Downloaded from www.artofhacking.com

TAP

MAR-APRIL 1979 No. 56

THE PROGRAMABLE BLUE BOX

BY

PETER PIPER

The Phone Phreak like everyone else must keep pace with technology. We therefore give you The Programable Blue Box.

The Box presented here offers excellent stability with both voltage and temperature. It uses 9 IC's, all of which are readily available. And uses two ordinary 9 volt alkaline batteries. Current drain is relatively low - 24 ma. in standby, about 30 ma. sending tones.

Circuit Description

When a key is pressed, the diode matrix in fig. 1 produces a binary code on lines A through D corresponding to the key pressed. Note the code 0000 is not used here, it is reserved for 2600. Whenever a key is pressed the S line also goes high, indicating a valid code on lines A thru D.

In fig. 2, lines A thru D and S go into the 2519 - a hex 40 bit shift register. Only 5 out of the 6 shift registers are used. The input of the 6th should be grounded. The S line also goes to a debouncing circuit and schmitt trigger composed of the two inverters and associated parts. The NAND gate takes either the signal from the schmitt trigger or the system clock and generates the clock signal for the shift register. This is a negative going pulse of about 20 us. So each time a key is pressed, the data at the input to the SR is shifted in. An LED lights whenever a key is pressed to indicate this.

When all numbers are entered, and it is desired to send tones, the SEND key is pressed. This key triggers a flip-flop formed by two NOR gates, and does 4 things. It inhibits the input circuitry from the keyboard so no more numbers can be entered. It brings the recirculate line of the SR high so the data is not lost once it is sent. It enables the output circuitry by way of the ED line; And it enables the system clock to shift out the data.

When data is shifted out of the SR it appears on output lines A thru D. In fig. 3 these go into 2 groups of analog switches. Each group contains 16 switches. A binary code at the input of these switches connects the corresponding output to the Z input of the 4051's. Hex F of the code 0011 is present at the input, output line 3 is connected to Z. This places the correct resistor for the desired tone in the circuit. Line D is used for generating the 2600 tone. Each shift of the SR thus places data at the input of the analog switches and selects the proper resistors for the 2 oscillator circuits. The outputs of the oscillators are summed through the two 3.3K resistors and sent to the telephone earpiece. The tones are gated on and off by the ED line. When all the tones are sent, the S line goes from high to low and resets the send and clear flip - flops.

The basic operation of the box has just been described. There are a few additional features that should be mentioned however.

The CLEAR key triggers its own flip - flop (formed by the other 2 NOR gates.) and does the same things as the SEND key with two exceptions. The recirculate line of the SR is held low, thus clearing memory and the two oscillators are not enabled so no tones are produced.

The DEL key is used to delicit between sequences of numbers. When pressed, it clocks the SR without placing any data on its input lines. This feeds the circuitry into believing that all the times have been sent.

The 2600 tone is generated by pressing the SEIZE key. This is the only key that does not use the common bus. When pressed, it enables the oscillators, and sends to the only data at the input to the analog switches is 0000 when NO tones are not being sent, the top oscillator generates 2600.

Construction

The easiest means of construction is wire wrap. With a little care the box can be built quite compactly. All IC's except the SR use only the 5 pins for supply. The 7 uses plus and minus 9. Both the Vss and the Vee of the 4051's should be grounded. Vdd is plus 9. The input to the one unused shift register should be grounded. DON'T BE ANTHUSIASTIC IN ITS OUTPUT. The trimpots should be 1C or 2C turn cermet type construction. All resistors should be carbon film 5% carbon composition. Section 4 offers better temperature stability at the same price. The 2600 pf. capacitors associated with the oscillators must be polystyrene. The end with the band should be the grounded end. The LED may see like a power wasting frill to some, but it is needed. As a place to tell you if your data has been accepted or when memory is clear.

MAR-APRIL 1979 No. 56

The wiring for the trimpots is not shown to avoid a mess. The leads are in two groups - bottom group 300,1FC,11CC, 10CC,17KO - top group 9CC,11CC,12CC,17KO,26CC. Wiring is easy though. Just wire the output line for a particular key to the corresponding pot. Ex. digit 4 is 7CC and 11CC. So output line 4 of the top group goes to 11CC and output line 4 of the bottom group goes to 7CC. Like C is for 2CC, wire up all used outputs this way. Also, don't try to skimp by using single turn pots or one term trimmers. The ease of tuning and insensitivity to vibration is well worth the 2C turn trimpots and the extra resistors.

The hardest part to locate is probably the SR. It is available from Jaws Electronics,1021 Howard St.,San Carlos, Ca. 94070, for $4 at this writing. All other parts are available from several sources - shop around.

Calibration and Use

There are a few methods that can be used to calibrate this box. A DIP switch can be added to the output of the SR to pull these lines up to plus 9 volts. If this is used just set the switch to the code for the desired key. Ex. 0101 for key 5. And press the SEIZE key to enable the oscillators. You can also wire up a 1C in plus that can be used to replace the SR. Connect the input pins to their respective outputs and substitute this plug for the SR. When a key is pressed on the keyboard and the SEIZE key is held, the desired tone will be heard.

To use the Box, first clear memory by pressing the CLEAR key. (the prototype seemed to always have a clear memory when power was first applied, but I'm not sure this will be the case with all units.) Enter your desired numbers by pressing the respective keys. The LED should light each time a key is pressed to signify acceptance of that entry.

Next, call your favorite 800 number and press the SEIZE key for about a second. When you hear the Ker-chunk press CEND. Cut once a very little tone!

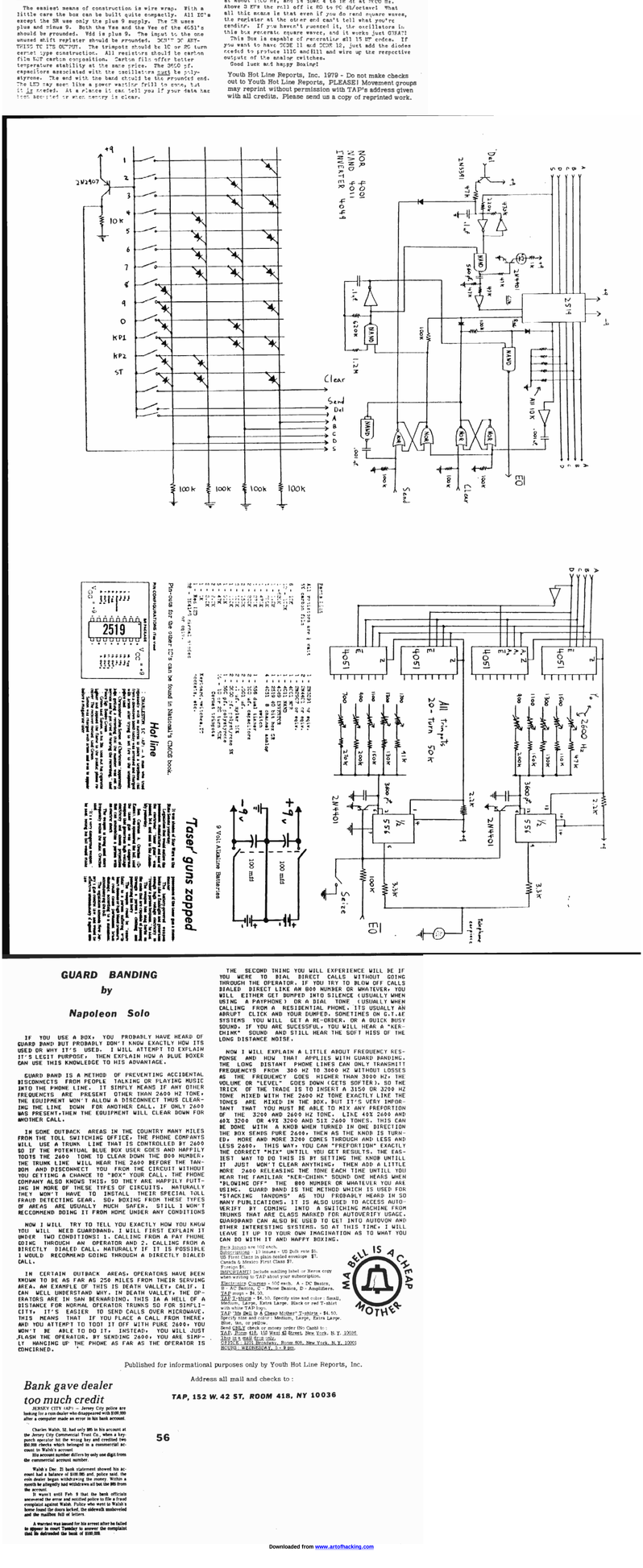
The DEL key is used when it is necessary to separate sequences of numbers, such as for overseas calls. Ex. To call 044 1 246 8CCG, enter 8C C11 C44 1C then press the DEL key and enter 8P C44 1 24G 6CCC CC. Then you press the SEND key, the first sequence will be sent like you too will talk. Press the SEND key again and the second sequence will be sent.

I'd like to say a word at this like about square waves and the Blue Box. For some reason some people seem to think you can't use them. A square wave is made up of a fundamental frequency and the odd harmonics. So a 600 Hz square wave is really made up of a 600 Hz fundamental with harmonics of 1800,4800,6CCC,8KO and so on. The entire telephone network has only a bandwidth of about 3 KHz, however. A typical telephone channel starts to roll off at about 1100 Hz, and is down 4 to 10 DB at 2400 Hz. Above 3 KHz the roll off is 80 to 90 db/octave! What all this means is that even if you do send square waves, the receiver at the other end can't tell what you're sending. If you haven't guessed it, the oscillators in this box generate square waves, and it works just GREAT!

This Box is capable of generating all 15 12F codes. If you want to have CODE 11 and CODE 12, just add the diodes needed to produce 11IC and 11I and wire up the respective outputs of the analog switches.

Good luck and Happy Boxing!

Youth Hot Line Reports, Inc. 1979 - Do not make checks out to Youth Hot Line Reports, PLEASE! Movement groups may reprint without permission with TAP's address given with all credits. Please send us a copy of reprinted work.



IF YOU USE A BOX, YOU PROBABLY HAVE HEARD OF GUARD BAND BUT PROBABLY DON'T KNOW EXACTLY HOW ITS USED OR WHY IT'S USED. I WILL ATTEMPT TO EXPLAIN IT'S LEGIT PURPOSE, THEN EXPLAIN HOW A BLUE BOXER CAN USE THIS KNOWLEDGE TO HIS ADVANTAGE.

GUARD BAND IS A METHOD OF PREVENTING ACCIDENTAL DISCONNECTS FROM FALSE CLEARING OR PLAYING MUSIC INTO THE PHONE LINE. IT SIMPLY MEANS IF ANY OTHER FREQUENCIES ARE PRESENT OTHER THAN 2600 HZ TONE, THE EQUIPMENT WON'T ALLOW A DISCONNECT THUS CLEARING THE LINE DOWN FOR ANOTHER CALL. IF ONLY 2600 WAS PRESENT, THEN THE EQUIPMENT WILL CLEAR DOWN FOR ANOTHER CALL.

IN SOME OUTBACK AREAS IN THE COUNTRY MANY MILES FROM THE ELL SWITCHING OFFICE, THE PHONE COMPANYS WILL USE A TRUNK LINE THAT IS CONTROLLED BY 2600 SO IF THE POTENTIAL BLUE BOX USER GOES AND HAPPILY TOOTS THE 2600 TONE TO CLEAR DOWN THE 800 NUMBER, THE TRUNK LINE WILL HEAR HIS 2600 BEFORE THE TANDOM AND DISCONNECT YOU FROM THE CIRCUIT WITHOUT YOU GETTING A CHANCE TO PLACE YOUR CALL. THE PHONE COMPANY ALSO KNOWS THIS, SO THEY ARE HAPPILY PUTTING IN MORE OF THESE TYPES OF CIRCUITS. NATURALY THEY WON'T HAVE TO INSTALL THEIR SPECIAL TOLL FRAUD DETECTING GEAR, SO, BOXING FROM THESE TYPES OF AREAS ARE USUALLY MUCH SAFER. STILL I WON'T RECOMMEND DOING IT FROM HOME UNDER ANY CONDITIONS

NOW I WILL TRY TO TELL YOU EXACTLY HOW YOU KNOW YOU WILL BE GUARDBANDED. I WILL FIRST EXPLAIN IT UNDER TWO CONDITIONS: 1. CALLING FROM A PAY PHONE GOING THROUGH AN OPERATOR AND 2. CALLING FROM A DIRECTLY DIALED CALL. NATURALLY IF IT IS POSSIBLE I WOULD RECOMMEND GOING THROUGH A DIRECTLY DIALED CALL.

IN CERTAIN OUTBACK AREAS, OPERATORS HAVE BEEN KNOWN TO BE AS FAR AS 250 MILES FROM THEIR SERVING AREA. AN EXAMPLE OF THIS IS DEATH VALLEY, CALIF. I CAN WELL UNDERSTAND WHY. IN DEATH VALLEY, THE OPERATORS ARE IN SAN BERNARDINO. THIS IS A HELL OF A DISTANCE FOR NORMAL OPERATOR TRUNKS SO FOR SIMPLICITY, IT'S EASIER TO SEND CALLS OVER MICROWAVE. THIS MEANS THAT IF YOU PLACE A CALL FROM THERE, AND YOU ATTEMPT TO TOOT IT OFF WITH PURE 2600, YOU WON'T BE ABLE TO DO IT, INSTEAD, YOU WILL JUST FLASH THE OPERATOR. BY SENDING 2600, YOU ARE SIMPLY HANGING UP THE PHONE AS FAR AS THE OPERATOR IS CONCERNED.

THE SECOND THING YOU WILL EXPERIENCE WILL BE IF YOU WERE TO DIAL DIRECT CALLS WITHOUT GOING THROUGH THE OPERATOR. IF YOU TRY TO BLOW OFF CALLS DIALED DIRECT LIKE AN 800 NUMBER OR WHATEVER, YOU WILL EITHER GET DUMPED INTO SILENCE (USUALLY WHEN USING A PAYPHONE) OR A DIAL TONE (USUALLY WHEN CALLING FROM A RESIDENTIAL PHONE. ITS USUALLY AN ABRUPT CLICK AND YOUR DUMPED. SOMETIMES ON C.T.&E SYSTEMS YOU WILL GET A RE-ORDER, OR A QUICK BUSY SOUND. IF YOU ARE SUCESSFUL, YOU WILL HEAR A "KER-CHUNK" SOUND AND STILL HEAR THE SOFT HISS OF THE LONG DISTANCE NOISE.

NOW I WILL EXPLAIN A LITTLE ABOUT FREQUENCY RESPONSE AND HOW THAT APPLIES WITH GUARD BANDING. THE LONG DISTANT PHONE LINES CAN ONLY TRANSMIT FREQUENCYS FROM 300 HZ TO 3000 HZ WITHOUT LOSSES AS THE FREQUENCY GOES HIGHER THAN 3000 HZ, THE VOLUME OR "LEVEL" GOES DOWN (GETS SOFTER). SO THE TRICK OF THE TRADE IS TO INSERT A 3150 OR 3200 HZ TONE MIXED WITH THE 2600 HZ TONE EXACTLY LIKE THE TONES ARE MIXED IN THE BOX. BUT IT'S VERY IMPORTANT THAT YOU MUST BE ABLE TO MIX ANY FREQUENCY OF THE 3200 AND 2600 HZ TONE. LIKE 40% 2600 AND 60% 3200 OR 49% 3200 AND 51% 2600 TONES. THIS CAN BE DONE WITH A KNOB WHEN TURNED IN ONE DIRECTION THE BOX SENDS PURE 2600, THEN AS THE KNOB IS TURNED MORE AND MORE 3200 COMES THROUGH AND LESS AND LESS 2600. THIS WAY, YOU CAN "PREFORTION" EXACTLY THE CORRECT "MIX" UNTILL YOU GET RESULTS. THE BEST WAY TO DO THIS IS BY SETTING THE KNOB UNTILL IT JUST WON'T CLEAR ANYTHING. THEN ADD A LITTLE MORE 2600 RELEASING THE TONE EACH TIME UNTILL YOU HEAR THE FAMILIAR "KER-CHUNK" SOUND ONE HEARS WHEN "BLOWING OFF" THE 800 NUMBER OR WHATEVER YOU ARE USING. GUARD BAND IS THE METHOD WHICH IS USED FOR "STACKING TANDOMS" AS YOU FREQUENTLY HEAR IN SO MANY PUBLICATIONS. IT IS ALSO USED TO ACCESS AUTOVERIFY BY COMING INTO A SWITCHING MACHINE FROM TRUNKS THAT ARE CLASS MARKED FOR AUTOVERIFY USAGE. GUARDBAND CAN ALSO BE USED TO GET INTO AUTOVON AND OTHER INTERESTING SYSTEMS. SO AT THIS TIME, I WILL LEAVE IT UP TO YOUR OWN IMAGINATION AS TO WHAT YOU CAN DO WITH IT AND HAPPY BOXING.

Back issues are 1CC each.
Subscriptions - 12 issues - US Bulk rate $5.
US First Class in plain sealed envelope $7.
Canada & Mexico First Class $7.
Foreign $8.
Back issues MUST include mailing label or Xerox copy from envelope to TAP about your subscription.

Electronics Courses - 10C each. A - DC Basics, B - AC Basics, C - Phone Basics, D - Amplifiers.
TAP mugs - $4.50.
TAP T-shirts - $4.50. Specify size and color. Small, Medium, Large, Extra Large. Black or red T-shirt with white TAP logo.
TAP "Ma Bell Is A Cheap Mother" T-shirts - $4.50. Specify size and color - Medium, Large, Extra Large. Blue, tan, or yellow.
Make checks or money order (No Cash) to:
TAP, Room 418, 152 West 42 Street, New York, N.Y. 10036
Allow 4-6 week first class.
OFFICE: 1001 Broadway, Room 800, New York, N.Y. 10001
HOURS: WEDNESDAY, 5 - 9 pm.

Published for informational purposes only by Youth Hot Line Reports, Inc.

Address all mail and checks to :

TAP, 152 W. 42 ST, ROOM 418, NY 10036

Bank gave dealer too much credit

JERSEY CITY (AP) — Jersey City police are looking for a rum dealer who disappeared with $100,000 after a computer made an error in his bank account.

Charles Walsh, 52, had only $85 in his account at the Jersey City Commercial Trust Co., when a keypunch operator hit the wrong key and credited two $50,000 checks which belonged to a customer to Walsh's account.

His account number differs by only one digit from the commercial account number.

Walsh's Dec. 31 bank statement showed his account had a balance of $100,085 and police said the ends dealer began withdrawing the money. Within a month he allegedly had withdrawn all but the $85 from the account.

It wasn't until Feb. 9 that the bank officials uncovered the error and notified police to file a fraud complaint against Walsh. Police who went to Walsh's home found the doors locked, the sidewalk unswept and the mailbox full of letters.

A warrant was issued for his arrest after he failed to appear in court Tuesday to answer the complaint that he misbranded the bank of $100,000.

Downloaded from www.artofhacking.com