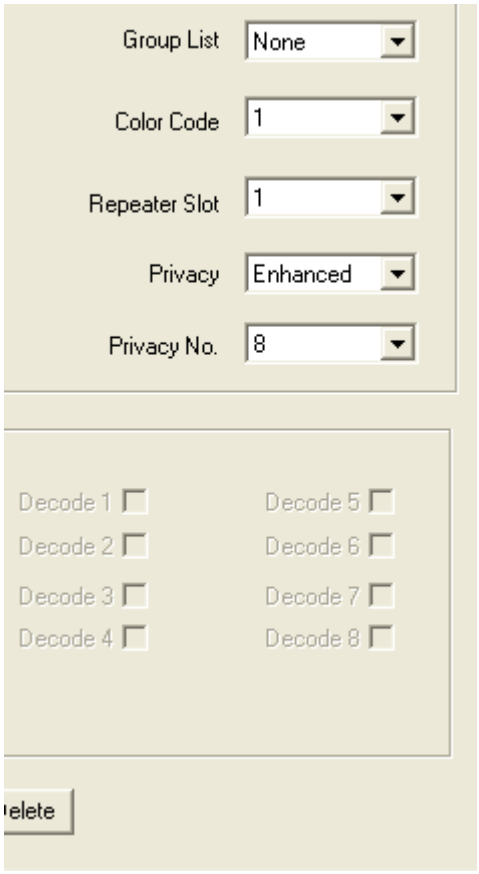
E1 расшифровывается как Enhanced Privacy Channel 1, E2 Enhanced Privacy Channel 2...

Открывая канал E1 мы видим:

В правом нижнем углу мы видим Enhanced и номер ключа шифрования, здесь Privacy Key No. 1.



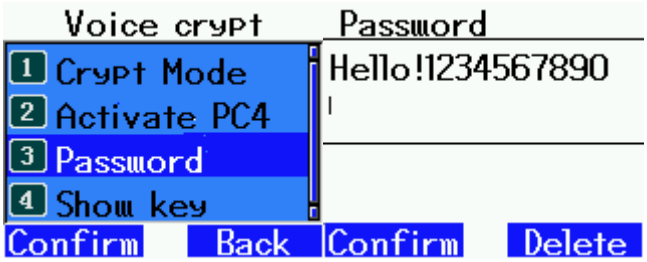
Другой пример с каналом E8:


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

Базовый режим конфиденциальности Motorola с внутренним ключом шифрования

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

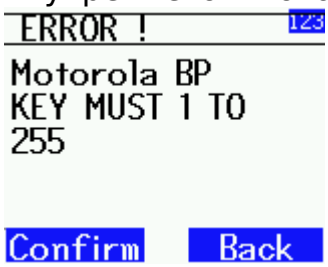
Перейти к **3 Password** и введите пароль длиннее 4 символов (или вообще без пароля):

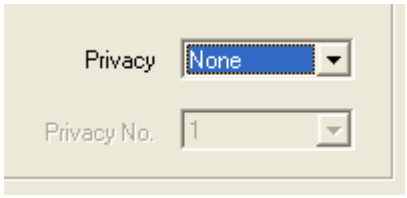


Если пароль состоит из цифр от 1 до 255, то режим пароля имеет приоритет над режимом внутреннего ключа, а базовая конфиденциальность использует пароль в качестве ключа шифрования. В противном случае используется внутренний ключ шифрования, запрограммированный на активном канале.

Перейти к **4 Show Key** :

Если вы находитесь на канале без активного расширенного режима, вы получите следующее сообщение об ошибке (из-за отсутствия активного внутреннего ключа шифрования):

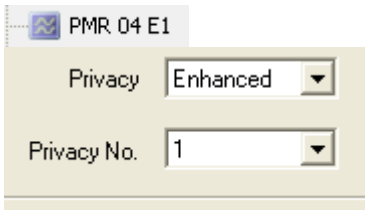




На главном экране не будет ничего, указывающего на то, что шифрование не активно:

Если канал включен в расширенном режиме, то это зависит от содержимого крайнего правого байта ключа шифрования:

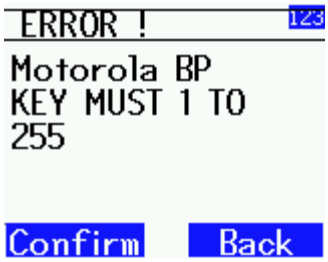
В следующем примере канал E1 использует ключ расширенной конфиденциальности No 1:



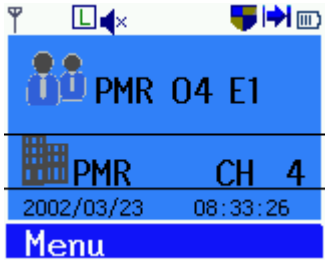
Но крайний правый байт ключа шифрования 1 находится в 0:

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

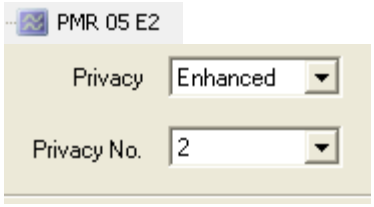
Таким образом, вы получите это сообщение об ошибке в **4 Show key** :

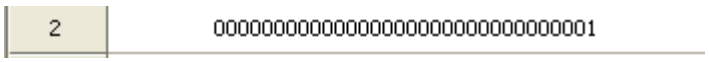


И ничего не будет отображаться на главном экране:

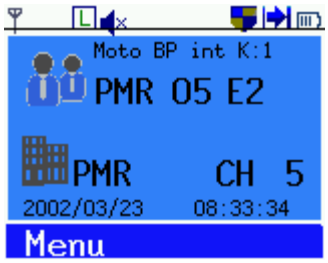


Если мы перейдем на канал E2, который использует ключ конфиденциальности No 2:

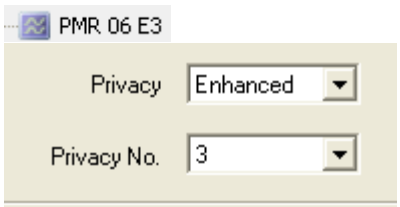


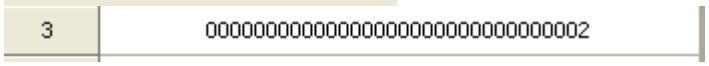


Крайний правый байт равен 01, ключ Basic Privacy 1 будет активирован: "Moto BP int K:1" расшифровывается как «Motorola Basic Privacy internal key» и буква K для номера ключа шифрования (здесь 1).

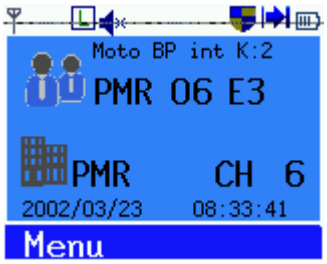


Если мы перейдем на канал E3, который использует ключ конфиденциальности No 3:

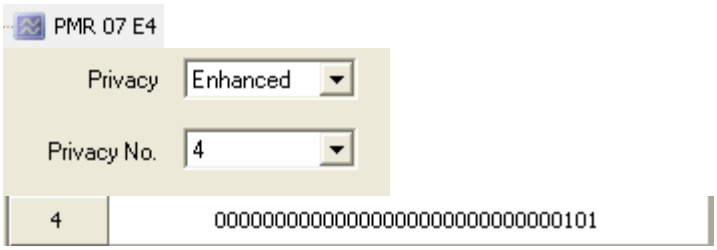




Крайний правый байт равен 02, это ключ Basic Privacy 2, который будет активирован:

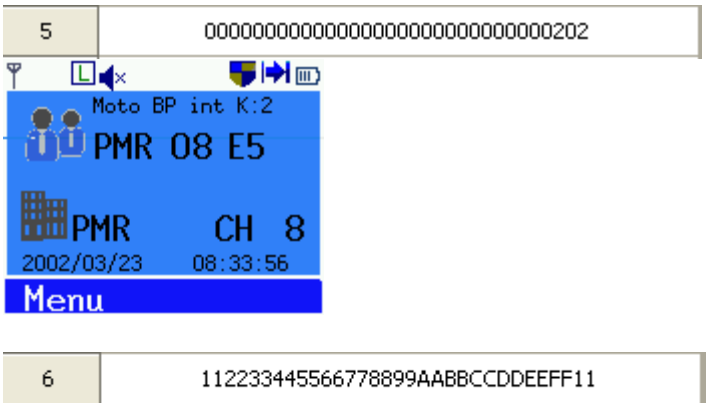


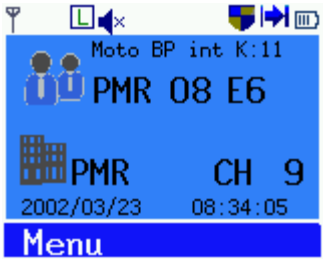
Если мы перейдем к каналу E4, который использует ключ конфиденциальности No 4:



Есть два байта 01, но это крайний правый байт, который используется для базовой конфиденциальности, поэтому будет активирован ключ шифрования Basic Privacy 1:

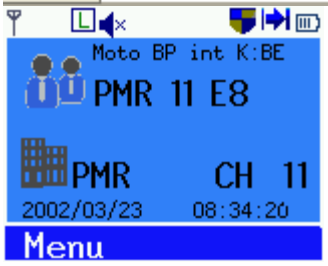
Вот примеры для остальных каналов:





7	74581225622174788112236655123336

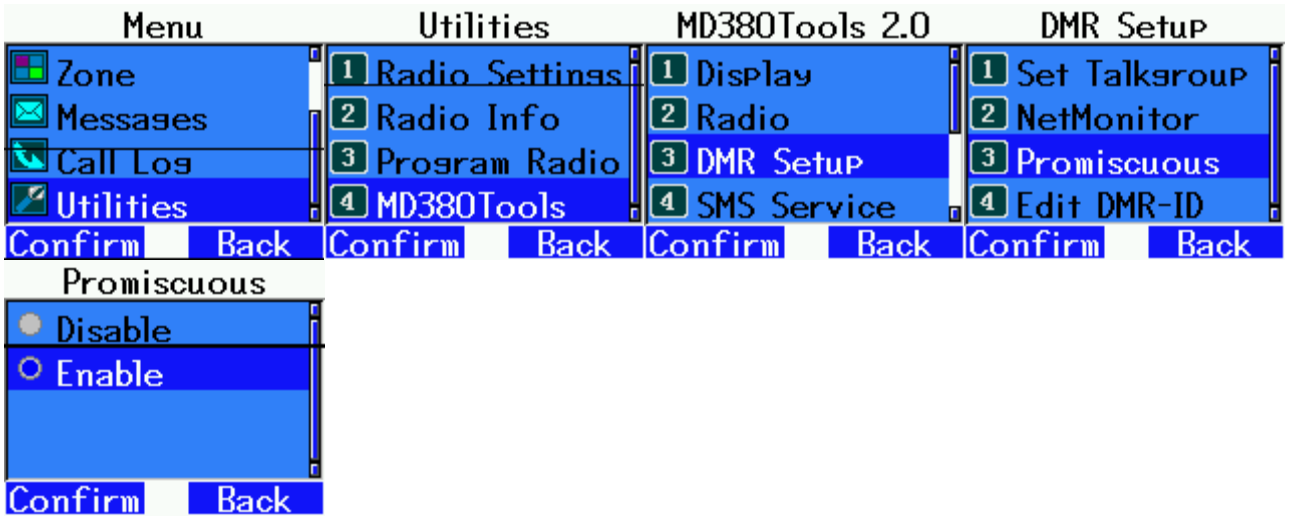
8	ABCDEDCBABCDDBCABDBCABDABBABBDBE



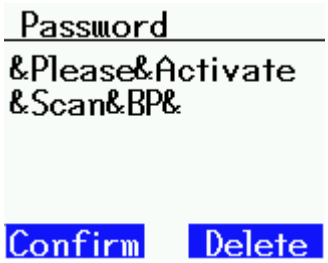
Есть еще одна скрытая опция: вы можете отсканировать и автоматически найти ключ шифрования Motorola Basic Privacy.

Сначала вы должны настроить MD380 так, чтобы он получал все сообщения, это режим Promiscuous.

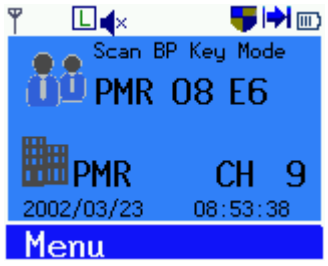
Перейти к :



Затем перейдите в раздел «Пароль» и введите секретный пароль:



Затем вы переключаетесь в режим Базовый сканер конфиденциальности Motorola:



Дождитесь начала зашифрованной связи Motorola Basic Privacy, как только ключ шифрования будет найден, вы услышите звуковой сигнал, после чего соединение будет слышно четко.

Как только прием прекратится, вы увидите найденный ключ шифрования:

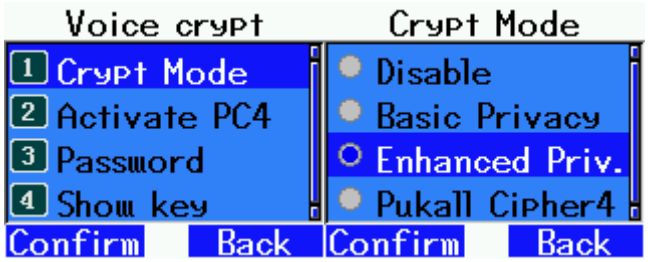
Если вы хотите перезапустить новое сканирование, вы можете нажать клавишу PTT один раз или нажать клавишу #.

Внимание, этот режим работает только с официальным устройством Motorola, потому что Motorola представила бэкдор для сканирования ключей. Бэкдор отсутствует в Voice Crypt, поэтому вы не можете найти ключ Basic Privacy другого Voice Crypt.

Чтобы выйти из режима Motorola Basic Privacy Scanner, вы можете повторно ввести тот же скрытый пароль, что и выше, или выключить и снова включить MD380.

Расширенный режим конфиденциальности Tytera с внутренним ключом шифрования

Перейти к **Crypt Mode** и выберите **Enhanced Privacy**:



Дальше все будет зависеть от того, на каком канале вы находитесь.

Перейти к **Show key :**

Если вы видите сообщение об ошибке:

Дело в том, что вы не находитесь на канале повышенной конфиденциальности. Иногда вам также приходится переключаться на другой канал и возвращаться к нему, чтобы он был учтен.

Если вы используете расширенный канал конфиденциальности, появится 128-битный ключ шифрования, используемый расширенным алгоритмом конфиденциальности Tytera.

В приведенном ниже примере это конфиденциальность No 5:

На главном экране появится "Tyt EP int K0:2": Это означает «Внутренний ключ Tytera Enhanced Privacy» с K0 (крайний правый нулевой байт: 2).

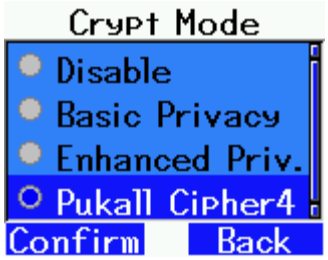
Ключ K0 не является полноценным 128-битным ключом шифрования (не хватает места на экране, чтобы отобразить все), но он позволяет пользователю узнать крайний правый байт и, следовательно, быстро проверить, какой ключ шифрования используется. Полный ключ шифрования отображается с помощью **Show key :**

Пример с другими ключами шифрования:

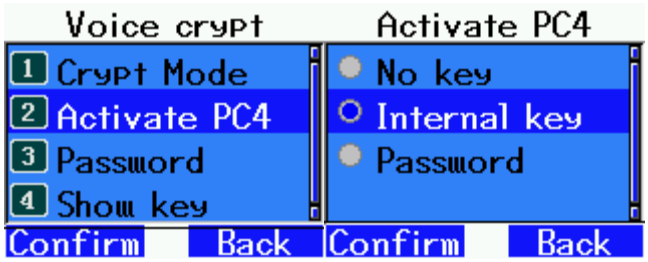

TYT EP KEY
123
ABCDEDCBABCDDBC
ABDBCABDABBABBD
BE
Tyt EP int KO:BE
PMR 11 E8
PMR
CH 11
2002/03/23
08:38:03
Confirm
Back
Menu

Режим шифрования PC4 с внутренним ключом шифрования

Перейти к **Crypt Mode** и выберите **PC4 Cipher**:



Перейти к **2 Activate PC4** и выберите **Internal key**:



Как и в случае с Tyt Enhanced Privacy, ключ шифрования, который вы используете, будет зависеть от канала, на котором вы находитесь.

Show Key показывает активный ключ шифрования, а крайний правый байт активного ключа шифрования отображается на главном экране (при необходимости прочтите раздел Tyt Enhanced Privacy для объяснения байта K0).

Расширенная часть шифра PC4

Шифр PC4 активен в наиболее безопасном режиме (253 раунда шифрования). Однако некоторые MD380 могут иметь слишком медленный процессор (CPU), что может привести к низкому качеству голоса.

Можно уменьшить количество раундов шифрования, если у вас слишком медленный процессор. Все MD380 должны быть настроены на одинаковое количество раундов, чтобы иметь возможность взаимодействовать друг с другом.

Это скрытое меню, чтобы активировать его, вам нужно перейти в **8 Voice Crypt:**

Перейти к **3 Password :**

Затем необходимо ввести специальный пароль со строчными прописными буквами и специальными символами : « **&Please&Activate&Round&Config&** »

Выйдите из меню и вернитесь в меню, появилось скрытое меню:

Затем вы можете уменьшить количество раундов (это также снижает безопасность и должно быть сделано только в том случае, если процессор слишком медленный, а голос плохой):

На главном экране вас предупреждают, что вы находитесь в режиме с уменьшенным количеством раундов, и это отображается для PC4 с паролем или ПК4 с внутренним ключом шифрования:

Вы можете сделать так, чтобы это скрытое меню снова исчезло, повторно введя тот же специальный пароль во второй раз.

Конфигурация MI

Шифр PC4 - это алгоритм блочного шифрования в режиме ECB. Это означает, что идентичные данные в разных голосовых кадрах будут зашифрованы одинаково, если используется один и тот же ключ шифрования. Так обстоит дело, например, с кадрами тишины.

Чтобы избежать этого, существует дополнительная опция, которая добавляет случайные данные, чтобы одинаковые кадры тишины шифровались по-разному.

Это повышает безопасность, но снижает качество голоса, так как удаляются биты в голосовых кадрах.

Вы можете выбрать от 4 до 6 бит на голосовой кадр. С 6 битами безопасность лучше, чем с 4 битами, но звук хуже.

Это скрытое меню, для его активации нужно перейти в **8 Voice Crypt :**

Перейти к **3 Password :**

Затем необходимо ввести специальный пароль строчными буквами и специальными символами: « **&Please&Activate&MI&Config&** » :

Выйдите из меню и вернитесь в меню, скрытое меню находится здесь:

В главном меню вы будете уведомлены MI4 или MI6, если вы находитесь в режиме MI Config.

В идеале все участники обсуждения должны использовать одну и ту же конфигурацию MI, но это не обязательно, расшифровка возможна, даже если не все используют одну и ту же конфигурацию MI.

Вы можете сделать так, чтобы это скрытое меню снова исчезло, повторно введя тот же специальный пароль во второй раз.

Шифрование RC2

Voice Crypt предлагает еще один режим шифрования: RC2 в режиме CFB.

Это шифр шифрования, созданный Роном Ривестом и усовершенствованный Александром Пукаллом (удаление уменьшенных размеров ключей шифрования и увеличение внутреннего состояния RC2 до 1024 бит).

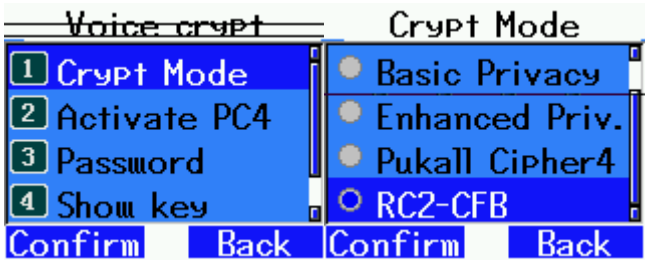
Размер ключа шифрования составляет 128 бит при использовании внутренних ключей шифрования или до 420 бит при использовании пароля из 60 символов.
Он также использует 6-битную конфигурацию MI, поэтому этот режим RC2 ухудшает качество звука голоса.

Это скрытое меню, для его активации нужно перейти в **8 Voice Crypt :**

Тогда **3 Password :**

Затем необходимо ввести специальный пароль строчными буквами и специальными символами: « **&Please&Activate&RC2&Encryption&** » :

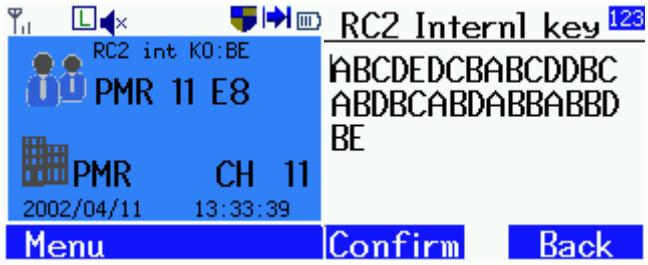
Выйдите из меню и вернитесь в меню, скрытое меню находится здесь:



Вы можете сделать так, чтобы это скрытое меню снова исчезло, повторно введя тот же специальный пароль во второй раз.

Чтобы использовать режим с паролем, включите Password в Activate PC4 (даже если ПК4 не активен, а RC2).

Вы также можете выбрать **Internal Key** :



Сброс

В случае возникновения проблемы и если ничего не работает должным образом, вы можете сбросить все параметры.

Перейти к **Utilities - 4 MD380 Tools- 7 Developer – 4 Config Reset**