

Mexican Hackers Mafia

“La revista que Telmex preferiría que no leyeras”



DISCLAIMER:

Esta revista electrónica fue creada con el propósito de entretener y proporcionar material de investigación al pueblo mexicano y a nuestros hermanos hispano parlantes. Nosotros en la MHM no nos hacemos responsables del uso que se le dé a la información contenida en ella.

Los textos, gráficas y diagramas publicados aquí, se exponen con el fin de proporcionar datos y material técnico y de investigación mismos que deberán ser empleados siempre con fines educativos.

Los autores de cada texto son los únicos responsables de la veracidad de sus publicaciones y las ideas y opiniones dadas a conocer no necesariamente representan las del editor o el grupo.

Contenido

Tema	Autor	Página
Introducción	--oSUKARu--	4
La declaración del Hacktivism	Hacktivism.com	5
K0m0 yamar de "a grapa" a cualquier p ^a rte del mund ^o	(".oP&Ko.")	7
Decodificación de tonos multi frecuencia	--oSUKARu--	9
Bug en REDIAL??? de TELMEX	George X	12
Indicador de Estado Telefónico	o0ShellGhost0o	14
3n\$amblador kon manzana\$ 1 ^a parte	(".oP&Ko.")	16
El programador JDM	--oSUKARu--	19
El Escorpión –Trasmisor FM	o0ShellGhost0o	21
The Aztek Box	Phreakers.com.mx	23
Extensión al Seminario de Programación	Cheve	25
Despedida	--oSUKARu--	46

Introducción

Notas del Editor

Bienvenidos a la quinta entrega del eZine phreak de México para el mundo. Me complace decirles que este numero es uno de los mejores en cuanto a contenido y calidad del mismo refiere. Debo agradecer a todos los que nos enviaron sus textos ya que sin ellos esta revista simplemente no sería lo mismo que es.

Hemos hecho cambios de nuevo en cuanto al aspecto visual de la revista ya que el numero pasado quedo demasiado pesado y no queremos que ocurra de nuevo. Además de los cambios visuales hemos hecho cambios en la forma en que escribimos los textos, en esta edición notarán que los textos están redactados de una forma un poco más técnica y ordenada. Nos gustaría mucho saber que piensan de estos cambios, así que si lo desean pueden escribirnos en los foros de Tecnología Mexicana con sus sugerencias y comentarios.

Ahora con el crecimiento de la cultura phreak en México que se ha venido dando en los últimos meses se vienen muchos y muy importantes cambios dentro del mundo underground del phreaking. La introducción de la Aztek Box, así como los diversos proyectos que hemos preparado para este numero son el inicio de esta transformación.

El pueblo mexicano siempre se ha caracterizado por su creatividad innata, y precisamente por eso queremos que participes con nosotros a despertar la creatividad de los demás lectores escribiendo en los foros tus ideas de prototipos y sus aplicaciones.

Sabemos que algo que les sobra a los lectores de MHM es creatividad y sus ideas les podrán servir a otros lectores a despertar la suya.

Por ultimo, quiero felicitar a Opio por su excelente trabajo en la realización del logo de portada, quien ganó con un total de 100 votos y un 31% a favor en nuestro segundo concurso de diseño. El diseño en si es el que adorna la portada de esta revista.

Y pues sin más por el momento, los invito a leer y empaparse de conocimiento.

¡Animo!

--oSUKARu--

LA DECLARACIÓN DEL HACKTIVISMO

*afirmaciones de libertad
en apoyo de una internet sin censura*

PROFUNDAMENTE ALARMADOS porque la censura de la Internet patrocinada por los gobiernos se está diseminando rápidamente con la asistencia de las corporaciones transnacionales,

TOMANDO COMO BASE los principios y propósitos consagrados en el Artículo 19 de la Declaración Universal de los Derechos Humanos (UDHR) que declara que, "Todo individuo tiene derecho a la libertad de opinión y expresión; este derecho incluye la libertad de sostener opiniones sin interferencia y a buscar, recibir e impartir información e ideas a través de cualquier medio y sin consideración de fronteras", y el Artículo 19 del Convenio Internacional sobre los Derechos Civiles y Políticos (ICCPR) que afirma,

Todo individuo tendrá el derecho de sostener opiniones sin interferencia.

Todo individuo tendrá el derecho a la libertad de expresión; este derecho incluirá el derecho a buscar, recibir e impartir información e ideas de todo tipo, sin consideración de fronteras, tanto por medio oral, escrito o impreso, en forma de arte o por cualquier otro medio de su elección.

El ejercicio de los derechos provistos en el párrafo 2 de este artículo conlleva tareas y responsabilidades especiales. Por lo tanto puede estar sujeto a ciertas restricciones, pero éstas solamente deberán ser tal como están provistas por la ley y son necesarias:

Por respeto a los derechos o reputación de otros.

Por la protección de la seguridad nacional o el orden público, o de la salud o moral pública.

RECORDANDO que algunos estados miembros de las Naciones Unidas han firmado el ICCPR, o lo han ratificado en tal manera que impide a sus ciudadanos usarlo en cortes legales,

CONSIDERANDO que tales estados miembros continúan suprimiendo voluntariamente el acceso libre y abierto a la información publicada legalmente en Internet, a pesar de las nítidas palabras del ICCPR al referirse a que la libertad de expresión se extiende a todos los medios de comunicación,

TOMANDO NOTA de que las corporaciones transnacionales continúan vendiendo tecnologías de la información a los regímenes mas represivos del mundo con pleno conocimiento de que lo usarán para rastrear y controlar a una ciudadanía ya bastante hostigada,

TOMANDO EN CUENTA que la Internet se está convirtiendo rápidamente en un medio de represión en vez de un instrumento de liberación,

TENIENDO EN MENTE que en algunos países es un crimen reclamar el derecho de acceder a la información publicada legalmente, y otros derechos humanos básicos,

RECORDANDO que los estados miembros de las Naciones Unidas han fallado al presionar a los más distinguidos violadores de los derechos de la información hacia un estándar más elevado,

CONSCIENTES de que negar el acceso a la información podría conducir a un deterioro espiritual, intelectual y económico, promover la xenofobia y la desestabilización del orden internacional,

PREOCUPADOS porque los gobiernos y las transnacionales se entienden para mantener el statu quo,

PROFUNDAMENTE ALARMADOS porque los líderes mundiales han fallado al tratar el asunto de los derechos de la información directamente y sin equívocos,

RECONOCIENDO la importancia de luchar contra los abusos a los derechos humanos con respecto al acceso razonable a la información disponible en la Internet,

POR LO TANTO ESTAMOS CONVENCIDOS de que la comunidad hacker tiene el imperativo moral de reaccionar, y entonces

DECLARAMOS:

QUE EL RESPETO TOTAL POR LOS DERECHOS HUMANOS Y LAS LIBERTADES FUNDAMENTALES INCLUYE LA LIBERTAD DEL ACCESO EQUITATIVO Y RAZONABLE A LA INFORMACIÓN, SEA POR RADIO DE ONDA CORTA, CORREO AEREO, TELEFONÍA SIMPLE, LA INTERNET GLOBAL O CUALQUIER OTRO MEDIO.

QUE RECONOCEMOS EL DERECHO DE LOS GOBIERNOS A PROHIBIR LA PUBLICACIÓN DE CIERTOS SECRETOS DE ESTADO OPORTUNAMENTE CATEGORIZADOS, PORNOGRAFÍA INFANTIL, Y ASUNTOS RELACIONADOS CON LA VIDA PRIVADA Y LOS PRIVILEGIOS PERSONALES, ENTRE OTRAS RESTRICCIONES ACEPTADAS. PERO NOS Oponemos AL USO DEL PODER DEL ESTADO PARA CONTROLAR EL ACCESO A LOS TRABAJOS DE LAS FIGURAS CRÍTICAS, INTELECTUALES, ARTÍSTICAS Y RELIGIOSAS.

QUE LA CENSURA DE LA INTERNET RESPALDADA POR EL ESTADO EROSIONA LA COEXISTENCIA PACÍFICA Y CIVILIZADA, AFECTA AL EJERCICIO DE LA DEMOCRACIA Y PONE EN PELIGRO EL DESARROLLO SOCIOECONÓMICO DE LAS NACIONES.

QUE LA CENSURA DE LA INTERNET APOYADA POR EL ESTADO ES UNA SEVERA FORMA DE VIOLENCIA ORGANIZADA Y SISTEMÁTICA CONTRA LOS CIUDADANOS, DESTINADA A GENERAR CONFUSIÓN Y XENOFobia, Y ES UNA CONDENABLE VIOLACIÓN DE LA CONFIANZA.

QUE ESTUDIAREMOS LAS FORMAS Y MANERAS DE BURLAR LA CENSURA DE LA INTERNET RESPALDADA POR LOS ESTADOS Y QUE IMPLEMENTAREMOS TECNOLOGÍAS PARA DESAFIAR LAS VIOLACIONES DE LOS DERECHOS A LA INFORMACIÓN.

Publicado el 4 de julio del 2001 por Hacktivismismo y el **CULT OF THE DEAD COW**.
<http://www.hacktivismismo.com>

KOMO YAMAR DE "A GRAPA" a CUALQUIER PARTE DEL MUNDO

por ("·oPàKo·")

Hola de nuevo mi pequenio saltamontes se que es lo que quieres, quieres hablar con quien sea, a donde sea y pagar cero varos, necesitas relajarte y respirar, "puedes dejar de hacer todo lo que sea menos respirar..." (si se lo dices a una ninia cuando se histeriza, uy...), este truquin te aconsejo tratarlo primero de un telefono de tarjeta (no de preferencia) o de alguna farmacia o tiendita (este si) q rente el suyo (el de moneditas), xq yo ya lo hize, pero todavia no llega el recibo, no lo he hecho de uno de tarjeta, pero solo te cobrarian el pešo del minuto (solo me lo se para el defecado, o sea el DF luego lo investigo de otro lado).

Para hacer esto a lo mejor y necesitas un poco de "sicologia psocial" o un mucho de seguridad, recuerda que no ha mayor y mejor seguridad que la del pendejo...

...:[000]:... Marca el teléfono 5420-9898

.....:--aquí hay una variante--:.....

hay veces que te contesta alguien (por lo gral. hombre) y hay veces que no... sino te contestan pasa al ...:[011]:..., si te contesta aquí viene la prueba si eres hombre o raton...

-telefonista- T3LM3X
-tu- Buenos(as) dias/tardes/noches sr/srita (se educadosiempre)
-telefonista- Buenos(as) dias/tardes/noches
-tu- habla fulano de tal "de aqui" (jaja no güey de aya, tienes que verte un poco naco para que crean que trabajas en telmex) de la central numero \@\$%*!?. (vas a una esquina y hay una caja girs metalica que dice telmex y que tiene un numero en rojo o en amarillo dices ese numero) en San Juan Diegüito el chico (la colonia, la puedes ver en cualquier letrero de esquina o la preguntas), quien habla?
-telefonista- telefonista de tal en que te puedo ayudar
-tu- mira mano tengo un problema con un pendejo direccinamiento y tengo que cambiar 3... dame tono no?
-telefonista- como nó... tuuuuuuuuuuuu (es el tono de la linea)

...:[001]:... En ese momento marca cualquier numero y terminalo en cat
....:--x si hay algun pendejin cat=gato esta al lado del 0 (#)--:.....

DECODIFICACIÓN DE TONOS MULTI FRECUENCIA

Ideas generales, aplicaciones y propuesta de diseño

INTRODUCCIÓN

Todo phreak alguna vez en su vida se ha topado o llegará a necesitar diseñar un circuito el cual emplee los tonos emitidos al presionar un numero en el teclado matricial del teléfono.

Existen una infinidad de proyectos que pueden ser realizados en conjunción con un teléfono, desde proyectos de automatización y control hasta proyectos de espionaje.

Es raro entonces encontrar tan poca información al respecto, sobre todo en nuestro idioma. Con este articulo intentare explicarles un poco de cómo funcionan los tonos DTMF, como están compuestos y les daré unas cuantas ideas y propuestas de proyectos que pueden resultar bastante interesantes.

INTRODUCCIÓN A LOS DTMF

DTMF significa *Tono Dual de Multi Frecuencia* (Dual Tone Multi Frequency) y se entiende como la suma en tiempo real de dos ondas senoidales de diferentes frecuencias.

En un teclado matricial los tonos que representan cada una de las teclas son formados por la suma de un tono en frecuencia baja y un tono en frecuencia alta. Estas frecuencias están distribuidas en forma de columnas y renglones como se muestra en la Tabla 1.

Frecuencias de Banda Alta

		1209	1336	1477
<i>Frecuencias de Banda Baja</i>	697	1	2	3
	770	4	5	6
	852	7	8	9
	941	*	0	#

Tabla 1. Correspondencia de tonos y frecuencias.

También existen cuatro tonos más llamados A, B, C y D, que son empleados principalmente en empresas u oficinas gubernamentales en las que se requiera de más tonos que en un teléfono residencial debido al uso de varias líneas o un PBX.

Las frecuencias de los tonos fueron diseñadas para evitar problemas de ruido y otros aspectos acústicos al estar enviado o recibiendo información a través de una línea telefónica.

DECODIFICANDO DTMF

Gracias a los avances en la tecnología, hoy en día no tenemos que preocuparnos en diseñar un sistema de filtros para reconocer los tonos que han sido enviados. Varios fabricantes ofrecen circuitos integrados con la posibilidad de decodificar la señal de audio entrante y mandarla a través de una o más salidas en formato digital.

La mayoría de los IC's antiguos emplean un sistema como el que aparece en la figura 1.0.

En donde la entrada de audio es la señal proveniente de la línea telefónica, D1, D2, D4 y D8 son las salidas en binario del numero correspondiente y Dv es el *strobe* (señal de tono valido).

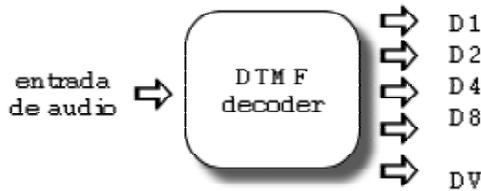


figura 1.0

Diagrama a bloques de un decoder DTMF.

Los nuevos integrados sin embargo emplean comunicación serial evitando así tener que emplear un mayor numero de puertos al conectarlo a un microcontrolador.

Algunos de los IC's más empleados son: MC145436, MSM6843 y el SSI204 de motorola, oki y silicon systems (aun cuando algunos de estos modelos ya están discontinuados en EU, aquí en México aun pueden ser adquiridos a precios relativamente bajos).

APLICACIONES Y PROPUESTA DE DISEÑO

Algunas de las aplicaciones que se le pueden dar a este sistema son, como lo mencione anteriormente, de automatización y control e incluso se le puede dar una aplicación de espionaje.

Hoy les daré la idea de un circuito de espionaje que por causa de tiempo no he realizado, pero que me gustaría mucho que de desarrollarlo me hicieran saber sus

comentarios y observaciones a través de los foros o al correo que ya todos conocen.

El proyecto nace de observar que cada día más y más personas utilizan estos días el teléfono para realizar transacciones bancarias, realizar llamadas a través de un PBX, o simplemente revisar los mensajes grabados en su contestador telefónico.

El objetivo principal del circuito es proporcionar una herramienta que pueda ser empleada junto con una beige box (ver *eZine 1 MHM*) para descifrar las contraseñas enviadas por medio de tonos multi frecuencia.

La idea se muestra plasmada en un diagrama a bloques en la figura 1.1.

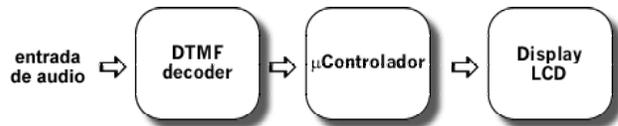


figura 1.1

Diagrama a bloques de un decoder de contraseñas

La entrada de audio va conectada directamente a la línea telefónica por medio de la beige box. Al ir recibiendo los tonos de los diferentes números presionados, el decodificador DTFM entrega a la entrada del microcontrolador el numero binario correspondiente el cual es identificado y guardado en memoria por el microcontrolador el cual mandará la señal necesaria al display de cristal líquido para ver los números que componen la contraseña tecleada.

El microcontrolador cuenta con un programa el cual permite, por medio de pulsadores avanzar, retroceder, guardar y borrar los números capturados.

NOTAS FINALES

Espero que este artículo haya sido de su agrado y que les haya interesado el proyecto de captura de contraseñas.

Cualquier duda o comentario al respecto pueden ponerlos en los Foros de Tecnología Mexicana y con gusto serán contestados por un servidor.

Saludos a todos,

--oSUKARu--

Bug en REDIAL??? de TELMEX

By George X

.....
DISCLAIMER:

El Articulo esta hecho en base a la regla de libre expresi3n en la constituci3n.

Este Archivo da a conocer un uso educacional del sig. documento el autor y sus dem1s ayudantes no se responsabilizan de las jaladas que se puede hacer con la informaci3n sig.

.....

~=Historia=~

Un dia jugano el telefono tratando (Joder Telmex XD) buscando algo con que hablar gratis buscando, claves de PBX colge y una persona del che banco santander me hablo y como no le dije informacion (de alguien que ni vive en mi casa) me dijo "Eres Bruto Animal No ayudas en nada".

Entonces sabrab que me puse de la verga use mi identificador de llamadas le volvi hablar (Jejeje Le Dije Fuck You) y le comente mi historia y me volvio a colgar entonces yo cortado no vi y me quede esperando como 5 segundos (Shockeado %) y luego hablo solito y volvio a marcar todo mi tel y yo y me contesto la pendeja y le dije estúpida y le colge dije fue u error espere el che recibo y vi que solo me cobraron 1 y yo feliz por mi decubrimiento ya sabran XD.

--[Como Funciona]--

Bueno me dedique mas de 1 semana buscando diciendole a mis cuates he ise una probalidad (Soy Gran Matematico) y salio que tenias un fallo o probalidad de que no salga de 15% asi que no manden una bola de mails que diga no sirve ya explique de 5 casas 1 no sirve y en otras 4 si.

Mira marcan el numero que quieran cuelga el del otro tel (asi que ve como le explicas XDDD) y cuelgas en menos de 3 segundos (el del que le llams)

Esperas como unos 20 segundos y pan!!! gratis habla, habla. Este truco solo funciona con local y nacional no internacional.

Greetz To:

** A mi Equipo de hackers que se hasta apenas empezando para que cuando vean esto se animen a seguir: HaCkInG ThE PIAAnEt Integrantes:

- Olyster
- MalaAccion
- Psycho
- Hckcoliman

** A mi brother por la help de no decir a mis jefe XD- el_we

** a mis cuates (No hackers)

- Steal 1080
- nathan
- Slash
- Mayoral

** Especial entre todos a la ayuda de [WoLvE] (Ensfarme a al mudno phreaker)

*****Thnks to MHM Por Publicar este articulo*****

Copyrigths By **George X**
Dudas del texto Enviar Mail George_x2@hotmail.com

INDICADOR DE ESTADO TELEFÓNICO

Funcionamiento, y circuito práctico

INTRODUCCIÓN

Después de haber leído el artículo de oSUKARu sobre decodificación de contraseñas por línea telefónica que desarrollo para este eZine, me vino a la mente otro proyecto que puede ser añadido a la beige box (para cuando terminemos de incluir todos nuestros circuitos y modificaciones le cambiaremos el nombre de beige box a *MHM box* ^_^).

INDICADOR DE ESTADO TELEFÓNICO

Todos sabemos que al levantar un teléfono se producen cambios en el voltaje de la línea. Basta con levantar dos teléfonos al mismo tiempo para ver que la calidad de la señal cae así como el volumen del audio.

El cambio en la línea depende mucho de en donde nos encontremos, que modelo de teléfono empleemos, cuantos teléfonos descolguemos, también depende de si los teléfonos están conectados en serie o en paralelo, etc...

El voltaje nominal con el que trabaja normalmente un teléfono es de $-48V$ DC, y al contestar este voltaje cae hasta aproximadamente $-7V$ DC.

CIRCUITO DEL PROYECTO

El circuito fue diseñado con una sola meta en mente, sencillez. Todos sabemos que lo que representa a la beige box es su simplicidad y facilidad de uso, es por eso que este diseño se pensó de la forma que pudiera ocupar el mínimo espacio y que fuera lo más fácil de realizar posible. Y sobre todo que no requiera de alimentación externa para funcionar.

En la figura 1.0 se muestra el esquemático del proyecto.

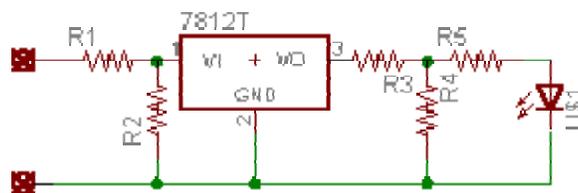


Figura 1.0
Esquemático del Indicador de Estado.

FUNCIONAMIENTO

El funcionamiento es bastante simple y se basa simplemente en divisores de tensión por medio de resistores y un regulador de voltaje. El voltaje de entrada es reducido por medio del primer divisor de tensión para luego es regulado a 12V, este voltaje es después reducido de nuevo para prender el LED.

Sabiendo que el voltaje al desconectar el teléfono es de alrededor de 7V el LED no prendera a menos de que la línea este desocupada.

MATERIAL

Regulador a 12V 7812

R1 Resistor 10K ohm

R2 Resistor 4K7 ohm

R3 Resistor 1K ohm

R4 Resistor 510 ohm

R5 Resistor 470 ohm (puede ser cambiado a un valor menor para obtener mayor luminosidad)

Varios (cables, cautín, soldadura, etc.)

FORMA DE USO

Se conecta primero el teléfono por medio de la beige box para estar seguros de que no se encuentre en la línea la señal senoidal de timbre.

Se conecta el circuito, si el LED esta apagado significa que la línea esta en uso, en caso de que el LED prenda significará que la línea no esta ocupada y podemos realizar nuestra llamada.

IDEAS PARA MEJORAR EL PROYECTO

Este proyecto es realmente un diseño muy básico que sin embargo cumple con su propósito, pero esto no significa que no pueda ser mejorado. Hay muchas cosas que se le pueden adicionar, como un detector de timbre, un circuito de bloqueo de línea para que automáticamente cuelgue en caso de que llegaran a levantar la bocina los dueños de la línea, en fin un sin numero de cosas más pero eso se deja al lector.

En caso de que el LED prenda muy tenue, retiren R3 y R4 del circuito y experimenten con valores de R5 hasta encontrar la intensidad deseada.

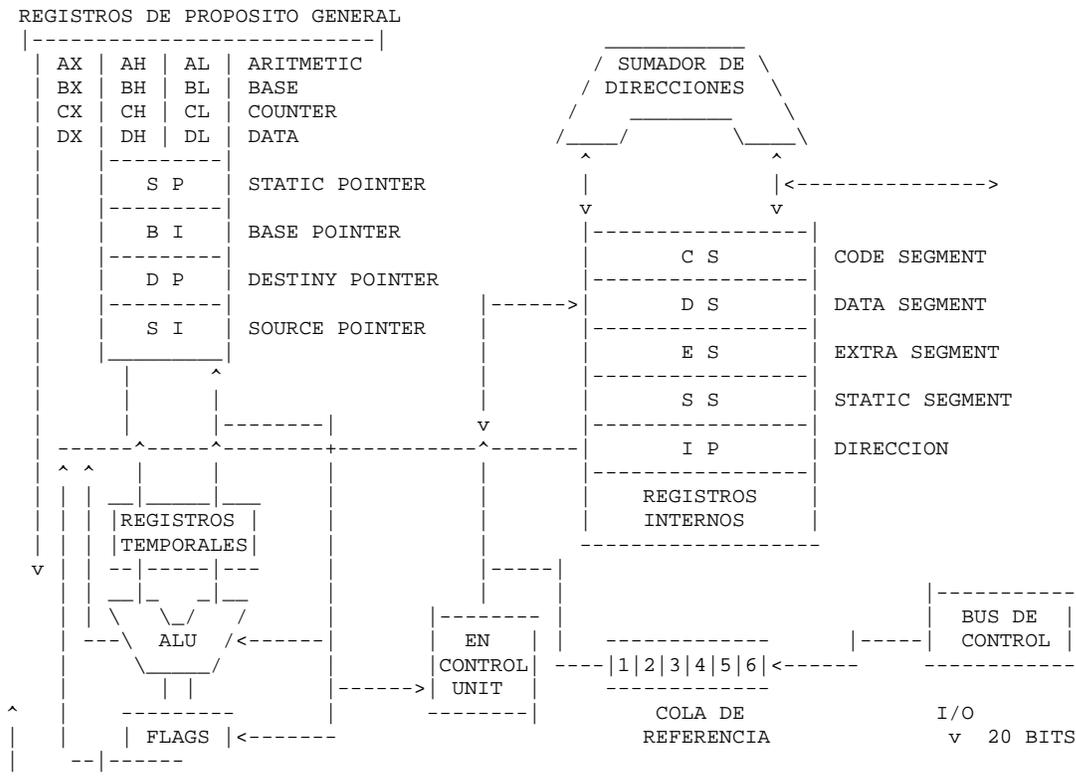
3N\$AMBLADOR KON MANZANA\$ 1ª parte

por (".oPáKo.")

Si cuando lees este e-zine y entras a la parte de programar en ensamblador y si ves cosas como MOV AX, [BX] y no tienes la menor idea de que sea, entonces este curso es para ti.

El ensamblador es el lenguaje de mas bajo nivel despues del mismisimo lenguaje maquina, tal vez no el mejor ni el mas facil ni el mas usado, pero si en el que puedes contener el maximo codigo en el minimo espacio.

Asi junciona esto:



(_..'ja soy una pistola que chido me quedo el diagrama'.._)

- CS -Aquí está el código del ensamblador.
- DS -Aquí están los datos del programa.
- SS -Apunta al inicio del segmento de pila (la parte baja del RAM).
- ES -registro que guarda al elemento extra (apunta al inicio de la pila).
- REGISTROS DE PROPOSITO GENERAL -Procesan la info que puede funcionar como 8 registros de 1 byte o 4 registros de 2 bytes.

El procesador asume por default que la info se encuentra en "AX", como registro base "BX", pueden ser utilizados como "SI" y "DI". A "CX" lo toma como contador y "DX" apoya al procesador en operaciones de "I/O" (entrada y salida) y se complementa con "AX" para hacer operaciones de 32 bits.

Lo mas basico (pero mas usado)

MOV	-mover	MOV AX, BX	-mueve "BX" a "AX"
ADD	-sumar	ADD AX, 2	-sumale 2 a "AX"
SUB	-restar	SUB BX, AX	-restale "AX" a "BX"
LEA	-leer	LEA SI, variable	
INC	-incrementar	INC CX	-incrementa CX (CX+1)
DEC	-decrementar	DEC CX	-al reves
JMP	-saltar	JMP INSTRUCCION	-va a una instruccion
DW	-define datos de 2bytes	DATO DW 5	-define que DATO=5
[BX]	-contenido de BX	MOV AX, [BX]	-mueve el contenido de "BX" a AX

```

PAGE 60, 132 \
TITLE EJEMPLO |
MODEL SMALL  | CABECERAS
STACK 64     /

.DATA        \
DATO1 DW 5   | DECLARACION
DATO2 DW 2   | DE
SUMA DW ?   | DATOS
RESTA DW ?  /

.CODE       \
MAIN PROC FAR |
MOV AX, @DATA | INICIO DEL
MOV DS, AX    / CODIGO

MOV AX, DATO1 \ AQUI
ADD AX, DATO2 | SUMAMOS
c:\borlandc\bin\
MOV SUMA, AX  /

MOV BX, DATO1 \ AQUI
SUB BX, DATO2 | RESTAMOS
MOV RESTA, BX /

MOV AX, 4C00H \
INT 21H      | ACABA
MAIN ENDP   | AQUI
END MAIN    /

```

para poder convertir todo esto en un "ejemplo.exe" tenemos que hacer el programa en un editor de texto que no guarde caracteres de mas, o sea como el vi, edit, notepad, etc y se guarda como "ejemplo.asm", despues usamos el TASM (como el que viene en el borland en la carpeta de bin y generamos un ".obj" y el TLINK para hacer el ".exe" asi
c:\borlandc\bin\TASM ejemplo.asm
c:\borlandc\bin\TLINK ejemplo.obj
y ahora en la carpeta
esta ejemplo.exe y ya...

COMO PROGRAMAR UN PIC

Una de las dudas que más contesto por correo es *¿cómo se programa un PIC?* Así que pasaré a detallar los pasos que se requieren para hacer la programación de un PIC16F84.

Antes de empezar necesitamos tener listo el archivo hex que va a ir dentro del PIC y el programa ICPROG.

Se abre el programa ICPROG y se selecciona el tipo de integrado que vamos a programar, una vez hecho esto se prosigue a abrir el archivo .hex en el que se encuentre el código que queremos meter al micro. En este momento deberás de ver que los números que se encontraban por defecto en la venta del ICPROG han sido cambiados por los datos contenidos en tu hex.

Teniendo conectado el JDM al puerto serial presiona F3 o ve al menú SETTINGS -> HARDWARE, ahí selecciona el tipo de programador y el puerto en el que se encuentra conectado. Como se muestra en la figura 1.1

Por lo general, los valores predeterminados te serán suficientes.

Una vez terminado de configurar tu programador basta con presionar F5 para

que comience la programación del microcontrolador.

Es recomendable que en las opciones de programación selecciones la casilla de "verify during programming" para que el ICPROG vaya revisando que todo este bien mientras programa el integrado.

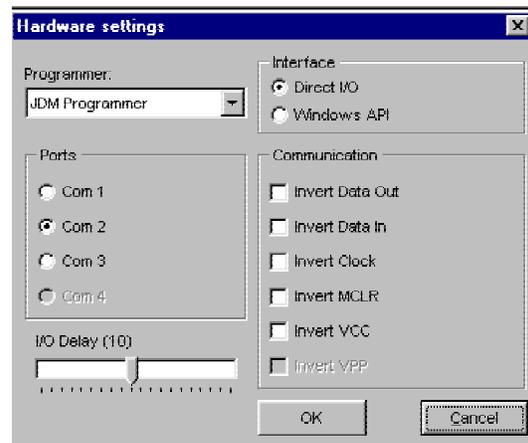


Figura 1.1 Configuración del Programador a usar.

ULTIMAS NOTAS

No falta decirlo, pero el JDM es uno de los programadores más recomendables, especialmente para novatos debido a su sencillez de construcción y de uso, además de la variedad de microcontroladores que es capaz de programar.

--oSUKARu--

Para obtener más información acerca de este programador y los diferentes tipos de integrados que es capaz de programar visita la pagina personal de su creador en <http://www.jdm.homepage.dk> o busca en www.google.com

EL ESCORPIÓN

Diseño de un transmisor de FM

INTRODUCCIÓN

Para cualquier hobbista o phreak es bastante útil contar entre sus herramientas con un circuito que sea capaz de transmitir voz a distancia de manera inalámbrica. Las aplicaciones pueden ser varias dependiendo de la imaginación de cada persona y van desde una alternativa a los comunes “walkie talkies” hasta un “bug” para escuchar las conversaciones que ocurren en un cuarto. (Otro posible aditamento para la beige box ^_^)

Después de investigar varios tipos de transmisores miniatura encontré, gracias a un amigo, un circuito lo suficientemente potente como para transmitir voz a más de 50m de distancia y lo suficiente chico para poder ser escondido en caso de que eso se requiera.

CIRCUITO DEL TRANSMISOR

En la figura 1.0 se muestra el diagrama esquemático.

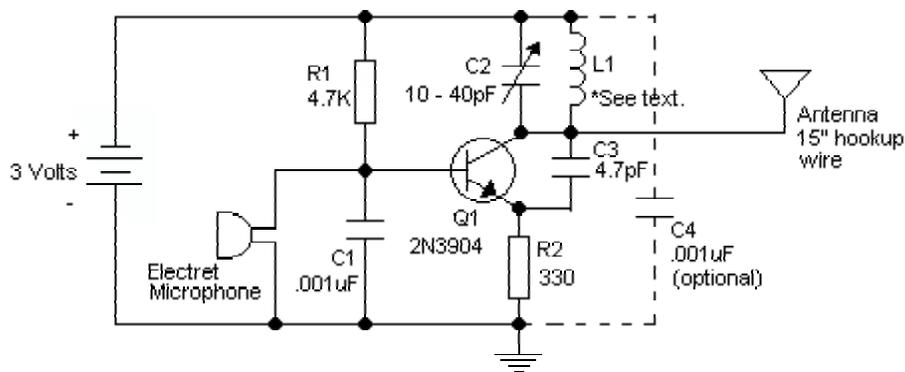


Figura 1.0
Diagrama esquemático

Quizás la ventaja más notable del circuito es su sencillez para armarlo, ya que el circuito en si no requiere ser diseñado con mucha precisión.

La bobina 1 se forma enrollando un alambre de calibre 22 ga. Sobre un tornillo o clavo de $\frac{1}{4}$ de diámetro hasta formar 8 vueltas en total, es recomendable que la separación entre vueltas no sea muy grande y sobre todo que se mantenga uniforme en toda la bobina.

C4 es un capacitor opcional, sin él el circuito funcionará sin problemas pero se puede llegar a obtener un mayor rango de cobertura además de obtener un mejor funcionamiento del transmisor.

MATERIAL

Resistor	R1	4.7 K
Resistor	R2	330 Ohm
Capacitor	C1, C4	0.001 uF
Capacitor	C3	4.7 pF
Capacitor Variable		10 - 40 pF
Microfono		Electret
Transistor		2n3904 (o equivalente)

CONSIDERACIONES AL DESARROLLARLO

En el diagrama original se especifica que el circuito sea alimentado con 3V, es recomendable emplear baterías de reloj para ocupar el menor espacio posible.

La bobina puede llegar a ser remplazada por una bobina “dibujada” en el circuito impreso formando un dibujo de una espiral con las venas y sacando la antena del centro de este.

El capacitor variable es difícil de conseguir en tiendas de electrónica pero si tienes algún radio de pocos componentes (de esos que venden en los tianguis por 20 pesos) es muy probable que encuentres uno ahí.

COMENTARIO FINAL

Creo que no necesito decirles las aplicaciones que puede llegar a tener un transmisor de audio por FM, así que dejaré que su imaginación le encuentre un propósito idóneo.

The Aztek-Box

By: www.Phreakers.com.mx team

Seguramente se estarán preguntando , que hace esta nueva boX? pues muy sencillo , imagina que necesitas hacer una llamada muy importante, pero el teléfono publico al que acudes esta rodeado de gente muy extraña.

Si haces todo como debe de ser no tendrás que estar cerca del teléfono para poder hablar. El Proceso de instalación es muy variado, y esta box si es instalada adecuadamente puede ser indetectable.

Puede que el proceso de instalación sea largo, y además son pocos los modelos de payphones en los que funciona, Pero que mas da? es mexicana y además nunca subestimes la mente de un verdadero phreak , la cual se las ingeniaría de cualquier manera para poder instalarla.

Antes que nada pasemos al material:

Necesitamos:

- 2 bases pequeñas para teléfonos inalámbricos , lo mas pequeñas posibles y que ocupen un voltaje algo bajo hablamos de 3 a 9 volts.
- Una cajita de esas que tienen una entrada y dos salidas que normalmente se usan para sacar extensiones de la línea de teléfono rápidamente(opcional).
- Una caja de las que usamos en la beige box.

El procedimiento es mas que sencillo y mas que obvio así que espero que no haya reclamaciones de algún tipo ya que ni siquiera hay la necesidad de hacer diagramas

Lo que vamos a hacer es (pinchar) el payphone con una beige box pero en vez de sacar la línea directo al teléfono , la sacaremos a nuestra mini base del teléfono inalámbrico , la cual al ocupar muy poco voltaje podemos sustituir la corriente por pilas y la base al ser pequeña podemos esconderla fácilmente y con posibilidad de poder cambiar la pila, pero para que es la segunda base te preguntarás?

Pues muy fácil, es tan sencillo que ya te lo has de imaginar , es para que no tengas que recargar el teléfono en la misma base que esta instalada , esta box es bastante sencilla y útil así que no tendrás problemas , si , tiene sus retos pero son mas bien del tipo imaginativos que del tipo tecnológicos , para esconder la base y hacer la instalación necesitaras bastantes huevos , y

también bastante ingenio pero una vez colocada es de lo mas cómodo , por que puedes llamar gratis desde una distancia considerable y además que es menos comprometedora.

Los teléfonos en los que se deben instalar son de preferencia Publitel que se encuentran en zonas raras en el DF o los típicos que encontramos en las papelerías o tienditas la mayoría funciona con una línea de teléfono regular y la terminal o teléfono es el que hace todo el proceso de cobro y todo , lo único que estaríamos haciendo seria colgarnos de otra línea pero de manera mas segura este método también sirve para la línea de tu edificio por ejemplo , si te da flojera andar subiendo cada que quieres hacer una llamada hasta tu azotea y no quieres sacar un cablesote hasta tu casa , pues esta box es de lo mas útil .

Cualquier duda consulten : www.phreakers.com.mx o a www.hakim.ws
ambos en la sección de foros podrán plasmar sus dudas sugerencias o comentarios

Shouts:
n3z, hkm, Kinship, Taer, and the phreakers mexico team.

Seminario de Programación

Por Cheve

Habiéndose terminado el seminario de programación de XRoleX en el numero anterior, ahora Cheve nos hizo llegar esta extensión con algunos modelos que no habían sido incluidos.

PROGRAMACION AT&T 3630

1. ENCENDER

READY

2 presionar MENU, MENU, * 7 7 7 3 3 6 * (o MENU, MENU, * 0 0 7 3 3 6 *)

CMT REV 850 046 (versión de software. Presionar volumen hacia arriba

<i>DISPLAY</i>	<i>DATO</i>	<i>AVANZAR</i>
<i>NAM SELECT X</i>	<i>1-4</i>	<i># , volumen hacia arriba</i>
<i>SIDH</i>	<i>24592</i>	<i># , volumen hacia arriba</i>
<i>SCM</i>	<i>10</i>	<i># , volumen hacia arriba</i>
<i>MIN</i>	<i>52 99 47 .xxxx</i>	<i># , volumen hacia arriba</i>

Presionar MENU ; END para salir de la programación

Para checar el número telefónico presionar MENU, 5, MENU.

PROGRAMACION AUDIOVOX CMT 410

1. ENCENDER.

2. 2. MARCAR 000 FCN # 1 (EN CASO DE QUE EL EQUIPO YA HAYA SIDO PROGRAMADO PONDREMOS LOS ULTIMOS TRES DIGITOS DEL NUMERO TELÉFONICO QUE TENGA EN ESE MOMENTO).

3. 3. APARECERA COMO SIGUE :

PARAMETRO	DATO	AVANZAR
01	52 99 47 XXXX	STO
02	XXX	STO
03	24592	STO
04	0X	STO
05	10	STO
06	1	STO
07	01	STO
08	0334	STO
09	0	STO
10	1000	STO
11	10101000	STO
12	11100000	STO
13	00	STO
14	000	STO
15	XXX	STO
16	00000	FCN SEND FCN CLR

4. 4. PARA PONER EN BANDA "B", PRESIONAMOS FCN 01 Y APARECERA PRF EN PANTALLA ESPERAMOS A QUE DESAPAREZCA Y LISTO.

**PROGRAMACION AUDIOVOX PR350
TOSHIBA TCP-9300**

1. ENCENDER.

5. 5. MARCAR 000 FCN # 1 (EN CASO DE QUE EL EQUIPO YA HAYA SIDO PROGRAMADO PONDREMOS LOS ULTIMOS TRES DIGITOS DEL NUMERO TELÉFONICO QUE TENGA EN ESE MOMENTO).

6. 6. APARECERA COMO SIGUE :

PARAMETRO	DATO	AVANZAR
01	52 99 47 XXXX	STO
02	XXX	STO
03	24592	STO
04	0X	STO
05	10	STO
06	1	STO
07	01	STO
08	0334	STO
09	0	STO
10	1010	STO
11	10101000	STO
12	11100000	STO
13	00	STO
14	000	STO
15	XXX	STO
16	00000	FCN SEND FCN CLR

4. PARA PONER EN BANDA “B”, PRESIONAMOS FCN 01 Y APARECERA PRF EN PANTALLA ESPERAMOS A QUE DESAPAREZCA Y LISTO.

**PROGRAMACION AUDIOVOX TDMA 2500
DIGITAL**

1.- **Presionar END para encender el teléfono y no dejando de presionar ingresar antes de 10 seg. 6972814.**

2.- **En la pantalla saldra:**

Multi NAM

1->NAM1 Only **Presionar esta opción (1) para programar solo el NAM1**

2->NAM1&NAM2

3->NAM1~NAM3

Item	dato	avanzar
-------------	-------------	----------------

Go To Level 2 (Scan, etc.) ↑
 Go To Level 3 (PSID/RSIDs) ↑
 Go To Level 4 (Oher DCC) ↑
 EXIT
 Save > YES presionamos YES para salvar información
 Cancel > NO

3. Este teléfono es solo para la banda B.

Características importantes del teléfono

- • 25 tipos de timbre (incluidas opciones de timbrado con melodía musical)
- • ID de línea de origen (últimos 20 números)
- • Devolución de llamadas con números telefónicos incrustados para mensajes de texto
- • Almacenamiento de 200 números
- • Marcación rápida de 99 números incluido buzón de voz
- • Súper marcación de 9 números incluido el buzón de voz
- • Marcación de 2 tarjetas de llamada diferentes
- • Acceso rápido a los últimos 40 números marcados
- • Recibe mensajes de texto con 2KB de almacenamiento
- • Acceso rápido al servicio de buzón de voz
- • Información de duración de la llamada
- • Cifrado digital de la voz

PROGRAMACION ERICSSON DH318vi / DH368vi / DF388 vi

1. ENCENDER
2. MARCAR **923885**, MENU APARECERA:

PANTALLA	TECLEAR	AVANZAR
PROGRAM	1	
NAM 1-4 or 0 for SID		
ESN XXX XXXXXXXX		Rcl
MOBILE ID 1 ?	5299 47 XXXX	Rcl
A-Key	5299 47 XXXX	Rcl
SID 1	24592	Rcl
Alpha-Tag		Rcl
LOCK CODE		Rcl
Go To Level 2 (Scan, etc.)		Rcl
Go To Level 3 (PSID/RSIDs)		Rcl

Go To Level 4 (Oher DCC)

Rcl

EXIT

Save > YES

presionamos YES para salvar información

Cancel > NO

3. PARA PONERLO EN "BANDA B"

PRESIONAMOS MENU HASTA QUE APAREZCA **System Opt** PRESIONAMOS YES (SEND), Y CON MENU SEGUIMOS BUSCANDO HASTA QUE APAREZCA **System Type**, PRESIONAMOS NUEVAMENTE YES (SEND) Y CON MENU SELECCIONAMOS **PREF ONLY** Y PRESIONAMOS YES (SEND) PARA FIJAR LA BANDA.

PROGRAMACION ERICSSON DF688, DH680, DH600

1. ENCENDER

2. MARCAR **923885**, ↓:

PANTALLA	TECLEAR	AVANZAR
ESN XXX XXXXXXXX		↑
MOBILE ID	5299 47 XXXX	↑
A-Key	5299 47 XXXX	↑
SID	24592	↑
SOC	0000	↑
Home A-Tag		↑
Fav. A-Tag		↑
Neu. A-Tag		↑
Lock Code		↑
Go To Level 2 (Scan, etc.)		↑
Go To Level 3 (PSID/RSIDs)		↑
Go To Level 4 (Oher DCC)		↑

EXIT

Save > YES

presionamos YES para salvar información

Cancel > NO

3. Este teléfono es solo para la banda B.

PROGRAMACION ERICSSON KF 788

1. ENCENDER

2. MARCAR **923885**, ↓:

PANTALLA	TECLEAR	AVANZAR
ESN XXX XXXXXXXX		↑
MOBILE ID	5299 47 XXXX	↑
A-Key	5299 47 XXXX	↑
SID	24592	↑
SOC	0012	↑
Home A-Tag		↑
Fav. A-Tag		↑
Neu. A-Tag		↑
Lock Code		↑
BAND ORDER	23456781	↑
Go To Level 2 (Scan, etc.)		↑
Go To Level 3 (PSID/RSIDs)		↑
Go To Level 4 (Oher DCC)		↑

EXIT

Save > YES *presionamos YES para salvar información*
Cancel > NO

3. 3. Este teléfono es solo para la banda B.

PROGRAMACION ERICSSON R280d

1. ENCENDER
2. MARCAR **923885**, MENU:
3. PROGRAM NAM 1-2, Para programar NAM1, presionar 1. Para programar el NAM2, presionar 2

PANTALLA	TECLEAR	AVANZAR
ESN XXX XXXXXXXX		↑
MOBILE ID 1	5299 47 XXXX	↑
A-Key 1	5299 47 XXXX	↑
SID 1	24592	↑
SOC 1	0012	↑
Home A-Tag 1		↑
Fav. A-Tag 1		↑
Neu. A-Tag 1		↑
Lock Code		↑
Band Order 1	baDFABCE (no modificar)	↑
Go To Level 2 (Scan, etc.)		↑
Go To Level 3 (PSID/RSIDs)		↑
Go To Level 4 (Oher DCC)		↑

EXIT

Save > YES *presionamos YES para salvar información*
Cancel > NO

3. Este teléfono es solo para la banda B.

PROGRAMACION DEL LA DIRECCIÓN IP

1. 1. **PRESIONA MENU 5 (BROWSER).**
2. 2. **PRESIONAR MENU 9, 5, 2**
3. 3. **PEDIRA PASSWORD, PRESIONAR 00000 (5 CEROS)**
4. 4. **PRESIONAR 1, 3**
5. 5. **PRESIONAR BACK PARA BORRAR LE NUMERO QUE TRAE PRE-PROGRAMADO, E INGRESAR LA DIRECCIÓN IP (12 DIGITOS).**
6. 6. **PRESIONAR YES Y DESPUES MENU.**

PROGRAMACION JRC 8330

1. ENCENDER.
2. Teclar : FCN 1 FCN 1234 FCN, aparecerá en pantalla “Locked”.
3. Oprimir #322867# FCN, aparecerá “Sys 1” presionamos vol para el Sys 2.
- 4. 4.** Oprimimos FCN y veremos en pantalla “01 Sys 1 on “, y programamos como sigue :

Vol. derecha (>>>) es para cambiarnos de parámetro.
FCN es para entrar al parámetro para grabar los datos.

	Parametro	Dato	Avanzar
2	Area code	529	FCN >>>
3	Phone number	9 47xxxx	FCN >>>
4	SIDH	24592	FCN >>>
5	ACCOLC	0x	FCN >>>
6	Roam Inhibit	Off	FCN >>>
7	MIN Mark	Off	FCN >>>
8	IPCH	0334	FCN >>>
9	IDCCH	0333	FCN >>>
10	IDCCH	0334	FCN >>>
11	Control Chanel	21	FCN >>>
12	SCS	On	FCN >>>

Para salir oprimir CLR CLR, aparece en pantalla STORED. Teclar FCN y saldra “STORING”.

PREFIJO : 152 (98 hexadecimal)

PROGRAMACION FUJITSU PCX

1. ENCENDER (PONERLO EN LOCKED) (FCN *) o (FCN 9)

2. 2. APAGAR

3. 3.

3. ENCENDER Y PRESIONAR # 626 # 7764726 EN DIEZ SEGUNDOS .
COMENZARA UN TONO CONTINUO

4. PRESIONAR Y SOSTENER LA TECLA * . EL TONO SE CONVERTIRA INTERMITENTE.
SOLTAMOS * HASTA QUE TERMINE DICHO TONO

5. APARECERA LO SIGUIENTE :

PARAMETRO	CONCEPTO	DATO	AVANZAR
01	SIDH	24592	STOR
02	LOCAL USE	1	STOR
03	MIN MARK	1	STOR
04	MIN	52 965 4XXXXX4	STOR
05	SCM	14	STOR
06	IPCH	0334	STOR
07	ACCOLC	0X	STOR
08	P.S.	0	STOR
09	GIM	10	STOR
10	LOCK	XXXX	STOR
11	CALL TIME	1	STOR
12	LOCK MODE	1	STOR
13	CALL REST.	1	STOR
14	SIDH INHIBIT	00000	STOR
15	SIDH INHIBIT	00000	STOR
16	SIDH INHIBIT	00000	STOR

6. AVANZAMOS HASTA QUE APAREZCA EL PARAMETRO 01 Y PRESIONAMOS SEND PARA FINALIZAR LA PROGRAMACION.

7. PARA PONER EL TELEFONO EN "BANDA B" PRESIONAMOS FCN 1 Y CON LAS TECLAS DEL VOLUMEN SELECCIONAMOS EL SISTEMA "B SYSTEM ONLY" Y PRESIONAMOS

PROGRAMACION MITSUBISHI

AH-350/ 355/250

1. 1. ENCENDER

2. 2. PRESIONAR END Y SIN DEJAR DE PRESIONAR END, MARCAR 6972815 Y SOLTAMOS END.

PANTALLA	TECLEAR	AVANZAR
No. Tel.	52 99 47 xxxx	TALK
SID	24592	TALK
SecCode	xxxx (candado)	TALK

ContFCN

ExitEND para salir presionar END.

PROGRAMACION MITSUBISHI
AT-1000 carry

1. 1. ENCENDER EL EQUIPO, Y AL TERMINAR EL TONO DE ENCENDIDO PRESIONAR LA TECLA DE END Y AL MISMO TIEMPO MARCAR 5474432 Y SOLTAMOS END APARECERA COMO SIGUE.

PANTALLA	TECLEAR	AVANZAR
Dual 0		send
Phone No.	529947xxxx	send
Sidh	24592	send
Sec Code	xxxx	send
L.U.	1	send
Ex	1	send
Ipch	0334	send
Accolc	(cero y el último dígito)	send
Gim	10	send
RI	0	send
SID op	0	send
Lock 01		send
Lock 02		send
Pref.01	00000	send
Pref. 02	00000	send
EMG.No	0100	send

end (para salir de la programación)

PARA PONER EN BANDA PRESIONAR FCN 8 Y SELECCIONAR CON LAS TECLAS DE * o # HASTA QUE APAREZCA SYSTEM B ONLY PRESIONAMOS FCN y End para salir.

(PREFIJO 134 / 86)

PROGRAMACION MOTOROLA FX 1500

PROGRAMACIÓN DEL “SID y NUMERO TELEFONICO CELULAR”

1. Encienda el equipo.
2. Presione FCN 0000000000000 (13 ceros), RCL
3. Oprima * para avanzar en los pasos de la programación.
4. Paso 1. Se desplegará en la pantalla SYST.ID. Ingrese el SID de la región
5. Paso 2. Ingrese el código de País + primer número de la clave lada de la ciudad: 52+ n
6. Paso 3. ingrese el Número Celular a 7 digitos
7. Paso 4. Nivel de Potencia: Ingrese 08
8. Paso 5. ACALL: Ingresar 0 y el último dígito del número Celular
9. Paso 6. GRO ID MARK: ingrese el número 10
10. Paso 7. Código de Seguridad: ingrese 000000 (6 ceros)
11. Paso 8. Código de Seguridad: Poner 000 (3 ceros)
12. Paso 9. Frecuencia más baja de la banda B: Poner 334
13. Paso 10. Bit Option: Poner 011100
14. Paso 11. Activar o desactivar módulos: ingrese 11111
15. Presione la tecla SEND y el teléfono se apaga automáticamente

PROGRAMACION MOTOROLA FX 2500

- 1. 1. CONECTAR**
- 2. 2. HACER PUENTE COMO SE MUESTRA**

Nota : despues de conectar la base a la toma de corriente se conectará cualquier auricular de carry phone Motorola por la parte de abajo de la misma base y se procederá a puentear el equipo para poder entrar al modo de prueba

- 3. 3. APARECERAN NUMEROS FLASHANDO (Indicando que si entramos al modo de prueba)**

4.MARCAMOS # 55 #

PARAMETRO	DATO	AVANZAR
1	24592	*
2	10101101	*
3	5299 47 XXXX	*
4	08	*
5	0X	*
6	10	*
7	000000	*
8	XXX	*
9	004	*
10	00001100	*
11	00000000	*
12	0334	*

13	0333	*
14	0334	*
15	021	*
16	1111011	*

Aparecerá una comita (apóstrofe) indicando que termina el proceso.

Apagamos el equipo y desconectamos (Listo)

La banda se activa por de fault

-
-

PROGRAMACION MOTOROLA FX 5000

1. ENCENDER

<i>Paso</i>	<i>Descripción</i>	Nota	LED
2	Para entrar al modo de programación presionar simultáneamente * y #, por tres segundos, con el auricular “colgado” (en la base). El foco del teléfono deberá apagarse (turn off).		Apagado
3	Presionar seis veces el número cero y después STO	1	Naranja
4	Ingrese el SIDH (24592) y después STO	2	Verde intermitente
5	Ingrese el número telefónico a 10 dígitos 5299 xxxxxx y después STO. (MIN)	2	Rojo intermitente
6	Presione 1 y después STO. (L.U.)	2	Naranja intermitente
7	Presione 0X y después STO. (ACCOLC)	2	Rojo, verde intermitente
8	Presione 10 y después STO. (Group ID)	2	Rojo, naranja intermitente
9	Presione seis ceros (000000) y después STO	2	Naranja
10	Presionar SND para almacenar y salir de la programación.		

NOTAS:

1. Hasta que el LED se apague, se podrá presionar los 6 ceros y STO. Si por alguna razón el código de seguridad fuera diferente a 6 ceros, el LED permanecerá en verde.
2. Un ingreso incorrecto de los parámetros seguido del STO, el LED indicará un error flasheando rojo/verde rápidamente. Se permanecerá en el paso de la programación donde éste se produjo. Se podrá volver a poner el valor correcto y hasta que sea así se pasará al próximo paso de la programación.

PROGRAMACION MOTOROLA CARRY PHONE

1. ENCENDER
2. PRESIONAR FCN (13 VECES EL NUMERO 0) RCL
3. APARECERA LO SIGUIENTE:

PARAMETRO	AVANZAR	DATO	AVANZAR
01	*	24592	*
02	*	529	*
03	*	9 47 XXXX4	*
04	*	08	*
05	*	0X4	*
06	*	10	*
07	*	000000	*
08	*	XXX	*
09	*	0334	*
10	*	011100	*
11	*	11110	*
01	SEND		

3. PARA PONER EN "BANDA B"
PRESIONAR RCL * * * * HASTA QUE APAREZCA "SCAN B" Y PRESIONAMOS STO

NOTA: EN CASO QUE SE QUIERA PROGRAMAR UN SEGUNDO NAM (ES DECIR UN SEGUNDO NUMERO TELEFONICO) ENTRAREMOS A LA PROGRAMACION NORMAL Y AVANZAMOS HASTA EL PARAMETRO 10 Y PONDREMOS 011110 DESPUES AVANZAMOS AL PARAMETRO 01 PRESIONAMOS SEND Y ENTRAREMOS A LOS PARAMETROS DEL SEGUNDO NAM LOS CUALES SE PROGRAMARAN DE LA MISMA FORMA

PROGRAMACION MOTOROLA PT 500

1. ENCENDER
2. PRESIONAR STO # (12 VECES EL NUMERO 0) RCL
3. APARECERA LO SIGUIENTE:

PARAMETRO	AVANZAR	DATO	AVANZAR
01	*	24592	*
02	*	529	*
03	*	947 XXXX	*

04	*	10	*
05	*	0X	*
06	*	10	*
07	*	000000	*
08	*	123	*
09	*	334	*
10	*	011100	*
11	*	110	*
01	SEND		

3. PARA PONER EN "BANDA B"

PRESIONAR RCL * * * * HASTA QUE APAREZCA "SCAN B" Y PRESIONAMOS STO

PROGRAMACION MOTOROLA POPULOUS

1.- ENCENDER EL TELEFONO Y MARCAR 74663 # FCN FCN

APARECERA enter number , METEMOS EL NUMERO A PROGRAMAR .
PRESIONAMOS STO Y * PARA GRAVAR Y AVANZAR.

2. 2. METEMOS EL SIDH 24592. STO Y * Y APARECERA entry done

3. 3. listo.

PROGRAMACION MOTOROLA UNIVERSAL

(Incluye Startac y Vader)

1. ENCENDER

2. PRESIONAR FCN (13 VECES EL NUMERO 0) RCL

3. APARECERA LO SIGUIENTE:

PARAMETRO	AVANZAR	DATO	AVANZAR
01	*	24592	*
02	*	529	*
03	*	947 XXXX	*
04	*	10	*
05	*	0X	*
06	*	10	*
07	*	000000	*
08	*	123	*
09	*	334	*
10	*	011100	*
11	*	11110	*
01	SEND		

3. PARA PONER EN "BANDA B"

PRESIONAR RCL * * * * HASTA QUE APAREZCA "SCAN B" Y PRESIONAMOS STO

NOTA: EN CASO QUE SE QUIERA PROGRAMAR UN SEGUNDO NAM (ES DECIR UN SEGUNDO NUMERO TELEFONICO) ENTRAREMOS A LA PROGRAMACION NORMAL Y AVANZAMOS HASTA EL PARAMETRO 10 Y PONDREMOS 011110 DESPUES AVANZAMOS AL PARAMETRO 01 PRESIONAMOS SEND Y ENTRAREMOS A LOS PARAMETROS DEL SEGUNDO NAM LOS CUALES SE PROGRAMARAN DE LA MISMA FORMA

PROGRAMACION STARTAC Digital 7797

1. ENCENDER

2. 2. PRESIONAR # 24592 # * SND

3. 3. Aparecerá en pantalla Nam Prog?
*= Yes #= No, presionar *

4. 4. En la pantalla aparecerá Security Code,
Presionar 000000 (6 ceros)

5. Mostrará el ESN, presionamos Snd

6. En la pantalla aparecerá Phone #
Meter Número celular de 10 dígitos (52 99 47 XXXX ejemplo) Snd

7. Cabe mencionar que este teléfono es dual mode (analógico/digital) y dual band (TDMA 800 MHz y TDMA 1900 MHz) y es solo para TELCEL (banda B).

Para programar el segundo NAM

Encender teléfono

presionar # 24592 # 2 # * Snd. El teléfono mostrará Nam 2 Prog

entonces proceder de la misma manera que en el primer NAM

Esta es la programación para equipo digital (modelos M3097, 7790, 7797, etc.), consta de 20 pasos: (Ejemplo)

Paso 1. Paso 1. FCN 00 * * 83786633 STD # US' 55 # 24580 (aparece en el display)
Paso 2. Paso 2. * 10110101 (aparece en el display)
Paso 3. Paso 3. * Ingresar NIP (059xxxxxx)
Paso 4. Paso 4. * 11 (aparece en el display)
Paso 5. Paso 5. * 05 (aparece en el display)
Paso 6. Paso 6. * 10 (aparece en el display)
Paso 7. Paso 7. * 000000 (aparece en el display)
Paso 8. Paso 8. * 728 (aparece en el display)
Paso 9. Paso 9. * 4 (aparece en el display)
Paso 10. Paso 10. * 00000100 (aparece en el display)
Paso 11. Paso 11. * 00001000 (aparece en el display)
Paso 12. Paso 12. * 0334 (aparece en el display)
Paso 13. Paso 13. * 0333 (aparece en el display)
Paso 14. Paso 14. * 0334 (aparece en el display)
Paso 15. Paso 15. * 021 (aparece en el display)
Paso 16. Paso 16. * 0737 (aparece en el display)
Paso 17. Paso 17. * 0708 (aparece en el display)
Paso 18. Paso 18. * 0737 (aparece en el display)
Paso 19. Paso 19. * 1011011 (aparece en el display)
Paso 20. Paso 20. '01 # Se apaga el teléfono

Del paso 4 al 19 sólo darle * para avanzar y no cambiar ningún parámetro, para terminar usar el paso 20.

PROGRAMACION NEC 2600 DIGITAL

1. ENCENDER

5. 2. PRESIONAR # 24592 # * SND

6. 3. Aparecerá en pantalla Nam Prog?

1 = Yes 2 = No, presionar 1

4. Mostrará el ESN, presionamos Snd

5. En la pantalla aparecerá Phone Number

Meter Número celular de 10 dígitos (52 99 47 XXXX ejemplo) Snd

7. Cabe mencionar que este teléfono es dual mode (analógico/digital) y dual band (TDMA 800 MHz y TDMA 1900 MHz) y es solo para TELCEL (banda B).

PROGRAMACION NEC DT 2000

1. ENCENDER

1. 1. PRESIONAR # 7764726 # SND

MEM # 01 MEM # 71

NOTA: HACER ESTE POCEDIMIENTO EN 15 SEGUNDOS DESPUES DE ENCENDER EL EQUIPO

Pantalla		Dato	Avanzar
Nam No.1 NAM-1			#
Phone No.	MIN	5299 XXXXXX	#
Lock Code	Lock	XXX	#
Home Area	SID	24592	#
Edit ASID?		0	
G.I. Mark	GIM	10	#
First P-CH	IPCH	0334	#
Second P-CH		0737	#
Sys Select		0=B	#
ACCOLC	ACCOLC	0X	#
MIN Mark		1=Yes	#
Local Use		1=Yes	#
EMG-No.		100	#
FCN State		00000000	#
EDIT XSID		0	
PREFER SID SHOW HOME		1	
EDIT PRSID		0	
View Test Reg		0	
View Reg Accept		0	

3. PRESIONAR CLR Y SOSTENER HASTA QUE APAREZCA "TEST MODE".

4. PRESIONAR RCL # 02 PARA SALIR DE PROGRAMACION

5. PARA PONER EN "BANDA B" PRESIONAR FCN 54 Y CON LA TECLA DE RCL SELECCIONAMOS "B ONLY" Y PRESIONAMOS STO PREFIJO 229

PROGRAMACION NEC EXEC 700/960

1. ENCENDER
2. PRESIONAR 157 * 09 # 408 FCN RCL 76
RCL # 01
RCL # 71

NOTA: HACER ESTE POCEDIMIENTO EN 15 SEGUNDOS DESPUES DE ENCENDER EL EQUIPO

PANTALLA	AVANZAR
Nam No	
Nam - 1	#
Phone No.	
52 99 47 xxxx	#
Lock code	#
xxxx	
Home Area	#
24592	
G.I: Mark	#
10	
First P-CH	#
0334	
SyS Select	#
0=b	
ACCOLC	#
0x	
Min Mark	#
1=yes	
Local Use	#
1=Yes	
EMG-No.	#
100	
FCN State	#
00	

3. PRESIONAR CLR Y SOSTENER HASTA QUE APAREZCA "TEST MODE".
4. PRESIONAR RCL # 02 PARA SALIR DE PROGRAMACION
5. PARA PONER EN "BANDA B" PRESIONAR FCN 54 Y CON LA TECLA DE RCL SELECCIONAMOS "B ONLY" Y PRESIONAMOS STO

NOTA : PREFIJO DEL NEC 700 ES 135
EL PREFIJO DEL NEC 960 ES 189

PROGRAMACION NOKIA 8260 digital

1. ENCENDER

2. PRESIONAR * 3001 # 12345 # y aparecerá

Field Test

NAM1 *Seleccionamos NAM 1 presionando Select, para avanzar NAM2
Con las flecha del teclado frontal hacia abajo. ✓*

NAM3

	<i>Presionar</i>	<i>dato</i>	<i>presionar</i>	<i>avanzar</i>
HOME SYSTEM ID	Select	24592	ok	✓
HOME SOC	Select	12		✓
OWN NUMBER	Select	52 99 47 xxxx	ok	✓
alpha tag				✓
PSID/RSID				✓
DEFAULT SETTINGS				✓

Para salir y almacenar la programación se apaga y se enciende nuevamente

PROGRAMACION RAPIDA

*Marcar * # 639#*

*celular No. ? 52 99 47 XXXX ok
code ? 24592 # 1234 # 2 ok
accepted*

PROGRAMACION NOKIA 8800 digital

1. ENCENDER

2. PRESIONAR * 3001 # 12345 # y aparecerá

Field Test

NAM1 *Seleccionamos NAM 1 presionando Select, para avanzar NAM2
Con las flecha del teclado frontal hacia abajo. ✓*

NAM3

	<i>Presionar</i>	<i>dato</i>	<i>presionar</i>	<i>avanzar</i>
HOME SYSTEM ID	Select	24592	ok	✓
HOME SOC	Select	12		✓
OWN NUMBER	Select	52 99 47 xxxx	ok	✓
alpha tag				✓
PSID/RSID				✓
DEFAULT SETTINGS				✓

Para salir y almacenar la programación se apaga y se enciende nuevamente

PROGRAMACION RAPIDA

*Marcar * # 639#*

*celular No. ? 52 99 47 XXXX ok
code ? 24592 # 1234 # 2 ok
accepted*

PROGRAMACION NOKIA C16 (corta)

- 1.- Encender el equipo*
- 2.- Meter 52 9624 xxxx (min) * 24592, SEND, SEND*
- 3.- Apagar equipo y listo*

PROGRAMACION NOKIA C16 (larga)

- 1.- Encender marcar # 000000 # # 953739 # MEM 99 MEM MEM ó*

*# 000000 ### 953739 # SEL * 49 SEL SEL*

2.- Apagar y encender nuevamente, aparecerá

WHICH NAM ?

*3.- Seleccionamos el Nam que se quiera programar del 1 al 4, y
avanzamos con la tecla de volumen hacia arriba*

Sidh 24592 vol. arriba o con SEL

Número tel. 52 99 47 xxxx "

Gim 10 "

4.- Aparecerá SAVE NAM, presionamos SEND , SEND :

5.- Para salir de programación presionamos END, END

6.- Apagamos y encendemos

*7.- Para ponerlo en sistema B, presionar SEL 11 seleccionamos con las teclas
del volumen hasta que aparezca banda b*

Aquí terminamos por este numero con la extensión al seminario de programación por Cheve, en el próximo numero aparecerán los modelos restantes.

Despedida

Ultimas Notas del Editor

Otro año ya se nos va, el próximo 15 de Enero nosotros en la MHM cumplimos nuestro segundo año como grupo completamente enfocado al phreaking y a la electrónica underground y queremos agradecer a todos los que nos han seguido desde el inicio y sobre todo a los que nos conocen desde antes de que decidiéramos dar el cambio radical que nos transformo en lo que somos.

Es muy estimulante saber que somos el primer grupo que se atrevió a experimentar con el phreaking en tiempos en que muy pocas personas en México lo hacían, y que hemos llegado a influenciar o, hasta cierto punto, animar a más y más gente a trabajar e investigar en esta área del underground que se encontraba un tanto olvidada.

La entrevista con el iniciador del phreaking, el icono mundial, Capt'n Crunch, por desgracia no pudo ser llevada a cabo a tiempo para aparecer en esta edición debido a la apatía de la comunidad. MegaHz, quien iba a realizar la entrevista, recibió muy pocos e-mails con sus preguntas para realizar dicha entrevista lo que ocasionó un retraso que condujo a no tenerla lista a tiempo para este ezine.

Esto no es en ninguna forma para resaltar la imagen de que los mexicanos somos huevones, porque no lo somos. Pero si en una invitación a todos los que les interese un tema a involucrarse en él como es debido. Estoy seguro de que muchos de ustedes pensaron que sus ideas no iban a ser tomadas en cuenta y eso evitó que mandaran sus correos con aportaciones.

Recuerden que la Mexican Hackers Mafia la hacemos todos, no podría existir sin las aportaciones, tanto en ideas, textos, comentarios, etc, de ustedes nuestros lectores. No tengan miedo a involucrarse; México va a subir, pero se necesita del apoyo de todos para lograrlo.

¡Viva México Cabrones!

--oSUKARu--

EOF