16 de Septiembre 2001

mexican hackers mafia
http://osukaru.cjb.net
mhm@kmfms.com

Contenido

Introducción

Bienvenidos al primer e-zine Mexicano dedicado al phreaking y el estudio de la electrónica underground. No quiero aburrirlos con el clásico texto de quienes somos y que hacemos aquí así que seré lo más breve posible.

Mexican Hackers Mafia (MHM para los amigos ;) nace alrededor de cuatro años cuando un grupo de entonces estudiantes de bachillerato se reunió con el propósito de hackear el sitio web de una preparatoria a la cual uno de nosotros asistía. Desde entonces muchas cosas han cambiado, cada uno de los integrantes originales tomo su propio camino, muchos integrantes han entrado y muchos se han ido, pero el cambio mayor se dio una tarde de Enero del presente año, para ser más precisos el 15/01/01, día en que se decidió dar un giro en cuanto al grupo y la página referían, se decidió formar el primer grupo organizado enfocado a el estudio de la telefonía y la electrónica underground en México.

Gracias al excelente recibimiento que tuvieron la página y el foro se decidió emprender la tarea de realizar una revista electrónica que diera a conocer de manera periódica los sucesos, artículos e información más importante enfocada a esta creciente parte del movimiento hacktivista en México.

Este, nuestro primer e-zine cuenta con información en su mayoría inédita y de un alto interés, que varía en nivel para proporcionar una gama lo más amplia posible de conocimiento, que puede ser disfrutado tanto por el novato como por los más avanzados en estos temas.

Contamos con textos escritos por colegas hackers de España y Argentina además de los escritos por colegas nacionales. Cabe aclarar que toda la información aquí expuesta es enfocada a México, pero eso no excluye a otros países que cuentan con el mismo tipo tecnología.

Agradezco a todos los que mandaron sus textos y a todo aquel que de alguna forma u otra ha contribuido con el desarrollo del phreaking en nuestro país.

Por ultimo aprovecho para mandar un saludo a todo el equipo de AcidKlan, a los webmasters de Hackers.com.mx a Raza-Mexicana y a todos los que nos han apoyado.

-=oSUKARu=-

DISCLAIMER

MHM y sus miembros no nos hacemos responsables del uso que se le de a la información contenida en está revista electrónica.

Los textos, gráficas y diagramas dadas a conocer por éste medio se exponen con el único fin de proporcionar datos técnicos y de investigación; y deberán ser empleados únicamente para fines educativos.

Estudio de Tarjetas de 128 bit

- Capitulo I -

By PitufoEnrike

Antes de Empezar

Bueno antes que nada quería comunicarles a todos aquellos phreakers en especial a los que se dedican al estudio de las tarjetas de teléfono, que en mi país ARGENTINA el día 20 / 08 / 2001 se realizó un parche en las cabinas de Telefónica Argentina, este parche consistía en cambiar el sistema.

A partir del año pasado en nuestro país las cabinas eran compatibles con las tarjetas de 256 bits y 128 bits pero después de la fecha ya mencionada solamente las cabinas de esta empresa funcionan con tarjetas de 128 bits. Es decir que todas las personas que poseían tarjetas de vieja generación dejaron de funcionar (Yo puedo decir prácticamente que la mitad del país, " de cada 10 personas que yo veía en una cabina 5 tenían emuladores de las viejas generación). Pero las cabinas de su empresa competidora TELECOM, creo yo, que siguen funcionando con tarjetas de vieja generación pero aun no he visto a nadie con un emulador en la actualidad en esas cabinas.

Este es el primer documento que me atrevo a escribir, no será mucho pero sé que algunas personas puedo llegar a ayudar. Tal vez mas adelante escriba otros documentos relacionados con este tema, pero es cuestión de tiempo.

La base de datos de una tarjeta telefónica (El contador octal)

Bueno como todos sabemos, las tarjetas chips, cualquiera de ellas poseen una base de datos en su interior, nuestras tarjetas de vieja generación las de 8 contactos eran de 256 bits pero dada ya su inexistencia no hablaremos mas de ellas, nos enfocaremos solamente en las famosas tarjetas de 6 contactos que realmente son tarjetas de 128 bits o precisamente de 16 bytes (del 1 al 16), a esta altura debemos saber que un byte se compone de 8 bits, si multiplicamos 8 x 16 obtenemos 128 (esto esta muy claro.

Con mi lector The Electron 2.7 que para mí es el mejor que he tenido entre mis manos he leído bastantes tarjetas de diferentes países y a continuación voy a ponerles los datos y a explicarles que significa cada uno de ellos (quiero recordarles que este informe se enfoca solamente en el contador octal que puede ser de 4 o de 5. En la Argentina por lo que yo he comprobado solamente se utiliza el contador octal de 4.

- Tarjetas Argentinas

0 A1 ← Tarjeta Telefónica en Argentina
1- 2B ← Pais de la Tarjeta
2- 67 ← Fabricante
3- C0 ← Valor máximo de la Tarjeta
4- 20 ← Numero de Serie
5- 02 ← Numero de Serie
6- 11 ← Numero de Serie
7- 28 ← Checksum
8- 00 ← Crédito de la tarjeta — Contador Octal de 5 — Contador Octal de 4 — x 4096
9- 00 ← Crédito de la tarjeta — Contador Octal de 5 — Contador Octal de 4 — x 512
10- 7F ← Crédito de la tarjeta — Contador Octal de 5 — Contador Octal de 4 — x 64
11- 3F ← Crédito de la tarjeta — Contador Octal de 5 — Contador Octal de 4 — x 8
12- 0F ← Crédito de la tarjeta — Contador Octal de 5 — Contador Octal de 4 — x 1
13- FF ← Seteados a 1 de fabrica
14- FF ← Seteados a 1 de fabrica
15- FF ← Seteados a 1 de fabrica

Como vemos el contador octal se encuentra a partir del byte 08 al byte 12, e aquí el valor de la tarjeta en hexadecimal.

Por ejemplo, si agarramos una de las tarjetas argentinas, en el byte número 12, **" 0F "** que en binario seria **00001111** vemos que se compone de cuatro unos, a este cuatro lo multiplicamos por 1 como he puesto anteriormente en la base de datos y obtenemos un 4 que en realidad seria **$ 0,04**, luego agarramos el byte número 11, **"3F"** que en binario seria **00111111** y vemos que se compone de seis unos, a este seis lo multiplicamos 8 y obtenemos un 48 que en realidad sería **$ 0,48**, luego agarramos el byte 10, **"7F"** que en binario seria **01111111** que se compone de siete unos, este siete lo multiplicamos por 64 y obtenemos 448 que seria **$ 4,48**, a los otros dos bytes no hace falta realizar el procedimiento por que son 00. Ahora sumamos los valores obtenidos:

0,04 + 0,48 + 4,48 = $ 5,00 (Muy Fácil)

El valor máximo que yo pude comprobar es de **$ 46,80** es decir he puesto a partir del byte 9 al 12 todos FF pero no se los recomiendo ya que en Argentina no existe tarjetas de semejante valor (creo yo) y telefónica podría sospechar, por otra parte no intenten poner FF a partir del byte 08 por que la cabina no tomará la tarjeta. Es decir que las tarjetas de este país tienen solamente contador octal de 4.

Agradecimientos

Sinceramente debo agradecer a todas aquellas personas que se iniciaron a partir del foro de AAS y sus derivaciones ZACKY, DARKEB, MURDOCKDJ, SHELLGHOST, JMB4U, DARKMAN2010 y otros que no recuerdo, en su mayoría comunidad española, que realmente tengo un muy buen concepto del poder de imaginación que tienen, no voy a empezar a decir quienes son por miedo a olvidarme de alguien, ustedes sabrán.

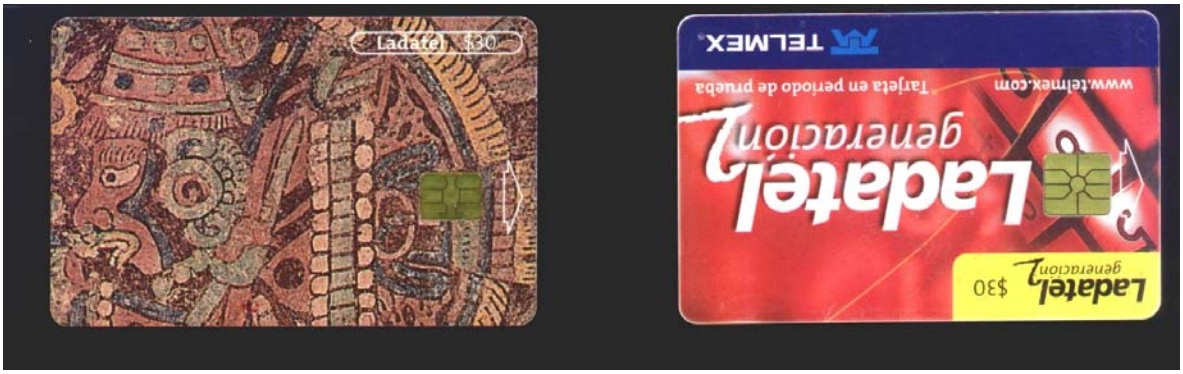
También al canal #Cabinas del IRC Hispano donde se encuentran todo los "GROSOS" de este mundillo.

Nota

Cualquier error por favor comunicarse a: tecnicoinfroma@yahoo.com.ar

Autor : PitufoEnrike
País : MENDOZA – ARGENTINA
Creado el : 03 / 09 / 2001
Sitio Oficial : http://www.tecnicos.da.ru

Tarjetas de 128 bits de Telmex



Fotos por Paco_1585

INTRODUCCIÓN A LOS MICROCONTROLADORES: P I C 1 6 F 8 4 A

por o0ShellGhost0o

Introducción:

En la actualidad esta muy de moda aprender a programar algún tipo de microcontrolador, sobre todo los hechos por la casa Microchip, denominados PICs (Programable Integrated Circuit). Nosotros nos estaremos enfocando específicamente en el 16F84, microcontrolador utilizado por excelencia en la fabricación de emuladores de tarjetas telefónicas en el área del phreaking, aunque puede ser empleado en miles de proyectos tanto hobbistas como underground, su uso puede ir desde una beige box avanzada hasta un modchip para tu consola preferida o un controlador de MP3 ‘s...

El PIC16F84 se encuentra en la gama media de microcontroladores de Microchip, cuenta con un total de 35 instrucciones a aprender lo cual lo hace idóneo para el aficionado que tenga interés en aprender micros.

Quizás la mejor excusa para aprender este modelo en especifico es porque –dejando aparte el hecho de que es uno de los más empleados en la actualidad- la estructura y forma de programación de todos los PICs es sumamente similar, y al aprender a programar un microcontrolador de gama media se tiene cubierto casi por completo la programación de la gama baja y se requiere un esfuerzo mínimo para aprender a programar la gama alta.

Antes de entrar en materia me gustaría aclarar que este texto esta enfocado hacia el novato en microcontroladores por lo que trataré de mantenerlo lo más entendible y conciso posible, así es que todos los Súper-coders que están leyendo esto les puede resultar un poco aburrido ya que revisaremos los elementos más básicos y no entraremos en mucha profundidad.

Ahora sí, dicho lo anterior comencemos :)

Datos Relevantes:

Memoria de Programación	RAM (bytes)	EEPROM (bytes)	Máxima Frecuencia (MHz)
1K Flash	68	64	20

Arquitectura.

La arquitectura del procesador sigue el modelo Harvard. En esta arquitectura, la CPU se conecta de forma independiente y con buses distintos con la memoria de instrucciones y con la de datos.

La arquitectura Harvard permite a la CPU acceder simultáneamente a las dos memorias. Además, propicia numerosas ventajas al funcionamiento del sistema.

Segmentación.

Se aplica la técnica de segmentación (“pipe-line”) en la ejecución de las instrucciones.

La segmentación permite al procesador realizar al mismo tiempo la ejecución de una instrucción y la búsqueda del código de la siguiente. De esta forma se puede ejecutar cada instrucción en un ciclo (un ciclo de instrucción equivale a cuatro ciclos de reloj).

Las instrucciones de salto ocupan dos ciclos al no conocer la dirección de la siguiente instrucción hasta que no se haya completado la de bifurcación.

Formato de las instrucciones.

El formato de todas las instrucciones es de la misma longitud.

Todas las instrucciones de los microcontroladores de la gama media tienen 14 bits. Esta característica es muy ventajosa en la optimización de la memoria de instrucciones y facilita enormemente la construcción de ensambladores y compiladores.

Juego de instrucciones.

Procesador RISC (Computador de Juego de Instrucciones Reducido).

El PIC16F84 cuenta con un total de 35 instrucciones.

Cualquier instrucción puede manejar cualquier elemento de la arquitectura como fuente o como destino.

Arquitectura basada en un “banco de registros”

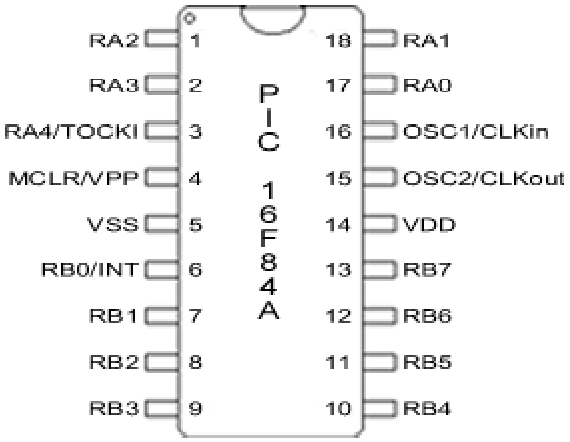
Esto significa que todos los objetos del sistema (puertas de E/S, temporizadores, posiciones de memoria, etc.) están implementados físicamente como registros.

PIN-OUT:

Como todo circuito integrado, el 16F84 tiene entradas y salidas. Por supuesto necesita una tensión de 5V (VDD) aplicada con respecto a la masa (VSS).

Posee dos puertos, el A y el B, cuyas terminales son marcadas RA0 al RA4 y RB0 al RB7 los cuales pueden ser programados como entrada o salida respectivamente.

El pin 3 (RA4) también cumple la función de entrada de un temporizador, el pin 6 (RB0) cumple la función también, de entrada de interrupción, y el pin 4 tiene la función de reset.



Disposición de los Puertos:

Cómo mencione anteriormente, el 16f84 cuenta con dos puertos de entrada o salida de datos. Estos puertos son: El puerto A de 5 patas y el puerto B de 8. Cada pata cuenta con una resistencia en pull-up (resistor conectado a la fuente) interna que puede ser desconectada mediante el programa. Estos resistores se desconectan automáticamente cuando una pata es programada como salida.

La pata 3, o sea, RA4/TOCKI, cuando es salida, se comporta como colector abierto, por lo tanto debemos poner una resistencia Pull-up a Vcc de 1 Kohm. Cuando es configurada como entrada, funciona como disparador Schmitt Trigger por lo que puede reconocer señales con un poco de distorsión.

Los pines 15 y 16 son únicamente para el oscilador externo el cual estudiaremos con más detalle más adelante. El pin 4, o sea, el Reset se debe conectar con una resistencia de 10 Kohm a Vcc para que el PIC funcione, si lo queremos resetear entonces pondremos un micro pulsador con una resistencia de 100 Ohm a tierra.

La máxima capacidad de corriente para los puertos se muestra en la siguiente tabla:

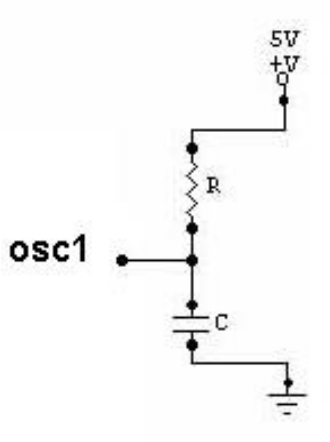
	PUERTO A	PUERTO B
PUEDE TOMAR	80 mA	150 mA
PUEDE ENTREGAR	50 mA	100 mA

Por último tenemos los pines 14 y 5 que son la alimentación la cual no debe sobrepasar los 5 Voltios. Para esto nos aseguramos poniendo un regulador de voltaje (7805) en nuestro circuito.

Es importante denotar que los pines de los puertos no utilizados los debemos conectar a +5V (Vcc) con una resistencia de 10 Kohm debido a que se trata de un dispositivo CMOS que de otro modo podría deteriorarse por captación electroestática.

Oscilador Externo:

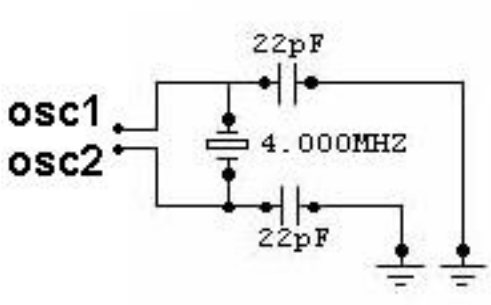
Es necesario para que nuestro PIC pueda funcionar, puede ser conectado de cuatro maneras diferentes. En la siguiente tabla encontraras los diagramas necesarios para su conexión y una breve descripción de cada uno.



Oscilador RC

Oscilador compuesto por una resistencia y un condensador.

Generalmente es empleado en aplicaciones que no requieren de mucha precisión.



Oscilador XT

Oscilador compuesto por un cristal y dos condensadores.

Se emplea en proyectos que requieren un poco más de precisión.

Oscilador HS

Oscilador compuesto por un cristal de alta velocidad.

Oscilador LP

Oscilador compuesto por un cristal de baja frecuencia y bajo consumo de potencia.

Ahora que ya tenemos una idea de lo que son los puertos, su configuración y los diferentes osciladores que hay, el siguiente paso importante para tener claro como debemos empezar a programar es conocer la tabla de registros.

Esta tabla está dividida en dos partes llamadas BANCO 0 y BANCO 1. Nos debemos interesar momentáneamente en: STATUS, PORTA, PORTB, TRISA y TRISB.

Para que nuestro PIC pueda trabajar debemos configurar sus puertos según sea el caso, como entrada o como salida, haciendo antes la acotación que si le asignamos un CERO(0) a un pin éste será SALIDA y si asignamos un UNO (1) éste será ENTRADA.

Esta asignación de pines se hace programando los registros TRISA y TRIS B.

TRISA es el registro donde se almacenan los bits que asignan un pin como entrada o salida del PUERTO A. Recordemos que el puerto A sólo tiene 5 pines, por lo tanto un ejemplo de esto sería:

Si TRISA (puerto A) es igual a 10110 entonces esto se leería,

TRISA	ASIGNACION	ESTADO
RA0	0	SALIDA
RA1	1	ENTRADA
RA2	1	ENTRADA
RA3	0	SALIDA
RA4	0	ENTRADA

El bit menos significativo se asigna desde RA0.

Si TRISB (puerto B) es igual a 00110000, entonces esto se leería,

TRISB	ASIGNACION	ESTADO
RB0	0	SALIDA
RB1	1	SALIDA
RB2	0	SALIDA
RB3	0	SALIDA
RB4	1	ENTRADA
RB5	1	ENTRADA
RB6	0	SALIDA
RB7	0	SALIDA

Ahora bien, pero como ponemos este número en TRISA y TRISB?

Para esto tenemos que ir a la tabla, la cual se divide en BANCO 0 y BANCO 1. Cuando el PIC arranca a correr el programa siempre se va a encontrar en el BANCO 0, por lo tanto debemos pasar al BANCO 1 para poder configurar los puertos asignando valores a TRISA y TRISB. Esto se logra a través del Registro STATUS, el cual nos servirá para cambiarnos de Banco.

7	6	5	4	3	2	1	0
R/W	R/W	R/W	R	R	R/W	R/W	R/W
IRP	RP1	RP0	/TO	/PD	Z	DC	C

C: Acarreo en el 8º bit.
1 = acarreo en la suma y no en la resta. 0 = acarreo en la resta y no en la suma
DC: Acarreo en el 4º bit de menor peso.
Igual que C.
Z: Zero.
1 = El resultado de alguna operación es 0. 0 = El resultado es distinto de 0
/PD: Power Down.
1 = Recién encendido o tras CLRWDT. 0 = Tras ejecutar una instrucción SLEEP
/TO: Timer Out.
1 = Recién encendido, tras CLRWDT, o SLEEP. 0 = Saltó el WDT

Es importante saber que este registro es de 8 BIT, o sea, ocho casillas, en la cual la No. 5 (RP0) define la posición del BANCO donde nos encontramos, por defecto siempre se encuentra en el BANCO 0.

Si en la casilla 5 (RP0) del registro STATUS hay un CERO entonces estamos en el BANCO 0. Si en la casilla 5 (RP0) del registro STATUS hay un UNO entonces estamos en el BANCO 1.

Pero como ponemos un UNO en la posición 5 del registro STATUS para entrar al BANCO 1? Aquí es donde empezamos a ver las instrucciones de programa.

La dos primeras a utilizar son:

BSF que significa BIT SET FILE REGISTER, es decir, pone un uno en la localización de la RAM especificada.

BCF que significa BIT CLEAR FILE REGISTER, es decir, pone un cero en la localización de memoria especificada.

Por lo tanto, para entrar al banco 1 tenemos que poner un UNO en la posición 5 del registro STATUS, lo que sería así:

Sintaxis:	**bsf STATUS,5**
	nota: las instrucciones pueden ser escritas en mayúsculas o minúsculas.

Ahora nos toca decidir según el proyecto que vallamos a hacer quien va a ser ENTRADA y quien va a ser SALIDA.

Supongamos entonces que todos los pines del puerto A van a ser ENTRADA y el puerto B SALIDA.

Tendríamos que asignar al puerto A : 11111
Y al puerto B : 00000000

Movamos entonces estos valores a TRISA y TRISB respectivamente a través de la siguiente sintaxis:

Sintaxis:	**movlw B'11111'** **movwf TRISA**

En la primera línea estamos moviendo el valor de 11111 a W. W es el Registro de Trabajo, el cual usaremos para almacenar momentáneamente los datos que queramos mover. Después que los datos están en el registro de trabajo W, los podemos mover a TRISA, de esta manera ya configuramos el puerto A. La ¨B¨ y las comillas es la manera más común de designar el dato como NUMERO BINARIO, de esta manera se nos hace más fácil saber en determinado momento a quién pusimos como ENTRADA o SALIDA.
Ahora configuremos el puerto B.

Sintaxis:	**movlw B'00000000'** **movwf TRISB**

De nueva cuenta tomamos el valor en binario y lo metemos a W, para después pasarlo al TRISB.

Configurado el puerto B nos salimos del BANCO 1 al BANCO 0 para empezar ya a programar.
Para salirnos del BANCO 1 solo debemos poner un CERO en la posición 5 (RP0) del registro STATUS.

Sintaxis:	**bcf STATUS,5**

En este momento nos encontramos en el BANCO 0.

Ahora ya conocemos el procedimiento a seguir para configurar las entradas y salidas de los puertos A y B de nuestro PIC lo cual es básico en la programación de este.

Por motivos de espacio, hasta aquí vamos a llegar en esta ocasión con el curso. Dependiendo de la respuesta que se tenga al respecto pensaré luego en escribir algo un poco más extenso y más avanzado. Mientras tanto, para toda la gente que quiera aprender más acerca de este versátil microcontrolador le recomiendo que se baje el DATASHEET del mismo, de la página web de Microchip (http://www.microchip.com).

Espero que esto les haya servido de algo a todos los que oían hablar del 16F84 y querían aprender un poco más de el.

.o0ShellGhost0o.

Mexican Hackers Mafia 2001
http://osukaru.cjb.net

Números Extraños

Por: eagle4

Estos números dan servicios que Telmex no da al publico espero que sirvan de algo.

*080 -información sobre el numero de teléfono.

*123456 -Este numero conecta a un servidor de uninet si se marca desde un teléfono normal desde un publico contesta una operadora de Telmex preguntando a donde quieres llamar.

*20# -Este es el buzón de voz

21 numero de teléfono # -Este numero si lo da al publico Telmex es para direccionar el numero de teléfono desde el que llamas a otro (¿quien dijo que este servicio se tenia que pagar? :-))

#21# -Este deshabilita el redirecionamiento de llamada

*43# -Este activa la llamada en espera (no se muy bien pero parece que tampoco tenemos que pagar por este, y si funciona el servicio)

66 -Este es el programador del timbre del buzón de voz.

Estos números activan algún servicio pero aun no descubro como utilizarlos
*51
*61
*67
*74
y este que no se que hace 01 700 es un servició como el 01 800 o el 01 900 pero no se para que servirá; espero que este texto sirva de algo.

Introducción al Phreaking: Beige Box

por: -=oSUKARu=-

Es nuestro primer e-zine, así que comenzare con un texto básico para todo aquel que quiera incursionar al mundillo del phreaking en nuestro país.

En este caso hablaré de una de las pocas boxes que realmente funcionan, y en su diseño más básico, la más fácil de construir y usar, la famosa BEIGE BOX.

Muchos de ustedes probablemente habrán visto alguna vez el teléfono que llevan los técnicos de Telmex colgado del cinturón de herramientas, habrán notado también como te los encuentras haciendo llamadas personales en lugar de ponerse a trabajar, y a más de uno de ustedes les agradaría la idea de poder hacer lo mismo... pues hoy es su día XD

Antes que nada tenemos que ver que es exactamente un teléfono de esos, así que empezaremos a analizarlo:

- El nombre técnico en ingles es: “Buttset” o “Lineman’s Handset”, es utilizado principalmente por la industria telefónica para hacer comprobaciones en las líneas.
- La principal característica de este aparatillo es el hecho de que trae un teclado en lo que sería el microteléfono de un aparato normal.
- En la parte inferior del handset se puede ver unos cables con puntas estilo caimanes que sirven para poder conectarse a cualquier línea.
- En algunos modelos de estos teléfonos se cuenta con un botón para quitar el sonido del micrófono.
- Unos modelos cuentan también con botones programables para marcado rápido de claves y teléfonos.

Un teléfono de estos cuesta alrededor de $100.ºº dólares y puede subir hasta casi $200.ºº dependiendo del numero de funciones que este traiga.

¿Un poco fuera del presupuesto de muchos de nosotros, verdad? Pero ¿para qué comprar algo que podemos construir nosotros mismos? Es aquí donde la beige box entra en escena... :)

Materiales y Herramientas a emplear:

- Cautín de lápiz o pistola.
- Estaño (soldadura).
- Una caja con conector RJ11 (ó RJ12).
- Cable (de preferencia retráctil).
- Dos puntas de caimán.
- Dos alfileres.
- Cutter o pinzas para pelar cables.
- Desarmador plano.
- Teléfono

Empezamos por tomar la caja con conector RJ12, la abrimos utilizando el desarmador plano y localizamos los tornillos de los contactos como se muestra en la figura:

Por el momento únicamente utilizaremos los marcados como Ring y Tip, generalmente asignados con los colores rojo y verde correspondientemente.

A continuación cortamos dos trozos de cable a un tamaño no mayor a 20 cm y soldamos las puntas de caimán a cada uno (recuerden comprar los caimanes de diferente color, de preferencia rojo y verde).

Una vez que tengas los cables soldados, suelda los alfileres a las cabezas de los caimanes. (Esto puede ser algo difícil, pero resultará muy útil cuando estemos utilizando nuestra caja).

Atornilla el cable con el caimán rojo a la terminal RING y el caimán verde a la terminal TIP.

Cierra la caja y ¡¡¡listo!!!

Ahora tu caja se debe de ver algo así:

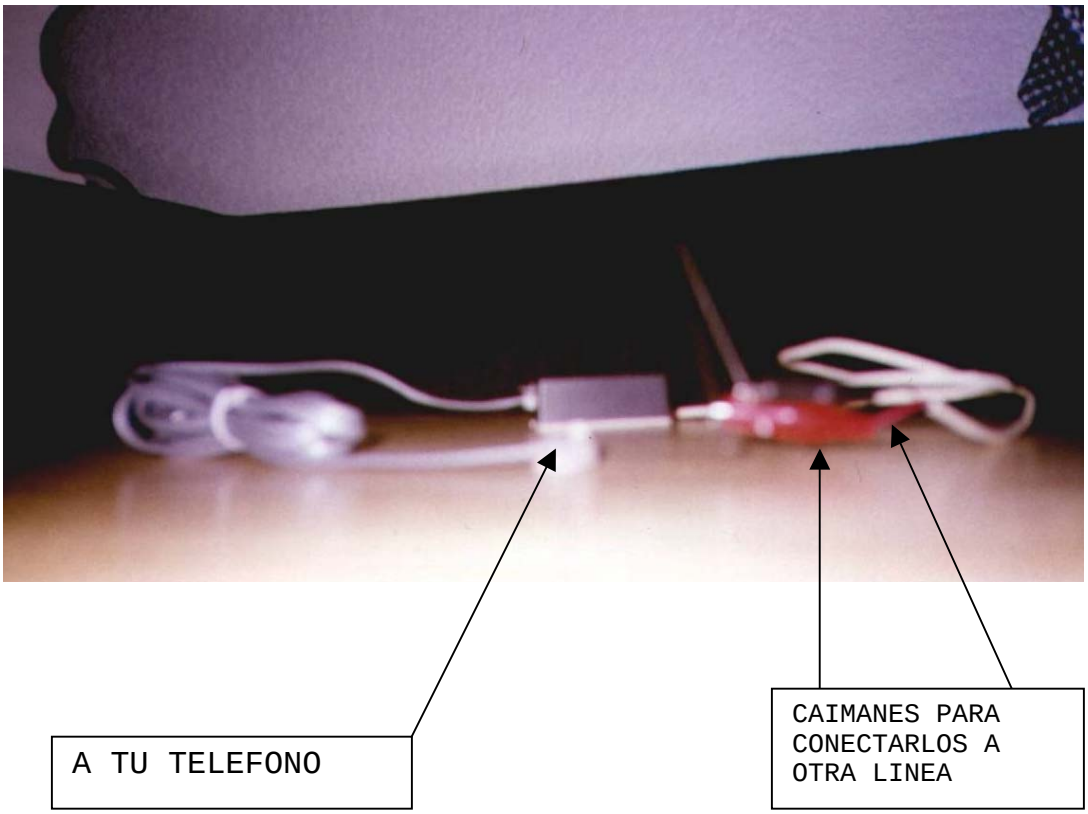


Foto por: Paco_1585

Como usar la BEIGE BOX:

Primero busca una caja de distribución de líneas telefónicas de Telmex que se encuentre abierta, generalmente en colonias de nivel bajo encuentras muchas de estas abiertas o únicamente sujetas por un alambre.

Ábrela, dentro de su interior encontraras una serie de pares de cables, por lo general vienen marcados como ring y tip según corresponda. De no ser así solo conecta tu beige box hasta que encuentres un par que te dé línea.

Ahora podrás realizar tus llamadas sin problema alguno. Solo recuerda que estas conectado a la línea de otra persona y que esta pagara por las llamadas que tu hagas, así que de preferencia NO hagas llamadas de larga distancia, ni abuses de una sola línea.

Por ultimo me gustaría aclarar que hacer esto es ilegal y por ningún motivo recomiendo que dicha práctica se lleve a cabo. Este texto fue escrito con fines educativos por lo que me deslindo de cualquier responsabilidad que se me pudiera adjudicar.

Un saludo,

-=oSUKARu=-
Mexican Hackers Mafia
http:// osukaru.cjb.net

OBTENCION DEL CHECKSUM PARA LAS TARJETAS DE 128 BIT ESPAÑOLAS.

Por Darkman

Como en México dudo que sirva este algoritmo, pues vamos a explicar la teoría.

En España todas las tarjetas tienen este formato:

E0 3C FA MA SE SE SE CK AA AA AA AA AA FF FF FF

A ver lo trato de explicar un poco

E0 3c es igual para todas las tarjetas

Fa es el fabricante

Ma es el dinero inicial máximo que tiene la card

Se es el numero de serie

Ck es el checksum

Aa es el ábaco del dinero

Ff siempre es ff en todas las cards

Ahora bien expliquemos pequeños conceptos:

1. - Si tenemos una card que usa un numero de serie y la gastamos, dicho numero de serie se anula en la centralita, entonces al intentar hacer una llamada con un emulador usando un numero de serie que la centralita tiene como gastado, pues esta no te deja, al principio solo te impedía llamar a los números internacionales y los 906 (números de pago en España), pero últimamente la central hacia la comprobación del numero de serie en todas las llamadas.

2. - Esto tiene una solución, cada vez que queramos llamar, simplemente cambiamos el numero de serie del emulador, pero esto tenia un problema, el "checksum", son los datos representados como "ck", si el checksum es incorrecto no acepta el numero. Pero que es el checksum, pues es el resultado a unas cuentas con los datos "fa","ma"y los tres "se", la cabina lo que hace para saber si la card es valida o no, primero comprueba que empiece por "e0" "3c", si no empieza por esto pues rechaza la card, luego coge los datos siguientes y les aplica una formula matemática, y comprueba el resultado con el contenido de la posición "ck" y si es igual pues manda los 3 "se" a la central para que lo verifiquen.

3. - Si la cabina hace esto, nosotros si tuviéramos el programa de la cabina podríamos estudiar el algoritmo, ya que si la cabina lo puede hacer es que lo tiene en su memoria, así que se "coge prestada" una cabina, tras estudiar la placa del lector de tarjetas analizas el micro que lleva, y miras el datasheet y o maravilla en España esta basada en un 80c31 que no lleva memoria de programa, así que a buscar una memoria prom, eprom o eeprom en esa placa, en mi país es la 27c256, la cual no tiene protección de código, pues la leemos.

4. - ya tenemos el programa de la cabina xddd. Ahora buscamos un desensamblador para dicho microprocesador, y lo desensamblamos, a continuación veremos un programa gigantesco que da miedo, pero es relativamente fácil encontrar donde comienza, si sabemos que la cabina lo que hace es comprobar si el comienzo es igual que las cards originales, es decir en España "e0", pues buscamos el dato "e0" en el programa, y cuando encontremos unas líneas en las que se ve que

coge una dirección externa al micro y la compara con "e0" hay tendremos el comienzo de la parte que nos interesa.

5. - a continuación hará una comprobación con el siguiente dato que sea = en todas las cards es decir el "3c" y en caso de que no sea el correcto pues saltara a una posición y si es correcto pues a otra, buscamos a la que sea correcta y analizamos las direcciones que va cogiendo, será algo así:

Cojo dato 4
Operación con dato 4
Guardo en xx
Cojo dato 3
Operación con dato 4
Guardo en xxx
....

Si sabemos que la card comienza con el dato e0 y lo consideramos posición 0, cuando hemos visto que cogía una dirección externa para leer la posición 0 de la card, es decir "e0", y sabemos la posición del checksum en la original, pues solo tenemos que sumar a la posición externa donde esta "e0" la posición donde esta "ck" en la original y sabríamos en que posición externa esta el "ck" así que cuando viéramos una comparación con dicha posición sabríamos que hay acababa el algoritmo del checksum

....
Cojo el resultado y lo compruebo con la posición donde estaría el checksum

****
Extracto de mi web, explicación real de como se obtuvo el ck de 128 para España

Sabemos que todas las tarjetas empiezan por E0 3C (almenos en los
mapeados que yo he visto) así que en el código desensamblado
tiene que haber una comparación con el valor #$E0 y con #$3C
(la cabina desecharía la tarjeta si esta no comenzase con #$E0).
Bien buscamos en el código y lo primero que encontramos esto:

```
2629 90 03 00 MOV DPTR,#$0300
262C E0 MOVX A,@DPTR
262D 54 F0 ANL A,#$F0
262F B4 E0 0B CJNE A,#$E0,$263D <----- comparación con #$E0.
2632 90 03 01 MOV DPTR,#$0301
2635 E0 MOVX A,@DPTR
2636 54 1F ANL A,#$1F
2638 B4 1C 02 CJNE A,#$1C,$263D
263B E4 CLR A
263C 22 RET
263D 74 FF MOV A,#$FF
263F 22 RET
```

La instrucción en la posición 262F es lo que buscamos. El código coge
el valor en #$0300, lo guarda en el acumulador y le hace un and con #$F0.
Comprueba si es igual y si no salta a $263D, donde mete #$FF en el
acumulador y retorna (supongo que será para indicar error). Si el
valor en #$0300 es valido coge el valor en #$0301 y le hace
un and lógico con #$1F, comprobando luego si se obtiene #$1C
(podemos comprobar que si hacemos esto con #$3C obtenemos #$1C).

Bien luego el programa guarda la información de la tarjeta en

la posición #$0300 en adelante.
Según Darkman el cheksum estaría en la posición #$0307
y el programa de la cabina al comprobarlo debe de referenciar esa
posición. Volvemos a buscar en el código asm y encontramos lo siguiente:

```
26C1 90 03 04 MOV DPTR,#$0304
26C4 E0 MOVX A,@DPTR
26C5 78 05 MOV R0,#$05
26C7 03 RR A
26C8 D8 FD DJNZ R0,$26C7
26CA F9 MOV R1,A
26CB 90 03 05 MOV DPTR,#$0305
26CE E0 MOVX A,@DPTR
26CF 78 03 MOV R0,#$03

26D1 03 RR A
26D2 D8 FD DJNZ R0,$26D1
26D4 FA MOV R2,A
26D5 90 03 06 MOV DPTR,#$0306
26D8 E0 MOVX A,@DPTR
26D9 03 RR A
26DA C4 SWAP A
26DB 6A XRL A,R2
26DC 69 XRL A,R1
26DD F9 MOV R1,A
26DE 90 03 03 MOV DPTR,#$0303
26E1 E0 MOVX A,@DPTR
26E2 FA MOV R2,A
26E3 90 03 02 MOV DPTR,#$0302
26E6 E0 MOVX A,@DPTR
26E7 6A XRL A,R2
26E8 C4 SWAP A
26E9 69 XRL A,R1
26EA F9 MOV R1,A
26EB 90 03 07 MOV DPTR,#$0307 <---- la dirección buscada.
26EE E0 MOVX A,@DPTR
26EF B5 01 02 CJNE A,$01,$26F4
26F2 D3 SETB C
26F3 22 RET
26F4 C3 CLR C
26F5 22 RET
```

Podemos comprobar que además de la posición #$0307 se referencia a las
#$0302,#$0303,#$0304,#$0305 y #$0306. Justo los bytes que intervienen
en el cheksum !!!!. Además al final hay una comparación que determina
si C es activado o no, lo mas probable es que C determine si el cheksum
es correcto.

Leyendo el código podemos obtener el algoritmo:

Primero obtenemos #$0304 y se desplaza 5 veces a la derecha, teniendo
en cuenta que el bit 0 pasa a ser el bit 7 en cada rotación. Se
guarda el resultado en el registro R1.

En segundo lugar coge #$0305 y hace el mismo desplazamiento 3 veces y
guarda el resultado en R2.

Tercero. Coge #$0306 lo rota una vez a la derecha e intercambia los
4 bits mas significativos con los 4 menos significativos. Efectúa
una operación XOR con el contenido de R2 y otra con el de R1, guardando
el resultado en R1.

Cuarto. Coge #$0303 y lo guarda en R2

Quinto. Coge #$0302 y hace una operación XOR con R2 (#$0303), intercambia los
4 MSB con los 4 lsb y hace otro XOR con R1. Guardando el resultado
final en R1.

Ultimo paso. Comprueba que el contenido de R1 es igual que el de #$0307
(el cheksum de la tarjeta).

En caso de que el cheksum de la tarjeta no sea valido devuelve C=0. En
caso contrario C=1.

Ya tenemos el algoritmo.

****
RESUMEN:
- Cogemos el cuarto lo rotamos 3 a la izquierda y lo llamamos "x"
- Cogemos el quinto lo rotamos 3 a la derecha y lo llamamos "y"
- Cogemos el sexto lo rotamos 3 a la izquierda y le hacemos XOR con "y" y con "x" y lo llamamos "z"
- Cogemos el tercero y lo llamamos "j"
- Cogemos el segundo y le hacemos XOR con "j" al resultado lo rotamos 4 a la izda. y le hacemos XOR con "z" y lo llamamos "checksum" XDDDD

by DARKMAN 27/08/2001

Trucos y Secretos de Telefonía Celular

por: SaldeAhi

Esta es una recopilación de trucos y secretos para teléfonos celulares escritos por un gran colega phreak, SaldeAhi.

Bloqueo rápido de tu Nokia

Tip para bloquear rápidamente tu nokia (no me refiero al bloqueo del teclado).

Si activas el autobloqueo de teléfono cada vez que apagas tu celular se bloquea (te pide el código) y al encenderlo te dice que esta bloqueado.

Ok, pero si tu desbloqueas tu teléfono haces una llamada y luego quieres bloquearlo sin apagar el teléfono has esto:

Presionas por un segundo el botón de apagar aparece un menú de opciones entre las cuales esta apagar, audio normal, silencio intemperie ,etc.

Si presionas 1 se apaga si presionas 2 se pone audio normal si pones 3 se silencia etc....

Pero si pones 11 se bloquea.

Recuerden solo experimentando descubrimos nuevas cosas y bugs de los celulares, personalmente yo he dañado como 20 de diferentes marcas pero ECHANDO A PERDER SE APRENDE

SIDs de la compañia B

24578	BC SUR, BC NORTE
24594	SINALOA, SONORA
24582	CHIHUAHUA, DURANGO
24581	NVO LEON, TAMAULIPAS, COAHUILA
24586	JALISCO, COLIMA Y MICHOACAN
24588	GTO, AGS, ZAC, QRTO, SLP
24590	TLAX, GUERRERO, OAXACA, VER, PUEBLA
24592	CHIAPAS, TABASCO, CAMPECHE, YUCATÁN, QUINTANA
24580	DF, EDO DE MEX, MORELOS, HGo

COMO GRABAR CONVERSACIONES DE TELEFONIA CELULAR

Me he dado cuenta investigando en los modos de escucha de ericson que solo escucho llamadas que se hacen desde un teléfono de la compañía A y desde los motorola solo se puede escuchar a la compañía B.

... con esto de antecedente vamos a grabar una conversación nuestra, el procedimiento es el siguiente (recomiendo las series nokia 51xx,61xx,8xxx)

Pasos:

1.- Poner en modo de prueba tu teléfono (field test) en 01 ------si es nokia-----

2.- Utilizando un teléfono motorola entramos al modo de escucha (a este teléfono hay que ponerle un manos libres , quitamos la bocinita y le ponemos un conector macho tipo RCA lo conectamos a un estereo con entradas de av.(se supone que debe estar familiarizado con los procedimientos de grabación, si no consulte a un amigo)).

3.- Si hacemos o recibimos una llamada leemos en pantalla después de contestar el canal donde se recibió la llamada le ingresamos al mot. el código 11xxx (donde xxx es el código del canal) y nos ponemos a grabar.

Recuerda este procedimiento es para si tu teléfono es de la compañía b. si es de la compañía a tendrás que utilizar el modo de escucha de un ericson y pones el código(después de haber entrado) yes 3c000xxx (donde xxx es el canal).

DATO CURIOSO si reprogramo un numero de un amigo en mi teléfono y el hace o recibe una llamada (y yo hago otra cualquiera puedo ver en que canal esta conversando por lo tanto lo podré escuchar o grabar según el caso

Nota: debes estar a menos de 10 mtrs.

Nota: Todos esto trucos han sido probados en teléfonos digitales ericson, motorola y nokia 6120
Recuerda que para estos trucos necesitas forzosamente dos teléfonos.

Seminario de Programación de teléfonos de la compañía A

CLAVES DE FABRICANTE

Cada serie electrónica de un equipo celular es única e inalterable, y se graba en el equipo al momento de ser fabricado, existe un convenio internacional, que asigna a cada fabricante de teléfonos celulares una o varias claves numéricas para que sea posible identificar quien fabricó un aparato en especial.

Así, un numero de serie electrónica, esta formado por once dígitos cuando se tiene en sistema decimal, los tres primeros indicaran que marca es el teléfono; si la serie se tiene en sistema hexadecimal, el numero de serie esta expresado mediante numeros (0,1,2,3,4,5,6,7,8,9) y/o letras (a,b,c,d,e,f) con un total de ocho caracteres, la clave de fabricante se obtiene a partir de los dos primeros digitos.

Por ejemplo: la serie **82123456** se convierte a decimal tomando primero el **82** que equivale a **130** en decimal, luego se convierte el resto de la serie **123456**, que equivale a **361100** en decimal, como se ve solo tenemos ocho dígitos que son **130 361100**, para completar los 11 dígitos ponemos dos ceros entre los tres primeros dígitos y el resto de la serie quedando **130 00 361100,** si hubieran resultado diez dígitos entonces solo se habría agregado un cero.

A continuación se presenta una lista de las principales claves de fabricante tanto en sistema decimal como hexadecimal.

FABRICANTE	DECIMAL	HEXADECIMAL
ANTEL	175	AF
AUDIOVOX	138	8A
CLARION (JAPON)	140	8C
CLARION (EE UU)	166	A6
DIAMONDTEL	134	86
ERICSSON	157	9D
ERICSSON	204	CC
FUJITSU	133	85
GENERAL ELECTRIC	146	92
GOLDSTAR	141	8D
HITACHI	132	84
MITSUBISHI	134	86
MOTOROLA	130	82
MOTOROLA	195	C3
MOTOROLA	212	D4
MOTOROLA	213	D5
MOTOROLA	224	E0
NEC	135	87
NEC (SERIE 800)	189	BD
NOKIA	165	A5
NOKIA	156	9C
NOKIA	219	DB
NOVATEL	142	8E
OKI	129	81
PANASONIC	136	88
QUALCOMM (CDMA)	159	9F
SAMSUNG (CDMA)	176	B0
SHINTOM	174	AE
SONY	154	94
SONY (CDMA)	211	D3
TANDY	165	A5
TECHNOPHONE	162	A2
TOSHIBA	138	8A
UNIDEN	172	AC

MODELOS INCLUIDOS EN ESTE E-ZINE

ANTEL 1300
AUDIVOX 120
AUDIOVOX CMT300/MVX500/MVX525/MVX550/MVX700/MVX750
AUDIOVOX MVX400
AUDIVOX MVX-605
AUDIOVOX MVX425/MVX450
AUDIOVOX MVX800 (VER TOSHIBA 9600)
AUDIOVOX CDM-3000
AUDIOVOX CDM 3300
AUDIOVOX CDM 4000
CLARION 3000 CT/5200CT
DIAMONDTEL 20X/90X/99X
DIAMONDTEL 22X/25X
ERICSSON AH237/238/AH300/310/320/AH628/630/AF738
FUJITSU COMMANDER /364/364A/POCKET/STYLUS
GE HOTLINE 5000/7000/7500
GE POCKETFONE (VER ERICSSON)
HANWHA F1100
LGC 330W
MITSUBISHI 1500
MITSUBISHI 3000/3500 (VER DIAMONDTEL 20X)
MITSUBISHI 4000 (VER DIAMONDTEL 20X)
MITSUBISHI 5000

ANTEL 1300 (ANALOGICO)

- **OBTENCION DE LA SERIE:**

ETIQUETA EN EQUIPO CON NUMERO DE SERIE EN HEXADECIMAL, COMIENZA CON AF Y DEBE CONVERTIRSE A DECIMAL, POR LO REGULAR SON NUMEROS PEQUEÑOS, POR EJEMPLO : 17500004567. TAMBIEN PUEDE OBTENERSE ENTRANDO A PROGRAMACION, YA QUE APARECE PARA CONFIRMAR QUE SE ENTRO CORRECTAMENTE.

- **PARA ENTRAR A PROGRAMACION:**

ENCENDER, PRESIONAR TECLA LATERAL MARCADA **M** LUEGO 626#7871300 **RCL, ESTO DEBE HACERSE EN MENOS DE DIEZ SEGUNDOS.**

AL ENTRAR A PROGRAMACION APARECE LA SERIE EN HEXADECIMAL, TECLEAR VARIAS VECES VOLUMEN HACIA ARRIBA HASTA ENCONTRAR **SELECT NAM 1-3** TECLEAR 1, APARECE EXIT 1-0 TECLEAR 1, APARECE EL NUMERO TELEFONICO.

- **PARA GRABAR LOS DATOS:**

1 TELEFONO	**CLR 10 DIGITOS TELEFONO VOLUMEN HACIA ARRIBA**
2 SIDH	**CLR 01525 VOLUMEN HACIA ARRIBA**
3 LOCAL USE	**CLR 1 VOLUMEN HACIA ARRIBA**
4 MIN OPT	**CLR 1 VOLUMEN HACIA ARRIBA**
5 IPCH	**CLR 0333 VOLUMEN HACIA ARRIBA**
6 ACCESS OVERLOAD	**CLR 02 VOLUMEN HACIA ARRIBA**
7 PREF SYST	**CLR 1 VOLUMEN HACIA ARRIBA**
8 GROUP ID	**CLR 00 VOLUMEN HACIA ARRIBA**
9 CANDADO	**CLR 1234 VOLUMEN HACIA ARRIBA**
10 END TO END	**CLR 1 VOLUMEN HACIA ARRIBA**
11 A/B SELECT	**CLR 1 VOLUMEN HACIA ARRIBA**
12 NAM PROG AREA	**CLR 1 VOLUMEN HACIA ARRIBA**
13 DISC TRANSM	**CLR 0 VOLUMEN HACIA ARRIBA**

- **PARA SALIR DE PROGRAMACION:**

PRESIONAR **STO, STO, END**

- **PARA PONER EN SISTEMA:**

FCN 5 CON **5** HASTA PREF ONLY **END**

- **PARA VERIFICAR EL NUMERO DE TELEFONO:**

RCL 00

AUDIOVOX CDM 120 (Completa) (DUAL)

1. Encender el teléfono.
2. Teclear la siguiente secuencia **#86904* * 89397#**.
3. Oprimir **1** para seleccionar el **NAM 1**.
4. Oprimir **2** para seleccionar **FULL SETUP**.
5. Oprimir **1** para seleccionar **NAM NAME**.
6. Teclear **IUSACELL** y después oprimir la tecla **MEM**.
7. Oprimir **2** para seleccionar **PHONE NUMBER**.
8. Teclear el número **10 DIGITOS** y después oprimir la tecla **MEM**.
9. Oprimir **3** para seleccionar **FM SETUP** y teclear los siguientes parámetros:

1. ACCOLC	Se deja igual	**MEM**.
2. 1ST PAGING	**333**	**MEM**.
3. HOMESYS ID	**01525 (R9)**	**MEM**.
4. AUTO REGIS	**YES**	**END**.

10. Oprimir la tecla **4** y teclear los siguientes parámetros:

1. MCC #	**000**	**MEM**.
2. MNC #	**00**	**MEM**.
3. ACCOLC	Se deja igual	**MEM**.
4. CHAN SET	**283**	**MEM**.
	384	**MEM**.
	691	**MEM**.
	777	**END**.

11. Oprimir **5** para ingresar **HOME REGIS** y seleccionar **YES** después teclear **MEM**.
12. Oprimir **6** para ingresar **FOREGN SID** y seleccionar **YES** después teclear **MEM**.
13. Oprimir **7** para ingresar **FOREGN NID** y seleccionar **YES** después teclear **END**.
14. Oprimir la tecla **5** para ingresar **HOME SYS** y después teclear:

HOME SID #1	**01525**	**MEM**.
HOME NID #1	**65535**	Teclear **MEM** hasta salir de este submenú.

15. Oprimir la tecla **6** para ingresar **LOCK SYS** y después teclear:

LOCK SID #1	**0**	**MEM**.
LOCK NID #1	**0**	Teclear **MEM** hasta salir de este submenú.

16. Oprimir la tecla **7** para ingresar **PRL ENABLE** y seleccionar **NO**:

17. Para salir de la programación oprimir **END END END** y la terminal se apaga sola.

AUDIOVOX CMT300/MVX500/MVX525/MVX550/MVX700/MVX750 (ANALOGICOS)

- **OBTENCION DE LA SERIE:**

ETIQUETA EN PARTE POSTERIOR EN DECIMAL QUE EMPIEZA CON **138**, CUALQUIER OTRO NUMERO NO SIRVE PARA OBTENER LA SERIE; SI NO TRAE LA ETIQUETA NO SE OBTENDRA DIRECTAMENTE.

- **PARA ENTRAR A PROGRAMACION:**

CLAVE FCN # 1 DONDE LA CLAVE PUEDE SER: LOS TRES ULTIMOS DIGITOS DEL NUMERO DE SERIE O DEL TELEFONO QUE TRAE PROGRAMADO, 123, 000, 111, DE NO FUNCIONAR ALGUNO DE ESTOS ACUDIR A SERVICIO TECNICO.

SI SE LOGRO ENTRAR A PROGRAMACION APARECE UN 01 EN LA PARTE SUP DE LA PANTALLA Y EL NUMERO QUE TIENE GRABADO ABAJO.

- **PARA GRABAR LOS DATOS:**

1 TELEFONO	**10 DIGITOS STO**
2 SEG	**123 STO**
3 SIDH	**01525 STO**
4 ACCESS OVERLOAD	**02 STO**
5 GIM	**00 STO**
6 LOCAL USE	**1 STO**
7 MIN OPT	**1 STO**
8 INITIAL PAGING CH	**0333 STO**
9 PREF SYS	**1 STO**
10 SCM	**1010 STO**
11 OPTIONS	**10111000 STO**
12 OPTIONS	**11100000**

- **PARA SALIR DE PROGRAMACION:**

FCN SND, APARECE UN DATO X EN LA PANTALLA, **FCN CLR**

- **PARA PONER EN SISTEMA:**

FCN 01 APARECE EN PANTALLA **PREF** ESPERAR A QUE DESAPAREZCA SOLO Y LISTO

- **PARA VERIFICAR EL NUMERO DE TELEFONO:**

RCL ** PROGRAMACION RAPIDA **CLR 01525524729XXXX FCN 6** SOLO SI YA TENIA LINEA DE BANDA A, SE USA SI NO SE CONOCE LA CLAVE PARA HACER LA PROGRAMACION COMPLETA, PERO NO ES CONFIABLE PARA EQUIPOS QUE TENIAN LINEA DE BANDA B, YA QUE CIERTOS PARAMETROS QUEDAN MAL.

AUDIOVOX MVX400 (ANALOGICO)

- **OBTENCION DE LA SERIE:**

ETIQUETA EN PARTE POSTERIOR EN DECIMAL QUE EMPIEZA CON **174**, CUALQUIER OTRO NUMERO NO SIRVE PARA OBTENER LA SERIE; SI NO TRAE LA ETIQUETA NO SE OBTENDRA DIRECTAMENTE.

- **PARA ENTRAR A PROGRAMACION:**

FCN 5 Y LA **CLAVE DE CANDADO** PARA QUE SE BLOQUEE, LUEGO **FUNC # 626 # FUNC**
APARECE UN NUMERO RARO EN PANTALLA COMO AVISO DE QUE SE ENTRO A PROGRAMACION.
SE PRESIONA VARIAS VECES SEND HASTA QUE APARECE **AREA CODE**

- **PARA GRABAR LOS DATOS:**

1 AREA CODE	**524 SEND**
2 TELEFONO	**ULTIMOS 7 DIGITOS DEL TELEFONO SEND**
3 SIDH	**01525 SEND**
4 ACCESS OVERLOAD	**02 SEND**
5 GIM	**00 SEND**
6 LOCAL USE	**1 SEND**
7 MIN OPT	**1 SEND**
8 CANDADO	**123 SEND**
9 CANDADO AUTOMATICO	**0 SEND**

10 APARECE LA CLAVE DEL PASO 8

- **PARA SALIR DE PROGRAMACION:**

END FCN END AL SALIR DE PROGRAMACION EL EQUIPO ESTARA BLOQUEADO, TECLEAR LA CLAVE DEL PASO 8 PARA DESBLOQUEAR.

- **PARA PONER EN SISTEMA:**

FCN 61 LO PONE EN SOLO A

- **PARA VERIFICAR EL NUMERO DE TELEFONO:**

AUDIOVOX MVX425/MVX450 (ANALOGICOS)

- **OBTENCION DE LA SERIE:**

ETIQUETA EN PARTE POSTERIOR EN DECIMAL QUE EMPIEZA CON **138**, CUALQUIER OTRO NUMERO NO SIRVE PARA OBTENER LA SERIE; SI NO TRAE LA ETIQUETA NO SE OBTENDRA DIRECTAMENTE.

- **PARA ENTRAR A PROGRAMACION:**

CLAVE FCN # 81 DONDE LA CLAVE PUEDE SER: LOS TRES ULTIMOS DIGITOS DEL NUMERO DE SERIE O DEL TELEFONO QUE TRAE PROGRAMADO, 123, 000, 111, DE NO FUNCIONAR ALGUNO DE ESTOS ACUDIR A SERVICIO TECNICO.

SI SE LOGRO ENTRAR A PROGRAMACION APARECE UN 01 EN LA PANTALLA Y LOS TRES PRIMEROS DIGITOS DEL NUMERO QUE TIENE GRABADO A UN LADO.

- **PARA GRABAR LOS DATOS:**

1 AREA	**524 VOL**
2 CIUDAD	**727 VOL**
3 NUMERO	**XXXX VOL**
4 CLAVE CANDADO	**123 VOL**
5 SIDH	**01525 VOL**
6 ACCESS OVERLOAD	**02 VOL**
7 GIM	**00 VOL**
8 LOCAL USE	**1 VOL**
9 MIN OPT	**1 VOL**
10 INITIAL PAGING CH	**333 VOL**
11 PREF SYST	**1 VOL**
12 SCM	**1010 VOL**
13 OPTIONS	**10100 VOL**
14 NO IMPORTA LO QUE SALGA	

- **PARA SALIR DE PROGRAMACION:**

FUNC SEND APARECE UN DATO CUALQUIERA EN PANTALLA, **FCN CLR**

- **PARA PONER EN SISTEMA:**

FUNC 7 CON **#** HASTA P SYS **END**

- **PARA VERIFICAR EL NUMERO DE TELEFONO:**

FCN 0

AUDIOVOX MVX 605 (ANALOGICO)

- **OBTENCION DE LA SERIE:**

TRAE UNA ETIQUETA EN LA PARTE POSTERIOR CON EL NUMERO DE SERIE ELECTRONICO EN DECIMAL E INICIA CON 174

- **PARA ENTRAR A PROGRAMACION CORTA :**

ENCENDER EL APARATO E INGRESE LA SIGUIENTE SECUENCIA

01525 (SIDH) SEGUIDO DE 10 DIGITOS DE NUMERO CELULAR.

EJEMPLO: 0152552XXXXXXXX

POSTERIORMENTE PRESIONE **FUNC # #** ,SEGUIDO DEL CODIGO DE CANDADO DE 3 DIGITOS, NORMALMENTE **123** DE FABRICA.

EL TELEFONO SE RESTAURARA Y ARECERA **"Ready"**

- **PARA PONER EN SISTEMA:**

PRESIONAR **FUNC 6** Y CON **FLECHA HACIA ABAJO** AVANZAR HASTA **A ONLY,** GRABAR CON **R/S**.

- **PARA VERIFICAR EL NUMERO DE TELEFONO:**

PRESIONE **FUNC # 1**

AUDIOVOX CDM 3000 (DUAL)

- **OBTENCION DE LA SERIE:**

TRAE UNA ETIQUETA EN LA PARTE POSTERIOR CON EL NUMERO DE SERIE ELECTRONICO EN DECIMAL E INICIA CON 138

- **PARA ENTRAR A PROGRAMACION:**

ENCIENDA EL TELEFONO PRESIONANDO LA TECLA DE PWR POR 2 0 3 SEGUNDOS. INTRODUZCA LA SIGUIENTE SECUENCIA EN MENOS DE 10 SEGUNDOS:

289 FCN # 1

- **PARA GRABAR LOS DATOS:**

AL ENTRAR A PROGRAMACION INTRODUZCA UNO A UNO LOS PARAMETROS DE LA SIGUIENTE LISTA.

NAM1 Setting	Yes	**F**
NAM1 Phone Number	10 DIGITOS DE NUMERO	**VOL**
Home SID	01525	**VOL**
NAM1 Simple Setting	Yes	**F**

- **PARA PONER EN SISTEMA:**

PRESIONAR **F 61** Y OPRIMIR LA TECLA DE **VOL** HASTA ENCONTRAR **PREFER** Y GRABAR LA OPCION ELEGIDA CON **F**

- **PARA VERIFICAR EL NUMERO DE TELEFONO:**

PRESIONAR **F 21**

AUDIOVOX CDM 3300 (DUAL)

4. **OBTENCION DE LA SERIE:**
Trae una etiqueta en la parte posterior con el numero de serie electrónico en decimal e inicia con 160 (HEX: A0).

4. PARA ENTRAR A PROGRAMACION:

4. Prenda el equipo y teclee la siguiente secuencia:

 # 86904 V V 89397 #

2. A continuación presione el numero de NAM que desea programar (**1**, para NAM1) **,** y enseguida **2** (con esto entra a la programación del NAM 1)**.**

3. Para seleccionar PHONE # presione **2**, e introduzca 10 DIGITOS DE NUMERO seguido de . , para grabar ; posteriormente presione **4** , para seleccionar el sistema analógico, enseguida presione **2** para entrar a 1 sth Paging y digite **333** seguido de.

4. Posteriormente presione **3**, para seleccionar Homesys ID e introduzca el sistema ID (para cada región es diferente) **01525** (para región 6), enseguida presione. para grabar y oprima END END END END para salir. El teléfono se apagará.

- PARA PONER EN SISTEMA:

Presionar MENU **72**, avanzar con **#** o ***** Hasta SYSTEM A ONLY seguido de . para guardar selección, después presione END para salir.

- PARA VERIFICAR NUMERO PROGRAMADO:
Presionar MENU **61**. Presione END para salir.

- **PARA SELECCIONAR NAM:** INGRESE **# # 9027 MENU 0** INGRESE CODIGO DE SEGURIDAD (0000 DE FABRICA) **81** SELECCIONE NAM Y PRESIONE.

AUDIOVOX CDM 4000 (DUAL)

1. Encienda el teléfono presionando la tecla de PWR por dos o tres segundos.

2. Inicie la programación digitando la siguiente secuencia en menos de diez segundos.

289 FNC # 1

3. Introduzca uno a uno los siguientes parámetros.

NAM1 Setting	Yes	F
Phone Number	10 DIGITOS DE NUMERO	VOL
Home SID	01525	VOL
NAM1 Setting	Yes	F

4. Para verificar el número programado presione **F 21**.

5. Para seleccionar el sistema de operación presione **FNC 51** y oprima la tecla de hasta encontrar PREF, enseguida presione **F** para grabar la opción elegida.

IMPORTANTE : Para desbloclear , se preiona al mismo tiempo **2 * rcl power** Aparece en pantalla (rest) ahora presionar **128 send** APUNTAR DE LOS NUMEROS QUE APARECEN EN PANTALLA EL (**2-4-6-8** ESE ES EL CODIGO DE BLOQUEO) Después presionar **141 send.**

CLARION 3000 CT/5200CT (ANALOGICO)

- **OBTENCION DE LA SERIE:**

PRESIONAR **FCN 6** Y APARECE EN DECIMAL EN LA PANTALLA

- **PARA ENTRAR A PROGRAMACION:**

ENCENDER, **CLR** ** **123123 ##** APARECE UN CERO EN LA PANTALLA PARA INDICAR QUE SE ENTRO A PORGRAMACION. TECLEAR UNO

- **PARA GRABAR LOS DATOS:**

RCL 1 SIDH **01525 STO**
RCL 2 LOCAL USE**1 STO**
RCL 3 MIN OPT **1 STO**
RCL 4 TELEFONO 10 DIGITOS STO
RCL 5 SCM **08 STO**
RCL 6 INITIAL PAGING **CH 333 STO**
RCL 7 ACCESS OVER LOAD **02 STO**
RCL 8 PREF SYST **1 STO**
RCL 9 GIM **00 STO**
RCL 0 CANDADO **1234 STO**

- **PARA SALIR DE PROGRAMACION:**

APAGAR Y ENCENDER, SI AL ENCENDER APARECE **ERROR**, SE DEBE COMENZAR OTRA VEZ TODO Y HACERLO MAS LENTAMENTE.

- **PARA PONER EN SISTEMA:**

FCN 4 CON **4** HASTA A ONLY **STO**

- **PARA VERIFICAR EL NUMERO DE TELEFONO:**

FCN 3

DIAMONDTEL 20X/90X/99X (ANALOGICOS)

- **OBTENCION DE LA SERIE:**

ETIQUETA EN PARTE POSTERIOR CON UN NUMERO EN HEXADECIMAL QUE EMPIEZA CON 86, SI NO TIENE ESTA ETIQUETA, NO SE PUEDE OBTENER EL ESN DIRECTAMENTE DEL EQUIPO.

- **PARA ENTRAR A PROGRAMACION:**

ENCENDER, MANTENER PRESIONADA TECLA **STO/END** MIENTRAS TECLEA **6972814** SOLTAR **STO/END** APARECE EL LETRERO DUAL INDICANDO QUE SE ENTRO A PRAGRAMACION, SE PRESIONA CERO PARA SOLO UN NAM, O UNO PARA DOS NAMS

- **PARA GRABAR LOS DATOS:**

DUAL	**0 ó 1 SEND**
PHONE 1	**10 DIGITOS DEL TELEFONO SEND**
SID 1	**01525 SEND**
LU 1	**1 SEND**
E 1	**1 SEND**
IPCH 1	**0333 SEND**
ACCOLC 1	**02 SEND**
GI 1	**00 SEND**
IR 1	**0 SEND**
DTX 1	**0 SEND**
SLO 1	**SEND**
E CAL 1	***911 SEND**

SI SE ESCOGIO 2 NAMS, AQUÍ EMPIEZAN A SALIR LOS MISMOS PASOS MARCADOS CON 2

SEC	**1234 SEND**
DUAL	

- **PARA SALIR DE PROGRAMACION:**

STO/END, SI AL SALIR DE PROGRAMACION APARECE **ERROR 2** SE PROGRAMO MAL; Y SE DEBE HACER TODO DE NUEVO.

- **PARA PONER EN SISTEMA:**

FCN 8 CON **#** HASTA PREF ONLY **CLR**

- **PARA VERIFICAR EL NUMERO DE TELEFONO:**

RCL #

DIAMONDTEL 22X/25X (ANALOGICOS)

- **OBTENCION DE LA SERIE:**

ETIQUETA EN PARTE POSTERIOR CON UN NUMERO EN HEXADECIMAL QUE EMPIEZA CON 86, SI NO TIENE ESTA ETIQUETA, NO SE PUEDE OBTENER EL ESN DIRECTAMENTE DEL EQUIPO.

- **PARA ENTRAR A PROGRAMACION:**

ENCENDER, MANTENER PRESIONADA LA TECLA **END** MIENTRAS SE TECLEA **6972814.** SOLTAR **END**, APARECE **NAM SEL** COMO INDICADOR QUE SE ENTRO A PROGRAMACION. PRESIONAR 1 PARA NAM 1 Y ASI HASTA 4 NAMS.

- **PARA GRABAR LOS DATOS:**

MULTIPLE NAM SELECT	**1,2,3, O 4 SEND**
TELEFONO 10 DIGITOS	**524729XXXX SEND**
SYST ID	**01525 SEND**
LOCAL USE	**1 SEND**
MIN OPT	**1 SEND**
INITIAL PAGING CH	**0333 SEND**
ACCESS OVERLOAD	**02 SEND**
GIM	**00 SEND**
ROAM INHIBIT	**0 SEND**
INVALID SYST ID	**SEND**
NO EMERG	***911 SEND**
SECURITY CODE	**1234 SEND**

- **PARA SALIR DE PROGRAMACION:**

END SI MARCA AL ENCENDER CHECK 2 SE PROGRAMO MAL Y SE DEBE HACER TODO DE NUEVO.

- **PARA PONER EN SISTEMA:**

FCN 32 CON **#** HASTA PREF ONLY **STO/CLR**

- **PARA VERIFICAR EL NUMERO DE TELEFONO:**

FCN 11

ERICSSON AH237/238/AH300/310/320/AH628/630/AF738/778 (ANALOGICOS)

- **OBTENCION DE LA SERIE:**

ETIQUETA EN PARTE POSTERIOR DEL TELEFONO, ESTA EN DECIMAL Y EMPIEZA CON 157 0 204; SI NO TIENE LA ETIQUETA AL ENTRAR A PROGRAMACION APARECE LA SERIE COMO PRIMER PASO.

- **PARA ENTRAR A PROGRAMACION:**

PRESIONAR Y SOSTENER **FCN** MIENTRAS TECLEAS **923885**, APARECE ESN EN DECIMAL COMO AVISO DE QUE SE ENTRO A PROGRAMACION, PRESIONAR **#** HASTA QUE APAREZCA NAM 1? O NAM 1-2?, PARA ESTE ULTIMO TECLEAR 1 PARA NAM UNO O 2 PARA NAM 2.

- **PARA GRABAR LOS DATOS:**

NO TELEFONO 10 DIGITOS	**#**
SUB NO MISMO NO TEL 10 DIG	**#**
EN ALGUNOS SALE AUTH KEY DEJAR IGUAL	**#**
SIDH	**01525 #**
INITIAL PAGING CH	**0333 #**
ACCESS OVERLOAD	**02 #**
GROUP ID	**00 #**
MIN OP	DEBE ESTAR EN **ON #**

APARECE YA SEA NAM 2? , NAM 1-2? , NAM 1-4?

- **PARA SALIR DE PROGRAMACION:**

END

- **PARA PONER EN SISTEMA:**

FCN 5 CON **5** HASTA PREF ONLY **STO END,** PARA EL **AF738 MENU 52 SEND** CON **MENU** HASTA PREF ONLY **SEND CLR**

- **PARA VERIFICAR EL NUMERO DE TELEFONO:**

FCN FCN, PARA EL **AF738 MENU 53 SEND**

FUJITSU COMMANDER /364/364A/POCKET/STYLUS (ANALOGICOS)

- **OBTENCION DE LA SERIE:**

DE LA ETIQUETA EN LA PARTE POSTERIOR SE TOMAN LOS ULTIMOS 6 DIGITOS Y SE LES ANTEPONE 13300.

- **PARA ENTRAR A PROGRAMACION:**

SE DEBE BLOQUEAR EL TELEFONO YA SEA CON TECLAS **F** Y **LOCK**, O CON **F 9,** YA BLOQUEADO, SE APAGA, SE ENCIENDE Y SE TECLEA **#626#7764726**, UN TONO COMIENZA A SONAR, PRESIONAR * HASTA QUE EL TONO TERMINE COMPLETAMENTE, SOLTAR * Y APARECE EL SIDH ACTUAL COMO CONFIRMACION DE QUE SE ENTRO A PROGRAMACION.

- **PARA GRABAR LOS DATOS:**

SIDH	**01525 STOR**
LOCAL USE	**1 STOR**
MIN OPT	**1 STOR**
TELEFONO	**10 DIGITOS STOR**
SCM	**14 STOR**
INITIAL PAGING CH	**333 STOR**
ACCESS OVER LOAD	**02 STOR**
PREF SYST	**1 STOR**
GIM	**00 STOR**
CLAVE CANDADO	**1234 STOR**

CON **VOL** AVANZAR HASTA EL PRIMER PASO (DONDE SE DIO 01525)

- **PARA SALIR DE PROGRAMACION:**

SEND

- **PARA PONER EN SISTEMA:**

FCN 13 PARA SOLO A

- **PARA VERIFICAR EL NUMERO DE TELEFONO:**

RCL F #

GE HOTLINE 5000/7000/7500 (ANALOGICOS)

- **OBTENCION DE LA SERIE:**

DIRECTA EN DECIMAL DE LA ETIQUETA EN LA PARTE POSTERIOR DEL EQUIPO, EMPIEZA CON 146, O AL ENTRAR A PROGRAMACION APARECE EN PANTALLA.

- **PARA ENTRAR A PROGRAMACION:**

ENCENDER, **04049 FCN FCN** APARECE LA SERIE PARA CONFIRMAR QUE ENTRO A PROGRAMACION.

- **PARA GRABAR LOS DATOS:**

AREA	**524 SEND**
TELEFONO 7 DIG	**729XXXX SEND**
SUB AC	**SEND**
SUB PHN	**SEND**
SIDH	**01525 SEND**
LOCAL USE	**1 SEND**
MIN OPT	**1 SEND**
INITIAL PAGING CH	**0333 SEND**
ACCESS OVERLOAD	**02 SEND**
PREF SYST	**1 SEND**
GIM	**00 SEND**
CANDADO	**1234 SEND**
HANDSFREE	**0 SEND**
HORN ALERT	**0 SEND**
AUTONOM REG	**1 SEND**
WHERE KNOWN	**0 SEND**
AUD CALL TIMER	**1 SEND**
CONTINUOS DTMF	1 SEND
EMERG NO	**911 SEND**
DUAL NAM	**0 ó 1 SEND**

- **PARA SALIR DE PROGRAMACION:**

END

- **PARA PONER EN SISTEMA:**

FCN 4, CON **#** HASTA PREF ONLY **END**

- **PARA VERIFICAR EL NUMERO DE TELEFONO:**

FCN 3, LUEGO **END**

HANWHA F1100 (SOLO DIGITAL CDMA)

ESN viene en etiqueta de la parte posterior del teléfono e inicia con 169 (A9).

PROGRAMACION:

Encender el aparato y presionar la siguiente secuencia:

*#7415963 avanzar con las flechas arriba/abajo (**cV** , **S^**) hasta que el apuntador se coloque en NAM 1 (Si lo requiere avance a NAM2, NAM3 O NAM4).

Enseguida presionar la tecla **M<** , aparecerá lo siguiente:

PHONE NUMBER , presionar **M<** , ingresar numeros celular 10 digitos y presionar **S ^** , Espere a que se guarde la información.

Avanzar con flecha arriba,abajo (**cV** , **S^**) hasta CDMA SETUP y presionar **M<** ,

Avanzar con flecha arriba,abajo (**cV** , **S^**) hasta SYSTEM SELECT y presionar **M<** hasta que aparezca la leyenda **system_A_only** y entonces presionar S ^

Avanzar con flecha arriba,abajo (**cV** , **S^**) hasta SID-NID y presionar **M<** , y aparecerá:

SID #1, ingresar **01525** y presionar **S ^** varias veces hasta que aparezca nuevamente SID-NID.
Para salir de programacion presionar **END END END**.

PARA VER NUMERO PROPIO: presionar **M< 0**.

PARA PONER EN BANDA: ***NO REQUIERE*** EQUIPO CDMA EN 800 MHz.

PARA CAMBIO DE NAM: Presionar **M< 8** ingresar codigo de seguridad (0000 de fabrica) . Presionar **51** y con **i>** seleccionar NAM y guardar opción con **S^.**

PROGRAMACION IP ADDRESS.

Presionar la siguiente secuencia: ***#43176** avanzar con las flechas arriba/abajo (**cV** , **S^**) hasta que el apuntador se coloque en UP LINK ADDRESS presionar **M<** , aparecerá ENTER IP1 presionar **M<** e ingresar direccion IP (196.018.091.201) grabar con **END**, ahora seleccionar ENTER IP 2 presionar **M<** e ingresar direccion IP (196.018.091.202) grabar con **END** y salir con **END END**.

LGC 330W (CORTA) (DUAL)

1. Prenda el aparato.

2. Inicie la programación tecleando **MENU 4 0,** seguido del código de seguridad **000000**, la pantalla mostrará la leyenda SUBSYSTEM, posteriormente presione **11** y **OK**.

3. Introduzca uno a uno los siguientes parámetros:

PHONE NUMBER	10 DIGITOS DE NUMERO	OK
HOME SIDE	01525	OK
NAME	IUSACELL	OK
BASIC NAM		
IS COMPLET	EXIT	OK

4. Verifique el número programado presionando **MENU 0**.

5. Seleccione el sistema de operación tecleando **MENU 41**, y seleccione con el sistema **Solo A (A only)**, grabe y salga con **OK**.

LGC 330W (LARGA) 11706394317

1. Prenda el aparato.
2. Inicie la programación tecleando **MENU 4 0,** seguido del código de seguridad **000000**, la pantalla mostrará la leyenda SUBSYSTEM, posteriormente presione **11** y **OK**.
3. Introduzca uno a uno los siguientes parámetros:

PHONE NUMBER	10 DIGITOS DE NUMERO		OK
HOME SIDE	01525	OK	
NAME	IUSACELL	OK	
BASIC NAM			
IS COMPLET	MORE	OK	
PHONE MODEL	7	OK	
WARRANTY	DEJAR IGUAL	OK	
SERVICE PROGRAMIN CODE	000000	OK	
SLOT CYCLE INDEX	2	OK	
NAM 1 CDMA PHONE	10 DIGITOS DE NUMERO	OK	
NAM 1 AMPS PHONE	10 DIGITOS DE NUMERO	OK	
NAM1 MOBILE DIRECTORY	10 DIGITOS DE NUMERO	OK	
MOBILE COUNTRY CODE	000	OK	
MOBILE NETWORK CODE	00	OK	
CDMA HOME SID 1	01525	OK	
CDMA HOME NID 1	65535	OK	
CDMA HOME SID 2	0	OK	
CDMA HOME NID 2	65535	OK	
CDMA HOME SID 3	0	OK	
CDMA HOME NID 3	65535	OK	
CDMA HOME SID 4	0	OK	
CDMA HOME NID 4	65535	OK	
AMPS HOME SID	01525	OK	
LOCK OUT SYSTEM 1	0	OK	

4. Verifique el número programado presionando **MENU 0**.
5. Seleccione el sistema de operación tecleando **MENU 41**, y seleccione con el sistema **Solo A (A only)**, grabe y salga con **OK**.

MITSUBISHI 1500 (ANALOGICO)

- **OBTENCION DE LA SERIE:**

ETIQUETA EN LA PARTE INFERIOR DEL TELEFONO TRANSPORTABLE, CON UN NUMERO QUE COMIENZA CON 86 CUALQUIER OTRO NO SIRVE PARA OBTENER LA SERIE.

- **PARA ENTRAR A PROGRAMACION:**

ENCENDER, PRESIONAR Y SOSTENER **CRL** MIENTRAS SE TECLEA **5474432**, EN MENOS DE DIEZ SEGUNDOS, SOLTAR **CLR,** APARECE DUAL COMO AVISO DE QUE SE ENTRO A PROGRAMACION.

- **PARA GRABAR LOS DATOS:**

DUAL	**0** PARA 1 NUMERO, **1** PARA 2 NAMS **SEND**
TELEFONO	**10 DIGITOS SEND**
LOCAL USE	**1 SEND**
MIN OPTION	**1 SEND**
INITIAL PAGGIN CH	**0333 SEND**
ACCESS OVERLOAD	**02 SEND**
GIM	**00 SEND**

SI SELECCIONO 2 NAMS AQUÍ EMPIEZAN DATOS DE LA SEGUNDA LINEA,

SEGURIDAD	**1234 SEND**
DISC TRANSM	**0 SEND**
ROAM INHIBIT	**0 SEND**
CONTINUO DTMF	**1 SEND**
SYST SELECT	**1 SEND**
DESABILITA TEL DISP	**0 SEND**
SIDH INVALIDO	**XXXXX SEND**
DUAL HS	**0 SEND**
RJ11 OPT	**0 ó 1 SEND**

DUAL

- **PARA SALIR DE PROGRAMACION:**

END

- **PARA PONER EN SISTEMA:**

FCN 13

- **PARA VERIFICAR EL NUMERO DE TELEFONO:**

RCL #

MITSUBISHI 5000/MT1192FO(R9)A (ANALOGICO)

- **OBTENCION DE LA SERIE:**

ETIQUETA DE SERIE EN HEXADECIMAL EN LAPARTE POSTERIOR DEL EQUIPO, EMPIEZA CON 86 Y SI NO LA TIENE CUALQUIER OTRO NUMERO NO SIRVE PARA OBTENER LA SERIE.

- **PARA ENTRAR A PROGRAMACION:**

ENCENDER, PRESIONAR Y SOSTENER END MIENTRAS SE TECLEA 6972815, SOLTAR END; APARECE MULTI NAM COMO INDICACION DE QUE SE ENTRO A PROGRAMACION.

- **PARA GRABAR LOS DATOS:**

MULTI NAM	1, 2 ó 3 SEGÚN EL NUMERO DE LINEAS QUE SE DESEA, SEND
TELEFONO	10 DIGITOS SEND
SIDH	01525 SEND
CODIGO DE SEGURIDAD	1234 SEND

- **PARA SALIR DE PROGRAMACION:**

END

- **PARA PONER EN SISTEMA:**

FCN 36 CON **#** HASTA PREF ONLY, **CLR**

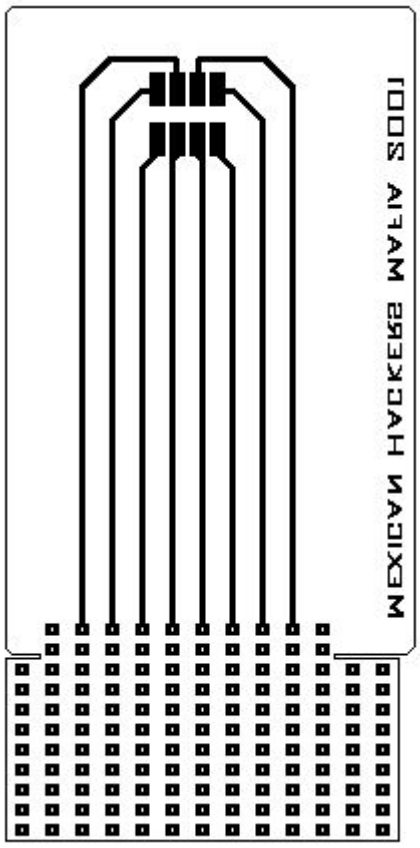
- **PARA VERIFICAR EL NUMERO DE TELEFONO:**

FCN 31, CLR

Tarjeta de Pruebas

Por: o0ShellGhost0o

En estos tiempos en los que el movimiento phreak se esta extendiendo en México han surgido varios proyectos que involucran el uso de tarjetas tipo smartcards, ya sea que alguien desee construir un emulador de tarjetas telefónicas, un logger, un blocker para algún sistema de TV por satélite, o cualquier otro proyecto relacionado podrá utilizar esta tarjeta de pruebas para sus experimentos.



Esta tarjeta tiene cierto parecido con las tarjetas pre-perforadas que venden en casas de electrónica, con la diferencia de que cuenta con los contactos de una tarjeta basada en la norma ISO7816.

Para poderla usar en cualquier proyecto que involucre tarjetas de este tipo he dejado pistas para todos los contactos de la tarjeta, lo cual hace que este diseño sea el único que necesitaras al hacer tus pruebas.

Gracias a la norma ISO7816 este diseño puede tener aplicaciones tanto en proyectos de tarjetas telefónicas (ya sean de 128, 256 o 512 bits), como en proyectos de tarjetas de monedero electrónico, tarjetas de televisión digital por satélite, incluso tarjetas inteligentes de control (por ejemplo las empleadas en ciertas universidades).

Las dimensiones de la tarjeta son un poco más grandes (a lo largo) de lo que seria una tarjeta telefónica, sin embargo sigue teniendo un tamaño muy compacto y a la vez con suficiente espacio para montar casi cualquier circuito de pruebas que se necesite.

Espero que este diseño ayude a todos aquellos que estaban buscando una interfase estilo smartcard para cualesquier propósito.

Por ultimo me gustaría comentar que por lo general no se encuentran tarjetas fenólicas del espesor de una smartcard (aprox. 0.75 mm) en las tiendas de componentes electrónicos por lo que necesitaran ir a un taller para que se las rebajen al tamaño deseado. De preferencia hagan esto antes de hacer el PCB, de lo contrario podrían atraer atención innecesaria. XDDD

Cualquier duda coméntenla en el foro de la página.

Mexican Hackers Mafia
http:// osukaru.cjb.net

Despedida

Quiero agradecer a todos los que hicieron posible este e-Zine:

- PitufoEnrike
- o0ShellGhost0o
- SaldeAhi
- Zajajin
- Darkman
- Paco_1585
- eagle4

También me gustaría agradecer a todos los que nos han mandado aportaciones para la página y a todos los que han cooperado al desarrollo del foro y en si a todos los que impulsan el desarrollo phreak en México.

Quiero comentar que para este nuestro primer e-zine recibimos artículos que por razones ajenas a nosotros no pudieron ser incluidos en esta edición, a aquellas personas les pedimos una sincera disculpa y prometemos incluir sus textos en nuestro próximo número.

Espero que hayan disfrutado este e-zine y sobre todo que les haya ayudado a comprender un poco más la tecnología electrónica empleada en nuestro país.

-=oSUKARu=-

EOF

"Muchos han llegado y muchos se han ido,
otros tantos vendrán en un futuro.
Una vez que esto se inició ya no hay vuelta atrás."

[decoy]