What's On 72-76 MHz?

By Ed Soomre

Located between television broadcast channels 4 and 5 is a unique portion of spectrum: 72-76 MHz. Its primary use is for point-to-point communications. Secondary uses include industrial low power two-way communications, radio call boxes and other specialized communications.

Frequencies are assigned every 20 kilohertz from 72.02-72.98 MHz, every 40 kilohertz from 75.42-75.58 MHz, and every 20 kilohertz from 75.62-75.98 MHz.

The FCC has designated this band for fixed operational stations in the aeronautical, public safety, industrial, land transportation, common carrier, and maritime mobile bands. Its use is subject to conditions of non-interference with TV broadcasting or other radio services, reduced transmitter output power, restricted antenna radiation patterns, and the use of proper emission.

BACK TO BASICS

Point-to-point communications between bases (control stations) and remote transceiver sites usually use two radio frequencies: the uplink frequency (base to remote transceiver) and downlink frequency (transceiver back to base). The remote transceiver is controlled at the base as if it were located right there.

Users of this band include Class C Citizens Band Radio Service for radio controlled aircraft, auditory training devices (used in institutional educational programs for handicapped persons), control of industrial heating equipment, radio communications developmental and test equipment and radio alarm systems (radio call boxes and fire alarm boxes).

Most likely the listener will hear the two major users: point-to-point communications (usually the downlink) and radio alarm systems. Highly directional antennas are used, but if the listener is located in the path between them, reception may be excellent.

Radio alarm system reception is best near a highway (for radio call boxes) or in a large metropolitan area (for fire alarm boxes). Most of these low-powered systems use omnidirectional antennas to transmit a series of tones for short periods of time. Many radio alarm system boxes are powered by batteries charged from solar energy.

Low-power industrial communications and paging can often be received near the factories or warehouses.

RECEIVING EQUIPMENT

The Regency MX5000 is an excellent receiver for this band, covering both AM and FM modes. Converters such as the Hamtronics CVR-72 can be connected to a conventional programmable scanner to receive this band in the 150-154 MHz range.

An omnidirectional scanner antenna (such as the Grove Omni II) can be used with very good results. For even better reception, a directional antenna (such as the Grove Scanner Beam II) and a preamplifier (such as the Grove Power Ant or Signal Amp II) is recommended since the antenna can be aimed at the transmitter location.

A citizens band or lc band ground plane can t used by cutting down tl radiator (vertical element and radials to approximatel 32".

HBO TO SCRAMBLE

Home Box Office (HBO) a leading pay TV satellit program source, has announced that it has begun shipment of its high-securit descrambling systems t authorized cable companie nationwide.

The present descrambling equipment is prohibitively expensive for individual subscribers to own, bu due to a new law, it wil become available in th future.

While the disappearanc of HBO from the quarry o home TVRO enthusiasts wil have an impact, there ar still approximately 80 channels from which home satellite terminals may choos other sources of entertainment.

The new scramblin system is considered th most advanced type o encryption outside of th Pentagon and is unbreakable or so say the developers a M/A-COM, a prominent encryption device manufacturer.

UNBREAKABLE CODES

by The Lazy Dog

(Ed.Note: Lazy Dog is a code name for this former member of the intelligence community. His credentials are unimpeachable and his personal insights reflected in this article are well worth reading. This two-part article will be concluded next month.)

From time to time MONITORING TIMES' editorials and features touch on the subjects of cryptology and secure telecommunications. These articles have been especially interesting to short-wave listeners, radio communicators, and to many of MT's general readers who are concerned with achieving message privacy. The contributors of these articles are to be commended in exposing subscribers to the general world of the classic cryptography of earlier years -- prior to the Korean War.

Such crypto-systems were, for the most part, simple substitution codes using paper and pencil manipulations. Some used random character generators whose outputs were joined with straight texts through the Vigenere tables to form decryptable gibberish (See MT, July 1984, p.13, "The Hawker and the OSS").

Later, super secret mechanical or electro-mechanical crypto machines were employed. Notable among these were the WWI German "Enigma Machine" and similar devices used by the U.S. military. Although the algorithm complexity of these boxes was of a high order they are, by today's standards of high-speed computer cryptanalysis, fairly easy to crack.

Crypto code clerks were instructed to defend these cipher methods, the code keys, and the machines with their lives -- never to let them fall into enemy hands.

Shortly after the Korean War, however, there came a renaissance in cryptography: the so-called "unbreakable" coding being used by government and industry today. Surrounding this science and technology are such buzz phrases as "pseudo-random algorithms based on the products of very large prime numbers," "trapdoor knapsack public key cryptosystems," "secure key distribution systems," "message authentication," and "the data encryption standard."

Yes, many of these modern cryptographic systems are truly unbreakable. And analysis by experts indicate that they will remain unbreakable even after cryptoanalytic attack by the successors to the very high speed Cray computers which may be postulated into the twenty-first century.

We make no apologies in introducing these esoteric subjects to MONITORING TIMES' readers; many are serious communicators who have personal and private requirements for absolute message security. We know that some among you already have at your disposal the hardware to encrypt and decrypt telecommunications using these modern techniques.

Our objective is to put you on the right track in obtaining the software necessary for their application. We hope to be able to direct you toward some simple means of "getting on the air," as well as encourage you to participate in and contribute to ongoing cryptographic development.

But first, let us examine some paradoxes and observations regarding the subject.

With the coming of the home computer microprocessor and its associated modem, the ordinary citizen may send messages in secure form without fear of their being compromised upon interception. Of course, there must be similarly programmed personal computers (PC's) on both ends of the circuit in order to effect the encryption and decryption process. But with the wide usage of home computers these days, soon virtually everyone will possess these means.

This is not a subject directed particularly t computer wienies or cryptie groupies, but to communicators. And that means almost anyone. Anyone who uses a telephone, or common carrie circuits, domestic anc international. Anyone wh uses a short-wave radio. Anyone who uses the mail.

A LITTLE PHILOSOPHY

Who said we necessarily have to transmit our encrypted messages by wire? We can encrypt onto the printed page or onto floppy disks or magnetic tape cassettes or even onto EPROM microchips and mail them tc Aunt Agatha in Prairie Junction for her to decode using the kitchen computer.

Incidentally, there are some ancient regulations in the United States and elsewhere intended to prohibit the general public use of encrypted messages on short-wave circuits, amateur and citzens band radio. Many radio teletype (RTTY) enthusiasts ignore these regulations, however, and go right ahead and use encryption on the airways. There has not been a serious U.S. test case in years wherein the use of cryptographic messages alone has caused the communicator to be "busted."

There have been a few cases wherein heavy handed U.S. bureaucrats have

☞

attempted to harass or intimidate users of encrypted radio transmissions. Those users who have stood up on their hind feet, however, and have said, in effect, "up your nose with a rubber hose," have found that the bureaucrats curl up and skulk away, never to be heard from again.

The general consensus among constitutional lawyers, and even within the U.S. Justic Department, is that these prohibitive regulations are outmoded, unenforceable, unconstitutional and contrary to our general concept of freedom of speech and privacy; and hence should be stricken from the books.

There are no prohibitions against transmitting messages in the Gaelic, Fijian, Swahili, or Serbo-Croatian languages. Cryptography is just another language; albeit a language wherein means are taken to seal its contents from unwanted intrusion.

The right to encrypt is a basic human right. Just as is the right to life, liberty and the pursuit of happiness. The use of encryption does not necessarily imply subversion, moral turpitude, of nefarious activity. Don't let anyone tell you otherwise. In this day and time of rampant interception, one almost has the obligation to encrypt.

We have heard it said now and again that, "If I've done nothing bad, who cares if my messages are intercepted and read; I've got nothing to hide." This, of course, is a silly, simplistic argument by the Pollyannas of the land. Everyone has something to hide, else we would not have window shades.

Information is power; and if we give it away to those who might use it against us, or who may wish to intimidate us -- even information which is seemingly innocuous -- we defraud ourselves. We hereby encourage all readers to encrypt whenever practicable.

That is the key word of this treatise: practicable. Never before in the history of man has the ordinary citizen had at his disposal a relatively inexpensive, swift, and practicable means of sealing his written communications, telegraphic or otherwise, from the unwanted intrusion of high institutions and governments.

Two technologies in conjuction have fallen together in this new age, providing the practical application of truly private communications. One is the wide-spread possession of home computers by ordinary folk. The other is the development of the "unbreakable" cipher systems.

PARADOX NUMBER ONE:

How can I, with my little Radio Shack Computer, my Apple IIe, my Commdore 64, my IBM PC or whatever, begin to pit my miniscule encryption capability against the multi-million dollar, nano-second, number crunching main frames of the big boys and still maintain secure communications?

"That's just it," said a noted cryptanalyst of current industry, "the code makers have far outrun the code breakers." You, with your little peanut whistle, can blast the Goliath nasties right off the map. Such is the nature of the new cryptology.

The Philistines of big government for several years tried to keep the mathematics of modern encryption out of the hands of the public. Tough knobs! "The Genie is out of the bottle, and you can't stuff him back," remarked a Ph.D.-type crypto specialist. It is rather like trying to put a Top Secret stamp on the multiplication table!

PARADOX NUMBER TWO:

The crypto systems of yesteryear were highly subject to compromise and cracking should an adversary capture your coding method, your crypto-machine, or your algorithm. The new systems, though infinitely more secure, are not compromised if the "other side" gets hold of your machine, or even gets hold of your encryption program! How do you like them apples?

One could actually give the plans of his crypto-machine and the cipher programs to the Soviets, the NSA, your mother-in-law, or the little boy who lives down the lane; and still, your code can't be broken -- even by the brainy guys who devised your system. This is provided, of course, that you do not give away the decryption key which you may devise and change now and then -- grade "B" movies to the contrary!

NEXT MONTH: How to get started in cryptography

INCLUDES 800 MHz COVERAGE
Regency hand held scanners
bring you all the action... wherever you are!
HX1000
HX2000
HX750
HX650