Do it yourself

Demon-Dialer

Construction, Operation & Reference Manual

Manual to version 1.10

Hack-Tic Technologies

+31 20 6001480
fax: +31 20 6900968

Appendum to
Do-it-yourself Demon-Dialer manual v1.10

- When taking the chips out of the static-protecting foam, make sure that you are grounded, and that no static can get at the contacts. When inserting the chip, hold the board in one hand and the chip in the other, this makes sure that board and chip are at the same potential.

- If you notice a 'startup-delay' on the amplifier when the battery is low, remove C9 from the board. This may increase the noise on the amplifier a little bit however.

- On page 4 of the manual the last capacitor in the printed list should read C10, not C9.

- The chip-sockets used in your kit may not have a notch as assumed on page 3 of the manual. Just make sure the notch on the chip matches the notch on the silk-screen and you will be fine.

- Your password may contain digits that are non-audible (^5 through ^0).

0. Building your Demon-Dialer

0.1 About this kit

Check the bag of parts to see that it contains:

- 1 printed circuit board (PCB)
- 1 bag containing 13 pushbutton switches
- 1 bag containing all the other parts, a complete list can be found in Appendix F
- a piece of anti-static foam holding 2 IC's, the MC68HC705C8P/DD (the heart of the Demon-Dialer) and the LM386N3, an amplifier chip. The foam also holds two IC-sockets for these chips.

The PCB consists of two separate parts. When you face the side that is printed on in white (the printing is called the 'silk-screen') and have the writing upright, the left part is the actual Demon-Dialer, and the right part is the keyboard. The keyboard connects to the Demon-Dialer through the supplied ribbon-cable. You can choose to keep these two parts together or you can cut them loose to make a more compact unit. If you want to cut the keyboard loose, it is best to do so before you put any parts on the board.

To cut the board first carve it a few times very carefully with a sharp knife along a steel ruler. Then carve the other side, until at least half the board is cut away. Make sure you cut even deeper between the mounting holes that are located at the corners of each part of the board. You can now break the board, although it is probably better to cut all the way through. A hack-saw might also be handy.

You're going to use a soldering iron to solder all the parts in. If you have never done so before it is probably a good idea to ask someone that has done it before to keep an eye on you. Do not use soldering irons any heavier than 30 Watts and make sure your soldering iron has a relatively fine tip. Use solder that has a rosin core and NEVER use plain solder and S-39.

0.2 The keyboard

The keyboard is easy to build. Just take the buttons, push them into the board on the side with the white printing on it and solder them on the other side. In order to keep all the buttons on the same height you may have to push fairly hard to secure them in place. To make it even flatter you can cut off the plastic nipples on the bottom of the keys. In this case make sure you hold the buttons in place while you are soldering to them.

Take the ribbon-cable and strip off about 5 mm from the ends of the insulation on all conductors on both ends of the cable. Take one end of the cable and stick it in the holes marked JP5 on the top-side of the board. Make sure the black wire

faces the '1' marked on the silk screen. Solder the wires on the bottom. For now, leave the other side dangling in the air. Your keyboard is done.

Let's move on to the actual Demon-Dialer. First take the 40 pin chip-socket and place it over the Hack-Tic logo on the top-side of the board. Make sure the notch lies over the notch next to the U1 designation. Solder the leads on the other side. Do the same with the small 8-pin chip-socket in position U2, again putting the notch in the socket over the notch on the silk-screen.

0.3 Resistors

All parts on the Demon-Dialer can be soldered in any order you choose. Our suggested way will work, but is not the only way. We suggest you now take one of the resistors (see list below) and put it into it's position on the board (on the top side). Make sure each lead of the resistor sticks through a different hole in the board and that the resistor lies flat on the board between the two holes. Now go to the bottom side and bend the leads sharply. Cut the leads with a pair of wire clippers close to the bend in the lead, but not so close that the resistor will fall out. Now solder the wires of the resistor and repeat this procedure until all resistors are done. Make sure that a component does not move until the solder is hard (takes only a few seconds at most).

You may wonder what a resistor lookes like, or how to find the right resistor, since the values are not printed on them. Resistors (in this kit) are small cilinders with 4 or 5 colored stripes that have leads coming out on both ends. They're also the most used parts in the Demon-Dialer. Resistors have color codes to identify them. A list of part numbers (as used on the Demon-Dialer silk-screen), resistor values (in Ohms) and the color-code on the resistor follows:

R1	10k	Brown-Black-Orange-Gold
R2	10k	Brown-Black-Orange-Gold
R3	10k	Brown-Black-Orange-Gold
R4	10k	Brown-Black-Orange-Gold
R5	100k/1%	Brown-Black-Black-Orange- -Brown
R6	100k/1%	Brown-Black-Black-Orange- -Brown
R7	100k/1%	Brown-Black-Black-Orange- -Brown
R8	100k/1%	Brown-Black-Black-Orange- -Brown
R9	100k/1%	Brown-Black-Black-Orange- -Brown
R10	200k/1%	Red-Black-Black-Orange- -Brown
R11	200k/1%	Red-Black-Black-Orange- -Brown
R12	200k/1%	Red-Black-Black-Orange- -Brown
R13	200k/1%	Red-Black-Black-Orange- -Brown
R14	200k/1%	Red-Black-Black-Orange- -Brown
R15	200k/1%	Red-Black-Black-Orange- -Brown
R16	200k/1%	Red-Black-Black-Orange- -Brown
R17	3.3k	Orange-Orange-Red-Gold
R18	200k/1%	Red-Black-Black-Orange- -Brown

R19	100k/1%	Brown-Black-Black-Orange- -Brown
R20	10M	Brown-Black-Blue-Gold
R21	12k	Brown-Red-Orange-Gold
R22	10k	Brown-Black-Orange-Gold
R23	10k	Brown-Black-Orange-Gold
R24	10k	Brown-Black-Orange-Gold
R25	10k	Brown-Black-Orange-Gold
R26	10k	Brown-Black-Orange-Gold
R27	10k	Brown-Black-Orange-Gold
R28	24.3k/1%	Red-Yellow-Orange-Red- -Brown
R29	20k/1%	Red-Black-Black-Red- -Brown
R30	1k	Brown-Black-Red-Gold
R31	24.3k/1%	Red-Yellow-Orange-Red- -Brown
R32	39k	Orange-White-Orange-Gold

0.4 Capacitors

There are five different types of capacitors on the board. The first type is a MKH or multi-layer capacitor. It's a silver-colored, rectangular little 'box' that has short wires sticking out along the short sides of the rectangle. They are as fragile as they look and they should be treated carefully. Do not bend the leads, but use a tool (or the table surface) to hold them in while you solder. It is not advisable to use you fingers for this since you will burn them, and you'll need them later on to push the buttons. After soldering you can clip off the excess wire. There are four MKH capacitors on the board. Here are their designations, values and what is written on them.

Silk	Value	Writing on capacitor
C5	10 nF/400 V	10n 400
C7	10 nF/400 V	10n 400
C8	100 nF/100 V	μ 1 100
C9	100 nF/100 V	μ 1 100

Next, there's the monolithic capacitor called C1 that has a value of 100 nF. It's the little blue thing with two wires that has '104M' followed by the Siemens logo written on it, followed by a second line that says 'Z5U63'. You can solder it in as if it was a resistor, bending the leads and clipping them before you solder.

The Styroflex capacitor is a relatively big round cylinder with wires coming out of both ends. It has 330 H written on it, and it's a 330 pF capacitor. Put it in the C6 position, preferably with the red stripe facing towards the X1 position, and solder it in.

It's time for the elco's (electrolytic capacitors). There are three of them:

Silk	Value	Writing on capacitor
C2	10 µF/35 V	10µF35V
C9	10 µF/35 V	10µF35V
C11	100 µF/6.3V	100µF6.3V

On one side of the elco is a minus sign pointing to the shortest lead. This lead should NOT be put in the hole marked "+" on the board. In other words: put them in right, or it will not work.

The fifth type is called a plate capacitor. There are two of them on the board. They are little grey things, that say 33p on them and their designations are C3 and C4.

0.5 The Diode

There is a small orange glass thing with a black stripe on it in your bag of parts. It is a diode, and it must be put in the right way around and should be soldered like a resistor. The black stripe on the diode must be on the side of the line within the D1 designation. It is (by the way) a 1N4148 diode, for those curious.

0.6 Transistors

There's five transistors in the Demon-Dialer. They are black with three wires coming out on one side. Here are their designations and types. The value is also written on each transistor.

Q1	BC557B
Q2	BC557B
Q3	BC557B
Q4	BC547B
Q5	BC547B

When you put them in, make sure that the round edge of the transistor lies over the 'round' side of the symbol printed on the silk-screen. The middle lead of the transistor should be bent a little bit to make the transistor fit the hole-pattern on the board. Just bend the leads on the back of the board, clip them off and solder.

0.7 The Crystal

The crystal is a fairly large metal object that has two wires coming out from one side. It is a 4.1943 MHz Crystal, and that is also written on it. The wires should be

bent because the crystal lies flat on the board in this design. The wires should be bent close to the crystal, but not touching the metal. Make sure it all fits (watch the elco behind it as you do it).

0.8 Connecting it all together

First take the ribbon-cable that connects to the keyboard and solder it into the holes marked JP4, again with the black wire at the '1' on the silk-screen. Put the chip marked MC68HC705C8P into the 40 pin socket with the notch facing towards C1. Put the small chip (marked LM386N3) into the 8-pin socket with the notch facing the big chip. Make sure all the pins on the chip really go into the socket. If you put the chips in the wrong way you may damage them as you apply power!

Now take a speaker of your own choice (we recommend you use one from a telephone earpiece) and connect it's wires through the two holes close to the crystal, marked 'SPKR'. Then connect 4 x 1.5 Volt batteries (or any other stable supply of 6 Volts DC) to the holes marked JP2. Make sure the polarity is right (it's marked on the silk-screen), because you WILL break the device if is not! There is no 'idiot-diode' in this device, which means that is not protected against putting the battery in the wrong way, but it also means your batteries last longer.

0.9 Testing

If you connect the batteries the device should produce an upgoing tone-sweep through the speaker. If you push buttons, it should produce DTMF-tones. If it does, your device probably works fine, and you can proceed to chapter 1.

0.10 You fucked up!

It's not working huh? Check your solder connections. If it looks as if a connection has not 'flowed' nicely around the wire or if the solder is not as shiny as on the other connections, solder that connection again. Make sure that you did not inadvertently connect two conductors on the print. Check the polarity on the elco's and the diode. Also check that the right parts are in the right places. Make sure the black wire in the ribbon cable is facing the '1' mark on the silk-screen on both sides. If the transistors and the chips are also in the right way, you have a problem! If you really can't fix it, try calling somebody you know that has done this kind of work before. If you applied power with the chips facing the wrong way or with the battery power reversed, the MC68HC705C8P/DD (the big chip) is almost certainly wasted.

Except for this chip, all parts to the Demon-Dialer can be obtained at your local electronics store.

1. The Basic Functions

1.1 Getting Started

Once the device is powered up by pressing the shift-key, a short upward tone sweep will emit from the system speaker. When changing batteries hold down the shift key when the power comes on to make sure the device starts up properly. If you power-up for the first time since changing batteries, all the settings will default to their standard values. This will also mean that in order to gain access to the system you will first have to type your system password. This password is supplied with the Demon-Dialer and should not (repeat NOT) be lost. The password that we supplied with your device is not archived at Hack-Tic Technologies or anywhere else, it's only in your device and on the piece of paper that came with it.

1.2 Getting In

As said, when the device starts up for the first time, you have to type a password. While you are typing this, the device will act like a normal Touch-Tone (tm) dialer. A word of warning here: Touch-Tones all sound similar, but a trained ear can identify all the digits. If you wish to keep your password a secret, it is advisable to cover the speaker with your hand while you type the password. If the wrong password is keyed in, the device will remain operative as a Touch-Tone (tm) dialer. To get access to it's more sophisticated functions, leave the device untouched for 30 seconds. The device will then auto-power off (6 seconds after a four beep alert-sound), at which point you can restart the device with the shift-key and start over.

Once the correct code is entered a victorious tune sounds, signalling you that it is now ready to emulate any in-band signalling system.

Ofcourse the security of this device depends fully on how secure the data is within the heart of it, the MC68HC705C8DD. The program in this chip (which also contains your password) is protected with a security-bit that tells the processor not to allow the outside world to read the contents of its PROM. We do not know of any methods to read the contents of a security-bit protected PROM short of probing on the surface of the chip itself, which is a hyper-expensive operation, even if you did get the bare silicon out of the package in one piece. In other words, it is IMPOSSIBLE for someone who does not know the code to prove that your device is anything but an ordinary DTMF-dialer.

If you decide not to deal with all this ultra-paranoid password nonsense, you can switch off the password protection using a special command sequence discussed later on.

1.3 Getting Used To It

Of all the in-band signalling systems, Touch-Tone (tm) (also known as DTMF to the more technically minded) is the most well-known. The Demon-Dialer includes many more systems, whose only similarity is that they use tones to get a message across. Modems all over the world use in-band signalling to send data. One might even find in-band systems used to signal information between phone-switches, or from mobile phones to their base-stations. Rumour has it that there exists countries that have payphones using in-band signalling to indicate coin deposits. An unlikely story, but you never know.

The Demon-Dialer starts up in Touch-Tone mode, but can be switched to a lot of other modes. Modes are numbered 0 through 19. Modes 0 through 9 are accessed by pressing shift and the * key together followed by the number of the mode. From now on we will refer to keys that are pressed with the shift down by printing a ^ in front of the key. Modes 10 through 19 are accessed by pressing ^* and then ^0 through ^9. Here is a list of modes currently implemented:

Mode 0	Touch-Tone (tm)
Mode 1	ATF1
Mode 2	R2-Forward
Mode 3	CCITT No. 3
Mode 4	CCITT No. 4
Mode 5	CCITT No. 5 / R1
Mode 6	RedBox
Mode 7	Special Line-signalling tones
Mode 12	R2-Backward

Mode 18 and 19 are RAM-modes, which means they can be user-defined. All the other modes are ROM-modes, which means they cannot be altered. See section 5 for more information about programming RAM-modes. To see the key-layout of all modes please refer to Appendix C.

At this point we would like to encourage you to play with the device a little bit and get used to its basic functions before we go on to the more sophisticated features.

2. Macro Mode

Now that you are familiar with the basic operation of the unit it is time for macros. A macro is nothing but a stored sequence of keypresses that can be played back. It means that you do not have to retype something that you may need to send multiple times. It also means that you can send sequences of tones at speeds otherwise impossible.

To work with macros you must first put the device in "macro mode". This is done by typing ^#. Two tones, the last one lower than the first tell you that you are now in macro mode. There are 10 different macros and they can be played by pressing 0 through 9 while in macro mode.

To record anything in the macros first press ^<M> (where <M> is the macro you wish to record). If the macro you are recording into is not empty the four-beep alert sequence will sound. Press # to confirm programming, or any other key to abort it. If it was empty you will get only two beeps and you can start programming right away. Now just press the keys that you want to put in the macro. The keys will produce one beep when you press them; they will not produce the sounds they would when pressed outside the macro mode. Don't worry, they'll sound just fine when the macro is played. If you wish to change modes inside the macro just do what you would normally do: press ^* followed by the mode you want.

It is even possible to nest macros. This means that inside one macro you can tell the device to play the contens of another macro. The nested macros are called by name which means that if macro B is nested inside macro A and the contents of macro B are changed, the change will also affect the nested B that is played as part of macro A. To nest a macro press ^# followed by the macro you wish to nest while recording a macro.

Of the special functions (see section 4), only ^* *4 and ^* * 5 (guard tone on and guard tone off) can be put in a macro.

To end macro recording press ^# followed by #. To go back to normal operation just press #. Two tones, the last one higher than the first will sound to indicate that you have left the macro mode.

3. The Frequency Table

Inside your Demon-Dialer is a frequency table. This table contains twelve RAM-based frequencies that you can change and 82 ROM-based (fixed) frequencies. Apart from the tone made during frequency stepping and sweeping, these are the only tones the device will ever produce. Some of the RAM-based frequencies have been used in modes 3 and 7 and have a default value that is loaded in them every time you change the batteries or reset the device. The table is listed in full in Appendix A.

4. Special Functions

A number of special functions is built into the device. They are all accessed by pressing `^* *` followed by the number of the function.

4.0 Function 0, Device Init

This function will initialize the device, wiping all macro definitions, RAM modes 18 and 19, all time-templates and RAM frequencies. It will also turn the password protection back on (if it was off). In other words: EVERYTING YOU EVER PUT INTO THE DEVICE IS GONE. When you press `^* * 0` an alert will sound. If you press `#` the Demon-Dialer will initialize, if you press anything else it will not.

4.1 Function 1, Frequency Programming

The Demon-Dialer has 12 locations in its memory where the user can define frequencies. These can then be used in user-defined keys or as guard tones. Type

`^* * 1 <frequency number> # <frequency> #`

The frequency number ranges from 0 to 11, the frequency has to be entered in Hertz. The system will acknowledge programming by playing a short sample of the frequency just programmed.

These user-defined frequencies as well as the ROM-based frequencies can be used when programming your own keys into modes 18 and 19, they can also be used as guard tones. The C3 mode uses two RAM frequencies (0 and 1) as its mark and space frequency respectively so that you can use it to emulate any Single Frequency system.

4.2 Function 2, Time Template Programming

The user of the Demon-Dialer can define up to 8 periods in milliseconds and then use these periods in User-Defined modes as durations for tones. Most of the time templates are also used in the ROM-modes of the device. The fact that a certain time-template has been used in a ROM-mode does not mean you cannot use it in one of your own modes. Time templates are programmed in a manner similar to the user-defined frequencies above. Typing

`^* * 2 <time-template number> <time in milliseconds> #`

will program a time template. Note that the time-template number itself is not followed by a pound because it is always one digit long (0-7). Here is a list of time-templates, what the system uses them for, and what their default values are:

```
0 - DTMF and C3 mark      (50 ms default)
1 - DTMF and C3 space     (50 ms default)
2 - C5/R2 mark            (50 ms default)
3 - C5/R2 space           (50 ms default)
4 - C5 kp time            (100 ms default)
5 - free
6 - C3 interdigit time    (500 ms default)
7 - free
```

4.3 Function 3, Guard tone programming

Guard tones are tones that are played simultanously with the real signalling. They are used to jam any filters on the line so that they act as if the signal you are sending is speech. The Demon-Dialer has three guard tones that it can store in memory. To program any of these three guard tones press

`^* * 3 <Guard tone number> <Frequency number> #`

The Guard tone number is 0, 1 or 2 and the frequency number is one of the ROM or RAM based frequencies. See section 3 and Appendix A for more info.

4.4 Function 4, Start guard tone

Pressing `^* * 4 <guard tone number>` will turn on that guard tone. It will then continously sound until it is turned off or another guard tone is started.

4.5 Function 5, Stop guard tone

If a guard tone is on, `^* * 5` will stop it. This command and the previous one are the only special functions that can be used inside macros.

4.6 Function 6, Frequency stepping

Pressing ^* * 6 <start frequency> # <step size> # will sound the start frequency. If you then press * the tone will step up with the step size specified, pressing 0 will step down. If you press # the tone will end. Frequencies have to be typed in Hertz.

4.7 Function 7, Continous sweep

This will sound a tone sweep through the full voice-range (0 - 4 kHz) and back in +/- 15 seconds and then start over. Pressing # ends the sweep.

4.8 Function 8, Password protection on

4.9 Function 9, Password protection off

If password protection is turned off, the device will not sound the down-going sweep when it times out, it will not sound the up-going sweep if it is turned on and the time-out period is shortened to 10 seconds. If the password protection is turned off, the device will come back alive at the same point in the software where it powered down. If you were programming a macro during power-down, you can finish it when you power up again by pressing shift.

4.10 Function *, Number scan

This function can be used to scan through numbers in a sequential way. Type ^* * * <play macro> <number macro> <step size> # to start the number scan. The device will then play the play macro and wait for the user to press either * or 0 to increment or decrement the <number macro> with the step size and then play the <play macro>. Pressing # will end the scan.

To use this you can either use the same macro to play and increment or decrement if you only wish to play the number itself. You can also use a different macro for playing and nest the number macro somewhere in it. The number macro has to have digits at the end, so that the Demon-Dialer knows what to increment or decrement. The contents of the number macro are changed by scanning.

4.11 Power off

If you press ^* ^* the system will power down after producing the short down-going sweep. The system also has an automatic power-down so that you can never leave it on and drain the batteries.

5. RAM-mode key programming

Modes 18 and 19 are user-programmable modes. This means that you can program a pause, a single tone or a double tone and even a whole sequence of tones to sound when a key is pressed. In each mode keys 0/9 and ^0/^9 as well as * and # (a total of 22 keys) can be programmed. To program a key first switch to mode 18 or 19 by pressing ^*^8 or ^*^9. Then type ^*#<key> where <key> is the key to be programmed. An alert tone will sound if the key is allready programmed. Press # to confirm reprogramming, or any other key to cancel.

You can now enter the data on the first silence or tone that you wish to attach to that key. Use the following format:

<# of tones> <timing type> <time> #[<tone 1 dB level>#<tone 1 freq #>#[<tone 2 dB level>#<tone 2 freq #>#]]

<# of tones> 0, 1 or 2 for silence, a single or a double tone. If you just type a # at this point, you tell the dialer that you are done programming this key. If you type # at the first tone, it means that you 'empty' the key.

<timing type> Four different timing types can be entered (0 through 3).

0 play fixed time, in this case <time> is entered in milliseconds

1 play while pressed when not used in macro mode, fixed time in macros. Again, <time> is entered in milliseconds.

2 play template time, in this case <time> is a time-template number (0-7).

3 play while pressed when not used in macro, template time in macros, <time> is a time-template number (0-7).

The <dB level> is entered as a value between 0 and 15, giving dB levels ranging from 0 to -15 dB of full volume. Presently only 4 dB levels are implemented, 0, -6, -10 and -15 dB. If you enter a different number, the machine will still store it, but rounds down the value to the nearest implemented value. Future versions of the Demon-Dialer may contain more possible dB levels.

The <freq #> is a number from the table as described in Appendix A.

If, after typing the <timing type>, an error-tone sounds the memory of the device is full. The sequence you are then programming is ended and key programming is finished. If you need more RAM you could consider emptying non-used keys in mode 18 or 19.

5.1 About timing and frequencies in the Demon-Dialer

The Demon-Dialer uses a crystal for its timing and frequency generation. The tolerance of the used crystal is guaranteed to be better than 0.01 %. This tolerance affects both timing and frequency accuracy.

For the Demon-Dialer, a millisecond programmed into the device is not really 1/1000 of a second. In fact it is 1/1024 of a second. So if you want 50 ms, you should not type 50, but 51. The tone will then last 49.8 ms, which is within 0.4 % of the range. For most if not all of your applications none of this will make any difference.

Frequencies programmed into the frequency table, including RAM-based frequencies and frequencies used in stepping are to the Hertz exact, ofcourse within the tolerance of the crystal.

5.2 dB levels and distortion, a little bit of theory

As said, the Demon-Dialer supports a number of different volumes. Inside your device are sinewave tables, 1 per volume. The phase in these tables is the same, only the amplitude differs per table. If you want to make a loud double tone, you may want to use 0 dB for both tones. This will however result in terrible distortion because you end up driving the D/A converter over its maximum level. More technically put: the combined level of the two tones should not exceed 0 dB. This means that for a double tone the maximum levels at which there is no distortion are -6 dB.

6. A few programming examples .....

If the contents of this manual have utterly confused you, here are a few examples that may help in understanding all the functions. These examples were constructed to make use of as much of the functions in the Demon-Dialer as possible.

6.1 Example 1, Using a guard tone while playing macros

In this example we will program a guarded clear forward in a macro. This means the clear-forward is played together with the guard-tone.

Type ^* * 3 0 2 #. This means that we have programmed guard-tone 0 to frequency number 2 from the frequency table. This is a RAM frequency which defaults to 0 Hz. We have to set it to something if we want to have a guard tone.

So now we press ^* * 1 2 # 3125 #. The system will then play a quick sample of that tone as a confirmation. Frequency 2 from the table is now programmed to 3125 Hz.

Now go to the macro mode (^#). Type ^0 to start programming macro 0. If something was in macro 0, the device will sound four beeps to warn you. Pressing # will erase macro 0 and overwrite it with what you are about to type. If on pressing ^0 only two beeps sounded you start typing right away (do not press #, for it will end up in the macro).

Press ^* * 4 0 to start the guard tone. This tone will not sound now, but only once the macro is played. Now press ^* 5 to go to the C5 mode, and then * to sound a clear forward. Then type ^* * 5 to end the guard tone. Finish off by typing ^# followed by # to end macro recording.

Now press 0 to hear your guarded clear-forward.

6.2 Example 2, Using templates to make an SF system

Suppose we want to use a 2280 Hz pulse system that uses 100 ms mark and space timing and 1000 ms interdigit delay.

Type ^* * 2 0 100 # to set time template 0 (mode 3 mark timing) to 100 ms. Also type ^* * 2 1 100 # to set the space timing to 100 ms as well. Then do ^* * 2 6 1000 # to set the interdigit time to 1000 ms.

Now press ^* * 1 0 52 #. If you look in the frequency table section, you will see that frequency number 52 represents 2280 Hz. Typing ^* * 1 1 74 # sets the space frequency to 0 Hz (silence).

Switch to mode 3 by pressing ^* 3 and use!

6.3 Example 3, Programming a RAM-mode

We will program key 0 in mode 18 to be the following sequence:

- A dual tone consisting of 1400 and 1700 Hz during 250 milliseconds
- a silence lasting 200 milliseconds
- and finally a single tone of 900 Hz lasting 400 millisenconds.

First go to mode 18 by typing `^* ^8`. Then press: `^* # 0` to start programming key 0. If an alert (4 beeps) sounds press # to confirm reprogramming. Then press:

`2 0 250 # 6 # 68 # 6 # 17 # 0 0 200 # 1 0 400 # 0 # 13 # #`.

The spaces are in there for easy-reading. The first part means: program 2 tones of timing type 0 (fixed time) that last 250 milliseconds, the first one at -6 dB, frequency number 68 (1400 Hz) and the second one also -6dB, frequency number 17 (1700 Hz). The other two sequences are similar and fairly easy to understand. If you are done press 0 hear the key that you have programmed.

6.4 Example 4, Macro nesting and number scanning

In this example we will scan numbers in C5 with the format `KP1 XXX ST`. To do this we make two macros. One is called the 'play macro', it holds the KP1, a reference to the part that has to be scanned (the number macro) and then an ST.

After typing `^#` to get to macro mode press `^0` top record macro 0. If you hear four beeps confirm reprogramming by pressing `#`.

Press `^* 5 ^3 ^# 1 ^5 ^# #`

Step by step, this means: switch to mode 5, play a KP1 (`^3`), nest macro 1 (`^# 1`), play an ST and stop recording.

Then program macro 1 to contain '000' as follows: `^1 [#] 000 ^# #` and leave macro mode (#)

Now type `^* * * 0 1 1 #` to scan using macro 0 as play macro, 1 as number macro and a step size of 1. The system will respond by playing the first sequence (KP1 000 ST). If you now press 0 you will get KP1 001 ST. If you then press * it will scan back to KP1 000 ST. If you press star again it will play KP1 999 ST, which (to this device) is before 000.

7. Demon-Dialer and outside world

You may have noticed the pin called AUX on the PCB of your Demon-Dialer and the 3 pins called JP1. The AUX pin is used to control an external hookswitch relay, JP1 is a serial port to connect your Demon-Dialer with a computer.

Note: Pin 1 is the pin closest to key 1 on the keyboard of the device.

7.1 Hookswitch Control

You can use the hookswitch control bit (AUX) to control an external relay to 'pick up the phone' and you can also pulse-dial through it. To toggle the hookswitch-control bit press ^* ^#.

As you have seen in the part about the frequency table, programming a frequency of 1 Hz means that the device puts the external hookswitch control bit in a high position (+5 V), a frequency of 2 Hz means putting it in a low position (0 V). All other frequencies will just sound and not affect the hookswitch bit. If frequency numbers 0 and 1 are at their default values (1 and 2 Hz) then you can pulse dial in mode 3. Time-templates 0 and 1 are used for mark and space timing respectively (default 50 ms). Time-template 6 is used for the interdigit time (default 500 ms). Please note that the device has only a 4 position keyboard-buffer so you can easily out-type it when pulse-dialling.

7.2 External Audio

The audio signal that comes out of the device is 2.0 Volt peak to peak. If you want to do any serious phreaking, you probably want to hook this device up to a phone-line directly. In appendix D is an example circuit for doing so.

7.3 Serial Interface

The serial interface consists of three pins, Ground (pin 1), RxD (receive data) (pin 2) and TxD (transmit data) (pin 3). Signals are sent asynchronously at a speed of 16384 bps. Format is 1 start bit, 8 data-bits, no parity, 1 stop-bit. The port is at TTL-level. Most computers will talk to it as it is. If your computers requires the real RS-232 levels, appendix D contains a circuit to convert voltages.

To use the serial interface single byte commands are sent to the Demon-Dialer. Keys 0-9 are sent as ASCII values 0 through 9 (not the characters, but the values). * is sent as 10, # as 11. To send shifted keys add 16 to the key code. These keys are then interpreted as if the user presses the key on the keyboard and holds it down. To release a key send code 255. All functions are accessible from the serial port,

except for turning the device on, this has to be done with the shift key on the device itself.

Apart from these functions, three extra functions have been incorporated. There is an upload function that lets you read the contents of all the relevant RAM in the device to the computer. Directly after issuing the upload command, ASCII character 'U', the Demon-Dialer sends a stream of bytes. The format of this data-packet is described in appendix B.

The download is used to put information in the Demon-Dialer's memory. The data-format is exactly the same as what the Demon-Dialer uses for the upload function. After sending the download command, ASCII value 'D', you send the packet of data as described in Appendix B. The Demon-Dialer does not do any error-checking on the incoming data. You can program impossible key or macro combinations which might cause the device to hang. To un-hang the device, remove the batteries and power up with the shift key pressed.

If you send an ASCII 'P' to the device, it will respond with a sequence containing:

- one byte Demon-Dialer Software version * 100
- one byte telling how many digits the password consists of
- several bytes containing the key codes for the password

Upload, Download and Password functions will only work once the password was entered correctly. Once the Demon-Dialer is powered up you can also enter the password using the serial interface.

Appendix A, The Frequency Table

RAM-based frequencies

```
0  - C3 (Mode 3) Mark Frequency. Defaults to 2 Hz, meaning off-hook
1  - C3 (Mode 3) Space Frequency. Defaults to 1 Hz, meaning on-hook
2  - Special Menu (Mode 7) frequency number 1. Defaults to 0 Hz
3  - Special Menu (Mode 7) frequency number 2. Defaults to 0 Hz
4  -      -
5  -      |
6  -      |
7  -      |-Free, no default value
8  -      |
9  -      |
10 -      |
11 -      -
```

ROM-Based Frequencies

```
12 - 700 Hz     -
13 - 900 Hz     |
14 - 1100 Hz    |- MF
15 - 1300 Hz    |
16 - 1500 Hz    |
17 - 1700 Hz    -
18 - 697 Hz     -
19 - 770 Hz     |
20 - 852 Hz     |
21 - 941 Hz     |
22 - 1209 Hz    |- DTMF
23 - 1336 Hz    |
24 - 1477 Hz    |
25 - 1633 Hz    -
26 - 1380 Hz    -
27 - 1500 Hz    |
28 - 1620 Hz    |
29 - 1740 Hz    |- R2 Forward
30 - 1860 Hz    |
31 - 1980 Hz    -
32 - 1140 Hz    -
33 - 1020 Hz    |
34 - 900 Hz     |
35 - 780 Hz     |- R2 Backward
36 - 660 Hz     |
37 - 540 Hz     -
38 - 1500 Hz    -
39 - 1700 Hz    |- Red
40 - 2200 Hz    -
41 - 1950 Hz    -
42 - 2070 Hz    }- ATT1
43 - 600 Hz     -
44 - 750 Hz     |
45 - 1200 Hz    |
46 - 1600 Hz    |
47 - 1625 Hz    |
48 - 1700 Hz    |
49 - 1900 Hz    |
50 - 2040 Hz    |
51 - 2100 Hz    |- Pilot
52 - 2280 Hz    |
53 - 2400 Hz    |
54 - 2500 Hz    |
55 - 2600 Hz    |
```

```
56 - 3000 Hz    |
57 - 3350 Hz    |
58 - 3825 Hz    -
59 - 147 Hz     -
60 - 350 Hz     |
61 - 400 Hz     |
62 - 440 Hz     |
63 - 450 Hz     |- Call Progress
64 - 480 Hz     |
65 - 500 Hz     |
66 - 620 Hz     -
67 - 950 Hz     -
68 - 1400 Hz    |- BIT
69 - 1800 Hz    -
70 - 1400 Hz    -
71 - 1850 Hz    |
72 - 2450 Hz    |- Call Progress
73 - 2600 Hz    -
74 -    0 Hz    -
75 - 2000 Hz    |- Special
76 - 2700 Hz    -
77 - 150 Hz     - Call Progress
78 - 550 Hz     - Modem tone
79 - 853 Hz     - EBS
80 - 960 Hz     - EBS
81 - 1070 Hz    - Modem tone
82 - 1270 Hz    - Modem tone
83 - 2025 Hz    - Modem tone
84 - 2225 Hz    - Modem tone
85 - 2713 Hz    - Loopback
86 - 2750 Hz    - Guard
87 - 2800 Hz    - Guard
88 - 2850 Hz    - Guard
89 - 2900 Hz    - Guard
90 - 2950 Hz    - Guard
91 - 3050 Hz    - Guard
92 - 3100 Hz    - Guard
93 - 3150 Hz    - Guard
94 - 3200 Hz    - Guard
95 - 3250 Hz    - Guard
96 - 3300 Hz    - Guard
97 - 3400 Hz    - Guard
98 - 3450 Hz    - Guard
99 - 3500 Hz    - Guard
```

Frequency Table in ascending order

0 Hz	-	74	1625 Hz	-	47
147 Hz	-	59	1633 Hz	-	25
150 Hz	-	77	1700 Hz	-	17,39,48
350 Hz	-	60	1740 Hz	-	29
400 Hz	-	61	1800 Hz	-	69
440 Hz	-	62	1850 Hz	-	71
450 Hz	-	63	1860 Hz	-	30
480 Hz	-	64	1900 Hz	-	49
500 Hz	-	65	1950 Hz	-	41
540 Hz	-	37	1980 Hz	-	31
550 Hz	-	78	2000 Hz	-	75
600 Hz	-	43	2025 Hz	-	83
620 Hz	-	66	2040 Hz	-	50
660 Hz	-	36	2070 Hz	-	42
697 Hz	-	18	2100 Hz	-	51
700 Hz	-	12	2200 Hz	-	40
750 Hz	-	44	2225 Hz	-	84
770 Hz	-	19	2280 Hz	-	52
780 Hz	-	35	2400 Hz	-	53
852 Hz	-	20	2450 Hz	-	72
853 Hz	-	79	2500 Hz	-	54
900 Hz	-	13,34	2600 Hz	-	55,73
941 Hz	-	21	2700 Hz	-	76
950 Hz	-	67	2750 Hz	-	86
960 Hz	-	80	2713 Hz	-	85
1020 Hz	-	33	2800 Hz	-	87
1070 Hz	-	81	2850 Hz	-	88
1100 Hz	-	14	2900 Hz	-	89
1140 Hz	-	32	2950 Hz	-	90
1200 Hz	-	45	3000 Hz	-	56
1209 Hz	-	22	3050 Hz	-	91
1270 Hz	-	82	3100 Hz	-	92
1300 Hz	-	15	3150 Hz	-	93
1336 Hz	-	23	3200 Hz	-	94
1380 Hz	-	26	3250 Hz	-	95
1400 Hz	-	68,70	3300 Hz	-	96
1477 Hz	-	24	3350 Hz	-	57
1500 Hz	-	16,27,38	3400 Hz	-	97
1600 Hz	-	46	3450 Hz	-	98
1620 Hz	-	28	3500 Hz	-	99

Appendix B, Serial Upload and Download data format

byte(s)	meaning
0	current mode
1	# of macro keys
2	offset in programmable key area to mode
19	
3	# of bytes in programmable key area
4-6	guard tones 0,1 and 2
7-22	time-templates
23-122	key area (always 100 bytes sent)
123-194	macro area
195-208	RAM frequencies

current mode	7	6	5	4	3	2	1	0
	p	i	o	m	m	m	m	m

p - set when password is entered correctly
i - key is played in macro mode when set
o - password protection off when set
mmmmm - current mode (0-19, 20-31 unused)

The guard tones are stored as freq #'s. Bit 7 of guard 0 set means a guard tone is played (not necessarely guard tone 0).

The time-templates are 2-byte values MSB first. The value is stored in ms. (1/1024 seconds actually)

The programmable keys are stored one after each other first 0-9 then * and # and finally ^0-^9. The keyarea format for each tone is :

7	6	5	4	3	2	1	0
l	n	n	t	t	h	h	h

l - when set indicates last tone of key, else indicates more tones are following
nn - # of tones (0,1,2)
tt - 0 means play fixed time hhh=high 3 bits
1 means play while pressed if not in

```
  macro, else fixed time
2 means play template time hhh=index
3 means play while pressed if not in
  macro, else template time hhh=index
```

If fixed time then next byte is lower 8 bits of time in 1/1024 secs If more than one tone then next bytes :

```
7 6 5 4 3 2 1 0
a a a a b b b b

aaaa - dB level tone a
bbbb - dB level tone b
```

Then for each tone a one byte freq #
This sequence is repeated until all tones of one key are done.
The RAM-frequencies are 2-byte values MSB first. The values are stored as 8*freq in Hz. So 1000 Hz is stored as 8000.
The macro area is a 72 byte area. It can hold up to 96 macro entries, which are stored as 6-bit values. The first 6 bit-value is stored in the 6 LSB of byte 0, the second 6-bit value is stored in the 2 MSB of byte 0 and the 4 LSB of byte 1, etc.

The macro entries have the following format :

```
0skkkk  key code skkkk where s = shift and kkkk 4-bit
key
   (kkkk = 0-11 for non-shifted and 0-9 for shifted
keys)

001100          : start guard tone 0
001101          : start guard tone 1
001110          : start guard tone 2
001111          : stop guard tone

1mmmmmm         : if 0 <= mmmmmm <= 19 sets mode mmmmm
                  if 20 <= mmmmm <= 29 nests macro mmmmm-
20

111111          : end of macro
```

Appendix C, The Demon-Dialer mode by mode

Mode 0, DTMF (default)

The tones in the right hand column are commonly reffered to as A, B, C and D. In military networks they are Flash Override, Flash, Immediate and Priority. The keys are played while pressed, in macros the mark is time-template 0, the space is time-template 1. These timings are also used in C3 / Pulse Dial.

	1209	1336	1477	1633
697	1	2	3	^1
770	4	5	6	^2
852	7	8	9	^3
941	*	0	#	^4

Mode 1, ATF1 (B-Netz)

This standard uses a 100 baud FSK modulated signal, using 1950 Hz as '1' and 2070 Hz as '0'. The start is preceeded by a 600 millisecond preamble of 2070 Hz. The Keys are defined as follows:

```
* (start)        01110 01000100010
# (stop)         01110 10000100001
^# (cancel)      01110 10101010101
0                01110 11000 0 00011
1                01110 10100 0 00101
2                01110 10010 0 01001
3                01110 10001 0 10001
4                01110 01100 0 00110
5                01110 01010 0 01010
6                01110 01001 0 10010
7                01110 00110 0 01100
8                01110 00101 0 10100
9                01110 00011 0 11000
```

Mode 2, R2-Forward

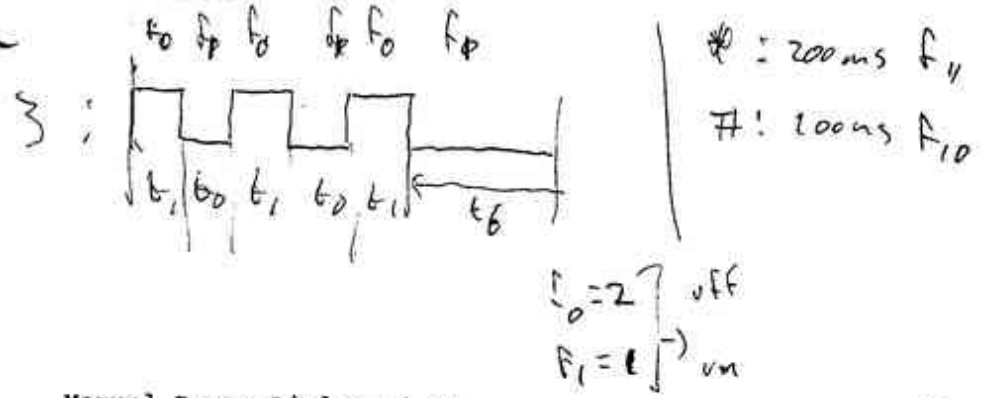
Key is played while pressed, in macro mode, each key is played for the duration of time template 2, and then a pause of time template 3 follows. Both time templates are also used as the mark and space timing of C5. They both default to 50 ms.

1	1380	1500
2	1380	1620
3	1500	1620
4	1380	1740
5	1500	1740
6	1620	1740
7	1380	1860
8	1500	1860
9	1620	1860
0	1740	1860
^1	1380	1980
^2	1500	1980
^3	1620	1980
^4	1740	1980
^5	1860	1980

Mode 3, C3 / Pulse dial

This mode is very flexible: signal is pulsed, mark and space timing of pulses are stored in time templates 0 and 1. They both default to 50 ms. This timing is also used for the DTMF mark and space.

The mark tone is stored in RAM-frequency 0 and the space is RAM-frequency 1. The space defaults to 2 Hz, which has a special meaning, it means the external relay is off-hook. The mark defaults to 1 Hz, which means on-hook. The interdigit delay is set in time template 6, it defaults to 500 ms. See the section 7.1 for more information.



Mode 4, C4

All digit signals have 35 ms pauses between the tones, interdigit delay is 100 ms.

```
x  = 2040, 35 ms
y  = 2400, 35 ms
X  = 2040, 100 ms
Y  = 2400, 100 ms
XX = 2040, 350 ms
YY = 2400, 350 ms
P  = 2040 + 2400, 150 ms
Clear Forward     PXX      *
Transit Seizure   PX       ^7
Forward Transfer  PYY      ^9
Terminal Seize    PY       #
1                 yyyx
2                 yyxy
3                 yyxx
4                 yxyy
5                 yxyx
6                 yxxy
7                 yxxx
8                 xyyy
9                 xyyx
0                 xyxy
11                xyxx
12                xxyy
13                xxyx
14                xxxy
15                xxxx
16                yyyy
```

Mode 5, C5

Digits are played while pressed, in macros they last for the duration of time template 2, followed by a pause of time template 3. In C5 ^1 is called 'Code 11', ^2 is called 'Code 12', ^3 is 'KP1', ^4 is 'KP2' and ^5 is 'ST'. ^6 lasts 500 ms, ^7 is 120 ms, ^8 is 120 ms, ^9 is 240 ms and ^0 is a silence of 50 ms.

1	700	900	^1	700	1700	
2	700	1100	^2	900	1700	
3	900	1100	^3	1100	1700	
4	700	1300	^4	1300	1700	
5	900	1300	^5	1500	1700	
6	1100	1300	^6	2600		
7	700	1500	^7	2400	2600	
8	900	1500	^8	2400		
9	1100	1500	^9	2400		
0	1300	1500	^0	0		

Mode 6, Redbox

These tones are used for payphone coin signalling in North America. There are three types of tones for different systems and three types of cadences for the coins.

Tones:

```
ACTS      = 1700    2200
IPTS      = 1500    2200
non ACTS  = 2200
```

Cadences:

```
$0.05 = 60 ms on
$0.10 = 60 ms on, 60 ms off, 60 ms on
$0.25 = 5 x (35 ms on, 35 ms off)
```

Key Layout:

	$0.05	$0.10	$0.25
ACTS	1	2	3
IPTS	4	5	6
non ACTS	7	8	9

Mode 7, special line signalling menu

This mode contains several line signalling tones from various systems, the * and # keys are user programmable. All frequencies are played while pressed, In Macro mode they will sound for 50 ms (not shifted) and 10 ms (shifted). In macro mode * is always 50 ms and # is always 10 ms.

```
1  = 2400 + 2600 Hz
2  = 2400 Hz
3  = 2600 Hz
4  = 2040 + 2400 Hz
5  = 2280 Hz
6  = 3000 Hz
7  = 1700 Hz
8  = 1900 Hz
9  = 2500 Hz
0  = silent
*  = RAM freq. #2 + #3  (50 ms)
#  = RAM freq. #2 + #3  (10 ms)
```

Mode 12 (^2), R2-Backward

Key is played while pressed, in macro mode, each key is played for the duration of time template 2, and then a pause of time template 3 follows. Both time templates are also used as the mark and space timing of C5. They both default to 50 ms.

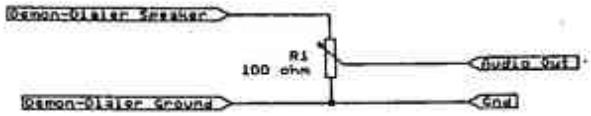
1	1140	1020	9	900	660
2	1140	900	0	780	660
3	1020	900	^1	1140	540
4	1140	780	^2	1020	540
5	1020	780	^3	900	540
6	900	780	^4	780	540
7	1140	660	^5	660	540
8	1020	660			

Mode 18 and 19 (^8 and ^9)

These modes are user programmable. The data is stored in 100 bytes in the format listed in Appendix B. See section 5 of this manual.

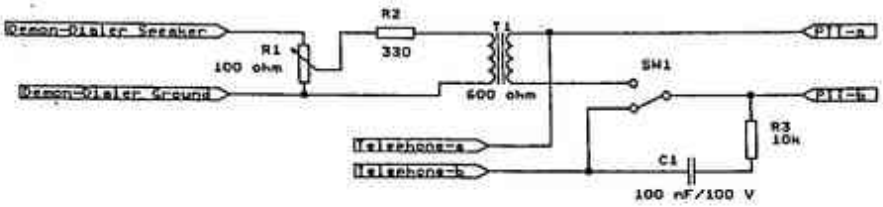
Appendix D, Sample schematics

Volume control

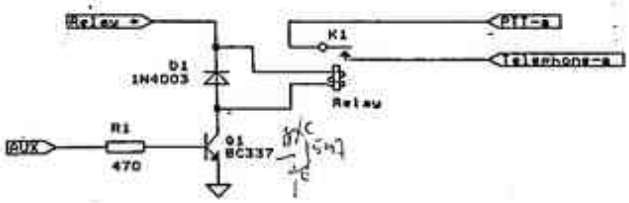


Audio to phone

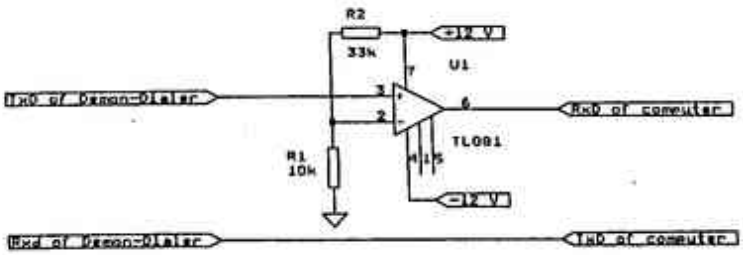
The switch is used as a mute for the phone while the demon dialer is making signalling tones, it can be omitted.



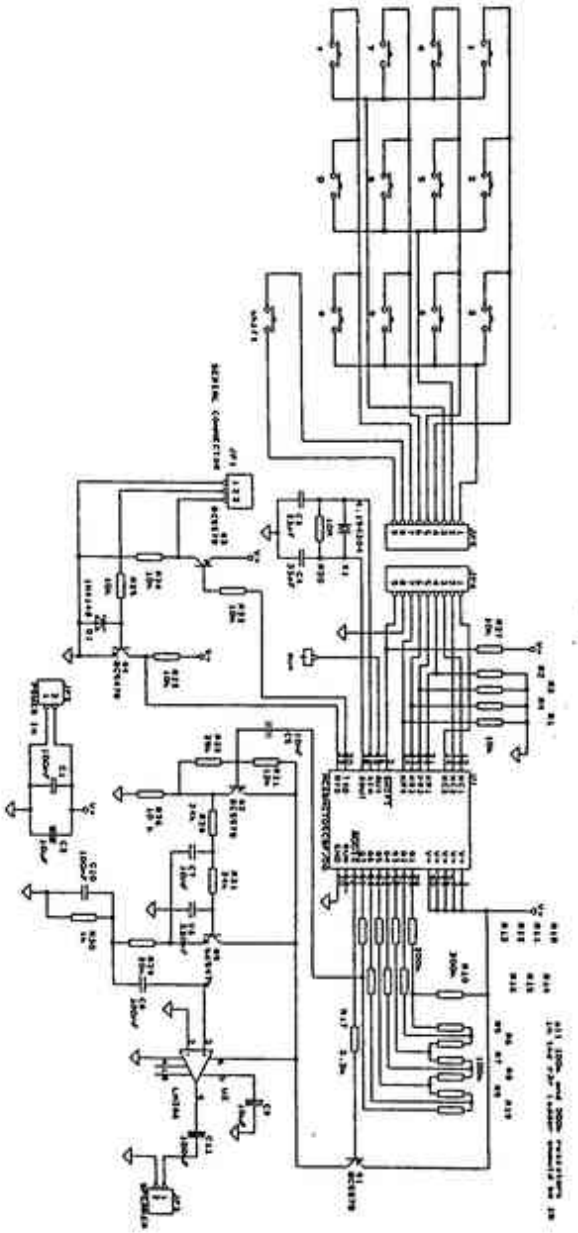
Hookswitch control



Converting to RS-232 levels



Appendix E, Demon-Dialer schematic

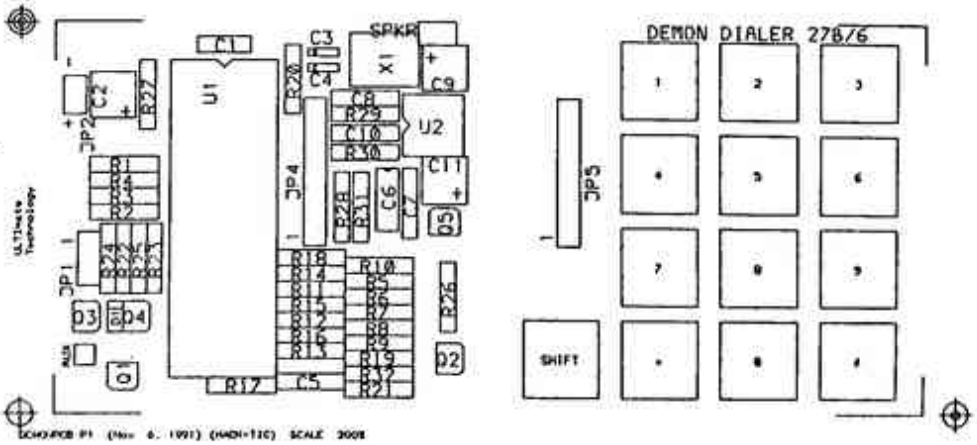


Appendix F, Demon-Dialer board

Parts List

1	1	C1	100nF/mono
2	2	C8, C10	100nF/multi
3	2	C2, C9	10uF/eloo
4	2	C3, C4	33pF/plate
5	2	C5, C7	10nF/multi
6	1	C6	330pF/poly
7	1	C11	100uF/eloo
8	1	D1	1N4148
9	3	Q1, Q2, Q3	BC557B
10	2	Q4, Q5	BC547B
11	10	R1, R2, R3, R4, R22, R23, R24, R25, R26, R27	10k
12	6	R5, R6, R7, R8, R9, R19	100k/1%
13	8	R10, R11, R12, R13, R14, R15, R16, R18	200k/1%
14	1	R17	3k3
15	1	R20	10M
16	1	R21	12k
17	2	R28, R31	24k
18	1	R29	20k
19	1	R30	1k0
20	1	R32	39k
21	13	SW1, SW2, SW3, SW4, SW5, SW6, SW7, SW8, SW9, SW10, SW11, SW12, SW13	B3F-4000('mousekey')
22	1	U1	MC68HC705C8P/DD
23	1	U2	LM386N3
24	1	X1	4.194304MHz crystal
25	1	PC board	27B/6

Silk Screen



Index