LOS NUMEROS cont'd

the numbers transmissions are used by the U.S. and the USSR to communicate with each other. They could be a backup system should the Washington-Moscow hot line be inoperative. The current transmissions are all test transmissions used to make sure the "numbers hot line" is operational. There is a landline link from Washington to the Virginia transmitter. Likewise, there is a link from Moscow to the Eastern European transmitter.

"The link from Moscow to Cuba is more of a puzzle. However, I am sure the USSR runs the Cuban transmitter rather than Castro's government.

"Note that the hot line was established in 1963. This is just about the same time that the numbers transmissions began.

"In the event of nuclear war, many electronic devices would be ruined by the blasts. A simple voice communication system is easier to repair and get back on line than a radio teletype or other more sophisticated device..."

Martin A.
full name and address withheld by request.

A thought provoking observation, Martin. I assume that you refer to the 4-digit Spanish transmissions. Thanks, Martin. Reader response to the above is eagerly solicited.

DEAR LUNA HABANERA

"I read with interest your column in the Monitoring Times and look forward to future issues. Of special interest is information in regards to the clandestine transmissions from Central America and Cuba, and hope it will be possible for you in some future issue to print up a list of the various stations currently (or in recent past) operating on the various bands, such as 15 September (5565 kHz), the many C.I.D. (6305, 6151, 11700, etc.) Also the "numbers" stations in Russian such as the 7410 kHz AM YL, ..."

B.H.S.
New Hampshire

Thanks for the letter, B.H.S. The most authoritative source of clandestine transmissions from Central America and Cuba is presented monthly in MT by John Santosuosso. I think you'll find what just what you're looking for in John's pirate radio column. You'll also find that John is the foremost expert in the field of clandestine and pirate operations.

As for the "numbers," the Apple--at this very moment--is churning out an updated listing of all types of "numbers" transmissions. Hopefully you'll find this listing in next month's issue of MT.

How about more information on the Russian numbers, B.H.S.? Thanks for your time.

INTERCEPTS

Column regular Zel Eaton checks in with some interesting intercepts this issue. Here's a portion of what's being monitored in Missouri:

0300Z 03/11/85 6998kHz AM
Morse code "N" continuous until 0306Z at which time German YL begins transmission of 5-digit groups

0317Z 03/14/85 4670 kHz AM
Spanish YL with 4-digit transmission

0212Z 04/08/85 4670 kHz AM
Same as above with the exception that signal covered a wide segment of the band (Very interesting, Zel.)

0231Z 04/08/85 6840 kHz AM
Spanish YL with 4-digit transmission

0410Z 05/01/85 11535 kHz AM
Spanish YL with 4-digit transmission

2336Z 05/08/85 12470 kHz AM
Tones as if someone keying an electronic organ. Signal 40 over S9. (These are possibly European embassy transmissions, Zel.)

Thanks for the nice list, Zel; sorry I couldn't include everything.

THE RETURN OF JAMES BECKETT

Mr. Beckett would like to know who lurks behind the name "Havana Moon." It's like this, James: it's not Bob Grove or John Santosuosso. I do, however, lurk.

James dabbles with ciphers and passes along a very simple cipher to see who can solve it. The Beckett Cipher goes like this:

26432 85447 89354 24825
54632 71458

Sharpen up those pencils, Bob Russ.

James wonders if numbers station operators read MT. He thinks that it might be possible to communicate with them through this column or other sections of this publication.

I have a deal this bilingual YL just might go for, James. Read about it near the end of this column.

James says that he copied WGY912 slow CW (with the WGY912 ID)--and sent in a report to the address given in MT. James says that the letter was returned and envelope marked no such address.

A FEMA project is now in the research stage, James. Give me two or three months.

FREQUENCIES TO WATCH

3070, 3074, 3080, 3090, 3445, 4010, 4025 and 4030 kHz. Also check 4044, 4049, 4057, 4188, 4825 and 5188 kHz. Five-digit Spanish reported to be heavy on all these frequencies after 0200Z. Let me know what you hear.

THE CIA SPEAKS

Be sure to write the CIA for its two multi-colored and very slick and glossy publications. FACT BOOK ON INTELLIGENCE and THE ACME OF SKILL can be yours FREE. Write to:

The Office of Public Affairs
Central Intelligence Agency
Washington, D.C. 20505

AUGUST OF 1976

Be sure to check your local library for the August 1976 (that's the correct date) issue of Popular Mechanics and the excellent Anthony Curtis article on "spy-and-number" transmissions. Many of the frequencies listed in the Curtis article continue to be active. Are you among our readers, Anthony?

Monitoring Times readers might wish to write Popular Mechanics to request consideration of a follow-up "numbers" article.

ESPIONAGE

There are some slight indications that Espionage--a bi-monthly publication in the pulp tradition--might entertain the notion of a "numbers" article. Contact the editors at:

ESPIONAGE
P.O. Box 1184
Teaneck, NJ 07666

LET'S MAKE A DEAL

I WOULD SAY IT'S ALMOST A SURE BET that 5-digit Spanish station operators read MT! I would also say it's almost a sure bet that these shadowy and (expletive deleted) technical misfits know a lot more about serious "numbers" monitors than we know about them.

Here's the deal: How about a special 5-digit Spanish transmission just for MT readers. In "Tom-and-Jane" language, here's the transmission schedule and procedure:

1.TIME.....0600Z
2.DATE...10 August 1985 Zulu (Saturday)
3.FREQUENCY.....5135 kHz
4.REPEAT....30 past the hour on 6500 kHz
5.IDENTIFIER.....007
6.GROUP COUNT.....50
7.1st 3 GROUPS...00351 99112 11136

Care to bet these (expletive deleted) misfits can't pull this off?

Just to make it a bit more easy: The time for the transmission is 2 a.m. New York time on 10 August 1985. That's a Saturday morning and very early. UNDERSTAND?

WE'LL BE LISTENING.

A REMINDER

All correspondence directed to this column will

MAKING AND BREAKING CODES WITH A HOME COMPUTER

by Chris Williams

A recent issue of Monitoring Times contained an excellent article by Bob Russ which discussed some of the history behind ciphers. In addition to covering the motivation for using them, it also described some of the basic ciphers employed in the past and the methods used to produce them.

As Mr. Russ pointed out, many of these ciphers are still around today; there are also, however, many new ciphers in current use and most of these are the result of the recent computer technology explosion. In this article, I'm going to demonstrate a computer encryption/decryption algorithm and use it to show some of the fundamental concepts of computer ciphers.

LETTERS ARE NUMBERS

Inside computers, all the letters of our alphabet have a numerical equivalent; the set of these equivalents is called ASCII (American Standard Code for Information Interchange). In addition to letters, all the rest of the characters on a keyboard also have equivalents and can therefore be understood by the computer. An ASCII table showing all these equivalents can be found in just about any computer book so I won't repeat it here.

The encryption technique we'll be discussing uses ASCII along with a machine language computer instruction called the "Exclusive OR" (XOR). The XOR function operates on two bits (A and B) and results as follows:

LOS NUMEROS cont'd

be assumed to be intended for publication unless otherwise indicated. YOUR CARDS AND LETTERS ARE ALWAYS WELCOME.

THANKS TO

Martin A., B.H.S., Zel Eaton and John Santosuosso. Thanks to CA for the color photo and the Miami information. A special thanks to James Beckett and his radio friends. Those friends being: Jim Craig and Bill Slep.

I HATE TO SAY THIS, BUT

Radio Marti finally made it and Castro is jamming the frequency like crazy. The program content is so drab that Fidel is wasting his time. Now a little of Madonna or Prince just might attract the under 40-year olds.

I suspect that by the time you read this that Cuban jammers will be very common on many American AM frequencies. I'm confident that Fidel has an ace up his beard.

DID YOU KNOW

Col. Rudolph Abel (now put to shame by the alleged Walker spy ring) was a GRU officer rather than a KGB officer.

Time now for an Anchor Steam and ...

Adios,

Havana Moon y Amigas

The views expressed in this column are those of Havana Moon and do not necessarily represent the views of the MT management, staff or readers. ●

MAKING CODES cont'd

A		B	
0	XOR	0	Equals 0
0	XOR	1	Equals 1
1	XOR	0	Equals 1
1	XOR	1	Equals 0

One, and only one, of bits A and B may have a value of 1 if the result of the XOR is to be 1. Since an ASCII character is eight bits long, XORing one character with another involves executing the above process eight times. The XOR instruction is common to most computers' assembly languages.

THE TECHNIQUE

The phrase we're going to encrypt is, appropriately enough, "LOS NUMEROS." We will do so by XORing each letter of that phrase with the result of XORing the preceeding letter. Because the first letter has no preceeding result we'll simply pick an initial letter at random. In this case, our initial seed will be the letter "S" which has an ASCII equivalent of 53 hexadecimal, 01010011 binary.

The letters of "LOS NUMEROS" have the hexadecimal ASCII equivalents 4C, 4F, 53, 20, 4E, 55, 4D, 45, 52, 4F, and 53. Notice the blank also has an ASCII (20) equivalent.

Now, taking the XOR of each of the bits of "S" with each of the bits of "L" yields (again in hexadecimal):

4C XOR 53 --- IF

We then use 1F as the preceeding result and continue the process for each of the hexadecimal ASCII equivalents:

Uncoded	Encoded
4F XOR 1F ---	50
53 XOR 50 ---	03
20 XOR 03 ---	23
4E XOR 23 ---	6D
55 XOR 6D ---	38
4D XOR 38 ---	75
45 XOR 75 ---	30
52 XOR 30 ---	62
4F XOR 62 ---	2D
53 XOR 2D ---	7E

Thus, in encrypted form, we have "LOS NUMEROS" as 1F, 50, 03, 23, 6D, 38, 75, 30, 62, 2D, and 7E. Few of these characters are equivalents for letters; some are punctuation or numbers and some have no direct keyboard representation at all.

This algorithm is not a simple number substitution cipher because each number is entirely dependent upon the previous value which is ultimately dependent on the initial seed. A different initial seed would change all the values resulting from the XORs.

An attractive feature of this technique is its ability to decrypt with essentially the same procedure used to encrypt. Watch:

Coded	Decoded
1F XOR 53 ---	4C
50 XOR 1F ---	4F
03 XOR 50 ---	53
23 XOR 03 ---	20
6D XOR 23 ---	4E
38 XOR 6D ---	55
75 XOR 38 ---	4D
30 XOR 75 ---	45
62 XOR 30 ---	52
2D XOR 62 ---	4F
7E XOR 2D ---	53

and there in the decoded column we have the original message.

WHY USE A COMPUTER?

The primary advantage of using such a computerized algorithm is the speed of the process on both ends of the circuit. This makes conversation more convenient because time needn't be spent leafing through a codebook. Both sender and receiver simply feed the characters into the computer and then read the results off the screen.

Another attraction for this particular approach is that the code is quite secure. The receiver must know both the procedure being used and also the initial seed.

There could also be several "stacks" of this technique on a message that would require it to be run through the procedure more than once and with different seeds. The receiving station would also have to know the number of stacks which, of course, adds to the security of the code.

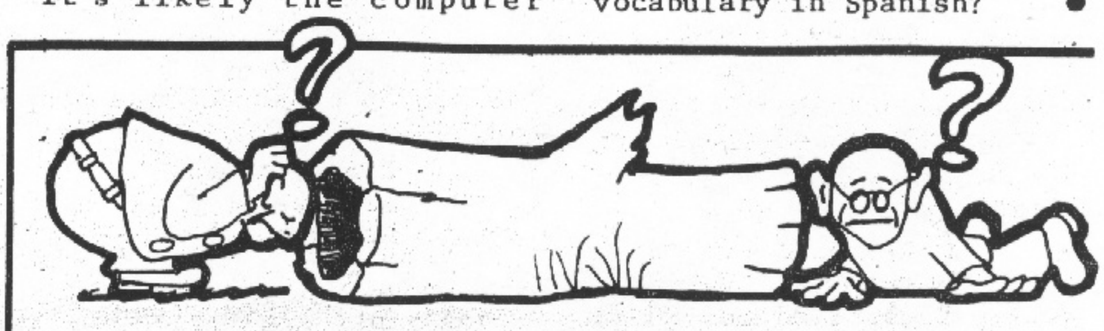
APPLICATIONS

One could certainly apply a decrypting computer to the encoded message and it's likely the computer would eventually hit on the correct combination of algorithm and seed. The more ambitious among you might want to program your personal computers to attempt decryption of some of those 5-character groups you've been intercepting.

I've no more idea that you what algorithm the transmitters are using so anything you might do will require your computer to use trial and error in varying degrees of sophistication.

One place I can help you is in defining success cirteria for your programs, i.e., how does the computer know when it has cracked a code? The solution to this can be found on word processors. The newer products have spelling checkers with large vocabularies implemented in the program.

One approach could be to look for a percentage of decryption match to the vocabulary. This assumes the language encrypted is English which isn't always the case. How about a spelling vocabulary in Spanish? ●



listener's log

MONITORING THE STOCK CAR RACES--CHARLOTTE STYLE
A frequency profile by
RADIO RESEARCH
10 Elf Lane
Greenville, SC 29611

CHARLOTTE MOTOR SPEEDWAY

464.725 Security
464.500+Race ControlTower
462.650+Operations
461.700 Operations
455.650 FM broadcast link
173.225 Parade
154.600 Operations
151.895 Parking
42.82 +Traffic-NC trooper
42.50 Traffic-NC trooper

GRAND NATIONAL DIVISION

461.050 #17 Lenny Pond/Sub
461.27 #71 Dave Marcus
461.812 ?
461.825 ? (Mike)
461.875 #44 Terry Labonte
462.175 #11 Darrell who?
462.550 ---(media)
463.462 #7 Kyle Petty
463.487 #7 Kyle Petty
463.700 #28 Cale Yarborough
#22 Bobby Allison
463.900 #27 Tim Richmond
463.925 ?
464.125 ?
464.573 #9 Bill Elliot?
464.625 ?
464.800 #43 Richard Petty
#84 Mike Alex also?
465.537 #00 Morgan Shepard
466.812 #95 Sterling Marlin
467.775 ?
468.562 #28 Cale Yarborough
468.612 ?
468.700 #28 (rpt on 463.700)
468.900 ?
468.975 #75 Lake Speed
469.125 ?
469.962 #9 (spotters only)

NOTE: Some race teams are using multi-channel radios and are switching channels at random during the races. Several different teams were monitored on the same frequency during the race.

HARRISBURG, PA, SCANNING
contributed by Tim Shingara

PENNSYLVANIA STATE POLICE

	Base xmit	Mobile xmit
A	155.580	155.790
B	155.670	155.910
C	155.505	155.850

33.040 Harrisburg river rescue
33.220 Buckeye Pipeline
33.380 Columbia Gas
33.600 Lancaster Co. FD
33.640 " (working)
33.700 Middletown FD #2
33.740 Lebanon FD
33.760 Middletown FD #1
33.800 Dauphin Co. FD #1
33.840 " #2
33.860 " #3