```
        úúúÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄ¿                    ÚÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄúúú       9-FEB-89
                        ÉÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ»    ÚÄÄÄÄÄÄÄÄÄúúú
      úúúÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄ¶      THE DNA BOX        ÇÄÄÄÄÙ ÚÄÄÄÄÄÄÄÄÄÄúúú
     úúúÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄ¶ Hacking Cellular Phones ÇÄÄÄÄÄÄÙ
                        ÈÑÍÑÍÑÍÑÍÑÍÑÍÑÍÑÍÑÍÑÍÍÍÑÍÑÍÑ¼
    úúúÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÙ                       ÀÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄúúú
                             P A R T   S I X
ÚÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄ¿
```

CELLULAR TELEPHONE MESSAGE CODES

==

The previous file (Part Five) listed the Message Formats and Message Words used by the Cellular Telephone system. Message words have variable sub-fields that are set to convey various information (such as dialed numbers, mobile phone ID, commands, requests, channel assignments etc.).

Here are the codes used in Message Word subfields during data transmissions.

==

Mobile Station Automatic Attenuation Levels

Mobile Attenuation Code (MAC)

	Power Classifications		
MAC	I	II	III
000	6	2	-2
001	2	2	-2
010	-2	-2	-2
011	-6	-6	-6
100	-10	-10	-10
101	-14	-14	-14
110	-18	-18	-18
111	-22	-22	-22

(Attenuation in dBW)

Nominal ERP Power Outputs

Class	ERP	Level
Class I	4W	(6 dBW)
Class II	1.6W	(2 dBW)
Class III	0.6W	(-2 dBW)

===

Station Class Mark (SCM)

SCM	Station Class, Transmission
xx00	Class I
xx01	Class II
xx10	Class III
00xx	Continuous Transmissions
01xx	Discontinuous Transmissions

(for example 0010 means Class I Continuous Transmissions)

==

Digital Color Code (DCC)

Received	Coded
00	0000000
01	0011111
10	1100011
11	1111100

=======================================

SAT Color Code (Supervisory Audio Tone)

Code	Frequency
00	5970 Hz
01	6000 Hz
10	6030 Hz
11	(not a channel designation)

====================================

Digit Code (for dialed numbers etc.)

Digit	Code
1	0001
2	0010
3	0011
4	0100
5	0101
6	0110
7	0111
8	1000
9	1001
0	1010 (zero is encoded as a binary ten)
*	1011
#	1100
Null	0000 (when no digit present)

===================================

Order and Qualification Codes

Order	Qual	Function
00000	000	page (or origination)
00001	000	alert
00011	000	release
00100	000	reorder
00110	000	stop alert

00111	000	audit
01000	000	send called-address
01001	000	intercept
01010	000	maintenance
01011	000	change to power level 0
01011	001	change to power level 1
01011	010	change to power level 2
01011	011	change to power level 3
01011	100	change to power level 4
01011	101	change to power level 5
01011	110	change to power level 6
01011	111	change to power level 7
01100	000	directed retry - not last try
01100	001	directed retry - last try
01101	000	non-autonomous registration - do not make whereabouts known
01101	001	non-autonomous registration - make whereabouts known
01101	010	autonomous registration - do not make whereabouts known
01101	011	autonomous registration - make whereabouts known
11110	000	local control

(All other codes are reserved)

==

Overhead Message Type

Code	Order
000	registration ID
001	control-filler
010	(reserved)
011	(reserved)
100	global action
101	(reserved)
110	word 1 of system parameter message
111	word 2 of system parameter message

=======================================

Global Action Message Types

Code	Action Type
0000	(reserved)
0001	rescan paging channels
0010	registration increment

0011	(reserved)
0010	(reserved)
0011	(reserved)
0100	(reserved)
0101	(reserved)
0110	new access channel set
0111	(reserved)
1000	overload control
1001	access type parameters
1010	access attempt parameters
1011	(reserved)
1100	(reserved)
1101	(reserved)
1110	local control 1
1111	local control 2

Restricted Central Office Codes.

Cellular phone numbers are NEVER issued with these patterns in order to prevent Word Sync patterns from occuring inside a command word.

1xx-xxxx
224-2xxx
288-2xxx
339-8xxx thru 339-0xxx
352-xxxx
416-2xxx
470-2xxx
508-2xxx
544-2xxx
568-1xxx thru 568-7xxx
595-8xxx thru 595-0xxx
663-xxxx thru 666-xxxx
672-2xxx
736-2xxx
790-2xxx
851-8xxx thru 851-0xxx
864-2xxx
899-xxxx
800-xxxx
928-2xxx
992-2xxx
909-xxxx
0xx-xxxx

Bose-Chaudhuri-Hocquenghem (BCH) Codes

Right now the best GUESS, based on available material, is that BCH coding is the way that the 12 bit Parity field is computed.

The "polynomial" that generates the code is given as:

$$gB(X)= X^{12} + X^{10} + X^{8} + X^{5} + X^{4} + X^{3} + X^{0}$$

Taking this verbatim in the usual way (superscripts meaning exponentiation) gives ridiculous results that would be difficult to compute at the 10 Kb/s data rate required by the Cellular Data Protocol. It makes more sense to interpret this notation to indicate that the bits of the message word are summed (in binary) in 12, 10, 8, 5, 4, and 3 bit bytes with 1 added.
That is: the word is broken up into a bunch of sub-bytes of a certain length, these are added together, the original word is again broken into sub-bytes of

the next length and those are summed ... until all listed lengths have been summed. THEN all of those sums are summed and 1 is added. The low order 12 bits of the results of this procedure are used as the parity bits. THIS IS ALMOST PURE SPECULATION. Confirmation is currently being sought at university engineering libraries, or by examining the parity bits in published examples or intercepted cellular messages.

The Parity bits are irrelevant to hacking Cellular ID codes however, because message words are repeated many times in each message block, and the ID fields (MIN1, MIN2, and SID) can simply be lifted from the most frequent (and most likely error-free) message words in the block.

HOWEVER: If BCH coding transforms the message bits as well as the Parity bits then the proper BCH coding algorithm becomes critical. If all else fails, diassembling the ROM firmware from a Cellular Phone should be conclusive.

```
ÚÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄ¿
³ The DNA BOX - Striking at the Nucleus of Corporate Communications.      ³
³ A current project of...                                                 ³

        Outlaw
     Telecommandos
   º³Ý³³þº³ÝÝ³³þ³Ý³º
   º³Ý³³þº³ÝÝ³³þ³Ý³º
   º01-213-376-0111º
```

Downloaded From P-80 International Information Systems 304-744-2253