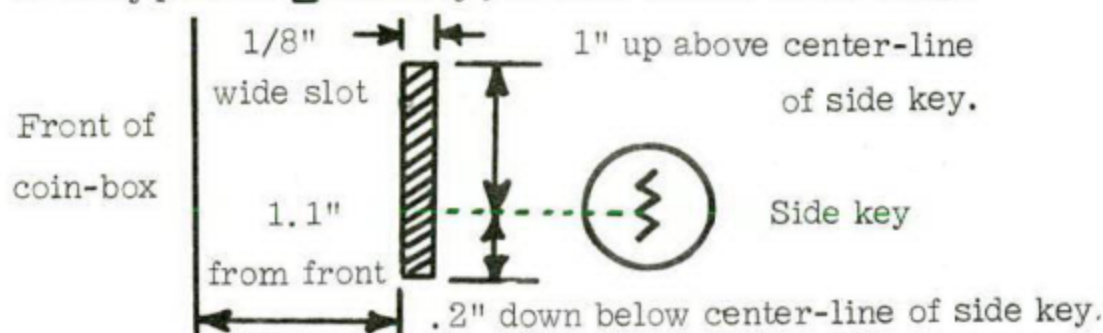


MORE FORTRESS FUN!

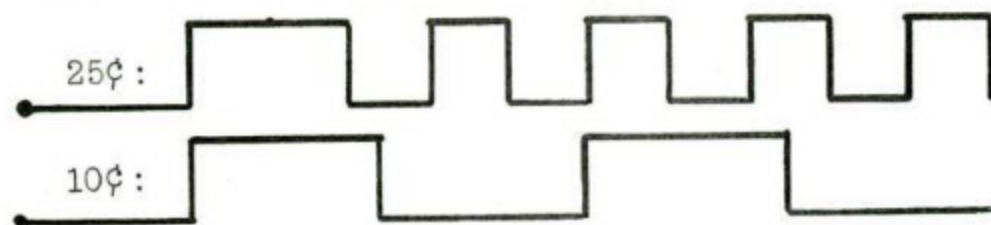
Last week, I met with "CJ" and "The Professor" and told them how much I would like a Fortress Fone of my very own to play with. About 1/2 hour after they left, they returned with one and gave it to me to open. "The Professor" was able to pick the upper lock after removing the shroud around it. It's only 4 levers. I immediately went to work on it while "CJ" bashed open the coin box. After he opened it, we made the following discoveries:

1. The drill pattern you published in #30 for the front plate would make it almost impossible to get the box open, because the bolts go thru double sets of slots before going into the outer shell of the phone. When the rotary plate is drilled as in #30, it should rotate and retract the bolts.
2. The right-hand bolt is really wide and protects the side lock (interlock).
3. The following cutting pattern would be better than a drilling pattern providing you have access to the side:



The cut should be 1.2" long, 1/8" wide, and 1" deep. It can be done with a special grindstone drill bit, and will shear off the interlock mechanism as well as cut the spiral front plate free so it can turn. We are checking reports of a puller for the cover. If there is such an animal, and if it does work, you'll hear about it first in TAP!

4. The tones' intervals are not generated by the coins pushing levers on the red box mechanism (like everyone thinks) but by a little relay which reverses the direction of the wheel that the levers cock. In other words, when a coin is dropped, the coin pushes a lever which cocks a wheel. The coin then drops into the drop chute, and the red box goes thru a 70ms delay to allow the coin to clear the mechanism. After that, a unijunction-timer circuit pulls in a relay which unwinds the wheel until it is back where it started. The number of times the relay ticks, pulling the wheel, is the number of beeps. If the wheel went 5 notches forward, a switch drops, telling the unit to do 35ms beeps (for a quarter). However, the first bleep will always be the same as the above-mentioned 70ms pre-bleep delay, because the coin will just be clear, and all of the pulses (beeps) are actually symmetrical square waves:



I will restate the specs on these tones because they are very important and must be known by all TAP readers. The 25¢ tones are 70ms on, 35ms off, 35ms on, 35ms off, 35ms on, 35ms off, 35ms on, 35ms off, 35ms on, 35ms off. The dime is 80ms on, 80ms off, 80ms on, 80ms off, 80ms on, 80ms off, 80ms on, 80ms off, 80ms on, 80ms off. These can be fudged to 70ms if needed, and better be generated digitally, because they'll fuck up with analog timers, "windows", and analog delays.

Then I made a few discoveries myself:

1. Coin Drop Mechanism - In my last letter, I asked about the "coin-sense relay" but couldn't figure how Bell knew about the money. Now I know! First, they use a low current (20ma) high voltage (50v) relay to release the money. Second, the relay resets a vane which senses the presence of the money. This vane cannot be checked by the operator. However, she can see the current drain caused by the drop relay pulling in. If the vane hasn't been hit by money, the coin-drop relay won't pull in even when the operator tries to make it. The good part is that she can't check the vane until she drops the money. So it doesn't matter when you drop your nickel, as long as you drop one before each time she collects. Also, she can't check it on



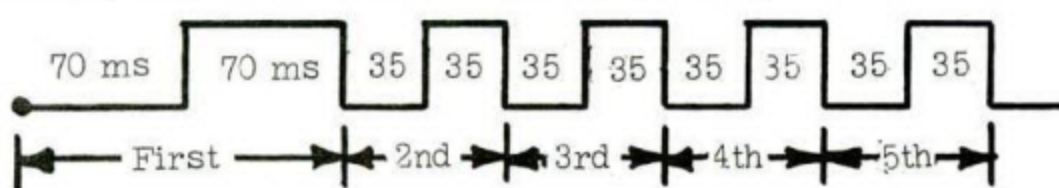
MAR-APRIL 1978

NO. 49

the initial three minutes because that drops automatically, and so you can talk for at least three minutes for free.

2. The pay phone red box tones drift with the outside temperature. So...before boxing away, make sure the pay-phone frequencies match your red box frequencies or you'll get screwed when you drop your 5¢.

3. As I told you last time, the 25¢ set of tones are 5 beeps, the first one twice as long as the rest:



All of the above info is confirmed by an in-depth experiment which can be done on any phone without taking it out of the booth!

1. Drop 5¢ into a pay phone. Listen to the side and hang up. The relay will pull the wheel back once and click.

2. Drop two nickels into the phone, one at a time. Listen to the receiver or the side of the phone. When the second nickel is dropped, two clicks of the relay are heard - as if a dime had been dropped.

3. Now for some fun: Drop a nickel, and then a dime. There are three clicks! Amazing, a 15¢ piece!

4. Now try dropping two dimes right together and you'll hear both dimes hit the bottom of the coin holding chute before you hear four clicks! a 20¢ piece!

5. Try a nickel and a quarter and get six clicks (30¢).

6. If you're fast enough, this will work too: Drop a nickel. Then two dimes together and you'll hear the familiar quarter sequence and not five nickel beeps.

Whether you are listening to the beeps thru the receiver or clicks on the side of the phone, you'll find these experiments interesting.

If you don't believe me about the timing of the tones on the 25¢ beeps, try tape recording them (have a friend call you from a pay phone and drop money) at 7 1/2 ips on a reel-to-reel recorder. Slow down the tape on playback to as slow as possible and mark the tape at the beginning and end of each bleep. When done marking, measure the marks and you can determine the tone durations. You will find most phones adjusted perfectly, whether single tone or mf phones, so the first bleep is twice as long as the rest.

If you should ever have access to a phone in a relatively private place, and wish to record the tones interference-free, get a phone pickup coil from someplace like Radio Shack (bletch!) and place it 3" behind the top keyhole on the right side of the Fortress Fone. It picks up the tones fine there.

Computer Wizard

Some Fortresses must have a mechanism defect. It seems that they will take two dimes or two nickels - a 50% savings! Please advise readers to deposit two nickels first and listen for second dial tone. This is for a 20¢ local call area.

Mugs

© Youth Hot Line Reports, Inc. 1978 - 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. WARNING: We will prosecute copyright violators.

THE PRINCIPLES OF TWX PHREAKING

by
Cheshire

INTRODUCTION

IN 1971, THE WESTERN UNION TELEGRAPH CO BOUGHT THE TELETYPEWRITER EXCHANGE (TWX) NETWORK FROM THE AMERICAN TELEPHONE & TELEGRAPH CO. UNDER THIS AGREEMENT, AT&T COULD NOT ENTER DATA COMMUNICATIONS UNDER 300 BAUD (30 CHARACTERS PER SECOND) UNTILL APRIL 1966. MEANWHILE, WHY WOULD ANY OF THE INDEPENDENT TELCOS BUILD WHOLE NEW EXCHANGES FOR THIS PA BELL PLAYTOY? THEY WOULDN'T, OF COURSE. THEY TRANSLATE FROM FUNNY TWX AREA CODES TO NORMAL TELEPHONE EXCHANGES. FIND THE RIGHT EXCHANGE, AND WIN THE TWX NETWORK.

TRANSLATING TWX EXCHANGES

THERE IS AN EASY WAY OF TRANSLATING A TWX EXCHANGE. THAT'S WHEN IT IS "GIVEN" TO YOU IN THE TWX DIRECTORY. TWX AREA CODES ARE USUALLY 510, 710, 810, & 910 IN THE UNITED STATES, AND 610 IN CANADA. SOME TWX MACHINES HAVE REGULAR TELEPHONE NUMBERS, BECAUSE THEY WERE INSTALLATIONS BEFORE THE MODEL 33 TELETYPE BECAME THE STANDARD OF OF THE TWX NETWORK. THESE OLDER MACHINES HANDLE THEIR OWN LIMITED SPEED CONVERSION, AND COMMUNICATIONS IS POSSIBLE BETWEEN THESE OLD MACHINES, ANDND THE NEWER MODELS.

ANYONE WITH A MODEL 33 (OR EQUIVILENT COMPUTER TERMINAL SUCH AS A COMPUTER DEVICES 1103, TI SILENT 700, OR TERMIFLEX HT-2) CAN SEND TO A TWX TERMINAL. A TWX MACHINE ANSWERS WITH THE SAME "CARRIER" TONE AS A COMPUTER DOES, SO YOUR TERMINAL WILL LIGHT ITS CARRIER LIGHT (IF IT HAS ONE). EACH MODEL 33 HAS A PROGRAMMED "ANSWERBACK" WHEEL IN IT. IT IS PROGRAMMED WITH AN IDENTIFIER OF 20 CHARACTERS OR LESS. THE FIRST THREE CHARACTERS ARE USUALLY CARRAGE RETURN (CR), LINE FEED (LF), RUB OUT (RO). THE LAST THREE ARE USUALLY, CR, LF, CONTROL Q. THE CONTROL Q CHARECTOR WILL TURN ON THE PAPER TAPE READER OF THE DISTANT TERMINAL (IF IT IS PROGRAMMED TO DO SO, WHICH MOST ARE). THIS LEAVES 14 CHARACTERS LEFT FOR IDENTIFICATION. AN EXAMPLE WOULD BE: NHLWINGSR DET. THIS IS THE ANSWERBACK OF THE DETROIT WINGS OF THE NATIONAL HOCKEY LEAGUE, AND WOULD FURTHER

SEEM TO BE THEIR PR DEPARTMENT.

THE TWX NUMBER OF THE WINGS IS 810-221-5033. AS WE LOOK DOWN THE LISTINGS FOR DETROIT IN A 1974 OR EARLIER TWX DIRECTORY (LATER ONES LUMP A WHOLE STATE TOGETHER) WE FIND LISTINGS FOR OLDER INSTALLATIONS. THE EXCHANGES FOR THESE OLDER MACHINES ARE 313-538, 313-222, 313-342, AND 313-755. WHEN WE HIT 222-5033, WE FIND THE ANSWERING TONE OF A TWX MACHINE. OTHER TWX MACHINES IN DETROIT ARE 810-221-5127 (DETROIT PD DET), 810-221-9458 (UNIROYAL DET), AND 810-221-5121 (MED EXAM DET).

DET IS, OF COURSE, THE CITY CODE OF DETROIT. OTHER CITY CODES ARE NYK FOR NEW YORK, LSA FOR LOS ANGELES, SFO FOR SAN FRANSISCO, AND CGO FOR CHICAGO. SMALL COMMUNITIES HAVE FOUR LETTER CITY CODES. I DON'T KNOW THE TWX TRANSLATIONS FOR ALL THE ABOVE CITIES, BUT THOSE SENDING TWX TRANSLATIONS TO TAP WILL GET A LIST OF THE FEW CITIES TRANSLATIONS ARE AVAILABLE FOR. I HAVE TRANSLATED CITIES WITH TRUCK STOPS, AND SENT MYSELF MESSAGES WHEN TRAVELING.

ANOTHER POSSIBILITY IS TO MAKE FRIENDS WITH SOMEONE WHO WORKS IN A SMALL OFFICE (OR A BRANCH OFFICE OF A LARGER COMPANY) AND USE THEIR TWX MACHINE. THE TRICK THEN IS TO CALL A TWX NUMBER THAT DOES NOT EXSIST AND LET THE PHONE COMPANY COMPUTER TELL YOU WHAT NUMBER IT THINKS YOU DIALED. THIS WORKS FOR VERY FEW CITIES.

EXAMPLE: THE WESTERN UNION TELEGRAPH CO IN UPPER SADDLE RIVER NJ IS 710-988-2251. IF WE DIAL 910-988-2253 ON A TWX MACHINE, WE'LL HEAR A RECORDING SAY "THE NUMBER YOU HAVE DIALED, 279-2253..." WHICH TELLS US THAT BY DJALING 201-279-2251 WE CAN REACH WU SALES UPSR. IF WE THEN LOOK CLOSELY AT THE NUMBER GIVEN FOR THE FYI NEWS SERVICE OFFERED TO TWX SUBSCRIBERS, THE NUMBER GIVEN IS 910-988-5956. BY DJALING 201-279-5956 AND THROWING THE HAND-SET INTO THE ACCOUSTIC COUPLER, OUR TERMINAL TYPES OUT "WU FYI MAWA" THE ANSWERBACK OF IBM SYSTEM 7 COMPUTER LOCATED IN MAHWAH NJ. THIS MACHINE IS UPDATED ONCE AN HOUR BY UPI OVER DEDICATED BACKED UP LEASED LINES. AS THE COMPUTER SENDS ITS ANSWERBACK, IT TRANSMITTS CONTROL E. CONTROL E SHOULD TRIP THE ANSWERBACK OF THE CALLING TWX MACHINE. SINCE THE COMPUTER WILL GO NO

FURTHER UNTILL IT RECIEVES SOMTHING, TYPE IN ANY RANDOM CHARACTERS ("XXXX") AND IT WILL LET YOU IN. TYPE CATALOG OR JUST "CATA" AS IT ONLY "SEES" THE FIRST FOUR CHARACTERS AFTER A SPACE. YOU CAN TYPE "NEWS WEAT SPOR (CR)" AND IT WILL GIVE YOU THE LATEST NEWS, WEATHER FOR 20 CITIES, AND SPORTS. THE CATALOG GIVES INSTRUCTIONS AND TELLS YOU WHAT INFORMATION IS AVAILABLE. THIS IS A "DIAL-A-JOKE" TYPE SERVICE, PAID FOR BY THE LINE CHARGES OF THE LONG DISTANCE CALL IN REACHING IT.

IT SHOULD BE NOTED THAT YOUR TERMINAL SHOULD BE SET FOR 110 BAUD, AND EVEN OR NO PARITY. HAVE FUN, HAPPY HACKING, AND REMEMBER,

TWX R4 PHREAKS

ATTN: MILO FONEBILL

Please get in touch with me through the TAP office.

Tom Edison

COMING NEXT ISSUE !!!

Our next issue, #50, marks the 7th anniversary of TAP. To mark the occasion, issue #50 will be a special double edition with color pages. I want this to be the best fuckin issue of TAP that we've ever put out! I'm asking all of our readers, especially those who have sat on their fat asses and done nothing to help out over the past years, to send in information, newsclips, articles, and columns. I want 8 pages just bursting with technical knowledge. Lets show Bell that we DO care!

LETTERS FROM READERS

Dear TAP,

Perhaps some of your readers would like to chat with ships on the high seas. This is now possible through a satellite called Marisat. Actually there are two currently operational: Atlantic and Pacific, and in a very short time there will be one for the Indian Ocean too. Enclosed is a list of most of the ships that you can contact and the list continues to grow. To place a call: engage your favorite 800 or 555 number, then box off to 800-243-3640 (or 264-9090 in Conn.). This gets you the Marisat operator. She will ask you billing information, so you should have a story made up as to who (what individual/or company) is calling and give her a number to bill it to (like IBM or Continental Bakery, or whatever). She doesn't have any way (presently) of knowing where the call is coming from. (It's going to cost somebody 10 bucks a minute!) And be a good guy and give her the ship's number (like SS Jonsson #1560201) and tell her you want to speak with..... oh, what the hell, the chief steward or cabin boy - anyway, the radio operator will get the call and you can bullshit with him. Sparks can tell you where the ship is, courses, speed, destination, etc.

Comsat has some other numbers that might prove fruitful if somebody knows how to exploit them: (203) 264-9030 is Data Test (associated digits 1800-922-4646, which may be a computer entry code?), 264-9040, 264-9050 (data set), and 264-9060. You might also try 264-4091/4092.

Has anybody ever "boxed" calls through TWX? I don't know if it's a usable system. (See article on TWX phreaking by Osbert Kilgallen in this issue of TAP.) Anyway Marisat has Telex capability too: 710-581-5920 (toll free). Additionally, AT&T long lines is 914-682-8252 and the United Nations language bank (free translations?) is 212-686-3061.

May the force be with you,
R2-D2

Greetings,

In Missouri, Southwestern Bell has forced itself upon an unwilling public. They now charge 20¢ per directory assistance call (after the first five free ones per month).

Well, in a burst of insight it came to me--and it has been verified by experiment and questions to operators. It is:

Call the 555-1212 number, using the 1 code, omitting the area code (as in calling directory assistance for another town in your area code). When the operator asks you "What city please?" just say the name of your town (in my case St. Louis)--and she says "go ahead." They have no way of knowing what town you are dialing from!! And there is no charge for the 555-1212 number.

I, also, note that Kansas City, Mo 555-1212 info uses computers to retrieve telephone numbers. When will I be able to access by computer the up to date directory listings?

Jeff

Back Issues are 50¢ each.

Subscriptions - 10 issues - US Bulk rate \$5.

US First Class in plain sealed envelope \$7.

Canada & Mexico First Class \$7.

Foreign \$8.

IMPORTANT! Include mailing label or Xerox copy when writing to TAP about your subscription.

Book - Monopoly \$1.20.

Electronics Courses - 50¢ 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.

Send ONLY check or money order (No Cash) to:

TAP, Room 418, 152 West 42 Street, New York, N.Y. 10036

This is a mail drop only.

OFFICE: 1201 Broadway, Room 608, New York, N.Y. 10001

HOURS: WEDNESDAY, 5 - 9 pm.

Shipboard Terminal Installations: An Update

At press time, the following vessels were equipped with shipboard terminals which have been commissioned for operation with the MARISAT System:

Ship	Country of Registration	Telephone/Telex Number	Answerback
Al Hasa	Panama	1330701	HCWD 1330701
Alaskan Star	United States	1501577	KGPJ 1501577
American Ace	United States	1500101	KFCV 1500101
Aquarius	United States	1500702	WSKS 1500702
Arco Anchorage	United States	1501104	WCIO 1501104
Arco Fairbanks	United States	1501103	WGWB 1501103
Arco Juneau	United States	1501102	KSBG 1501102
Arco Prudhoe Bay	United States	1501101	KPFD 1501101
Atrevida	Denmark	2610101	OVVZ 2610101
Ben Ocean Lancer	United Kingdom	2440401	GUUU 2440401
Cable Venture	United Kingdom	2440102	GUXZ 2440102
Chevron Hawaii	United States	1500401	KNFD 1500401
Crest	United States	1501576	WBGF 1501576
Donghae-Ho	Saudi Arabia	3743101	HYSJ 3743101
Duchess Diane	United States	1501574	MGNA 1501574
Eso Bangkok	Panama	1330101	HPXD 1330101
Eso Copenhagen	Liberia	1240102	ELSJ 1240102
Eso Malacca	Panama	1330102	HPDA 1330102
Eso Philippines	Panama	1330103	HPXW 1330103
Eso Wilhelmshaven	Liberia	1240101	ELVX 1240101
Fred H. Moore	United States	1500602	MOBL 1500602
Golden Bear	United States	1500501	WEZD 1500501
Indian Seal	United States	1503201	SEAL 1503201
Indus	Sweden	2370101	SLAT 2370101
Jonsson	Canada	1560201	VYXD 1560201
KDD Maru	Japan	3203177	JGOC 3203177
King Oscar	United States	1501201	WYVC 1501201
Kurama-Maru	Japan	3200102	JDDG 3200102
LASH Atlantic	United States	1500201	WEZU 1500201
LASH Italia	United States	1500204	WJAT 1500204
LASH Pacifico	United States	1500202	WIEE 1500202
LASH Turkiye	United States	1500203	WMIG 1500203
John A. MacDonald	Canada	1560101	CGBK 1560101
Mercury	United Kingdom	2440101	GJXH 2440101
Messiniaki Chara	Greece	2130101	SXRN 2130101
Mobil Aero	United States	1500601	WLBY 1500601
Mormacstar	United States	1500301	KGDF 1500301
Nai Maria Amelia	Italy	2150201	IBFR 2150201
Niobe	United States	1501575	KPKV 1501575
Ocean Ranger	Panama	1330702	HENB 1330702
Portobello	Panama	1330402	HPBJ 1330402
Phaedra	United States	1501573	WPSH 1501573
Puerto Rico	United States	1503202	WFJK 1503202
U.S. Olympic	United States	1503216	WYZQ 1503216
Pacesetter III	United States	1501477	WDBT 1501477
Post Enterprise	United Kingdom	2440201	GUHL 2440201
Queen Elizabeth 2	United Kingdom	2440301	GBTT 2440301
Royal Viking Sea	Norway	2310101	LECK 2310101
Sedco-709	United States	1500603	KBCG 1500603
Seismic Explorer	United States	1501476	WRHC 1501476
Texaco Georgia	United States	1502101	WLDW 1502101
Wild Gannett	United Kingdom	2440202	GWAQ 2440202

Dear TAP:

I understand that at some point in the recent past your readers, or your magazine itself were interested in knowing the frequencies for those digits that come after 9.

They are:	0 (10)	941.0	+	1336.0
	* (11)	941.0	+	1209.0
	# (12)	941.0	+	1477.0
	(13)	697.0	+	1633.0
	(14)	770.0	+	1633.0
	(15)	852.0	+	1633.0
	(16)	941.0	+	1633.0
	(17)	350.0	+	440.0

This information is available through many publications e.g. Bramco Controls Division, Ledex Inc., College and South Streets, Piqua Ohio 45356, (513) 773-8271. I trust this information will not be used for anything illegal or foolhardy. Bramco's booklet could give you more information.

one lonely Canadian

