Voice Crypt 1.0a

Criptografia de voz 1.0a

Criptografia de voz de alta segurança para Tytera MD380/MD390 versão UHF.

Este software é baseado em MD380TOOLS por Travis GoodSpeed, graças a ele por todo o trabalho feito. Este software não funciona em MD-UV380 e MD-UV390. Funciona em MD380 UHF e MD390 UHF (com e sem GPS). Não funciona em versões VHF. Voice Crypt usa o novo Vocoder, se o seu MD380 não é compatível com o novo Vocoder, então você não será capaz de usá-lo.

Motorola Basic Privacy modo pertence à Motorola, graças a eles para o trabalho feito. Não existe patente para o modo de Privacidade Básica.

O modo de privacidade aprimorada usa criptografia AES de 128 bits e pertence ao Tytera, graças a ele pelo trabalho feito. É, no entanto, um modo degradado do AES e muito menos seguro do que o AES da Motorola.

O modo PC4 Cipher pertence a Alexander Pukall, graças a ele pelo trabalho feito.

Voice Crypt não contém criptografia ARC4 e AES Motorola porque existe uma patente e impede seu uso legal, razão pela qual o modo de cifra PC4 foi escolhido porque é livre de royalties.

Este software é gratuito, é um Freeware.

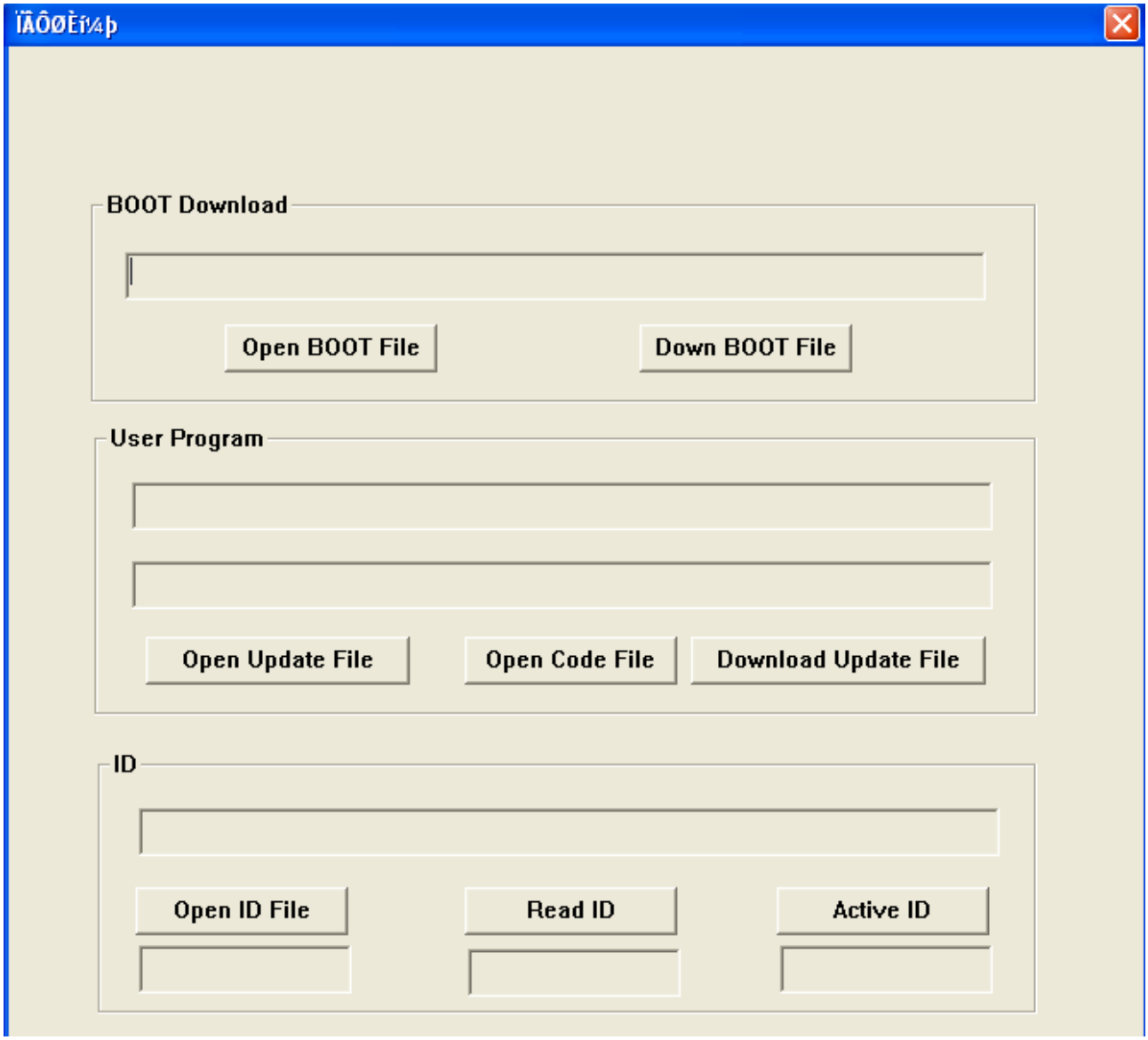
Este manual está em formato RTF para que você possa traduzi-lo para o seu idioma se você quiser distribuir Voice Crypt com uma tradução para o seu próprio idioma.

Como atualizar o firmware

Voice Crypt é baseado no firmware D013.020 (sem GPS) e S013.020 (com GPS). Se o seu MD380/390 não ligar depois de piscar, ele não é compatível com a versão 013.20. Em seguida, você precisará reflash seu firmware original.

Para piscar o seu MD380 inicie o programa Upgrade.exe:

No seu MD380 desligado, pressione as teclas 1 e PTT simultaneamente (as 2 teclas superiores à esquerda) e sem soltar as teclas ligue o MD380 (girando o botão de volume). A tela não exibe nada, mas o LED pisca vermelho / verde, o MD380 está pronto para ser piscado.


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

Clique em **Open Update File**, escolha o firmware Voice Crypt para GPS ou sem GPS e clique em **Download Update File.**

Voice Crypt é piscado no MD380. No final, desligue o MD380 e ligue-o novamente.

Recomenda-se fazer uma Redefinição após piscar para se certificar de que a Voice Crypt está funcionando corretamente (consulte a seção **Repor** no final deste manual).

Como começar rapidamente

Motorola Basic Privacy Mode com senha

Este modo é compatível com um rádio Motorola Basic Privacy na receção (RX). Ele pode transmitir em Privacidade Básica, mas na ausência de um quadro de cabeçalho Pi, um rádio Motorola não será capaz de reconhecer que é uma transmissão criptografada em Privacidade Básica. Por outro lado, dois MD380 serão capazes de transmitir e receber em Privacidade Básica.

Para configurá-lo, vá para:

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

Em seguida, vá para:

3 Password

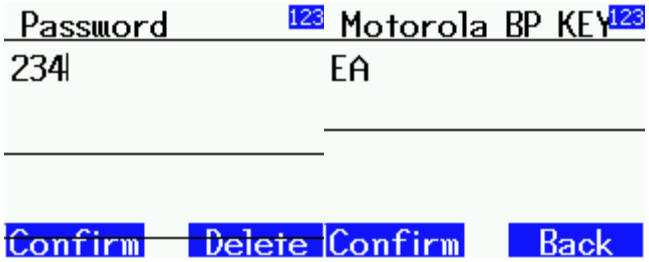
Introduza a chave de encriptação a utilizar em formato decimal (de 1 a 255). Você pode escrever 1, 01 ou 001. Não se esqueça de mudar para o modo de número (123) para escrever os números, caso contrário, você está no modo alfabético. Para mudar do modo (EN) para (123), prima a tecla # várias vezes. Não use o modo chinês, pois ele não é suportado.

Verifique se a chave de criptografia está ativada:

4 Show key

Se ele diz Motorola BP KEY 01 significa que a chave de criptografia está ativada.

Tente com a chave de encriptação 234 ativada **3 Password**, em seguida, olhe para dentro **4 Show Key**, a chave de encriptação é escrita em hexadecimal: EA



É a mesma chave de encriptação, mas **Show Key** mostra as chaves de criptografia em hexadecimal.

Você pode então enviar e receber em Privacidade Básica. A tela principal informa "Moto BP pas" para "Motorola Basic Privacy password" e "K:EA" para a chave de encriptação "EA" ativa em hexadecimal.

Você pode usar a mesma chave de criptografia para falar com outro MD380 ou você pode ouvir rádio Motorola com a mesma chave de criptografia.

Você pode alterar a chave de criptografia Moto BP sem ter que digitar novamente a senha usando as setas para cima e para baixo. Para fazer isso, você deve primeiro desbloquear essas teclas pressionando a tecla * 3 vezes seguidas.

Assim que as setas estiverem desbloqueadas, pode aumentar a chave de encriptação em +1 com a seta para cima ou diminuir a chave de encriptação em -1 com a seta para baixo.

No envio (TX) não é possível usar as setas para cima e para baixo para alterar a chave de criptografia. Por outro lado, na receção (RX) você pode usar as setas para cima e para baixo para alterar a chave de criptografia. Se estiver a ouvir um canal encriptado na Privacidade Básica e não souber a chave de encriptação, pode utilizar as setas para cima e para baixo para tentar as 255 chaves de encriptação possíveis (de 1 a FF em hexadecimal). Quando a chave de criptografia estiver correta, você ouvirá a conversa claramente. Quando a conversa terminar, você verá em qual chave de criptografia você parou.

Modo de codificação PC4 com senha

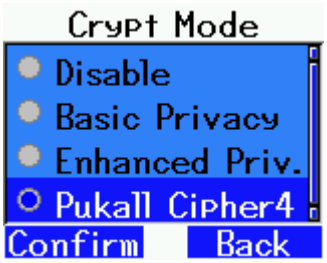
A cifra PC4 desenvolvida por Alexander Pukall usa chaves de criptografia que variam de 8 bits a 2212 bits, dependendo do comprimento da senha ou chave de criptografia. Funciona no modo ECB, foi criado especificamente para o modo de rádio DMR e é extremamente seguro.

Voice Crypt permite que você use chaves de criptografia que variam de 112 bits a 420 bits simplesmente porque a tela MD380 não exibe mais caracteres corretamente. Como a Cripta de Voz não permite o uso de caracteres chineses, caracteres Ascii em inglês (letras, números, caracteres especiais) são usados. Um caractere Ascii é de 7 bits.

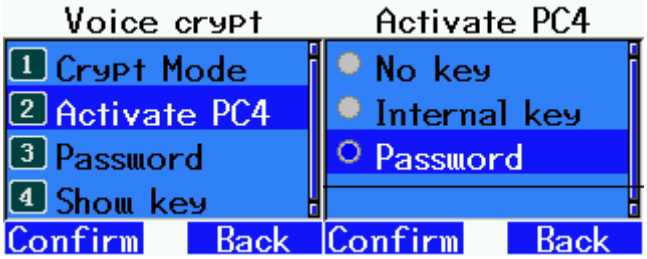
Voice Crypt permite senhas que variam de 16 caracteres a 60 caracteres. Assim, obtemos chaves de encriptação de 112 bits (16 * 7) a 420 bits (60 * 7). Acreditamos que isso é mais do que suficiente para combater todas as possíveis ameaças de escutas não autorizadas.

O PC4 Cipher é royalty-free e no domínio público, por isso não infringe qualquer patente Motorola para usá-lo em Voice Crypt.

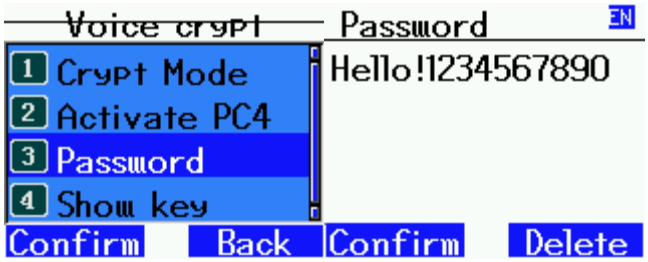
Ir para **Menu – Utilities – 4 Md380Tools – 8 Voice Crypt – 1 Crypt Mode – Pukall Cipher 4**



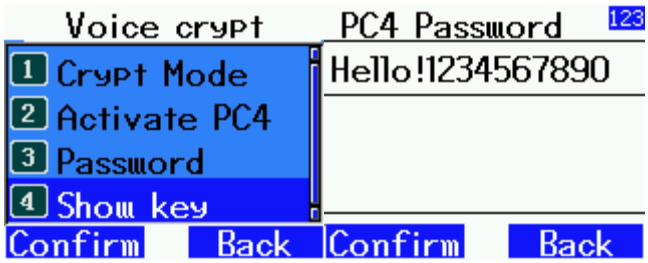
Em seguida, **2 Activate PC4** e escolha **Password** :



Em seguida, vá para **3 Password** e digite uma senha de pelo menos 16 caracteres (até 60 caracteres):



Você pode verificar se o PC4 está ativado clicando em **4 Show key** e deverá ver a mesma palavra-passe que introduziu, o que significa que o PC4 está ativado:



Na tela principal, você deve ver: "PC4 password" isso significa que o PC4 está ativado no modo "senha" (tenha cuidado você só verá se o Modo de Exibição estiver definido como OFF).

Em seguida, você pode se comunicar com segurança com outro MD380 que usa a mesma senha.

Modo de exibição:

Para ver a ativação da criptografia na tela principal, o modo de exibição MD380Tools deve ser definido como OFF, caso contrário, você não o verá.

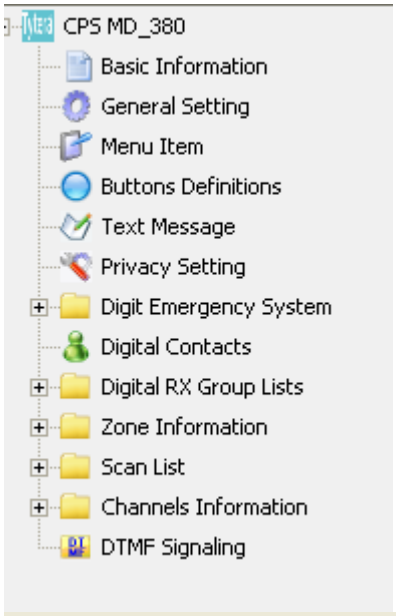
Você pode verificar isso indo para **Menu Utilities – 4 MD380Tools – 1 Display -4 Mode Display**


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 com chaves de encriptação internas

O software de programação (CPS) da Tytera permite que você insira chaves de criptografia para canais DMR.

No Tytera CPS, você pode clicar em Configurações de Privacidade para ver as chaves de criptografia:



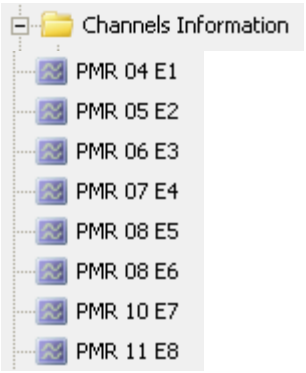
No.	Key Value(Basic)
1	FFFF
2	FFFF
3	FFFF
4	FFFF
5	FFFF
6	FFFF
7	FFFF
8	FFFF
9	FFFF
10	FFFF
11	FFFF
12	FFFF
13	FFFF
14	FFFF
15	FFFF
16	FFFF

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

Não utilize a coluna (Basic), use sempre a coluna (Enhanced) para colocar chaves de criptografia de 128 bits (16 caracteres hexadecimais), você pode criar 8 chaves de criptografia, como:

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

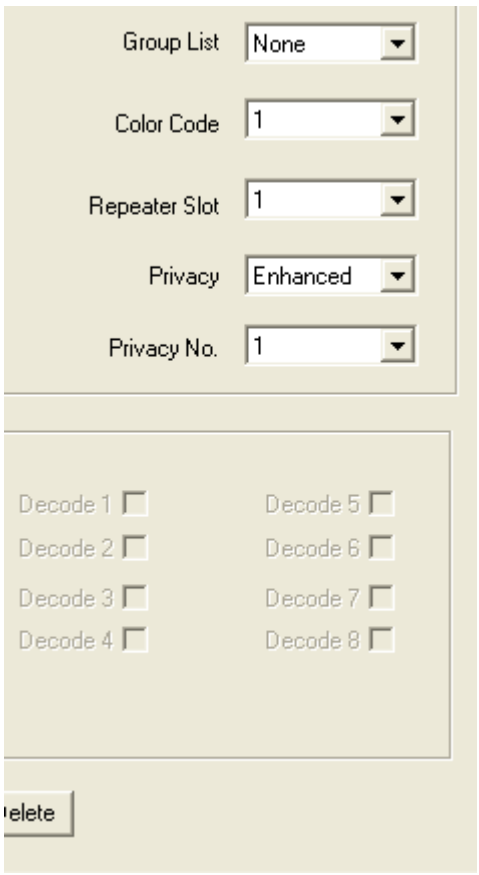
Na seção Informações sobre canais, você pode configurar seus canais:



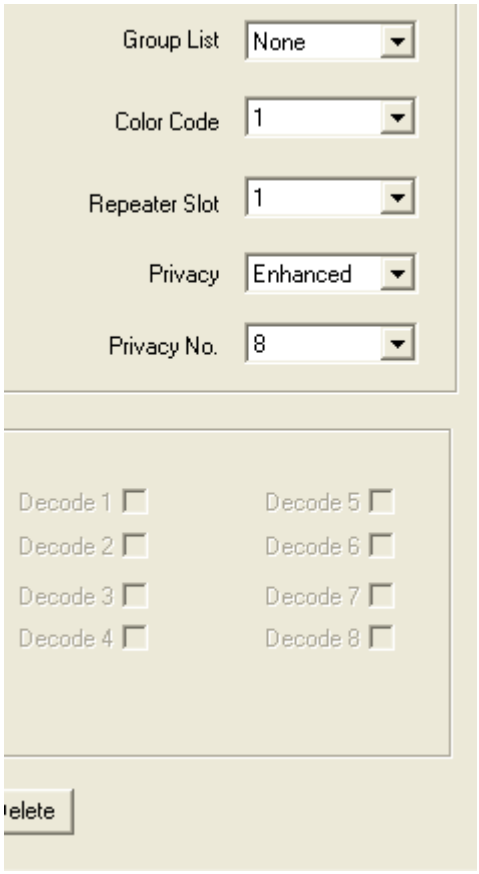
E1 significa Enhanced Privacy Channel 1, E2 Enhanced Privacy Channel 2...

Abrindo o canal E1 vemos:

No canto inferior direito, observamos Enhanced e o número da chave, aqui Privacy Key No. 1.

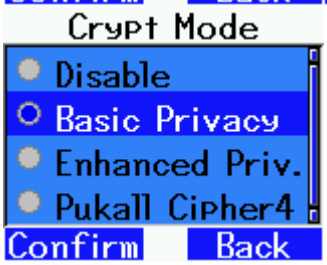


Outro exemplo com o canal E8:

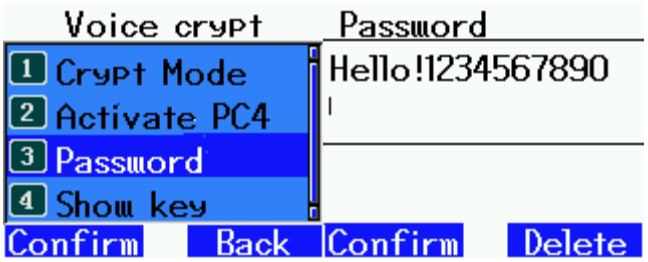


Motorola Basic Privacy Mode com chave de criptografia interna

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



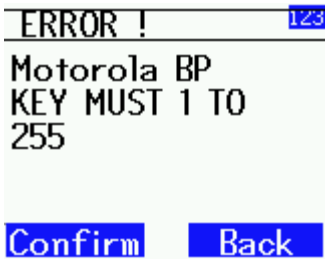
Ir para **3 Password** e digite uma senha com mais de 4 caracteres (ou nenhuma senha):

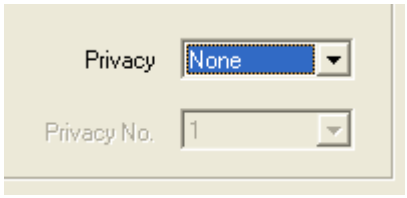


Se a senha consistir em números de 1 a 255, o modo de senha terá precedência sobre o modo de chave interna e a Privacidade Básica usará a senha como chave de criptografia. Caso contrário, ele usa a chave de criptografia interna programada no canal ativo.

Ir para **4 Show Key** :

Se você estiver em um canal sem o modo Avançado estar ativo, então você receberá esta mensagem de erro (porque não há nenhuma chave de criptografia interna ativa):

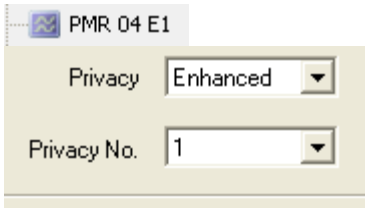




Na tela principal não haverá nada, indicando que a criptografia não está ativa:

Se um canal estiver habilitado no Modo Avançado, ele dependerá do conteúdo do byte mais à direita da chave de criptografia:

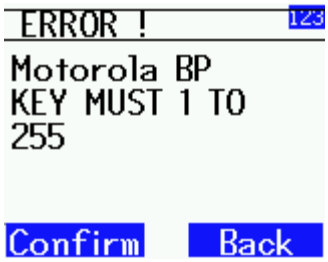
No exemplo a seguir, o canal E1 usa a chave de privacidade aprimorada nº 1:



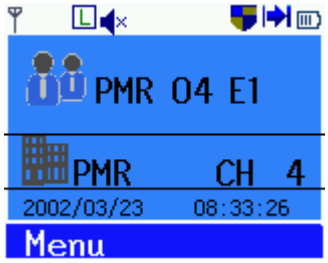
Mas o byte mais à direita da chave de criptografia 1 está em 0:

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

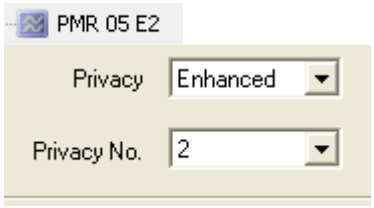
Então você receberá esta mensagem de erro em **4 Show key** :

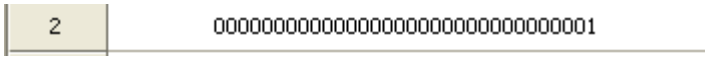


E nada será exibido na tela principal:

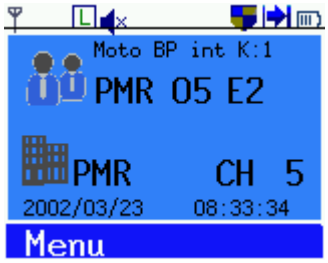


Se formos para o canal E2 que usa a Chave de Privacidade Nº 2:

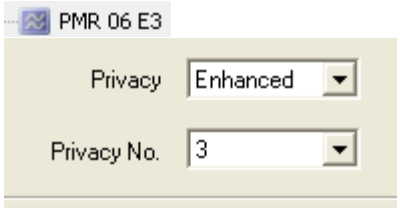




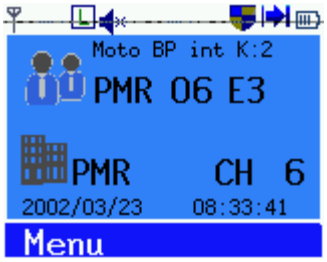
O byte mais à direita sendo 01, a chave Basic Privacy 1 será ativada: "Moto BP int K:1" significa "Motorola Basic Privacy internal key" e o K com o número da chave de criptografia (aqui 1).



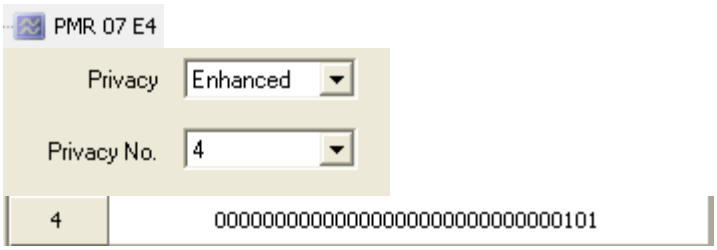
Se formos para o canal E3 que usa a chave de privacidade No. 3:



O byte mais à direita sendo 02, é a chave Basic Privacy 2 que será ativada:

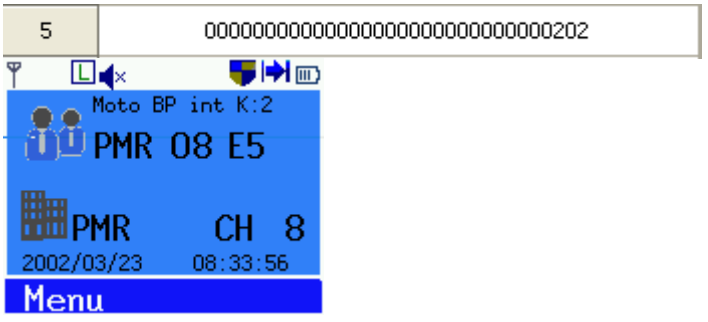


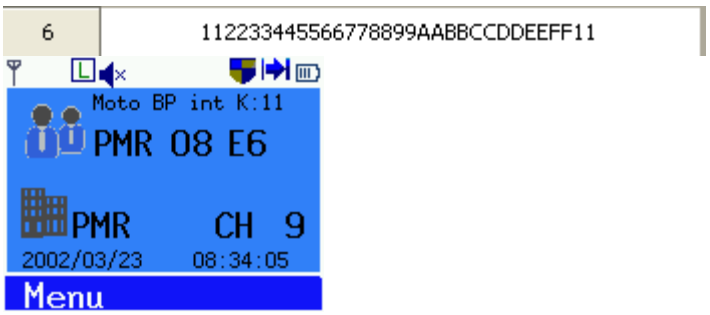
Se formos para o canal E4 que usa a chave de privacidade No. 4:



Existem dois bytes 01, mas é o byte mais à direita que é usado para Privacidade Básica, por isso é a chave Privacidade Básica 1 que será ativada:

Aqui estão os exemplos para o resto dos canais:





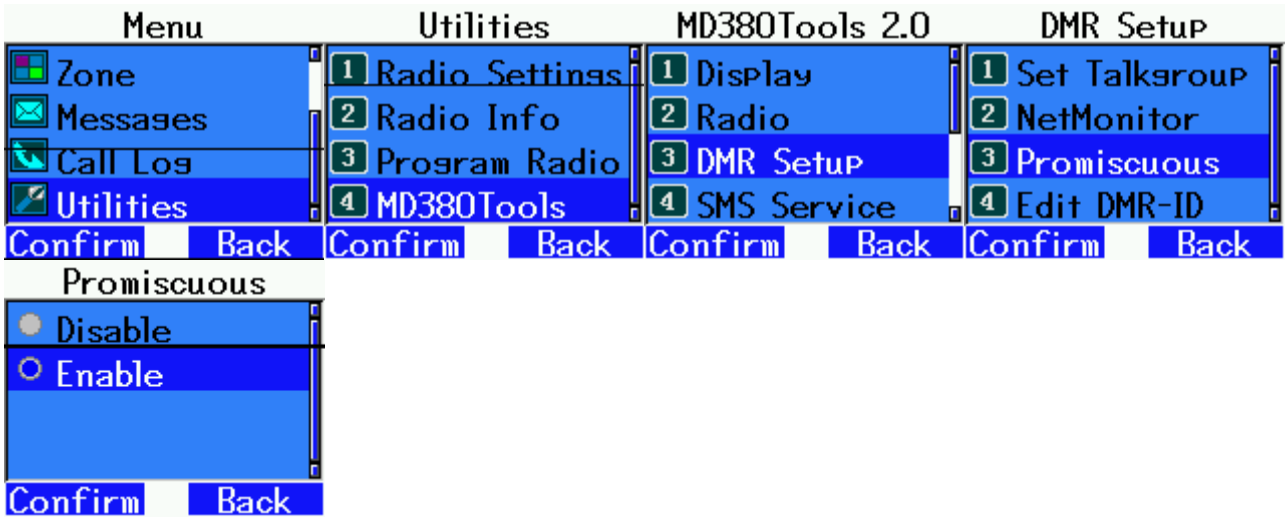
7	74581225622174788112236655123336

8	ABCDEDCBABCDDBCABDBCABDABBABBDBE

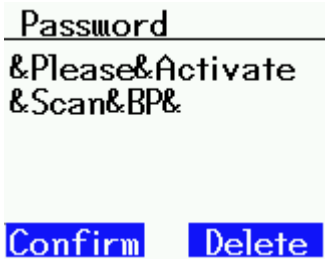
Há uma opção oculta adicional: você pode verificar automaticamente e encontrar uma chave básica de criptografia de privacidade da Motorola.

Primeiro você precisa configurar o MD380 para receber todas as comunicações, este é o modo Promíscuo.

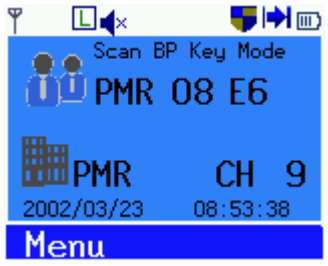
Ir para:



Em seguida, vá para Password e digite a senha secreta:



Em seguida, você entrará no modo Motorola Basic Privacy Scanner:



Aguarde até que uma comunicação criptografada Motorola Basic Privacy inicie, uma vez que a chave de criptografia é encontrada, você ouvirá um sinal sonoro e a comunicação será ouvida descriptografada.

Uma vez que a receção para, você verá a chave de criptografia que foi encontrada:

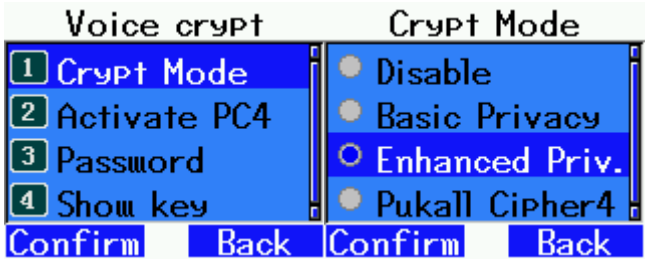
Se você quiser executar uma nova verificação, você pode pressionar o botão PTT uma vez ou pressionar a tecla #.

Tenha cuidado, este modo só funciona com um dispositivo oficial da Motorola porque a Motorola introduziu um backdoor para digitalizar chaves de criptografia. O backdoor não está presente no Voice Crypt, então você não pode encontrar a chave de privacidade básica de outro Voice Crypt MD380.

Para sair do Motorola Basic Privacy Scanner Mode, você pode digitar novamente a mesma senha oculta como acima ou desligar e ligar o MD380 novamente.

Modo de privacidade melhorado Tytera com chave de encriptação interna

Em **Crypt Mode** escolha **Enhanced Privacy**



Então tudo vai depender de qual canal você está.

Ir para **Show key :**

Se vir a mensagem de erro:

É que você não está em um canal de Privacidade Aprimorada. Às vezes você também tem que mudar para outro canal e voltar a ele para que seja levado em conta.

Se você estiver em um canal com privacidade aprimorada, a chave de criptografia de 128 bits usada pelo algoritmo Tytera Enhanced Privacy será exibida.

No exemplo abaixo é Privacidade No. 5:

Na tela principal aparece "Tyt EP int K0:2": Isso significa "Tytera Enhanced Privacy internal key" com K0 (zero byte:2 mais à direita).

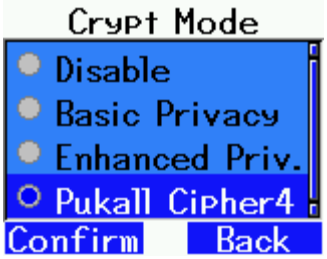
A chave K0 não é a chave de criptografia completa de 128 bits (não há espaço de tela suficiente para exibir tudo), mas permite que o usuário saiba o byte mais à direita, portanto, verifique rapidamente qual chave de criptografia está sendo usada. A chave de criptografia completa é exibida usando a opção **Show key**:

Exemplo com outras chaves de encriptação:

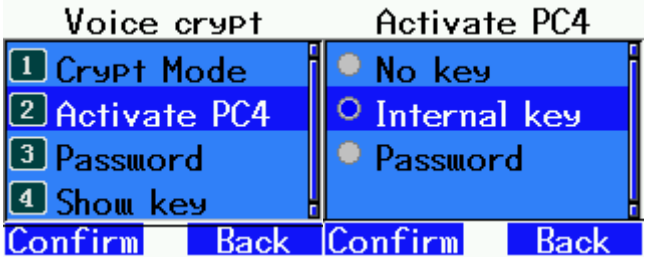

TYT EP KEY
123
ABCDEDCBABCDDBC
ABDBCABDABBABBD
BE
Tyt EP int KO:BE
PMR 11 E8
PMR
CH 11
2002/03/23
08:38:03
Confirm
Back
Menu

Modo de codificação PC4 com chave de encriptação interna

Em **Crypt Mode** escolher **PC4 Cipher**:



Ir para **2 Activate PC4** e escolha **Internal key**:



Tal como acontece com o modo Tyt Enhanced Privacy, a chave de encriptação que utiliza dependerá do canal em que se encontra.

Show Key mostra a chave de encriptação ativa e o ecrã principal mostra o byte mais à direita da chave de encriptação ativa (releia a secção Tyt Enhanced Privacy se necessário para a explicação do byte K0).

PC4 Cipher Peça avançada

PC4 Cipher está ativo no modo mais seguro (253 rodadas de criptografia). No entanto, alguns MD380 podem ter um processador muito lento (CPU), isso resultaria em voz de baixa qualidade.

É possível reduzir o número de rodadas de criptografia se você tiver uma CPU muito lenta. Todos os MD380s devem então ser configurados com o mesmo número de rodadas para poder se comunicar uns com os outros.

Este é um menu oculto, para ativá-lo você tem que ir para **8 Voice Crypt:**

Então **3 Password :**

Em seguida, você deve digitar uma senha especial com minúsculas, maiúsculas e caracteres especiais : « **&Please&Activate&Round&Config&** » :

Saia do menu e volte para o menu, o menu oculto apareceu:

Você pode então reduzir o número de rodadas (isso também reduz a segurança e só deve ser feito se a CPU estiver muito lenta e a voz estiver ruim):

Na tela principal você é avisado que você está em um modo com rodadas reduzidas e isso é exibido para PC4 com senha ou PC4 com chave interna:

Você pode fazer esse menu oculto desaparecer novamente digitando a mesma senha especial uma segunda vez.

Configuração do MI

PC4 Cipher é um algoritmo de cifra de bloco de modo ECB. Isso significa que dados idênticos em quadros de voz diferentes serão criptografados da mesma maneira se a mesma chave de criptografia for usada. É o caso, por exemplo, das molduras de silêncio.

Para evitar isso, existe uma opção adicional que adiciona dados aleatórios para que quadros de silêncio idênticos sejam criptografados de forma diferente.

Isso aumenta a segurança, mas diminui a qualidade da voz porque os bits nos quadros de voz são removidos.

Você pode escolher entre 4 e 6 bits por quadro de voz. Com 6 bits, a segurança é melhor do que com 4 bits, mas o som é pior.

É um menu oculto, para ativá-lo você tem que ir para **8 Voice Crypt :**

Em seguida, **3 Password :**

Em seguida, deve introduzir uma palavra-passe especial com letras minúsculas e carateres especiais: « **&Please&Activate&MI&Config&** » :

Saia do menu e volte ao menu, o menu oculto está aqui:

No menu principal, você será notificado pelo MI4 ou MI6 se estiver no modo MI Config.

Idealmente, todos os participantes de uma discussão devem usar a mesma configuração de MI, mas isso não é obrigatório, a descriptografia é possível mesmo que nem todos usem a mesma configuração de MI.

Você pode fazer esse menu oculto desaparecer novamente digitando novamente a mesma senha especial uma segunda vez.

Encriptação RC2

Voice Crypt oferece outro modo de criptografia: RC2 no modo CFB.

Esta é uma cifra de encriptação criada por Ron Rivest e melhorada por Alexander Pukall (remoção de tamanhos de chave de encriptação reduzidos e aumento do estado interno do RC2 para 1024 bits).

O tamanho da chave de encriptação é de 128 bits se utilizar as chaves de encriptação internas ou de até 420 bits se utilizar uma palavra-passe de 60 caracteres.

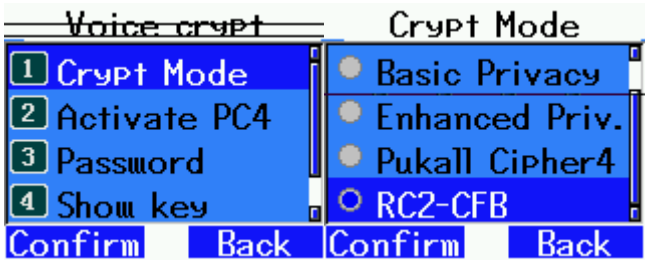
Ele também usa um MI Config de 6 bits para que este modo RC2 degrade a qualidade do som da voz.

É um menu oculto, para ativá-lo você tem que ir para **8 Voice Crypt :**

Em seguida, **3 Password :**

Em seguida, deve introduzir uma palavra-passe especial com letras minúsculas e carateres especiais: « **&Please&Activate&RC2&Encryption&** » :

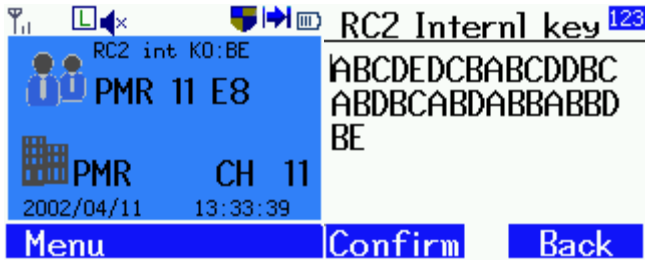
Saia do menu e volte ao menu, o menu oculto está aqui:



Você pode fazer esse menu oculto desaparecer novamente digitando novamente a mesma senha especial uma segunda vez.

Para usar o modo com uma senha, ative a Password em PC4 Activate (mesmo que PC4 não esteja ativo, mas RC2).

Você também pode escolher **Internal Key** :



Repor

Em caso de problema e se nada funcionar corretamente você pode redefinir todas as opções.

Ir para **Utilities - 4 MD380 Tools- 7 Developer – 4 Config Reset**