HOW YOU CAN INTERCEPT SECRET MESSAGES BEING SENT TO SPIES

W2MIL

Believe it or not, there are powerful radio stations all over the world sending out messages to spies every day, and you can hear them with an inexpensive shortwave radio and a simple antenna. You probably won't be able to decode them, but it's a real kick to tune into these clandestine signals.

Figure 1 shows the 60 year old shortwave radio I found on eBay to begin my search for the secretive numbers stations. They are called numbers stations because they verbally send out a series of numbers in groups of five, like "two, five, four, seven, one," or in Spanish," dos, cinco, cuatro, siete, uno, etc."

FIGURE 1. This vintage Hallicrafters S-38E shortwave radio picked up secretive numbers station HM01 in Havana, Cuba on 11635 kHz.

The spies hear them and copy down the ones addressed to them. Everyone else can hear them too, but only the spies know how to decode them.

They are broadcast in many different languages including Spanish, German, Russian, English, and Morse code, depending on who they're trying to reach.

The audio printout in **Figure 2** came from a station in Cuba and the Morse code in **Figure 3** came all the way from Russia.

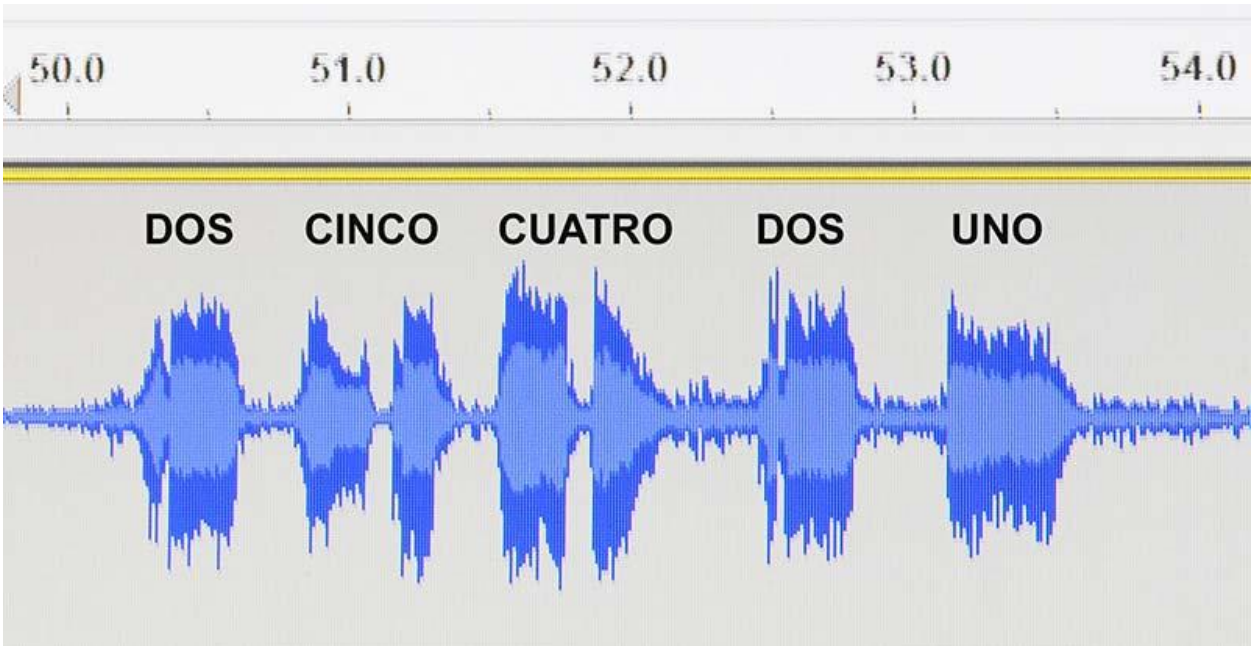


FIGURE 2. Audio printout of typical Spanish numbers received from station HM01 in Cuba.

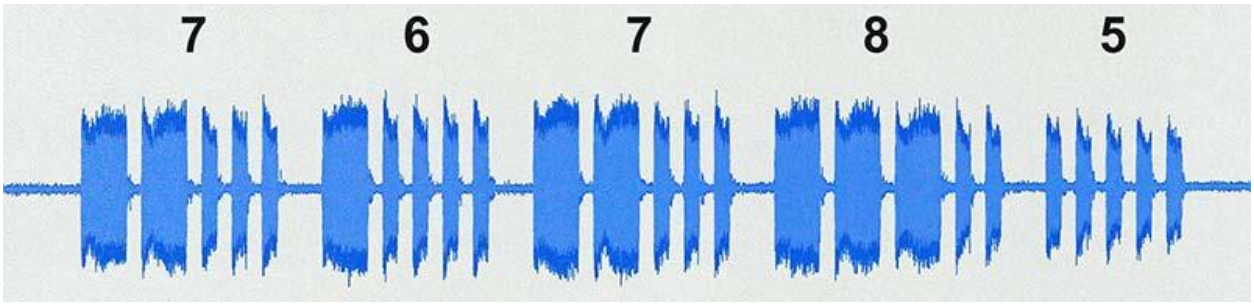


FIGURE 3. Audio printout of Russian station M12 using Morse code on 13481 kHz at 02:50 UTC.

PRIYOM.ORG

On the Internet, there's a website called **priyom.org** that you have to check out. It's dedicated to finding and listing every numbers station in the world. For years, a group of volunteers have taken it upon themselves to spend countless hours searching for and recording broadcasts throughout the world.

Their incredible website contains an extensive listing of the schedules, formats, and frequencies of dozens of stations. Many listings have a short recording of what you can expect to hear.

THE START OF MY ADVENTURE

Based on the **priyom.org** listings, I chose to start my spy-listening adventure with a station called HM01 which was located in Havana, Cuba. It transmits multiple times every day in Spanish.

Initially, I wondered, “How in the heck could I pick up a station 2,200 miles away from Southern California?” Actually, it turned out to be easier than I thought. The weekly schedule for HM01 is listed in **Figure 4**.

CUBAN NUMBERS STATION SCHEDULE
Station Identifier: HM01
Location: Havana, Cuba
Sponsor: Cuban DGI (Dirección General de Inteligencia)
Voice: Spanish, Female
Schedule: 11 hours/day, repeated on half hour
Frequencies: 9065 to 17480 kHz, depending on time and day
Start of each transmission: 3 minutes of voice, then tone, RDFT
Emission mode: AM and RDFT(Redundant Digital File Transfer)
For complete transmission format: See Priyom.org
To convert other time zones to UTC please use Internet
Adjust for Daylight Savings time as req'd

SCHEDULE			Mon, Wed Fri, Sun	Tue, Thu Sat
UTC Time	PST USA Time	EST USA Time	Freq (kHz)	Freq (kHz)
00:00 -04:00	4-8pm*	7-11pm*	------	------
05:00	9pm*	12 Mid	10860	11462
06:00	10pm*	1am	10345	14375
07:00	11pm*	2am	9330	13435
08:00	12 Mid	3am	9065	11635
09:00	1am	4am	9240	11462
10:00	2am	5am	9155	12180
11:00-15:00	3-7am	6-10am	------	------
16:00	8am	11am	11435	11435
17:00	9am	12 Noon	11530	11530
18:00	10am	1pm	11635	11635
19:00-20:00	11-12Noon	2-3pm	------	------
21:00	1pm	4pm	11635	16180
22:00	2pm	5pm	10715	17480
23:00	3pm	6pm	------	------

* if Mon in USA, use Tue frequency
* if Tue in USA, use Wed frequency
* etc.

FIGURE 4. Weekly schedule of Cuban station HM01. Transmissions repeat on the half hour, day and night.

SPOILER: *DO YOU WANT TO HEAR A SAMPLE OF THE SECRET MESSAGES THAT I INTERCEPTED?*

In the downloads for this article, there's a 1:40 minute MP3 recording of several of the stations that I found and recorded over a several week period.

BUT FIRST, THE VINTAGE HALLICRAFTERS RADIO NEEDED TO BE MODIFIED A BIT

The radio from eBay was in good condition, but its basic design incorporated a major electrical hazard. Many tube radios from that era did not use expensive power transformers. Instead, they powered the filaments and high voltage directly off the power line.

In many cases, one side of the line was physically connected to the chassis. This created a situation where the chassis could become electrically HOT.

To counter this, the manufacturers completely isolated the metal chassis by using plastic or wooden cases, plastic knobs, and fiberboard panels to prevent the customers from ever touching the chassis.

Luckily, there are easy ways to fix this hazard, like upgrading the original two-prong plug to a modern three-prong plug. Mr. Carlson's Lab has several excellent episodes that you should watch before servicing or restoring this type of vintage five-tube radio.

In the end, I elected to install a three-prong grounded plug, rewire the on/off switch, and add a small dedicated 30VA isolation transformer. You can see the transformer hanging out the back in **Figure 5**.

I also replaced all the old electrolytic and paper caps and aligned the IF. Easy, peasy!

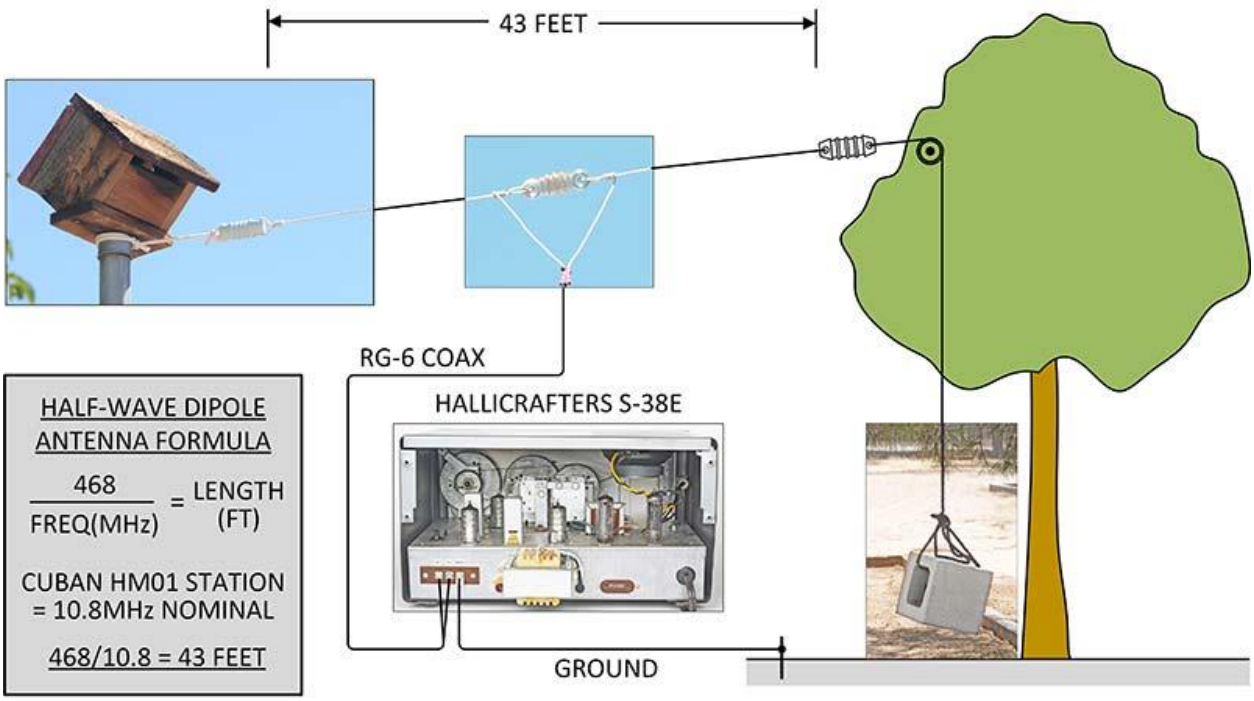


FIGURE 5. A dipole antenna is simple to set up. A good ground connection is a must.

TIME TO BUILD A CLASSIC DIPOLE ANTENNA

Now, it was time to string an antenna in my backyard. I calculated its length for the nominal frequency of the Cuban station and also planned to raise it a quarter wave off the ground.

So, I grabbed some insulators, ropes, a hank of #12 house wire, RG-6 coax, a pulley, and lastly, a block of concrete. Refer to **Figure 5** for the finished result.

I went for a dipole because I had the space, but a long piece of wire (20-50') hanging out a window would probably be enough. You also need a ground wire connected to the radio to get good reception.

It can be as simple as attaching a wire to a cold water pipe or laundry faucet in the house. Or, you can get fancy and drive a stake in the ground and hook it to that.

READY AT LAST

On that first night with the Hallicrafters on my desk and the antenna wires coming through the window, I clamped on the headphones and tuned to 11462 kHz at exactly 10:00 pm local. Nothing! Just a bunch of noise ... shhhhhhh! I had previously listened to the sample audio on the **priyom.org** website, so I knew what it should sound like. My imagination was running wild.

After 10 minutes, I was ready to quit when I heard a very faint, “ocho, uno.” I could hardly believe it! It quickly faded away, but I kept listening and after a few seconds it came back again, still very faint. In and out it went for about 10 minutes, then only shhhhhhh. I was gassed!

Over the next several weeks, I checked all the frequencies and times listed in **Figure 4**. On some days, the Spanish numbers were very clear and on other days the signal was lost in the noise. I recorded the best ones to prove that it wasn’t just my imagination. So, what now???

MAYBE I COULD DECODE THE NUMBERS

After reading on Wikipedia about how the numbers stations encrypt their messages, I learned that it was impossible to decode them. In fact, even using the fastest quantum computers working until the end of time would be futile. The crazy thing is that it only took two little pads of paper and a pencil to make an absolutely unbreakable code. I’ll explain how it works in a minute.

First, I want to touch on an encryption technique that many of you are probably familiar with.

It’s called the substitution method: A = F, B = Q, C = K, etc. It looks tricky, but this encryption can easily be broken by using frequency analysis. For example, the most repeated letters in the English language are E and T, so you look for which letters appear the most and go from there.

Substitution ciphers have been around since the days of the Romans. In fact, one of the most famous is called the Caesar cipher, named after Julius Caesar who used it for his private correspondence. It simply shifted the whole alphabet over by some number like four. Very easy to break.

You might remember the Little Orphan Annie decoder pin (**Figures 6** and **7**) used by Ralphie in the holiday TV movie called *A Christmas Story*. I saw one on eBay and had to have it. It was a cool little device that rotated, so you had to know where to set it to start. In the movie.


N
O
R
P
Q
S
U
T
20
21
22
23
24
25
26
1
2

FIGURE 6. The Little Orphan Annie Secret Society decoder pin used a substitution cipher to decode secret messages. It rotated to set up the initial key.

FIGURE 7. This little gem was produced in 1940 to decode messages at the end of each Little Orphan Annie radio show sponsored by the Ovaltine Company.

Ralphie's favorite radio program always ended with a secret message that used the decoder pin to read it. The announcer told the listeners to set the decoder to B-2. Then, Ralphie breathlessly decoded the secret message but was disappointed when the message was nothing more than "a stupid commercial" for the sponsor of the radio show.

HOW THE REAL SPIES DO IT

Real spies use what is called a One-Time Pad (OTP), filled with random numbers. Refer to **Figure 8**. The technique was first described in 1882 and mathematically proven to be unbreakable by information theorist Claude Shannon. It only takes two identical one-time pads: one for the sender and one for the receiver, plus some simple modular arithmetic to do it.

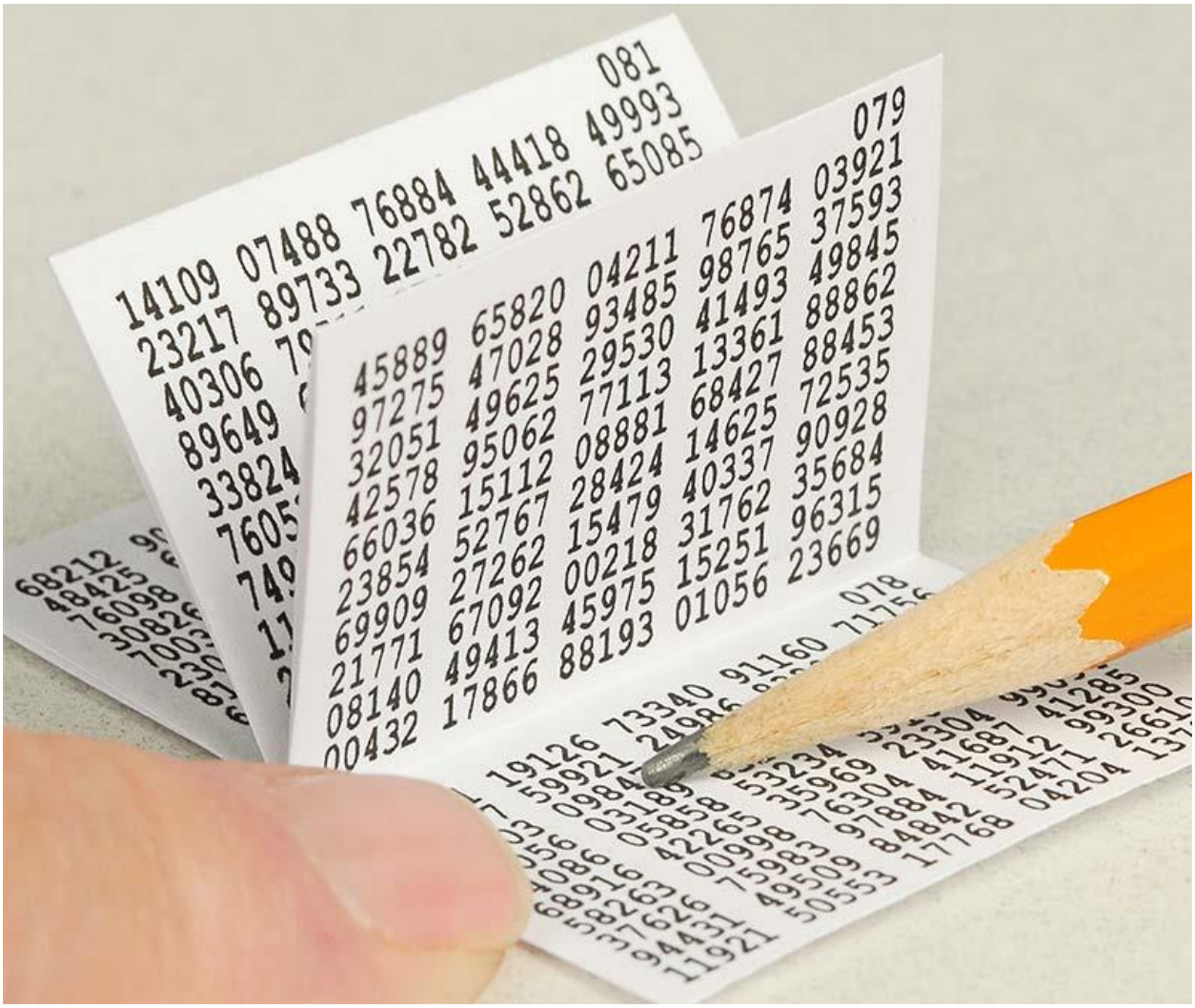
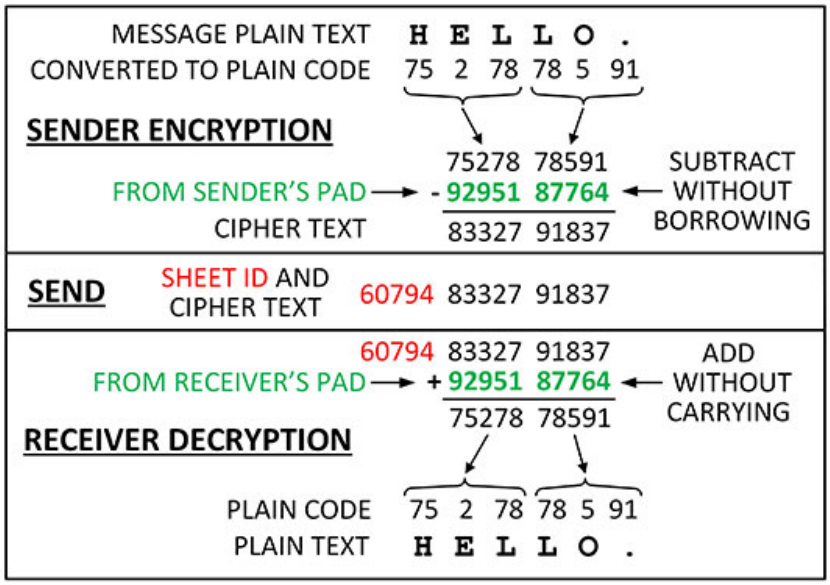


FIGURE 8. Both sender and receiver had identical copies of tiny One-Time Pads (OTPs) filled with random numbers. OTPs were small enough to be easily concealed.

Figure 9 shows an example of how “HELLO.” is encrypted and decrypted back again. At the bottom of **Figure 9** is a challenge for you to decode a very secret message. If you can do it, you might consider applying for a job at the National Security Agency (NSA) in Maryland.

EXAMPLE OF UNBREAKABLE ENCRYPTION AND DECRYPTION OF A MESSAGE USING A ONE TIME PAD



SECRET ONE TIME PAD OF SHEETS
CONTAINS TRUE RANDOM NUMBERS
(BOTH SENDER AND RECEIVER HAVE COPIES)

60794	92951	87764	23674	85130
23291	89851	59590	05498	08724
75112	33460	04787	40444	44243
38540	01912	33638	17807	47330
64953	96824	74726	67340	22814
96913	09346	97367	12906	23333
91118	34729	83530	27216	98642
27493	69151	68749	20557	60122
44632	77372	32570	53763	49359
85680	39089	15279	46672	04429

DESTROY SHEET AFTER ONE USE

LETTERS-TO-NUMBERS CONVERSION TABLE
(BOTH SENDER AND RECEIVER HAVE COPIES)

CODE-0	B-70	P-80	FIG-90
A-1	C-71	Q-81	(.)-91
E-2	D-72	R-82	(:)-92
I-3	F-73	S-83	(')-93
N-4	G-74	U-84	( )-94
O-5	H-75	V-85	(+)-95
T-6	J-76	W-86	(-)-96
	K-77	X-87	(=)-97
	L-78	Y-88	REQ-98
	M-79	Z-89	SPC-99

FIGURES, SUCH AS 411, ARE CONVERTED TO 90 444 111 111 90 BEFORE ENCRYPTION

CHALLENGE: CAN YOU DECRYPT THE CIPHER TEXT BELOW USING THE SIX UNDERLINED GROUPS OF NUMBERS ON THE SHEET ABOVE? THE 60794 IS THE SHEET ID AND DOES NOT NEED DECRYPTION.

CHALLENGE CIPHER TEXT: 60794 80972 60024 35818 73487 63151

FIGURE 9. See if you can follow the encryption and decryption process, then try decoding the challenge cipher text at the bottom.

The reason an OTP cipher can never be successfully attacked is that the numbers on the pads are truly random. There is no magic algorithm to find. No seed. The only way to attack it is by the brute force method. Unfortunately, this leads to an output of every possible message, intermingled with a ton of garbage.

For example, during a brute force effort, the output might produce, MEET AT 06:30. But the attack would also find MEET AT 07:30, 08:30, 09:30, 10:30, etc. There would also be MEET AT THE MARKET and MEET AT THE RIVER. Which one is correct?? There is no way to tell.

TRULY RANDOM OR PSEUDO-RANDOM NUMBERS — WHAT'S THE DIFFERENCE?

Truly random numbers are what make OTPs work. My computer can generate random numbers at the stroke of a key. However, we know they aren't really random. They're generated by an algorithm that produces pseudo-random numbers. They look random, but if you start with the same seed, the computer will always generate the same series of numbers. Not good!

Luckily, there are natural events such as radioactive decay and shot noise that are truly random. For example, Geiger counters go tic....tic tic tic....tic tic. If you sample the tics, truly random numbers can be generated. These days, there are hardware random number generators available that use noise sources to generate true random numbers.

There is another way that you, personally, can generate a fairly good stream of random numbers if you ever want to communicate with your friends in absolute secrecy. **Figure 10** shows 10-sided dice which are available at gaming stores for a few bucks. Just be sure to throw them against a backboard and read them from left to right, so you don't interject any bias in your readings.

FIGURE 10. Ten-sided dice (pentagonal trapezohedrons) can produce random numbers if you want to send unbreakable messages to your friends.

WHY ARE NUMBERS STATIONS EVEN AROUND?

Back in World War 2, there was a need to send orders to resistance fighters in occupied countries and also to secret spies. One way to do that was to send out coded messages using high-powered shortwave radio stations located hundreds or thousands of miles away. The messages were sent at certain times and on certain frequencies. They were usually repeated several times and on different frequencies in case the reception was not that great. Only ordinary shortwave radios were needed to receive them.

Tiny OTPs were provided to the agents to decode the messages. They were small enough to be hidden in cigarette lighters, ashtrays, and fake batteries. Some were printed on highly flammable nitrocellulose flash-paper for easy destruction.

In fact, a spy named Colonel Rudolf Abel was arrested and convicted of espionage in New York City in the 1950s and was found with OTPs in his possession.

Today, many countries still communicate with their operatives using numbers stations. Although, some transmissions contain high-speed encoded data streams too, not just numbers. The **priyom.org** website lists the various formats of each station.

HOTLINE BETWEEN WASHINGTON D.C. AND MOSCOW

In 1963, a hotline was established between Washington, D.C. and Moscow, but it wasn't a red telephone as depicted in the movies. It employed special teletype machines that used a one-time punched paper tape system similar to OTPs (see **Figure 11**). When the hotline was initially set up, each country prepared pairs of one-time punched tapes and sent one physical copy to the other country via the secure embassies.

FIGURE 11. Teletype machine used for the Washington D.C. to Moscow hotline in the 1960s. *Photo by Jim Kuhn at Lyndon Baines Johnson Library*.

To send a message to Moscow, Washington would enter the plain text and their one-time tape into the outgoing teletype machine where it would be combined and encrypted. The cipher text output would then be transmitted to the Kremlin over commercial telephone lines, including through the transatlantic cable.

In Moscow, they would enter the incoming cipher text and their copy of the one-time punched tape (provided earlier by the US) into their incoming teletype machine. The

printed output would display the original message in plain English text. Finally, they would translate it into Russian.

The beauty of the system was that neither country had to share classified algorithms. The countries only had to supply a paper tape containing a form of random numbers that was only good to decrypt the current message, then never used again.

Over the years, the hotline system has been upgraded many times and today it uses satellites, fiber-optic cables, and computerized encryption systems. No more punched tapes.

BACK TO THE SEARCH FOR MORE STATIONS

Now that I had nailed the station in Cuba, I wanted to hear others. Perhaps something from Russia. So, I started looking for a better receiver — especially one with a digital frequency readout. I soon found ads for beautiful receivers like the ICOM R8600, with its awesome waterfall display, that cost thousands of dollars. Yikes!

On eBay, I found the perfect radio for my budget: a Realistic DX-302 quartz-synthesized receiver with digital readout for $130. It was sold by RadioShack back in the ‘60s for about $400.

Figure 12 is a photo of it on my desk, tuned to WWV at 10.000 MHz. Even though it was vintage, I took a chance on not replacing the power supply caps and fired it up. Wow. The calibration was still right on the button. WWV was 10.000.

FIGURE 12. The DX-302 receiver with its digital readout was much easier to tune into the dozens of transmissions each day from around the world.

I then got serious and spent hours and hours, day and night, over the next several weeks tuning in the stations listed by **priyom.org**. Overall, I got mixed results. I heard Russian stations a few times, but most of the overseas stations were in the noise out here in California. I was a little disappointed, but perhaps someday I'll put up a three-element beam and see what happens.

Frankly, it was the thrill of the hunt that made this project so intriguing.

YOU TOO CAN DO IT!

If you have a shortwave radio or access to one — even a portable unit — you should consider giving it a try. There is nothing like that first time when you hear, "Uno, tres, ocho, cuatro, dos." Good luck, and thanks for listening! **RON MILIONE W2MIL/W2TAP**