

\$1.75

QEX¹¹³

WITH Gateway



ARRL Experimenters' Exchange

JULY 1991



KA9Q's thoughts on packet radio authentication systems (p.13).

QEX: The ARRL
Experimenters' Exchange
American Radio Relay League
25 Main Street
Newington, CT USA 06111

Non-Profit Org.
US Postage
PAID
Hartford, CT
Permit No. 2929

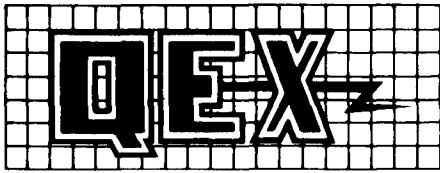


TABLE OF CONTENTS

QEX (ISSN: 0886-8093) is published monthly by the American Radio Relay League, Newington, CT USA.

David Sumner, K1ZZ
Publisher

Paul L. Rinaldo, W4RI
Editor

Lori Weinberg
Assistant Editor

Mark Forbes, KC9C
Geoffrey H. Krauss, WA2GFP
Bill Olson, W3HQT
Stan Horzepa, WA1LOU
Contributing Editors

Production Department
Mark J. Wilson, AA2Z
Publications Manager

Michelle Chrisjohn, WB1ENT
Production Supervisor

Sue Fagan
Graphic Design Supervisor

Dianna Roy
Technical Illustrator

Circulation Department
Debra Jahnke, *Manager*
Kathy Fay, N1GZO, *Deputy Manager*
Chetty Tardette, *QEX Circulation*

Offices
225 Main St, Newington, CT 06111 USA
Telephone: 203-666-1541
Telex: 650215-5052 MCI
FAX: 203-665-7531 (24 hour direct line)
Electronic Mail: MCI MAIL ID:215-5052
(user name ARRL)
Telemail address: ARRL
Internet:arrl@mcimail.com

Subscription rate for 12 issues:
In the US by Third Class Mail:
ARRL Member \$12, nonmember \$24;
US, Canada and Mexico by First Class Mail:
ARRL Member \$25, nonmember \$37;
Elsewhere by Airmail:
ARRL Member \$48, nonmember \$60.

QEX subscription orders, changes of address, and reports of missing or damaged copies may be marked: QEX Circulation.

Members are asked to include their membership control number or a label from their QST wrapper when applying.

Copyright © 1991 by the American Radio Relay League Inc. Material may be excerpted from QEX without prior permission provided that the original contributor is credited, and QEX is identified as the source.

PSK ANYONE? _____ 3

By John C. Reed, W6IOJ

A 1200-baud PSK demodulator designed specifically for narrow-band applications. A practical HF packet alternative.

COLUMNS

CORRESPONDENCE _____ 8

More on the Safari-4 and CDMA vs TDMA; 900/901 series; Graphics Interchange Language (GIL); and switching power supplies.

COMPONENTS _____ 10

By Mark Forbes, KC9C

The microprocessor—a programmable logic component. Also, MEC surface mount switch, 2-gigabyte disk drive, tiny RF mixer, and RF connectors.

VHF + TECHNOLOGY _____ 11

By Geoff Krauss, WA3GFP

Mid-year notes . . . VHF + radiation and microwave devices.

GATEWAY _____ 13

By Stan Horzepa, WA1LOU

U2MIR bids farewell and U5MIR wants to know "what's up?"; AMSAT-NA annual meeting and symposium; thoughts on BBS authentication; and new packet software releases.

On the cover:

With apologies to Gil, adapted from the December 1964 issue of QST.

JULY 1991 QEX ADVERTISING INDEX

AMSAT: 18
Communications Specialists Inc: 9
Down East Microwave: 18
Gracilis: 29
Henry Radio Stores: 20
Jacob Handwerker, W1FM: 9

Kantronics: Cov III
L. L. Grace: Cov II
P. C. Electronics: 7
Sinclabs Inc: 12
Yaesu USA Inc: Cov IV

THE AMERICAN RADIO RELAY LEAGUE, INC



The American Radio Relay League, Inc. is a noncommercial association of radio amateurs, organized for the promotion of interest in Amateur Radio communication and experimentation, for the establishment of networks to provide communications in the event of disasters or other emergencies, for the advancement of the radio art and of the public welfare, for the representation of the radio amateur in legislative matters, and for the maintenance of fraternalism and a high standard of conduct.

ARRL is an incorporated association without capital stock chartered under the laws of the State of Connecticut, and is an exempt organization under Section 501(c)(3) of the Internal Revenue Code of 1986. Its affairs are governed by a Board of Directors, whose voting members are elected every two years by the general membership. The officers are elected or appointed by the Directors. The League is noncommercial, and no one who could gain financially from the shaping of its affairs is eligible for membership on its Board.

"Of, by, and for the radio amateur," ARRL numbers within its ranks the vast majority of active amateurs in the nation and has a proud history of achievement as the standard-bearer in amateur affairs.

A bona fide interest in Amateur Radio is the only essential qualification of membership; an Amateur Radio license is not a prerequisite, although full voting membership is granted only to licensed amateurs in the US.

Membership inquiries and general correspondence should be addressed to the administrative headquarters at 225 Main Street, Newington, CT 06111 USA.

Telephone: 203-666-1541 Telex: 650215-5052 MCI. MCI MAIL (electronic mail system) ID: 215-5052 FAX: 203-665-7531 (24-hour direct line)

Canadian membership inquiries and correspondence should be directed to CRRL Headquarters, Box 7009, Station E, London, ON N5Y 4J9, tel 519-660-1200.

Officers

President: LARRY E. PRICE, W4RA
PO Box 2067, Statesboro, GA 30458

Executive Vice President: DAVID SUMNER, K1ZZ

Purposes of QEX:

- 1) provide a medium for the exchange of ideas and information between Amateur Radio experimenters
- 2) document advanced technical work in the Amateur Radio field
- 3) support efforts to advance the state of the Amateur Radio art.

All correspondence concerning QEX should be addressed to the American Radio Relay League, 225 Main Street, Newington, CT 06111 USA. Envelopes containing manuscripts and correspondence for publication in QEX should be marked: Editor, QEX.

Both theoretical and practical technical articles are welcomed. Manuscripts should be typed and double spaced. Please use the standard ARRL abbreviations found in recent editions of *The ARRL Handbook*. Photos should be glossy, black-and-white positive prints of good definition and contrast, and should be the same size or larger than the size that is to appear in QEX.

Any opinions expressed in QEX are those of the authors, not necessarily those of the editor or the League. While we attempt to ensure that all articles are technically valid, authors are expected to defend their own material. Products mentioned in the text are included for your information; no endorsement is implied. The information is believed to be correct, but readers are cautioned to verify availability of the product before sending money to the vendor.

Empirically Speaking...

Spotlight on the 13-cm Band

The 2300-2450 MHz, or 13-cm, band has received a great deal of attention in the United States preparation for WARC-92, and it may get a lot more at the Conference itself. Just to review the status quo:

• Internationally (that is in the international Radio Regulations), the band is allocated as follows (caps indicate primary, lower case means a secondary allocation):

Region 1	Region 2	Region 3
2300-2450	2300-2450	
FIXED	FIXED	
Amateur	MOBILE	
Mobile	RADIOLOCATION	
Radiolocation	Amateur	

• Footnote 664 allocates the band 2400-2450 MHz to the amateur-satellite service.

• The frequency 2450 MHz \pm 50 MHz is allocated to industrial, scientific and medical (ISM) applications, eg, microwave ovens.

• Within the United States, the band is allocated as follows:

Band (MHz)	Government	Nongovernment
2300-2310	RADIOLOCATION	Amateur
	Fixed	
	Mobile	
2310-2390	RADIOLOCATION	MOBILE
	MOBILE	
	Fixed	
2390-2450	RADIOLOCATION	Amateur

• The 2310-2390 MHz band is used for aeronautical flight test telemetry.

The FCC's *Second Notice of Inquiry (NOI)* on WARC-92 preparation proposed three options for Digital Audio Broadcasting (DAB), both satellite and terrestrial, one of which was 2390-2450 MHz. The *NOI* also asked if the ISM band could be reduced to 2420-2480 MHz. The broadcasters argued that home and vehicular DAB receivers would be clobbered by domestic microwave ovens. ISM interests said that shrinking their band would cause an economic burden on them. The ARRL and AMSAT filed in opposition to having DAB in the 2390-2450 MHz band and the *NOI*'s proposal to eliminate the amateur-satellite footnote 664 allocation of 2400-2450 MHz.

The FCC's *Supplemental NOI* solicited comments on sliding the DAB band downward to 2360-2410 MHz and allocating 2410-2450 MHz to the mobile-satellite service (MSS) for use in the Earth-to-space direction, while leaving the amateur service in the international table as a secondary service and the amateur-satellite service

retaining its 2400-2450 MHz band in footnote 664. Obviously, DAB would have been a very difficult sharing partner and in time could have denied useful amateur access to the 2390-2410 MHz band. The 2410-2450 MHz MSS usage, on the other hand, seemed to pose less of a problem.

In its *Order* released June 20, the FCC decided to propose the following for modification of the international frequency allocation table:

Region 1	Region 2	Region 3
2300-2390	2300-2390	
FIXED	FIXED	
Amateur	MOBILE	
Mobile	RADIOLOCATION	
Radiolocation	Amateur	
2390-2430	2390-2430	
Fixed	Fixed	
Amateur	Mobile	
Mobile	Radiolocation	
Radiolocation	Amateur	
MOBILE-SATELLITE	MOBILE-SATELLITE	
2430-2450	2430-2450	
FIXED	FIXED	
Amateur	MOBILE	
Mobile	RADIOLOCATION	
Radiolocation	Amateur	

A proposed footnote would be added to the 2300-2390 MHz band saying that some portion will be allocated to the broadcasting satellite (sound) service—DAB. There is a similar proposed footnote to have some portion of the 1429-1525 MHz band allocated to DAB as well.

A band around 1.5 GHz is preferred by the broadcasters for DAB, but the 1429-1525 MHz band is used for aeronautical test telemetry, and has been staunchly defended by the US Air Force and aircraft manufacturers. This has been a difficult issue for the FCC and the National Telecommunications and Information Administration (NTIA) to resolve, to the extent it is resolved.

What will happen at WARC-92 concerning DAB will be known only at its conclusion in March of 1992. If DAB is put squarely in the 1.5 GHz band, aeronautical telemetry would likely move some or all of its operations to the 2300-2450 MHz band. If DAB is split between 1.5 and 2.4 GHz, we would have broadcasting to contend with in the 13-cm band.

Although there have been some studies,

Continued on page 18.

PSK Anyone?

By John C. Reed, W6IOJ
770 La Buena Tierra
Santa Barbara, CA 93111

Everyone agrees the phase-shift keying (PSK) method used in the digital satellites has worked great. So why not consider 1200-baud PSK for other applications?—like 10-meter HF packet as an example. Thinking in these terms has resulted in the following PSK demodulator, designed specifically for narrow-band applications. All of the testing has been made using filters in both the transmitter and receiver having a confirmed -6 dB band pass of 1.8 kHz. The system is easy to tune (using the described tuning aid) and it operates with a receiver's output signal level varying over a <30 dB range. Packet connections can be made when the packet is a fraction of a second in duration (like someone calling CQ—no continuous carrier), and a signal strength of 6 dB or more above noise.

Up-Frequency Converter

Referring to the block diagram in Fig 1, you will note the first operation is an up-frequency mixer, converting the received PSK signal (1.5 kHz in this particular example) to 15 kHz. This process is generally not recommended because of difficulties in filtering the unwanted modulation products. However, in this particular application, the advantages listed below make the converter concept a key demodulator design feature.

1) The phase-locked loop (PLL) operating frequency (15 kHz) is far removed from the 1.5-kHz phase shift information band pass, reducing processing phase jitter by a factor of ten. Also, the more favorable filtering condition, 15 kHz rather than 1.5 kHz, reduces any PLL phase-error transient noise to a level that is of no consequence.

2) The 15-kHz PLL is much less sensitive to receiver tuning. The loop locks clean with any signal that approaches a level that can be processed. All of the testing has been performed with a minimum start frame sequence (40-ms duration, DWAIT-0, TXDELAY-1).

3) The 15-kHz filter is equivalent to an additional receiver IF. Its band pass is tailored to minimize phase distortions caused by the receiver's steep-skirt filtering.

4) The LO frequency adjustment performs an IF shift function similar to that of the receiver. As an example, if you choose to operate with a carrier of 2 kHz rather than 1.5 kHz, the receiver's band-pass center is shifted to 2 kHz with the receiver's IF shift; the converter's LO frequency is adjusted to 13 kHz rather than 13.5 kHz. The demodulator will then operate with the 2-kHz carrier with no other alignment adjustments.

Circuit Description

Refer to Fig 2, schematic of the up-frequency converter, and Fig 3, schematic of the demodulator. The description follows test points as noted on the schematics. Indicated ac voltages are peak-to-peak.

[A] R1 is adjusted for a noise level of 0.2 V after the

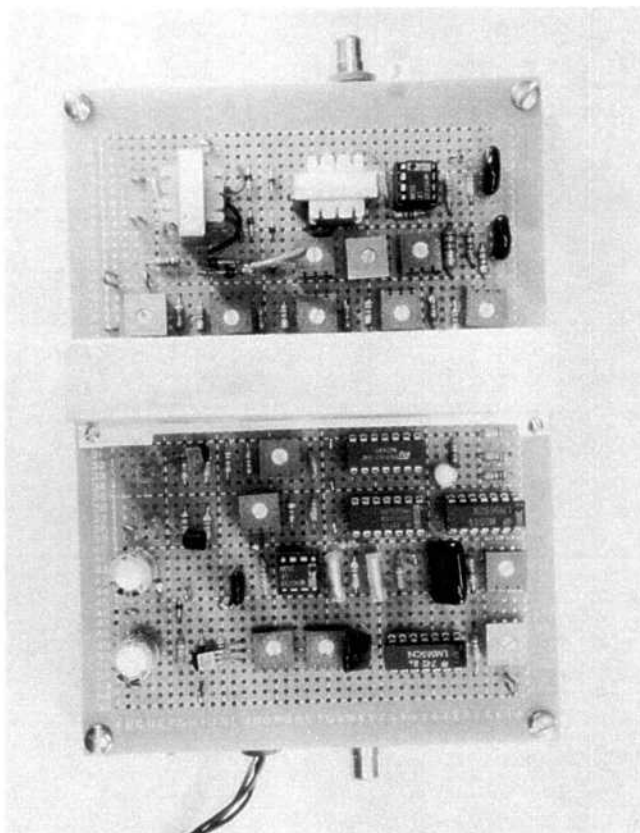
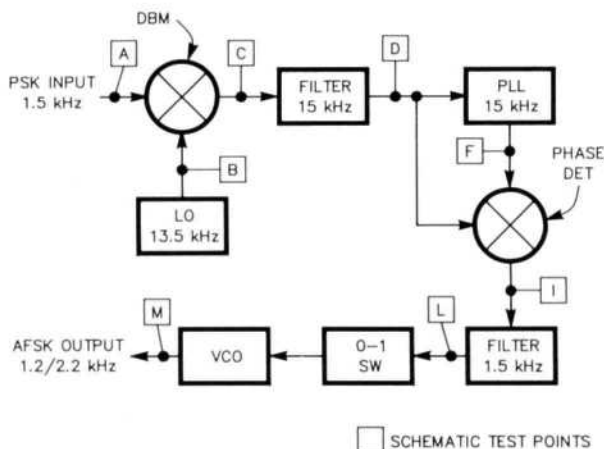


Photo 1—Demodulator mounted on $4\frac{1}{2} \times 6\frac{1}{4}$ -inch perf board. Note the shield isolating the 15-kHz filter from the demodulator transients.



SCHEMATIC TEST POINTS

Fig 1—Demodulator block diagram.

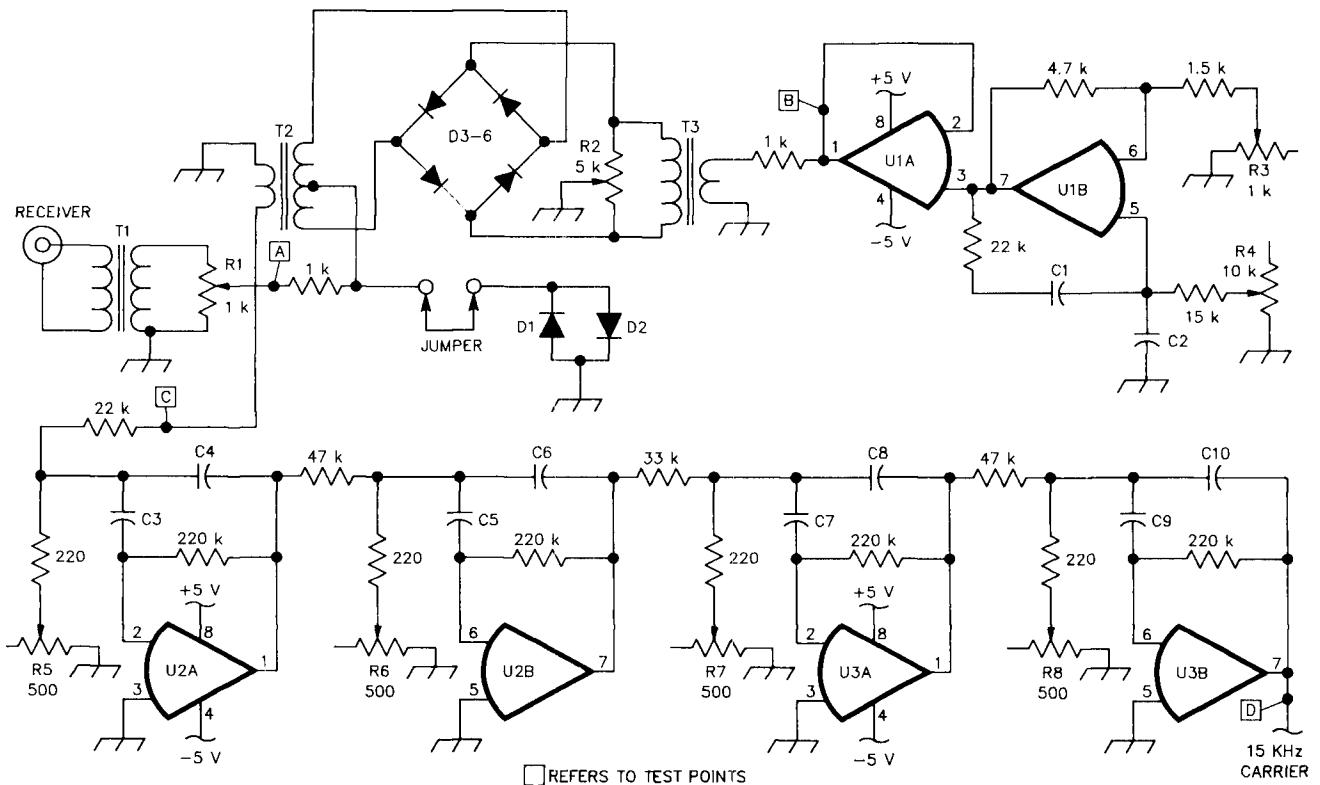


Fig 2—Schematic of the 15-kHz up-frequency converter.

- C1,2—510-pf mica
- C3-10—0.001- μ F mica
- D1,2—1N34A germanium diode
- D3-6—1N914/4148 switching diode

- U1-3—LF353 dual bi-fet op amp
- T1—Radio Shack 273-1374 isolation
- T2,3—Radio Shack 273-1380 output

receiver's output is set to the normal speaker/phone level. Clamping diodes D1 and D2 limit the range into the doubly balanced mixer (DBM) without distorting the phase-shift cross-over points. The operating range is 0.2 to 10 V. The jumper permits disconnecting the clamping diodes during filter alignment procedures.

[B] The LO has an output of 8 V. The RC oscillator feedback adjustment R3 is set for reasonable waveform results while still permitting the frequency adjustment R4 to cover a range of about 13 to 13.8 kHz (input carrier of 2 to 1.2 kHz). A buffer stage isolates the oscillator from the DBM load, ensuring optimum LO stability.

[C] The DBM output will primarily indicate the 15 kHz and the image frequency 12 kHz. The DBM balance adjustment R2 is set for optimum waveform symmetry.

[D] The filter is four identical RC active band-pass stages that are stagger tuned to give the desired passband. In this example, R6-8 are peaked at 1.1 kHz and R5-7 at 2.1 kHz (filter is slightly asymmetrical). The resulting 1.5-kHz passband shown in Fig 4 fits within the receiver's 1.8-kHz band pass. There is minor image frequency interference at the lower frequencies. This can be reduced by using the receiver's IF shift to make a carrier frequency of 2 kHz rather than 1.5 kHz. However, I have noticed no performance improvement by making this change. Apparently this image distortion is not significant consideration.

The saturated output is 1 V (2 V with the clamping jumper removed). There is unity signal gain between [A] and [D].

[D] through [L] The demodulator is similar to one described in September 1990 QEX ("Microsat Demodulator," by John C. Reed, W6IOJ). The detailed description will not be repeated. The free running PLL/VCO frequency is adjusted to twice the selected carrier frequency by R9 (30 kHz). R10 establishes the detector center operating level; adjust for maximum noise output at [J]. Symmetry of the output is set by R11. It should be adjusted such that NRZI inputs having the same configuration will result in outputs having an identical width configuration regardless of the output polarity.

[L] The demodulator NRZI output is monitored with LEDs D3 and D4 indicating either a 0 or 1 level output condition. They are useful for monitoring the receiver noise or in a test condition where there is a continuous input level.

[M] A keyed VCO makes the AFSK conversion. R12 is set for 2200-Hz output when the switch Q3 is turned on (0 level) and R13 is set for 1200-Hz output when the switch is open (1 level). The maximum output is 2 V.

Test Results

Most of the testing was performed in a closed loop condition. A signal was made in the HF receiver's frequency range with a special mixer connected to one of the inter-

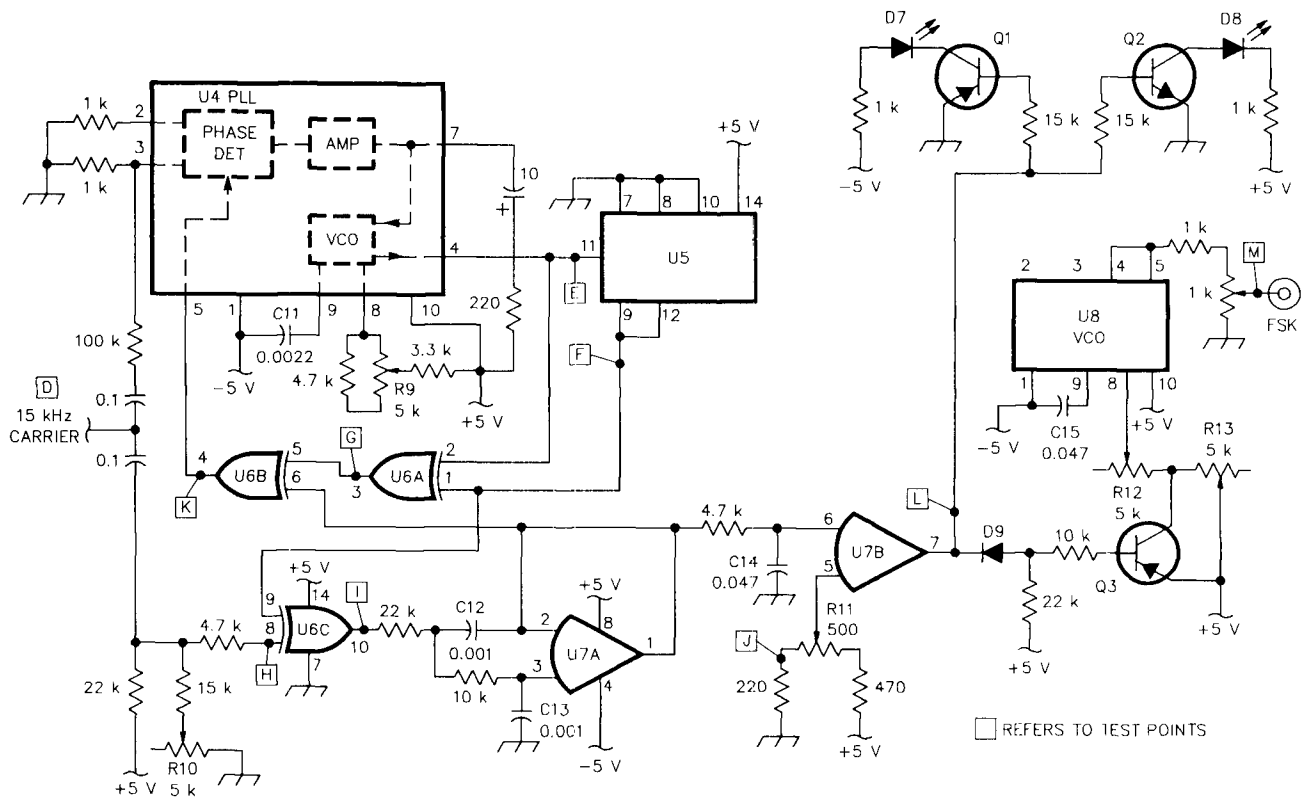


Fig 3—Schematic of the demodulator/AFSK converter

C11—0.0022- μ F mica

C12,13—0.001- μ F polyester

C14,15—0.047- μ F polyester

D7,8—LED Radio Shack 276-026

D9—1N914/4148 switching diode

U4,8—LM565 phase-locked loop

U5—4013 flip-flop

U6—4030 quad exclusive OR gate

U7—LF353 dual bipolar FET op amp

Q1,3—2N2907 PNP

Q2—2N2222A NPN

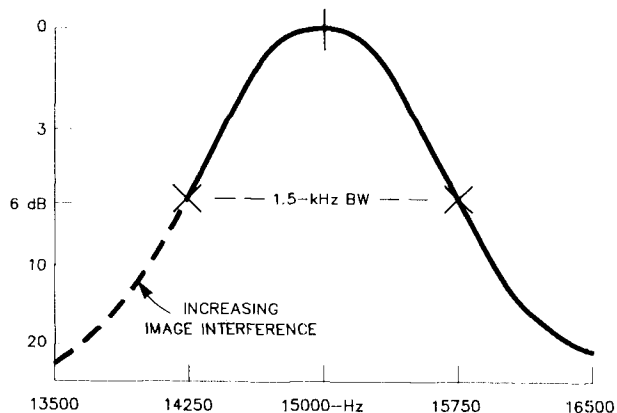


Fig 4—Bandpass of the 15-kHz filter.

mediate stages of my Mode-B satellite transmitter. Final closed loop tests were made using the TNC operating in the full duplex mode and with the other menu selections chosen to repeat packets with minimum delay. And finally, talking to myself with longer packets to make sure the

system did not develop a problem. The TNC was always set for a minimum 40-ms start frame period. Additional testing included talking to myself via the AO-13/Mode-B satellite, and monitoring the digital mode FO-20 satellite.

The closed loop tests during the developmental effort mainly relied on a 150-Hz pulse generator as a signal source. The pulse could be varied in duration from one to seven bits to simulate repetitive start frames or frames having multiple bits to evaluate the effects of overshoots from the various filters. A typical closed loop sequence of start frames is illustrated in the Fig 5 scope display. It is interesting to note the 3-bit processing signal delay (0.8 ms/bit). The PSK transmitter processing contributed a 0.9-bit delay, the HF receiver 1.3 bits, the up-frequency conversion 0.6-bit and the demodulator processing 0.2 bit. Noise performance is indicated in Fig 6. A pair of start frames were turned on at four frame intervals to provide the S/N comparison. The number of frames photographed is about 40 when considering the shutter speed and a 2/1 scope display count. Note there were no noise error signals during the integrated 40-frame photograph. Also, the PLL maintained a locked condition during the two-frame noise period. This is evident from the error-free pulse at the frame start. The multiframe integrated photograph makes the noise bits appear as low- and high-state solid lines.

The satellite AO-13/Mode-B connections simply con-

NRZI INPUT
start frames

PSK CONVERSION
(0.1 bit delay)

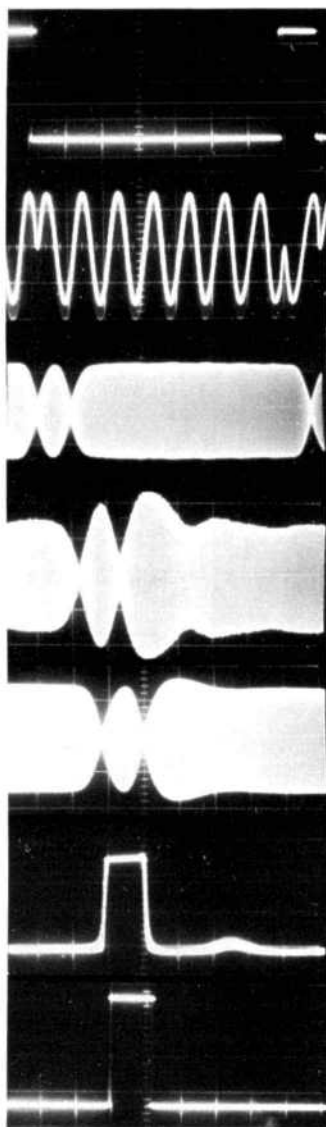
PSK TX ENVELOPE
(0.9 bit delay)

A RX ENVELOPE
(2.2 bit delay)

D 15 kHz FILTER
(2.8 bit delay)

J DEMOD DET
(2.9 bit delay)

L NRZI OUTPUT
(3.0 bit delay)



NOTE: □ REFERS TO CIRCUIT TEST POINTS

Fig 5—Scope pictures of a closed loop sequence.

firmed the closed loop test results. My Mode-B setup is in sad shape and a 10-dB S/N is about the best signal. Retries were common due to spin modulation (accentuated by my linearly polarized antennas). The results seemed to be identical to those experienced in the closed loop configuration.

There have been no problems in monitoring the digital mode FO-20, solid copy of a typical 12-minute pass. Mainly a test of large-signal capability. Having no AFC, it also was a test of the tuning aid. I had no problem in maintaining adequate Doppler tracking with dial tuning.

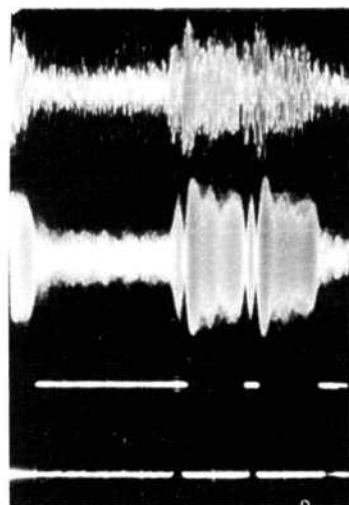
Tuning Aid

Audible tuning aid comparison methods have been used on HF with some success. However, PSK's single frequency format really enhances the performance of this

A RX OUTPUT

D 15 kHz FILTER

L NRZI OUTPUT



NOTE: □ REFERS TO CIRCUIT TEST POINTS

Fig 6—Noise performance. OFF 2 start frames—ON 2 start frames. Photo integration—20 traces.

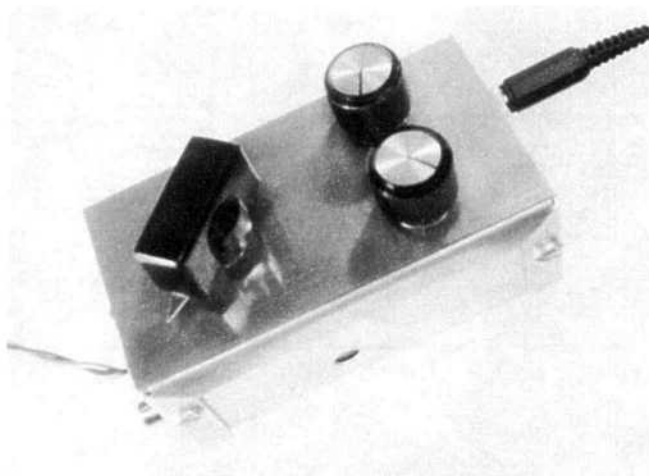


Photo 2—Tuning aid mounted in a 2 × 3¼ × 1¼-inch box. The large knob sets the reference frequency and the two small knobs the receiver output and the reference phone levels. Hole in chassis is access to the filter frequency trimmer.

method as compared to that of the conventional HF 300-baud output tone pair. The tuning aid uses a filter centered at the carrier frequency (1.5 kHz in this example) accentuating the carrier tone during the start-frame sequence. This tone is audibly compared to a stable reference tone. It is accurate and easy to tune even when used with signals having a minimum start-frame period.

Referring to the tuning aid schematic, Fig 7, the reference tone is formed by the square wave timer IC U1, R1 setting the frequency from 1.2 to 2 kHz. A combination of this reference tone and the receiver output, the relative amplitudes selected with R3 and R4, is filtered by the active bandpass filter U2A. The filter is trimmed to the selected carrier frequency by R2. The U2B follower provides the

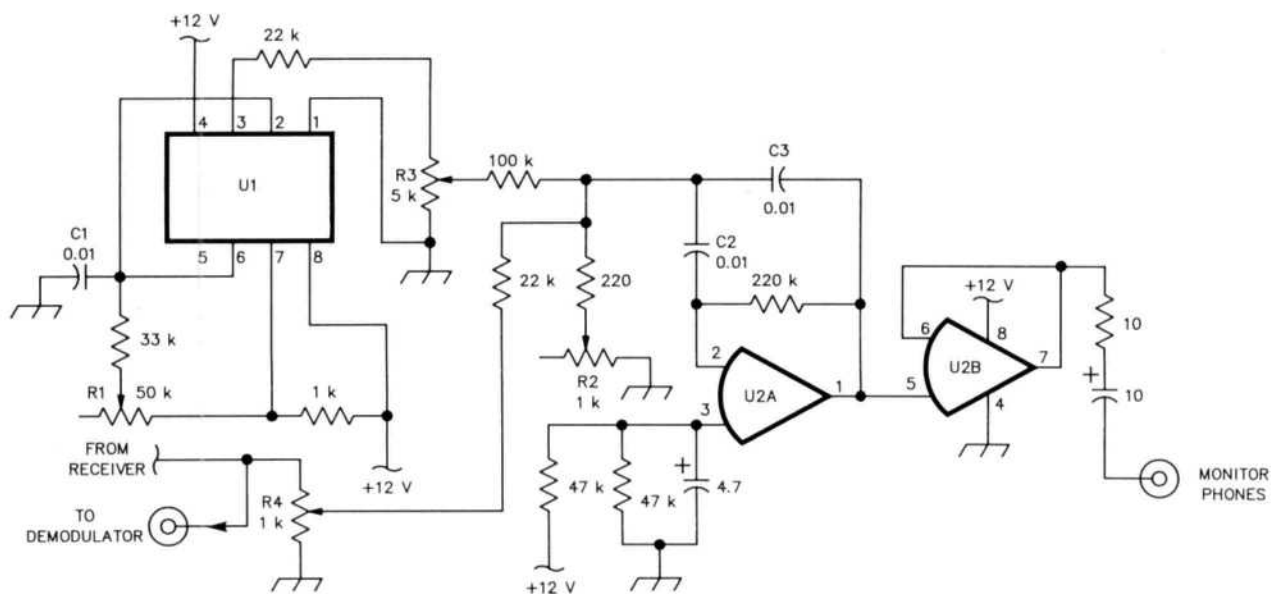


Fig 7—Schematic of the tuning aid.

C1—0.01- μ F mica
 C2,3—0.01- μ F polyester
 U1—555 timer
 U2—1458 dual op amp

R1—Reference frequency
 R2—Filter frequency
 R3—Reference level
 R4—Receiver level

necessary phone output level.

Operating procedure is to first set the reference frequency (1.5 kHz in this example) and trim the filter frequency for maximum phone response. Then adjust the receiver noise to a normal phone level, and finally set the reference signal so that it is barely audible through the receiver noise. With a little practice you will find it easy to match a threshold PSK signal to the reference tone with more accuracy than is required for a solid copy.

Summary

Narrow-band 1200-baud PSK with its excellent threshold

signal performance is a practical HF packet alternative. Its band-pass requirement is no more than that required for SSB and with a relatively simple modem it can be interfaced with typical SSB/TNC equipment. Why not give it a try on 28 MHz. With positive results it might be encouragement to change the current FCC 300-baud rule for frequencies lower than 28 MHz. As an alternative, making a similar rule related simply to a band-pass restriction encourages system development for optimum frequency utilization, ie, maximum symbols per second within a specified band pass.

AMATEUR TELEVISION

P. C. ELECTRONICS VISA - MC - UPS COD
 2522-Q PAXSON LN, ARCADIA CA 91007 818-4474565

HAMS SHOULD BE SEEN AS WELL AS HEARD!



Only \$89
 for the TVC-4G 70 CM
 ATV Downconverter
 to get you started

Value plus quality from
 over 25 years in ATV

The sensitive TVC-4G GaAsfet downconverter varicap tunes the whole 420-450 MHz band down to your TV set to channel 2, 3 or 4. Just add a good 70 CM antenna and you are ready to watch the live action. TVC-2G board only is avail. for \$49.

NOW SEE THE SPACE SHUTTLE VIDEO

Many ATV repeaters and individuals are retransmitting Space Shuttle Video & Audio from their TVRO's tuned to Satcom F2-R transponder 13. Others may be retransmitting weather radar during significant storms. Once you get bitten by the ATV bug - and you will after seeing your first picture - show your shack with the TX70-1A companion ATV transmitter for only \$279. It enables you to send back video from your camcorder, VCR or TV camera. ATV repeaters are springing up all over - check page 411 in the 90-91 ARRL Repeater Directory. Call (818) 447-4565 or write for our complete ATV catalog for downconverters, linear amps, antennas, and accessories for the 70, 33, & 23 CM bands.

Correspondence

More on the Safari-4 and CDMA vs TDMA

I have been following, with interest, a sequence of articles in *QEX*. This sequence includes the three-part "The Safari-4: A High-Integration, 4-Band QRP Transceiver," by Wayne Burdick, N6KR, and then the entire Correspondence section in *QEX* issue 109. First I would like to offer some comments regarding the letter by John H. Klingelhoefter, WB4LNM, and Wayne Burdick's answer to him.

The articles offered as references by WB4LNM for direct-conversion SSB receivers are quite old. I built a DCSSB receiver in 1985 using the NE602s in a highly integrated and compact receiver that achieved about 90-dB two-tone dynamic range. This was published in *EDN* and as Signetics AN1981, mentioned in Peter Traneus Anderson's letter in the same Correspondence section! Gary Breed, K9AY, offered "A New Breed of Receiver" in *QST* (Jan 1988) which offered a comparable level of integration. Also see Sept 1988 *QST* Technical Correspondence for more information and techniques on DCSSB receiver design.

Regarding the debate over superhet vs direct conversion, for my part this seems academic in so far as circuit complexity is concerned. I suppose one could count the number of active and passive devices and make the decision. A more relevant question is hinted in the N6KR challenge. Which design offers the best compromise of power consumption, performance (particularly the receiver), and size? My current "gut feeling" is that direct conversion SSB receivers can show a slight advantage over superhets.

A very important architectural advantage to the direct conversion receiver is that it lends itself better to higher levels of integration. Superhets require off-chip ceramic and/or crystal filters. With DCSSB receivers, filters, and for that matter, all-pass quadrature phasors, are easily integrated using gyrators, op amps, or even DSP filters. The main point is that the filters operate at baseband (audio) rather than at some HF IF. Consequently, if RF silicon IC foundries were to actually build linear DCSSB chips, I think there is no question that direct conversion techniques would show a significant advantage over superhets, even for high performance radios. This advantage was the main incentive for my work with the 602s at Signetics six years ago.

For now, a new device, the Plessey SL6442 is available. It features two mixers and a separate front-end AGC amplifier on one chip. The single mixer plus AGC amplifier will come out later this year and be called the SL6444. The SL6442 will enable DCSSB receiver builders yet another step to higher integration. Incidentally, the Plessey parts will work up to 1 GHz in contrast to the NE602's limitation of several hundred MHz.

One final comment on the N6KR design. Since the dynamic range of the '602 is about 90 dB maximum, I suspect that the Safari-4 suffers from a rather limited dynamic range. My suspicion arises from the fact that three NE602s are cascaded, each exhibiting about 20-dB conversion gain. Even allowing for filter insertion losses and the AGC range, I can imagine the second mixer, in par-

ticular, to be vulnerable. The product detector has the advantage of high selectivity ahead of it and since it is a CW receiver, hopefully only one carrier will appear at a time. This will help the intermodulation performance. I fear that this product detector would not do very well in an SSB mode, where intermod levels might become excessive. I presented some guidelines for using the NE601 in Technical Correspondence, *QST* May 1990.

On a completely different subject, Alan Rutz's, WA9GKA, letter carries some misleading information. Contrary to numerous reports in both the technical and non-technical press, CDMA or spread spectrum techniques offer no panacea to band congestion. There is currently a great debate between proponents of TDMA (time division multiple access) and CDMA (code division multiple access), also known as spread spectrum. Current estimates for the increased number of simultaneous users for CDMA are about 7 over systems now in common use including analog narrow-band FM. TDMA offers about a 5 to 1 advantage. Most current work in this area is taking place in cellular radio and the new license-free band at 902-928 MHz. My personal feeling is that some type of hybrid TDMA-CDMA system will be optimized for maximum simultaneous use for cellular radio. There is a set of simple equations which define processing gain and jamming margin. These quantities then set practical limits and relative powers of transmitters in CDMA systems. *The ARRL Handbook* has a description of direct sequence spread spectrum techniques, synonymous with CDMA.

The scenario of every amateur in the Chicago area using the same CDMA repeater at the same time without a problem is, to say the least, a generous assessment of CDMA capabilities, even with the advanced Qualcomm System. This is not to say I disagree with the sentiment of incorporating spread spectrum techniques into amateur use. There will certainly be a place for both TDMA and CDMA techniques. However, we should be careful to understand the advantages and also the limitations of new techniques before proposing applications for these techniques.—Robert J. Zavrel, Jr., W7SX, ARRL TA, 117 Locatelli Lane, Scotts Valley, CA 95066

900/901 Series

Has anyone done work on PIN diode switching for remote antennas instead of relays? Looking at the 900/901 series animal it would be interesting to have 6X2 PIN diode switches at both ends and only 2 coax runs up a tower. Maybe even 12X2 at the tower end for omni vs beam usage. Coax costs \$\$\$\$\$!

Actually, the 900/901 is underrated because if you had a radio in the car and an IR link to the house and a remote power supply and PIN diode remote antenna selection, you would have one heck of a radio for sure!

In the future, as prices fall, I want to try that technique on the 900/901 animal. One IR link to the house from the car and then a portable control head using ultra low power

to walk around the house! Correct, sick, warped, but in the true spirit of "Let's play ham radio."—Joseph Anthony Wolos, WA1OCK, 1139 St James Avenue, Springfield, MA 01104-1375

GIL-Graphics Interchange Language

Sporadically appearing in the packet radio literature is a wish or note on how nice it would be to be able to exchange drawings and certain forms of graphics via packet radio. Wait no more, for now *GIL* can do it!

With this PC-compatible program (MS-DOS), hams can now translate ASCII files into drawings and sketches, in color if desired, or even into musical tones or Morse-code output. *GIL* preserves the concept of plain-language ASCII files being transferred over the air, or via BBS systems, so that provisions of Part 97 regarding use of ASCII are not strained, and preserving a very high degree of data compression to assist disk-storage space.

The primary purpose behind *GIL* is to permit a convenient way for radio amateurs to send more than just plain ASCII text messages over the packet or RTTY radio links. Before *GIL*, there was no convenient way to transmit over the radio, or via bulletin board, reasonably small "files" containing enough information to reconstruct a good line drawing or cartoon.

GIL comes in a public domain .ZIP-type archive with GIL.EXE (the *GIL* executable program) and several other .GIL format files for your enjoyment. The most current version of *GIL* is located on the land-line HAMNET BBS at 216-942-6382 and 216-942-7516 in Cleveland, Ohio. —Glenn L. Williams, AF8C, Technical Advisor, 513 Kenilworth Road, Bay Village, OH 44140-2476

Switching Power Supplies

Timothy P. Hulick, W9QQ, is not the first to use a

switching power supply in a legal-limit HF power amplifier. In *QST*, August 1960, pp 16-17, Jo Emmett Jennings, W6EI, describes a similar supply. Both supplies are unregulated. W9QQ's supply provides 1500 mA at 2000-V output, while W6EI's supply provides 300 mA at 3000-V output. W9QQ uses 240-V ac input, while W6EI uses 115-V ac input. W9QQ's supply weighs 8 pound while W6EI's weighs 12 pounds.


W6EI uses self-oscillating push-pull germanium power transistors oscillating at a frequency of a few kilohertz. This supply emits audible noise when operating. The transformer is wound on a single steel-strip-wound toroid core of 4-inch outer diameter.

W6EI's transistors could not stand the full input voltage, and high-voltage, high-capacitance electrolytic capacitors were not available. He made do with low-voltage transistors, and some of the first computer-grade low-voltage electrolytic capacitors.

W6EI's elegant solution is to wind four identical sets of primary and feedback windings on the one core. He wires four identical oscillators, with two 2N174 transistors each, for a total of eight transistors. He wires a 5000- μ F, 25-V electrolytic capacitor across the dc input of each oscillator. He then wires these four dc inputs in series across the rectified ac input. The four oscillators being on one common core force the oscillators to share the input voltage evenly.

Modern high-power switching power supplies have active power-factor-correction circuits on their inputs. The circuits force the input current to be a sinewave in phase with the input voltage, and also provide safe current limiting. The circuits could be applied to W9QQ's supply. The benefits are: (1) shorted output protection; (2) automatic in-rush current limiting; (3) less input current for a given output power; and (4) automatic regulation against input voltage changes. —Peter Traneus Anderson, KC1HR, 990 Pine Street, Burlington, VT 05401

Surface Mount Chip Component Prototyping Kits—
Only **\$49⁹⁵**



CC-1 Capacitor Kit contains 365 pieces, 5 ea. of every 10% value from 1pf to .33 μ f. CR-1 Resistor Kit contains 1540 pieces; 10 ea. of every 5% value from 10 Ω to 10 meg Ω . Sizes are 0805 and 1206. Each kit is ONLY \$49.95 and available for Immediate One Day Delivery!

Order by toll-free phone, FAX, or mail. We accept VISA, MC, AMEX, COD, or Pre-paid orders. Company P.O.'s accepted with approved credit. Call for free detailed brochure.

COMMUNICATIONS SPECIALISTS, INC.
426 West Taft Ave. • Orange, CA 92665-4296
Local (714) 998-3021 • FAX (714) 974-3420

Entire USA 1-800-854-0547

IONSOUND™ by W1FM: DX'er Propagation Software
State-of-the-art skywave propagation prediction software covers 1.8-54 MHz for serious Amateur, Military, and SWL users. Menu-Driven selectable TX Power, Frequencies, TX/RX Antennas, Local Noise conditions, Bandwidth, Short/Long Path, Sunspot or Solar Flux. Choice of Latitude/Longitude or predefined locations shown in *QST* Magazine's 'How's DX?' IONCAP propagation prediction forecasts. Comprehensive Tabular Summary provides Signal-to-Noise Ratio, Rx Power and Microvolts, S/N and Path Availabilities, Total Link Reliability, Bearings, Distance, Delay, Takeoff Angles, Vertical and Oblique E/F Mode MUFs. IONOGRAM Chirp Plot graphics shows MUF and LUF, band opening reliabilities and Multipath. For IBM PC's and compatibles with Hercules Graphics or CGA/EGA/VGA. 320K RAM, minimum. ASCII manual on disk. \$33 for 5.25" DSDD; \$35 for 3.5" DSDD (3.5" disk includes coprocessor-only version). Add \$12.50 for detailed 46 page printed and bound User Manual. Prices include shipping. Info: 617-862-6742, evenings. See July 1990 CQ Magazine review. Send US Check / Int'l Money Order only to: Jacob Handwerker / W1FM, 17 Pine Knoll Road, Lexington, MA 02173, USA

As promised in the May column, this month I'll go into more detail about microprocessors. As I alluded to last time, a microprocessor is really a programmable logic component. Every one of the digital functions (gates, flip-flops, counters, etc) that has been discussed in this column can be implemented with a microprocessor. The key lies in the way that it's programmed. Programming for a PC is generally called *software*. When the software is permanently stored in Read Only Memory (ROM) it is called *firmware*, denoting that it is (generally) not intended to be modified in any way. This firmware is what defines the function of the microprocessor.

Of course, the microprocessor can also execute significantly more complex functions than those we looked at earlier. In reality though, the more complex functions are just combinations of these basic ones. So, it is the firmware that really makes a microprocessor go.

Microprocessors are classified by the number of bits that they work with in a single operation. The early 4004 was a 4-bit microprocessor, ie, it operated on four bits with each instruction. Note that in binary, four bits can represent only 16 possible numbers. That means that a 4-bit processor can have only 16 instructions, and can deal with numbers 0 through 15. Of course, these processors can concatenate, or string together several 4-bit numbers to represent larger numbers, just as we string together several base-ten numbers to represent larger values (we have only ten characters in our familiar base 10: 0-9). The 8080, Z80, 6800, 6502, and similar processors are 8-bit microprocessors. These were the most common microprocessor until the mid-1980s. With 8-bits, there are 256 combinations.

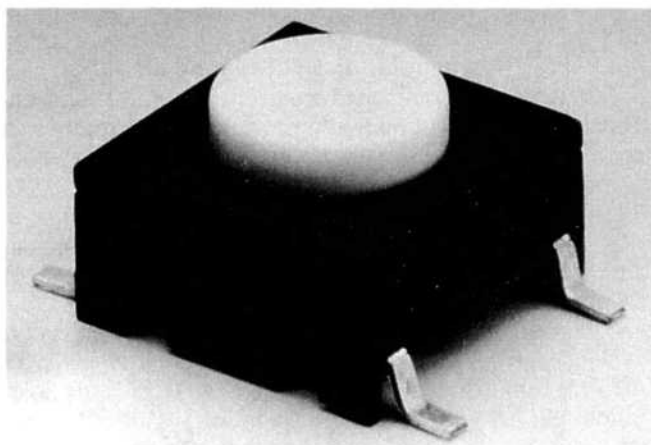
The majority of PCs today are based on the 16-bit microprocessor of the 8086 family. These are being supplanted by 32-bit microprocessors, such as the 80386 family. With 32 bits, extremely large numbers can be represented and operated on with a single instruction. To give you an idea of the power of today's 32-bit microprocessors, a scant 15 years ago many mainframe computers used a 32-bit CPU. Many minicomputers were based on 16-bit CPUs! Given the power of today's microprocessors, it has become almost impossible to determine what constitutes a microcomputer and what constitutes a mainframe.

That's it for this month's coverage of the microprocessor. Next time, I'll dig more deeply into the architecture of microprocessors and what really makes them tick.

MEC Surface Mount Switch

MEC has introduced a surface mounted momentary-contact switch. This tiny switch (see photo) mounts directly to the printed-circuit traces in the same way as surface mounted ICs, transistors, and other components. As with those surface mounted devices, this switch is sealed and can be immersed in solvents for cleaning. The dimensions of this tiny switch are 10.1-mm square by 6.4-mm high.

The electrical ratings of the switch are 50 mA at 24 V dc. This switch could be ideal for microcircuitry in ham applications. For more details on this very tiny switch, contact MEC A/S, Industriparken 23, DK-2750 Ballerup, Denmark.



2-Gigabyte Disk Drive

For really *large* disk drive needs, Fujitsu America has just introduced a 2-Gbyte, 5.25-inch disk drive...that's 2,000 Mbytes! The drive has an average latency of 5.6 ms, and can transfer data at up to 10 Mbytes/second over its synchronous SCSI-2 interface. In asynchronous mode, the drive will transfer at up to 3 Mbytes/second.

To get an idea of the density of this drive, each cylinder is capable of storing over 1 Mbyte of data, and the real density is more than 80 Mbits/square inch. Even with this degree of density, reliability hasn't been compromised; the MTBF is 200,000 hours. If you'd like more information on this \$6000 disk, contact Fujitsu America Inc, 3055 Orchard Drive, San Jose, CA 95134-2022, or call 408-432-1300.

Tiny RF Mixer

Continuing on the surface mount vein, RF Prime now offers an extremely small surface mount mixer line. The mixers cover frequencies up to 2.5 GHz, making them useful in most amateur projects. Local oscillator frequencies from 500 kHz to 1.5 GHz can be used with the mixers.

The complete mixer, with case, measures 0.25 x 0.31 x 0.20 inches! They also have a low-profile version that's just 1/8-inch tall. Contact RF Prime for information about these mixers and all of their RF products at: 11305 Sunrise Gold Circle, Rancho Cordova, CA 95742.

RF Connectors

I recently set out to find a source for in-line female UHF connectors, like you find on the pigtailed of all the current VHF/UHF transceivers. I didn't realize what a difficult task it would be to find these connectors! The "big company" (Amphenol) doesn't make these, so I had to beat the bushes. The source I found is Cambridge Products Corporation. They make a very wide range of RF connectors, including UHF, N, BNC, and all the popular connector styles. Their catalog, which lists all of their connectors, as well as crimping and stripping tools, can be obtained by writing to Cambridge Products Corp, 4880 N. Hiatus Road, Sunrise, FL 33351.

Mid-Year Notes

Yes, this should have been my June '91 column, but I missed the deadline; I was recovering from a second cataract operation (both eyes are never operated on at the same time so that if contaminants are present there is less chance of dual loss). I am mentioning my cataract problem, again, because I have been told that there was some chance that my trouble occurred at a relatively early age due to exposure to microwave energy! Now, I don't know that such is actually the cause, but I *did* work in the microwave field as an engineer 15-20 years ago, and I was exposed to some pretty powerful radiation. I know others who have been similarly exposed and who have had much more abrupt onset of visual loss; sometimes even permanent. Not in all cases, though. I don't have enough data, or training in this field to determine at what level a real hazard exists. *But* . . . I do believe that VHF+ers may be subjected to more danger if they are not very careful. Bottom line is: Know what you are doing *before* you work with VHF+ radiation. There is a good article on biological radio hazard in *The ARRL Handbook*; read it now, if you never have done so, and reread it every few months, just to keep it fresh in your mind.

On the other hand, no one may have to worry because the use of amateur microwaves may be, in my opinion, coming to a practical end. No, not by changes of any FCC regulation (yet), but due to a quickly enacted change in the contest rules. I gave the argument in my last column; in the interim, the Contest Advisory Committee very rapidly approved the imposition of a limited 4-band multioperator class for the VHF/UHF contests (eg, June VHF Contest rules, May 1991 QST). As I write this column (mid-May 1991) before the June '91 contest, I'll go out on a limb and predict that a number of the well-known multiop groups from past contests will: (a) be in limited multiop class this year; (b) concentrate on 6 m, 2 m, 432 and 1296 where the greatest number of QSOs and grids are likely to be worked; (c) *not* run any activity on 220/222 since the usage frequencies have not yet been settled and the number of possible contacts will be confused; and (d) *not* run any activity above 1300 MHz (ie, no microwave bands) because the number of points obtainable is not worth the cost/time of equipment building and roving. Actually, the limb I'm placing myself on is not a very dangerous place to be because I've already talked to one top-ten multiop group that has mothballed its 2300-and-up gear, and will be running in the limited category because they want to finally, after years of trying, win a number-one title! Just at the time that we should be doing all that is possible to increase activity on bands which may have WARC trouble, the incentive has been removed. Will the cellular telephones and the satellite TV get some of our spectrum? Maybe! And it would be the supreme irony if the FCC ends up using future contest activity reports as a prime example that amateur operators are no longer using some of their microwave allocations.

Just when the real incentive to work microwave has gone, it looks like potential performance is ready to take

another jump, as a new generation of discrete, smaller-signal microwave devices seems to be arriving. I just received data sheets on the KGF18XX series of GaAs HEMT transistors, from OKI Semiconductor (785 North Mary Avenue, Sunnyvale, CA 94086-2909). Readers will remember that HEMTs are truly state-of-the-art devices, hitherto available mainly to the military market and too expensive, at \$100+, for most amateur or commercial use. The three devices listed (1850, 1860 and 1870) differ, basically in their I_{dss} maximum current rating (50 to 100 mA), but all have a typical noise figure of 0.7 dB and associated gain of about 11 dB at 12 GHz! That's in a ceramic package, no less; this is good for easy handling, but the unpackaged chips (almost impossible for use in amateur facilities) are even better above a few GHz. At 2.3, 3.4 or 5.6 GHz the specs are below 0.5-dB NF, about 0.6-dB NF at 10 GHz. This is due to the high electron mobility design, with a two-dimensional electron "fluid" carrying the signal currents, and the use of a 0.25-micron wide gate; some 0.1-micron gate HEMTs give 1.9/2.3-dB NF and 13/9.2-dB gain at 60/94 GHz, respectively. The OKI devices have a maximum power output capability in the 100-mW class at a few volts V_{ds} , and might also find a good home in 5.6- and 10-GHz transmitters and transverters. The extraordinary feature is that, in a 4-lead ceramic package (similar to the standard -35 case) these devices are said to be priced in the \$11 each category. I have not found out if there is a minimum size/value order requirement, but even if there is, I'm sure that one of the usual sources will make these gems available in the near future. . . . If anyone still wants to build better amateur microwave gear.

I recently read an article about the next step beyond the HEMT, a device built with indium-phosphide (InP) material and specifically optimized for nonlinear characteristics, such as improve the harmonic generation (more gain and efficiency equals higher output power for millimeter wave generators). Understandably, the researchers at Varian building an InP FET with a nonlinearly optimized transconductance profile call it, no kidding, a NOTFET.

The main sources of amateur-use Microwave Monolithic Integrated Circuits (MMICs) have been Avantek and MCL (MiniCircuits Labs). The usual series of small-signal, broadband 0135-0835 devices are now also being manufactured by SGS-Thomson Microelectronics, 211 Commerce Drive, Montgomeryville, PA 18936-0835. SGS also has a few newer members of their MMIC family: an AMP0520 device in a 200-mil BeO package, with gain of about 10 dB at a P_{out} of +23 dBm (200 mW) at 1 GHz, when operating with +12 V dc (sounds good for a 902-MHz driver stage); an AMP0910 device in a 100-mil square package which cuts parasitics and allows 50-ohm cascadable gain strips to be built to beyond 3.5 GHz (good for stages on the 3456-MHz band; an AMP1023 device in a rectangular-flanges 230-mil package (like a small microwave Class-C power transistor) operable at 50 ohms single ended or at 25 ohms for push-pull amplifiers to 0.5 watts/device at 902 and 0.3 watts/

device at 1296; and the AMP1120 device, also in a 200-mil package. As usual, the data packages do not address the questions of price and minimum order size. I will try to get some additional information on these devices since SGS appears to be located only a short distance from my new QTH.

I received a letter from Peter Onnigian, W6QEU, at HAM-PRO Antennas (6199B Warehouse Way, Sacramento, CA 95826); they make a 6-element, 6-m Yagi based on the NBS models. Price is on the order of \$200. I did not mention this 15-foot beam, model H6-6, when I wrote of the other new 6-m beams several months ago.

Someone just popped their head into my office (this being done at lunch hour) and told me to be off 220-222 by August 28! Can they be taking it away so fast? Have you ever noticed that the give-to-amateurs grants (eg, getting us on 902-928 after WARC approval) proceed at an order of magnitude slower than the take-aways? For those of us running transverter-type systems, it should not be too hard to raise the local oscillator frequency by a mere 2 MHz and get back on 222.1 weak-signal work. I've seen a number of used 220/28 transverters advertised "for sale" in recent newsletters and magazine ads; it might be a good time for new 222 SSB operators to get some fairly decent equipment, cheap. Most such rigs use a 96-MHz crystal oscillator and a subsequent doubler to obtain the 192-MHz injection signal for heterodyne mixers. Changing the crystal to 97 MHz (units available from most crystal manufacturers advertising in any of the ham magazines) may not even require adjustment to get some output; best results will probably require some tweaking and peaking, but that can be done later on. CU soon on 222.1 SSB!

Or will it be some other frequency? Any reader on, or planning to be on, the "new" 222-225 MHz band should be aware that there are at least three different band plans, each being touted for adoption by ARRL. Each has somewhat different subbands for weak-signal, FM packet, etc. If you have not already done so, please review the alternatives and express an opinion to the VUAC (VHF/UHF Advisory Committee) person for your Division, so that they can take everyone's desires on this matter into account, in recommending a plan.

Of course, you may find it difficult to obtain the proposed band plans because VHF+ information sources keep getting harder to find. Has the *VHF/UHF and ABOVE* magazine disappeared? A new *terrestrial VHF+* newsletter is

available from John Carter, KØIFL, at PO Box 554, Union, MO 63084 (US subscription rate \$14.50/year—12 issues). It's a 6-10 page, mostly operating news effort that seems to be growing. I personally still have not found any newsletter with as much technical information as in recent bimonthly issues of the newsletter of the North Texas Microwave Society, available from WA5VJB.

Someone did show me a copy of *Elektor Electronics USA* which is a mainly audio hobby magazine from Europe. The April 1991 issue had a 144-to-50 MHz down converter transceiver; good design philosophy, but use parts unavailable in the US.



Sinclabs Specialty Products

TRANSVERTERS for 144, 220 and 222 MHz

12 VOLT POWER SUPPLY

2-WAY and 4-WAY COAXIAL POWER DIVIDERS

COAXIAL JUMPER CABLES

WATER COOLING JACKETS

VHF and UHF YAGIS

HF, VHF and UHF MOBILE ANTENNAS and MOUNTS

OMNIDIRECTIONAL VERTICAL ANTENNAS

50 ohm LOAD TERMINATIONS

LIGHTNING PROTECTION PRODUCTS

MOUNTING CLAMPS

CALL OR WRITE FOR OUR LATEST CATALOG

Sinclabs Inc., Specialty Products, 85 Mary Street,
Aurora, Ontario, Canada L4G 3G9
Phone: (416) 841-0624 Fax: (416) 841-6255

U2MIR BIDS FAREWELL AND U5MIR WANTS TO KNOW "WHAT'S UP?"

On *Mir* passes on May 24, the following packet-radio beacons were received from the space station.

U5MIR > CQ: FROM 24.05.91 YOU CAN CONNECT WITH U5MIR, PMS: U5MIR-1

U2MIR SENDS HIS BEST 73s TO ALL !!!

In a packet-radio contact with students in Australia, U2MIR indicated that he is not sure whether he wants to go up to *Mir* again. He has logged a record 18 months in space and has been on seven spacewalks, one that lasted 6 hours. He is in his early 40s and has a wife and two children who would probably not mind him being earthbound.

A few days later, KP4BJD, had a voice conversation on 2-meters FM with a member of the new *Mir* crew, Cosmonaut Sergey Krikalev, U5MIR. During the conversation, Sergey sent greetings to all and congratulated NASA on the launch of space shuttle *Columbia* (STS-40). He requested that packet-radio stations using the U5MIR-1 personal message system include news in their messages. The *Mir* crew needs entertainment and the usual content of the messages they now receive is "boring."

—from AMSAT and SpaceNews

AMSAT-NA ANNUAL MEETING AND SYMPOSIUM

AMSAT-NA will hold their annual meeting and symposium at the Los Angeles Airport Holiday Inn, November 8-10. There will be technical sessions each day of the symposium and a banquet Saturday evening. A field trip to the Jet Propulsion Lab will also be available.

Rooms may be reserved now (at a special AMSAT \$55 per night single occupancy room rate) by calling 1-800-465-4329. The advance registration fee for the meeting and symposium will be approximately \$15. The symposium chairman, Gene Davies, AA6NP may be called at 213-662-2820 (home) or 213-937-7942 (work).

—from AMSAT

THOUGHTS ON BBS AUTHENTICATION

I've had several requests for the "white paper" on cryptographic authentication of BBS messages that I wrote recently in response to a query by Paul Rinaldo, W4RI, of the ARRL. Paul is the chairman of the ARRL Digital Committee, of which I am a member.

In case anybody can't tell, the opinions expressed here are my own.—Phil Karn, KA9Q

Paul,

This is in response to your request to the Digital

Committee for comments on authentication schemes that might be used to verify the source and integrity of a message posted to an amateur BBS network. This letter consists of a quick tutorial on the various forms of cryptographic authentication, some personal judgments about their practicality and suitability for the problem at hand, and some personal opinions on the present regulatory situation.

The scheme that I talked about at the 1987 ARRL Networking Conference was for authenticating IP datagrams using DES, but the same principles apply to using any conventional secret key cipher to authenticate any kind of message. (By "authenticate a message," I mean verifying that the message was, in fact, sent by the claimed sender, and that the message contents have not been modified along the way.) Such schemes require all the stations involved to share a single secret key. Without the key, you cannot compute the proper authenticator for the messages you send, nor can you verify an authenticator received with an incoming message.

The difficulty of key management with a conventional cipher can range from "trivial" to "intractable" depending on the application. Key management is simple as long as there are only a few stations that need to generate or authenticate messages and all trust each other. For example, a DES-based scheme could be applied to a repeater to limit remote control to a few trusted stations. A single key known to the repeater would be shared by the control stations and kept secret from everyone else. An in-person meeting or the telephone would suffice for distributing the DES keys.

Now consider cases where the operators do not necessarily trust each other, eg, autopatch operation. Since many more stations use an autopatch than control the basic operation of the repeater, its owners may want individual accountability. A DES-based authentication system could still work if each user has his or her own key. The same system could be used to control access to a BBS. In either case, the "server" (the repeater or BBS) keeps a complete list of keys for all authorized users and logs each access. This is more work than the previous case, but it is still entirely practical.

Common to all these schemes so far is the assumption that only the server needs to authenticate a request, eg, the repeater controller or the BBS. It must protect its users' keys against unauthorized disclosure, but since the resource being protected by the authentication system is the server itself, the owner of the server has an incentive to do this.

But in the more general case where individual pairs of stations must be able to authenticate each other, things get much more complicated. Each pair has to have a key that

is known only to that pair; if you have N stations, you need a total of N^2 keys. All these keys must be exchanged by some secure means before authentication can occur and they must be kept secret. To do this for every pair of amateurs in the world is clearly impractical. And if you want any amateur to be able to verify the authenticity of, say, a "broadcast" BBS message (to carry on the amateur "self-policing" tradition, of course), there is no solution using conventional cryptography—the same key needed to verify a message could be used to forge one.

Some form of secret key authentication might still be practical between neighbors in a packet backbone or a BBS autoforwarding network. But this would authenticate only your immediate neighbors; it would not authenticate the origins of the traffic they pass from other nodes. For example, one BBS SYSOP could create illegal traffic and then pass it to a neighbor claiming that it originated somewhere else, and there would be no way to disprove this. So you really do want the authentication to be "end to end," not "hop by hop," so we are left with an unsolved key management problem.

One way to reduce the N^2 key problem is to establish a "key distribution center" that maintains a list of all the users' private keys. Users wishing to authenticate themselves to each other do so by first authenticating themselves to the key distribution center (KDC). The KDC then generates a "session key" (a random number) and sends it to the two parties encrypted in their own keys. The parties then decrypt the session key, yielding a shared secret that can be used for authentication. Still, only the parties involved can authenticate each other; someone listening in could not. (In most environments, this is an advantage; somebody else's conversations are none of your business.)

MIT has developed a system based on this model called "Kerberos." It is in operation at MIT and elsewhere (the code is free). Nevertheless, it has the drawback that authentication depends on the availability and reachability of the KDC. But the fact that the KDC must have a complete list of the users' private keys works against deploying multiple KDCs with copies of the database for redundancy; the more KDCs there are, the more opportunities for the database to be compromised. The scheme also assumes that all of the parties (the two users and the KDC) have the ability to communicate with each other in real time, a bad assumption for amateur packet radio.

So the inescapable conclusion is that authentication schemes based solely on private key cryptography are of limited utility in amateur packet radio; they cannot solve the general problem. Fortunately, there is a new alternative: public key cryptography (PKC). In PKC, the keys used for encryption and decryption are different. Furthermore, knowledge of the encryption key, K_e , does not imply knowledge of the decryption key, K_d ; in fact, the algorithms ensure that it is extremely difficult to determine K_d from K_e . The combination of K_e and its corresponding K_d is called a "key pair"; for this reason, public key cryptosystems are sometimes called "dual key" ciphers, as opposed to "single key" ciphers like DES.

The leading public key scheme, RSA, was invented by Ron Rivest, Adi Shamir and Len Adelman while at MIT. They hold a US patent on it that is being exploited by RSA Data Security, Inc. (There is no patent protection on RSA outside the US).

The original idea behind RSA was to allow you to publish K_e (hence the name, "public key" cryptography) so anyone could send you a secret message without prior arrangement. As long as you keep K_d secret, only you can decrypt it. But when used "backwards," RSA can also do authentication. If you encrypt a message using K_d (your decryption key, known only to you), then anyone can decrypt it using your K_e (your public encryption key). Anyone who decrypts such a message then knows that whoever generated it must have known your K_d . This procedure of using RSA in reverse is called "signing."

In practice, it is not desirable to run an entire message through RSA to authenticate it because it is very slow, much slower than secret key ciphers like DES. There is a better way. Functions exist to quickly "hash" a message of arbitrary length into a relatively small, fixed size "message digest." They are much like cyclic redundancy codes (CRCs) except that they are much more complex because they are designed to detect intentional "transmission errors" as well as natural ones. With a good function, it is computationally infeasible, even for someone who knows it, to produce two messages that hash to the same value or to determine the input that produces a given value. They are not ciphers because they have no key and their outputs cannot be "decrypted."

One message digest algorithm is "message digest #4" (MD4) by Ron Rivest, who has placed it in the public domain. MD4 takes a message of any length and produces a 128-bit (16-byte) result. Rivest conjectures that it would take on the order of $2^{1/2}64/$ operations to find two inputs that hash to the same value and $2^{1/2}128/$ operations to find an input that hashes to a given value. These are impressive numbers, so if the algorithm holds up under analysis, it should be quite secure in practice.

Given RSA and MD4, one authenticates a message by first computing its hash code with MD4. Then RSA is used to "sign" the hash code (by encryption with the sender's private key, K_d) and the result is appended to the message. The party wishing to authenticate the message also computes the message digest. It then decrypts the encrypted message digest received with the message (using the published key of the sender, K_e) and compares it to the value it has just computed. If they match, the message is genuine.

There still remains the problem of distributing the public keys. Although they may be freely read by anyone, they must still be protected against modification. Otherwise, someone might forge a signature of a message under someone else's name using a public-key/private-key pair of his own creation. If the receiver can be duped into accepting this bogus public key, then he will believe that the signature is genuine.

One way is to publish the public keys as widely as

possible in so many places that no one could possibly modify all of the copies of a particular key that reach the intended target of a deception. For example, the keys could be published on CD-ROM or they could be listed in the back pages of *QST*. But these schemes have two drawbacks: cost and time.

Another refinement, "certification," addresses this problem. If a "certifying authority" can be set up to sign the public keys of individual users with its private key, then only the public key of the certifying authority needs to be widely published. For example, the ARRL might select and publish its own public key in *QST*. It could then accept public keys from individual amateurs (accompanied with some non-cryptographic form of authentication, such as a notarized statement). The ARRL would sign the individual public keys with its private key and return the results. Note that the ARRL need *not* know the individual's private keys.

The signed public keys are known as "certificates." They can be distributed by the users themselves (eg, in a mail header) because anyone can readily verify their authenticity with the published ARRL public key. This eliminates the need for an on-line KDC. The ARRL's workload might be a problem, but a solution exists for this too: a hierarchy of certifying authorities. For example, each ARRL Division might act as the certifying authority for the amateurs in its area using a Division public key that has been certified by ARRL Headquarters. Divisions might further delegate the workload to their constituent Sections. The verification of an individual user's certificate would therefore require the certificates of all of the certifying authorities in the hierarchy, as well as, the published key of the ARRL.

So, in theory, anyway, authentication based on public key cryptography solves many of the problems associated with the earlier secret key schemes. However, many practical obstacles would still remain:

1. The RSA algorithm is patented in the US and the owners of the patent are holding it fairly close to their chest. Negotiations between RSA and the Internet Activities Board have been dragging on for several years now over an agreement for the use of RSA in the Internet. It is not at all clear how much the patent royalties will be or how they will be charged. (The leading theory is that the royalties will be tied only to the issuance of certificates, not to the actual implementation or use of RSA, but this is not yet final.) Would the use of RSA in amateur packet radio (resulting in the payment of royalties to RSA DSI) be considered as furthering the "regular business affairs" of RSA DSI?

2. The algorithms are, by amateur standards, quite complex. At a minimum, they would probably require every amateur to have a PC-class computer to hash and sign messages. Given that a major reason TCP/IP is still a relatively esoteric mode in amateur packet radio is the reluctance of many amateurs to upgrade from C-64s and "dumb terminals," it seems unlikely that universal user authentication could happen any time soon. And I won't even *begin* to discuss the user education issues.

3. Even if a full-blown RSA-based authentication

system, as described earlier, could be deployed, it is not clear that it would solve the specific problem that originally prompted your query. Someone accused of posting an illegal message to an amateur BBS could still claim that his secret key had been stolen and used by someone else. Or he could accuse the local "Section Certification Manager" of signing a bogus public key with his call sign on it and using it to "frame" him by sending verboten traffic. Even if a key really has been stolen and the owner notifies the certification authorities, how do they spread the word that the previously distributed public key is no longer valid? These issues are still the subject of much discussion in the research community. Furthermore, this technology has yet to have its first test in a court of law.

In summation, although I find cryptographic authentication to be a fascinating topic that has some potential for use in Amateur Radio, I do not feel that it is "ready for prime-time." Mandating its use at this time would be an enormous overreaction to the "problem" of controlling inappropriate BBS traffic.

Quite frankly, the FCC's heavy-handed behavior in this case has me greatly concerned. I think they are going after a fly with a battleship. I do not know whether they sincerely believe that they are "protecting" Amateur Radio or if they have some more sinister motive. I can only hope for the former, so we can reason with them. Every new development carries with it some risk of abuse; the more powerful the technology, the greater the risk. Amateur packet radio is no exception; even in its presently primitive state, it is useful enough to tempt some commercial entities to abuse it. We should be able to convince the FCC that requiring unrealistically stringent mechanisms to prevent even the occasional commercial abuse of amateur packet radio runs the far greater risk of destroying all of the good that it can do.

Lately, several of us (WA8DZP, K3MC, N6RCE, NG6Q and I) have been taking a close look at the low-power spread spectrum modems that are rapidly becoming available for use under Part 15 rules on 902-928 MHz and other shared ISM/amateur bands. In my own opinion, building high-speed (say, 100 to 500 kbit/s) metropolitan area networks under Part 15 rules seems entirely feasible, even with the 1-watt power limit, given proper design and engineering (good sites, directional antennas, power control, efficient channel access methods, etc). True, the performance of the existing generation of equipment is disappointing, mainly due to the lack of receiver processing gain in most models. But with the new FCC rules mandating the use of "true" spread spectrum receivers, plus the commercial drive behind this industry, it seems likely that the cost/performance ratio of this equipment will rapidly improve. Unfortunately, the same probably cannot be said for amateur packet radio gear, where the large scale production of inexpensive, high speed radio modems seems as far away as ever. Hence our initial interest in this technology.

But this latest blow from the FCC is making Part 15's absence of licensing requirements, content and/or usage restrictions look mighty attractive indeed, even though my

primary intent is to use the network for the kind of personal experimentation that has traditionally been done in the amateur service. Are the FCC's rules really "protecting" the amateur service if they scare off those who are most interested in making technical contributions to the service?

I think it is time that the FCC remove the burden of responsibility for content from automatic relay stations and loosen up its draconian definition of "business communications." A lot has happened to the telecommunications industry since the Eyebank Docket; in particular, it is certainly no longer the job of the FCC to protect a telephone company from "lost business." The amateur rules should be pragmatic with the realization that absolute prohibitions do far more harm than good.

A simple "hams shall not sell communications services" rule should suffice to make any abuses self-limiting because few hams are willing to use their time and their stations to help make money for others if they don't get a cut of it. Such a rule would be far clearer than the present "no business interest" rule. The current rule has spawned an entire generation of armchair amateur lawyers who revel in interpreting the rules in the most restrictive fashion possible. To see the chilling effect of the present rules, one only needs to look at how the field of computer networking is pretty much passing Amateur Radio by.

—from Phil Karn, KA9Q

LATEST PACKET-RADIO SOFTWARE RELEASES

The following packet-radio software was updated recently:

APLink version 5.04 (CIS HamNet library 9, file name: AP504.EXE)

G1EMM's Version of KA9Q's NOS version 1.6 (CIS HamNet library 9, file name: NOS16.EXE)

Macintosh TCP/IP version 2.2 (CIS HamNet library 9, file name: MTCP22.SIT)

MBBIOS version 3.5 (CIS HamNet library 9, file name: MBBIOS.ZIP)

PG.EXE version 910509m (CIS HamNet library 5, file name: PB0509.ZIP)

PRMBS/ROSERVER version 1.53 (CIS HamNet library 9, file name: RS153U.ZIP for full update, RS1523.ZIP for quick fix)

Rats Open System Environment Switch version 0422 (CIS HamNet library 9, file name: RS0422.ZIP)

TRAKSAT version 2.65 (CIS HamNet library 5, file name: TRKSAT.EXE)

WØRLI Mailbox version 13.1 (CIS HamNet library 9, file name: MB1301.EXE)

The following new software became available recently:

BBMSGEDT version 0.9 (CIS HamNet library 9, file name:

BM090.EXE) An IBM-PC program that allows AA4RE BBS SYSOPs to view and edit BBS message status.

F6FBB BBS (Available by sending three 5¼-inch or two 3½ disks and SASE to Salvador Caballe Micola, EA3BKZ, C/Pintor Vancells 203 4-2, 08225 Terrassa, Barcelona, Spain) A WØRLI/WA7MBL-compatible PBBS program for the IBM XT and AT that is popular in Europe. It supports up to 50 channels simultaneously and can be interfaced to an external multiplexer.

KISS Filter (CIS HamNet library 9, file name: KISSFI.ZIP) An IBM-PC program that removes unwanted packets from raw KISS files.

NOS Kit (CIS HamNet library 9, file name: NOSKIT.ZIP) A program that automatically installs NOS on an IBM PC.

PG.EXE Modified for the AEA PK-232 TNC (CIS HamNet library 5, file name: PGM232.EXE) A modification of the IBM-PC satellite broadcast software for use with AEA's PK-232.

Poor Man's Packet (PMP) (Available via anonymous FTP from helios.tn.cornell.edu) PMP is TNC emulation software for an IBM PC that only requires a simple one-chip modem connected to the computer's parallel port.

TCP/IP NOS from (CIS HamNet library 9, file name: WINNOS.ZIP) A multi-window version of NOS for the IBM PC.

View (CIS HamNet library 9, file name: VIEW.ZIP) VE3PZR's SMTP mailer for NOS on an IBM PC that is an alternative to Bdale's Mailer (BM).

Whats-Up version 1.00 (CIS HamNet library 5, file name: WU100E.ZIP) A satellite tracking and telemetry decoding program for the IBM PC.

If "(CIS HamNet . . .)" follows a software listing, it indicates that the software is available for downloading from CompuServe's HamNet. Also, some of this software may be available for downloading from ham-radio-oriented telephone BBSs and some may be available on disk from Tucson Amateur Packet Radio (TAPR), PO Box 12925, Tucson, AZ 85732-2925, phone 602-749-9479 (write or call TAPR concerning availability).

GATEWAY CONTRIBUTIONS

Submissions for publication in Gateway are welcome. You may submit material via the US mail to 75 Kreger Dr, Wolcott, CT 06716, or electronically, via CompuServe to user ID 70645,247, or via Internet to horzepa@gdc.portal.com. Via telephone, your editor can be reached on evenings and weekends at 203-879-1348 and he can switch a modem on line to receive text at 300, 1200 or 2400 bit/s. (Personal messages may be sent to your Gateway editor via packet radio to WA1LOU@N1DCS or IP address 44.88.0.14.)

The deadline for each installment of Gateway is the tenth day of the month preceding the issue date of QEX.

ARRL 10th Computer Networking Conference

CALL FOR PAPERS

A call for papers has been issued for the 10th ARRL Amateur Radio Computer Networking Conference. The deadline for receipt of camera-ready papers is **August 12, 1991**. Those wishing to submit a paper(s) for this year's Networking Conference should contact Maty Weinberg at ARRL, 225 Main Street, Newington, CT 06111, tel 203-666-1541, or fax 203-665-7531, for paper guidelines and/or an authors package.

Topics will include, but are not limited to, HF packet investigations, network development, digital signal processing, digital speech, hardware, software, protocols, packet services, packet satellites and future systems.

THE CONFERENCE

The 10th ARRL Amateur Radio Computer Networking Conference will be held September 27-19, 1991, at the Radisson Airport Hotel, San Jose, California. The Conference is being hosted by the Northern California Packet Association.

A special conference rate of \$69, single or double occupancy, has been arranged with the Radisson Airport Hotel. Contact the hotel directly at 800-333-3333 for reservations. Be sure to mention the ARRL CNC to get the special rate.

The hotel is located near the San Jose International Airport. The Radisson offers shuttle service to and from the airport. Ask about this service when you make your reservation.

American Airlines is the official airline for the conference. You can receive a discount on air fares by calling American Airlines at their Meeting Service Desk at 800-433-1790 and refer to this conference.

Friday, September 27, 13:00-17:00. Three concurrent in-depth technical sessions will be available. These planned tutorials are expected to include: Digital Signal Processing; Spread Spectrum and Part 15; and Packet Satellite. These sessions are priced separately and will include handouts and an afternoon break.

19:00-21:30. Dinner. As an option, you can sign up for our special group dinner—a LUAU! It will be right at the hotel, so you can relax and enjoy yourself.

Saturday, September 28, 08:30-17:00. Presentation of CNC Papers. As in past years, we'll gather up all the papers submitted for presentation and divide them into the time available. Everyone will have a chance to present a paper. The published proceedings and lunch (at noon) are included in the conference fee.

18:30-21:00. Dinner. We've arranged for an optional dinner at the hotel complete with a guest speaker.

21:00-24:00. BOF sessions. 10 or 15 minutes really isn't enough, so we've planned break-out rooms for "Birds Of a Feather" sessions. During the day we'll have sign-up sheets so discussion groups can form and really get into topics of greatest interest.

Sunday, September 29, 9:00-13:00. ARRL Digital Committee meeting.

09:30-13:00. A demo room will be available. We're hoping that you'll bring a rig and show off your latest work. We may also have some exhibitors.

10:00-13:00. We're going to present various newcomer tutorials. These tutorials may be for the first-time packet user, while others might be for the first-time TCP/IP user. The demo/exhibit room and newcomer tutorials will be open to all hams and prospective hams whether signed up for the rest of the conference or not.

And finally, the San Jose Technology Center is a short light-rail ride away and they have a fantastic high-tech museum called The Garage. Although a trip to the garage isn't an official part of the CNC, we're sure a large group will be planning a visit on Sunday. We'll try to help plan this outing during the conference. We'll likely work out a late morning and early afternoon trip.

REGISTRATION FORM

To receive a registration form and more complete information of the 10th ARRL Amateur Radio Computer Networking Conference, contact Maty Weinberg at ARRL (address and phone above) or get in touch with Glenn Tenney, AA6ER, Fantasia Systems, Inc, 2111 Ensenada Way, San Mateo, CA 94403, tel 415-574-3420, fax 415-574-0546.

25th Central States VHF Society Conference

The 25th Central States VHF Society Conference will be held July 25-28, 1991, at the Sheraton Inn in Cedar Rapids, Iowa. An excellent and varied series of activities and technical presentations are planned. It should also be noted that this year marks the 25th anniversary of the CSVHF Society and will be well celebrated by all. With these points in mind, the 1991 CSVHFS Conference promises to be no exception to the high quality and superb technical presentations for which these events are traditionally famous. The conference is open to all members as well as nonmembers. It is a must-attend event for both the inexperienced and experienced VHF/UHF operator. For more information, contact Rod Blocksom, K0DAS, 690 East View Drive, Robins, IA 52328 (phone 319-393-8022) or Ron Neyens, N0ICH, 8616 C Avenue Extension, Marion, IA 52302-9524 (phone 319-377-3207).

Microwave Update 1991

Microwave Update 1991, sponsored by the North Texas Microwave Society, will be held October 18-20, 1991, in Arlington, Texas. Technical presentations will be held Friday and Saturday, noise figure measurements on Friday night, and a Texas-Style BBQ will be served Saturday night. Special family activities are also planned.

If you're interested in presenting a paper, contact Al Ward, WB5LUA (2375 Forest Grove Estates Road, Allen, TX 75002). He'll give you information on topics and general guidelines for submitting papers (if you just want an Author Package, contact Maty Weinberg at ARRL HQ). September 1, 1991, is the deadline for receipt of papers.

For more information on Microwave Update 1991, please contact Al Ward, WB5LUA, at the above address.



JOIN AMSAT

Support the Amateur Space Program

AMSAT Has Established Amateur Radio As a Permanent Resident in Space!

From operating any of 12 Amateur satellites circling the globe today to participating in Amateur Radio activities from the Space Shuttle, the benefits of space based Amateur Radio are available to you by becoming an AMSAT member. Our volunteers design, build and launch state-of-the-art satellites for use by Radio Amateurs the world over. We provide educational programs that teach our young people about space and Amateur Radio. Most of all, we provide our members with an impressive array of member benefits including:

- Operating aides such as discounted tracking software and land line BBS.
- An extensive network of volunteers to provide you local technical assistance.
- The AMSAT Journal, your bi-monthly periodical devoted to the Amateur Space program.

It's Fun! It's Easy! It's Exciting!

JOIN TODAY. For more information, call or write for your free information packet. Or send your dues now, check or charge: \$30 U.S., \$36 Canada/Mexico, \$45 all else. (\$15 towards the AMSAT journal.)

AMSAT, P. O. Box 27, Washington, D.C. 20044

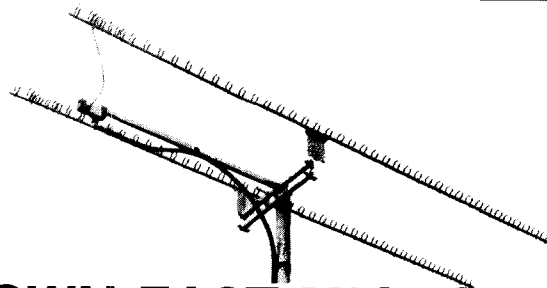
(301) 589-6062; Fax: (301) 608-3410

Empirically Speaking

Continued from page 2.

no one has a good handle on the interference from ISM to the amateur services, MSS or DAB. Until such studies show which services are compatible with ISM and under what circumstances, no one is eager to plan systems near 2450 MHz.

With the above uncertainties, the tendency would be to wait and see about the 13-cm band. Yet, according to the FCC's Order, the amateur services would still retain its secondary allocations in this band. It behooves us to do the necessary studies to determine the potential impact of new sharing partners and get a better grasp of operating in the presence of ISM interference. These questions aside, it would seem imprudent to delay developing amateur systems for the 13-cm band in view of the lower bands becoming more congested.—W4RI



DOWN EAST MICROWAVE

Amateur Microwave Antennas and Equipment

902, 1269, 1296, 2304,
2320, 2400, 3456 MHz

TROPO, EME, WEAK SIGNAL,
OSCAR MODE L, MODES,
ATV, REPEATERS

LOOP YAGIS, POWER DIVIDERS, COMPLETE ARRAYS
KIT FORM OR ASSEMBLED AND TESTED

SOLID STATE LINEAR AMPLIFIERS FOR 902 & 1296 MHz

Write for Free Catalog to:

DOWN EAST MICROWAVE

Bill Olson W3HQT, Box 2310 RR1
Troy, ME 04987 (207) 948-3741

