BY DON ROTOLO,* N2IRZ

D-STAR Digital Data, CryptoUP

More Encryption and D-STAR Digital Data

Until now, all of my D-STAR experience has been in DV (Digital Voice) mode, which is quite similar to conventional FM repeater operations. Recently, the NY City D-STAR repeater installed a DD (Digital Data) repeater module, opening up a new and exciting mode for digital operations.

DV mode uses a relatively narrow (6 kHz) occupied bandwidth for FM-quality digital voice communications. You can send short (20 characters maximum) text messages, most often used for station information (for example, mine says, "Don N2IRZ near NYC") and low-rate (about 950 bits/sec) data on the DV signal. The repeaters are intelligent, and many of them are gatewayed to one another, meaning that crossband local contacts as well as contacts through other D-STAR repeaters worldwide are easy and commonplace.

DD mode turns your D-STAR radio into what can be thought of as a 10-watt wireless network adapter. The data rates are modest by modern broadband standards—128 kb/s raw throughput—but way faster than any dial-up modem. The DD repeaters that I have read about all offer essentially unrestricted access to the public Internet, much like the WiFi connection at Starbuck's, allowing web and e-mail access. D-STAR, by gatewaying into the Internet, has become almost everything the AX.25 packet radio network always wanted to be—albeit using wires.

This month we'll go through the details of configuring your computer and radio to operate in DD mode. Before we start, however, some caveats: I am running Windows® XP Pro, using an ICOM ID-1 D-STAR radio, and the K2DIG repeater I use was down when I wrote the final version of this column. If you are using a different operating system and/or D-STAR radio, or if my notes and memory are failing, you may need to do things a little bit differently.

If you run into trouble, I recommend logging on to <http://www.k5tit.org/>, the website of the Texas Interconnect Team. I have found this website to be the best source of D-STAR information out there. Not only are the tutorials accurate and useful, the folks on the forum are genuinely helpful and full of the famous Texas friendliness.

The following assumes you are familiar with your D-STAR radio in DV mode, there is a local repeater with a DD mode repeater in place, and you have a computer with networking enabled (that is, it has an Ethernet connection and a web browser).

The first step is to make contact with the local repeater operators to have your callsign registered with the DD mode repeater control system. Since we're operating on amateur radio frequencies, we need some sort of access control to prevent unauthorized users. The way this is implemented in our case is to have all authorized callsigns registered, and a static IP (Internet Protocol) address assigned for each callsign. This is very different from most broadband connections, which assign an IP address on-the-fly from a pool of addresses available to that service provider, a service known as DHCP (Dynamic Host Control Protocol).

The repeater operator needs to confirm that your callsign is registered and provide you with your unique IP address, along with telling you the gateway and DNS server IP addresses they are using. For example, on K2DIG, the callsign N2IRZ is associated with the IP address 10.60.xxx.xxx (real address obscured for security reasons), and both the gateway IP and DNS IP addresses are 10.0.0.1, following the K5TIT standard.

I disconnected the regular network cable from my main computer and connected a 10Base-

*P.O. Box 114, Park Ridge, NJ 07656
e-mail: <n2irz@cq-amateur-radio.com>

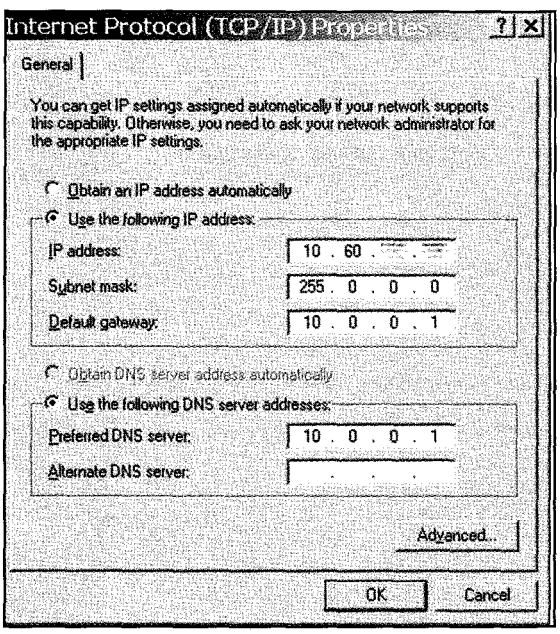


Fig. 1– The Network Connection Properties screen. D-STAR Digital Data mode requires a static IP address, and this is where you can set your computer for that. You need to obtain and verify the correct settings with the repeater operator.

Visit Our Web Site

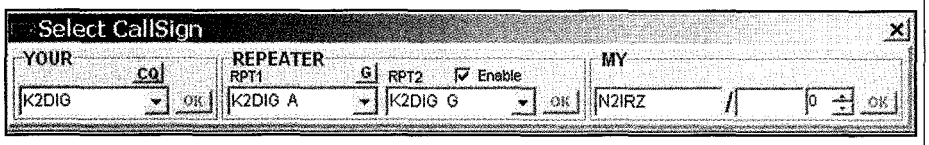


Fig. 2– The ID-1 Callsign Settings window. Again, verify the correct settings with your repeater operator. These must be set correctly or nothing will work.

T (CAT-5) cable to the ID-1. Be careful, because the CAT-5 cable end is the same as used for the microphone; the Ethernet connector on the radio is on a short pigtail wire coming out the back.

With the regular network disconnected, I reconfigured my network connection to account for the static IP address and DNS server. To get to this screen I opened up the Control Panel, selected Network Connections, right-clicked on the "Local Area Connections" entry, and selected "Properties" from the pop-up menu. I then selected "Internet Protocol (TCP/IP)" and clicked on the Properties button. After writing down the existing settings (so I could get my regular Internet back!), I selected the "Use the following IP address" radio button and filled in the three entries as shown in fig. 1. I also selected "Use the following DNS server address" and entered the "Preferred DNS server" IP address provided by K2DIG. When I was done, I clicked OK and then Close to memorize the settings.

Next I configured the ID-1 to operate in DD mode, using the Windows®-based ID-1 software. While I am sure it is possible to configure the ID-1 via the front panel, only try this as a last resort, and even then, have the manual and plenty of time.

When I traded e-mails with the folks at K2DIG, I also asked for the frequency of the DD repeater, which is 1253.000 MHz. Therefore, the first thing I did was set the proper frequency. I also stored it in memory, but this is optional. Next I set the operating mode (using the MODE button) to DD, at which point the TX Inhibit indicator is switched on. If this is not on, click on the "TX inh" button; you don't want to start transmitting until everything is properly configured!

Although this is a simplex repeater, the ID-1 has two different settings for simplex operation: RPS (*Repeater* Simplex) and *ordinary* simplex. In RPS mode the ID-1 expects to be communicating with a repeater, since it trades important operating information with the repeater. If you are using DD mode with a DD repeater, set the repeater mode (using the RP button) to RPS, while if you are using DD mode directly with another D-STAR user, use the standard simplex setting (as opposed to RP+ and RP–, which are duplex).

Finally, I set the various callsigns. Working from left to right, the YOUR callsign is the repeater's—K2DIG. The RPT1 callsign is K2DIG A, since I am accessing it on a 1.2-GHz port (other letters are used for other bands). RPT2 must be enabled, and that has the gateway port's callsign, K2DIG G. Last is MY callsign, N2IRZ.

With the radio properly connected to the computer, the network connection monitor (to get to this screen, open

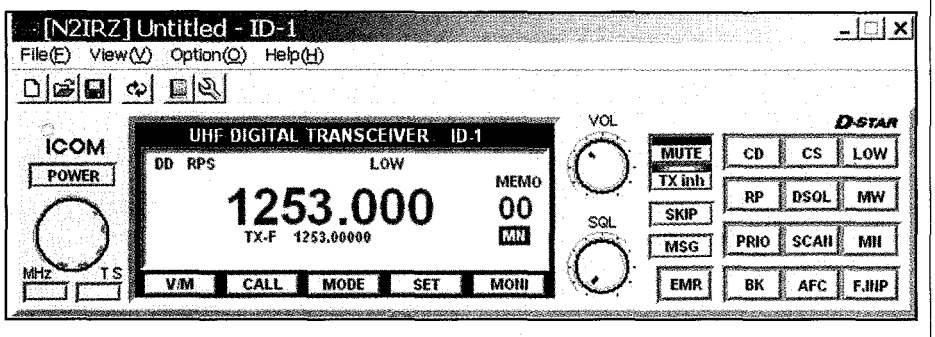
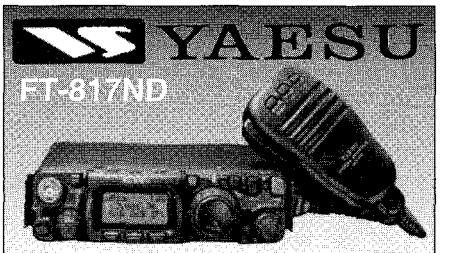
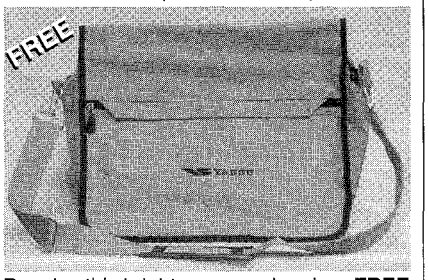


Fig. 3– The front panel of the ID-1, as seen in the Windows® control application. Note the DD and RPS indicators, which confirm Digital Data and Repeater Simplex modes, respectively. Even though the DD repeater is simplex, it is a repeater and the radio expects to be able to exchange control information with it. Also note the green "TX inh " indicator, which shows that the radio will not transmit until the inhibit function is released.



The **Yaesu FT-817ND** is an improved, deluxe version of the hugely popular FT-817. It includes 60 meter coverage plus the new high capacity FNB-85 battery. The radio is a fully self-contained, battery-powered, low power amateur MF/HF/VHF/UHF transceiver. Great for portable QRP operation!

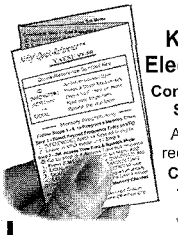


Receive this bright orange urban bag **FREE** with your FT-817ND from Universal Radio. Visit **www.universal-radio.com** for details!

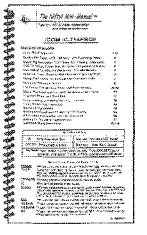
universal radio inc.

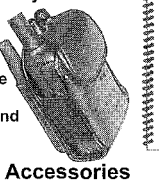
Universal Radio
6830 Americana Pkwy.
Reynoldsburg, OH 43068
◆Orders: 800 431-3939
◆Info: 614 866-4267
www.universal-radio.com

Radio Setup Guides



Short Form Guides For:
Kenwood, Icom, Yaesu, Elecraft and Ten-Tec Radios
Condensed step-by-step procedures Simplify Setup and Operation
Available for most recent model radios.
Color printed and fully laminated.





Complete line of Leather & Neoprene Radio Gloves and Pouches for HT's and other radios.

Nifty! Ham Accessories
1601 Donalor Drive • Escondido, CA 92027
(760) 781-5522 • www.niftyaccessories.com

Ham4Less.com
ARROW Satellite Antenna
$55.00
800-230-0458
www.Ham4Less.com
"Your Online Discount Store"

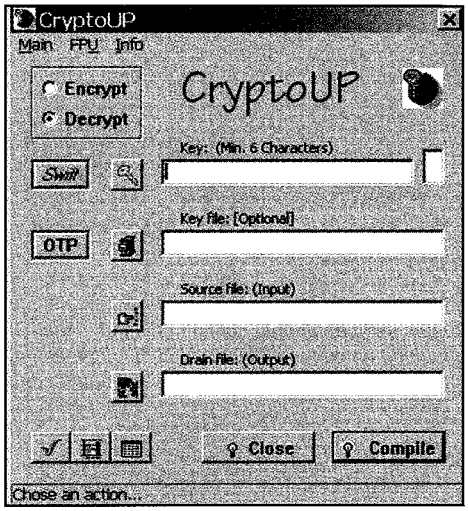


Fig. 4– The main window of CryptoUP, written by Paul-Adrian Braissant, HB9CUF. The encryption and decryption of files is made as easy as possible. While the NSA can break the encryption, your average hacker will have a hard time with it.

Control Panel/Network Connections, double-click on "Local Area Connections") will indicate a connected state, at 100 Mbps (at least on my PC), and a count of the packets exchanged with the radio. Note that this status is between the computer and the radio, not between the radio and the DD repeater. You can reset the packet count by clicking Disable, and then Enable. If this is not showing a connected state, check your Ethernet connection.

With everything configured, we can try the big test: First, enable transmit by clicking on "TX inh" to switch off the indicator. The ID-1 will start transmitting very short bursts almost immediately. Then open a browser window. After some delay (because of the data rate) the page should start loading. Your repeater trustees may have made certain websites unavailable, so if your regular home page doesn't come up, try <www.arrl.org> or some other ham-friendly site.

When I first tried this, it did not work. As a matter of fact, it took several tries to get it working. The first problem was that I had set the radio to regular simplex instead of RPS. Next, I had inadvertently lost the "G" on the RPT2 callsign, as well as having the wrong callsign in the YOUR field. The last issue was the most difficult to diagnose: The repeater was off the air (as I mentioned earlier) because of a bad antenna connection. It was a good thing I had reached out to a local DD-mode user (while trying to address the settings problems), who confirmed for me that DD wasn't working at the moment. I initially thought I was going insane, as I checked and rechecked, everything was set perfectly, and it had worked before!

If you need assistance in troubleshooting, your first step should be to reach out to the repeater folks, or another local user. Check the online resources as well. Don't be discouraged by failure. When you're on the edge of technology sometimes things just don't work.

Now is probably a good time to talk about a concept I learned as a Novice: Who pays? The racks of repeaters, amplifiers, computers, the associated equipment, and even the political goodwill used to acquire the site don't come for free. Someone, somewhere, pays for it all. Like a heavy load, many hands (or wallets) makes for a lighter burden. If you are or become a regular user of a repeater, make the effort to reach out to the repeater trustees and offer to share some of the burden. Cash is good, but if money is tight, offer your assistance, even if it's just sweeping the floor after a maintenance session. It's the right thing to do.

More Encryption

Back in August 2006, I presented my case for encryption sometimes being permitted under Part 97 of the FCC rules. Just a few months ago, the ACA (Australian Communications Authority, similar to the USA's FCC) created a new rule allowing amateurs in that country to encrypt communications for the purpose of obscuring their meaning in three specific circumstances: remote control of an unattended station, telecommand of a satellite, and during emergency communications. I am pleased to see that Australia's licensing and rulemaking agency has seen fit to explicitly permit these kinds of operations.

After the August 2006 column, several hams brought other aspects of encryption to my attention—for example, TWISTER (April 2007). More recently, Paul-Adrian Braissant, HB9CUF, wrote to me to introduce a more general file and data encryption application, which he named CryptoUP.

CryptoUP is an application that runs under any 32-bit Windows® version (meaning Windows® 95 or later, even Vista). You start the application, specify an encryption key, pick the input file and type an output file name, and click "Compile." A fraction of a second later the encrypted file is ready. There is an optional feature that breaks up a file into five-character groups, a technique commonly used for RTTY and other HF transmission modes.

After downloading the file (a 4.5 MB zip file, or a 1.5 MB compact install file) from <http://www.geocities.com/cryptoup/>, unzip it to a temporary directory and run the .EXE file within. The InstallShield Wizard takes you through the installation in a comfortable and convenient fashion. Installation takes under a minute and consumes less than 2 MB of hard-disk space. Two applications are installed: CryptoUP and FindSR, the latter being a utility to analyze encrypted files, for which I did not find a need.

After starting the application, you minimally need to type in a key, the input file, and the name you'd like for the output file. Select "Encrypt" and click Compile. It really is that easy, but if you like, you can also select several options to optimize the application for your purpose.

The key is, well, the key to the whole process. If you encrypt a file, and then lose the key, there is simply no easy way to recover the file. It's gone forever. Be sure to select a key that is not only memorable, but one that is not easily guessed—not your callsign, for example. I could go into a dissertation about selecting a strong key, but instead some useful features can ease this burden.

First of these features is the use of a Key File, a file that is about the same size as the file to be encrypted—too short and the encryption is not as strong. A unique secondary key is synthesized from the contents of the file, and this process is repeatable. If you know the other party has a copy of the file, you can send the primary key in the open and simply tell the other party the name of the file you used to generate the key.

Second is the OTP (One Time Pad) feature. OTP refers to the practice of creating a file of single-use keys, each of which is discarded after a single use. Both parties have a copy of all of the keys, and they need to keep track of which ones have already been used. The term comes from a pad of paper, which has a key written on each page. Once the key is used, the page is removed and discarded, revealing the next key.

Last, you can also insert a key extension character. This allows you to use the same key several times, but with a different digit or letter at the end. Unauthorized parties can decrypt a file more easily if they have several files that use the same key; changing the extension helps minimize this risk.

There are also three levels of encryp-

tion: reasonable, good, and top. The higher the encryption level, the more time it takes to compile the file. This is selected using the "Swift" button, which has a unique, three-level functionality. If you use the OTP function, this one is disabled.

The main menu allows all functions to be performed using the keyboard and as shortcut keys, if a mouse is unavailable. The FPU menu offers some options for the computer's Floating Point (math) Unit. Although the default settings are perfectly adequate, some advanced users may want to fiddle with the settings to alter how the application does its calculations. The info menu simply shows the version of CryptoUP.

At the bottom, a single button will convert a file from its regular form to five-character groups. Note that this does not encrypt the file, so make sure you do that first. On receiving the file, press the same button to bring it back to normal format and then decrypt it.

Even though this application is very simple to use, I do miss having a help file. There is a text help file, but it doesn't really discuss how to use the application, or explain any of the concepts and how to put them to best use. I have asked Paul-Adrian to consider expanding the help file, so that may have been implemented by the time you read this. All things considered, it's not too difficult to figure out either.

CryptoUP is a handy utility for encrypting files. Unlike TWISTER, which is useful only for text messages, CryptoUP can be used for images, MS Word® files, spreadsheets, and even programs and applications. For emergency management situations, maintaining the privacy of people identified in the information you need to transmit can be accomplished quickly and easily without worrying about the file format. As we well know, a minute saved could make all the difference.

D-STAR DD mode won't replace my cable modem connection, but if the power goes out or the cable fails, I know that I can still access the Internet, particularly for emergency communications. Even my regular e-mail system works, albeit slowly, so there is no learning curve. Here in northern New Jersey it is not unusual to have a situation affecting the local area while the folks in New York City (where K2DIG is located) are doing just fine. It's nice to know D-STAR has this capability. Also, if I need to send data files, if they need to be encrypted, I now have a convenient way to do this. Until next time . . .

73 de Don, N2IRZ