A Protocol for Leibowitz

Travis Goodspeed, Sergey Bratus

You say a radio, I say a parser

- You say a **parser**, I say a **weird machine** to be programmed

- Radios are parsers too!
    - They're machines driven by **input** we can craft

- They are just too simple as machines to contain much extra ("weird") state

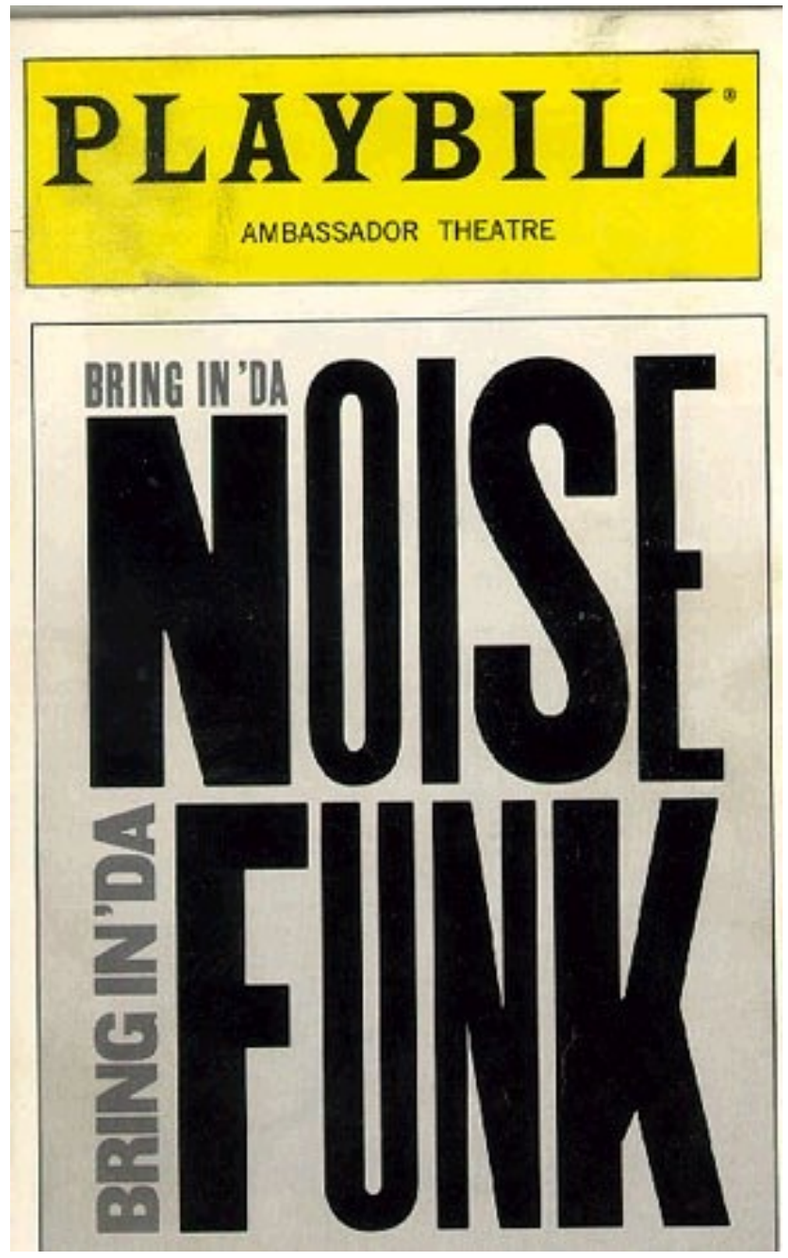
    - so we must look for other parser surprises

Parser differentials FTW

- There are two ways (noiseless) parsers can surprise you:
  - run away & execute your logic, up to full Turing
  - see two (or more) **different** things in **one** message
- Security schemes assume **equivalent** parsing
  - X.509 csr/cert differentials, Android Master Key, ...
    - "What good is a crypto signature if you disagree about what's been signed?"

Bring in 'da noise, bring in 'da PHY

- Damaged Preamble+SFD loses/warps entire message
    - "I yell past you at X, you'll never hear a thing"
    - Packet-in-packet
- Receiver hears a message that was never sent
    - (up to **not a single byte** in common with what the sender thought it sent: "1/8th of a nybble")



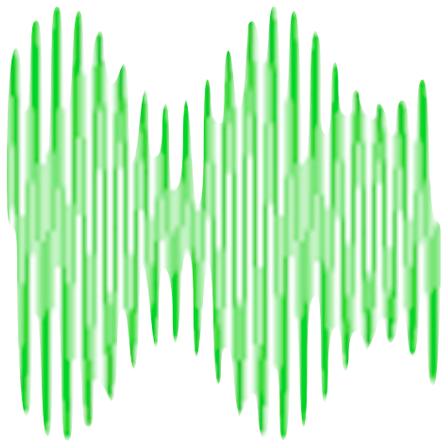
Mission statement

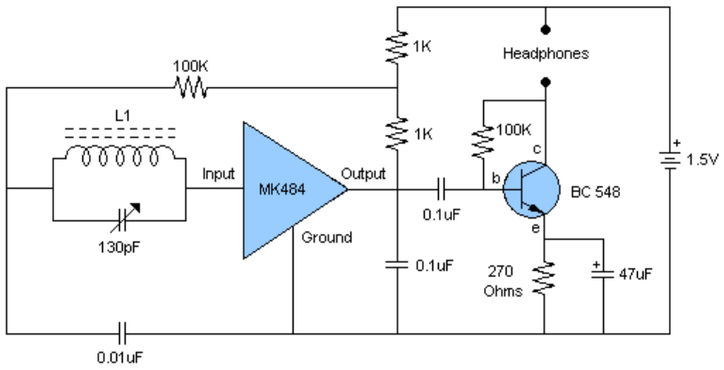
- "To boldly construct signals that one could send with a **commodity transmitter** and that would appear ordinary to a **standard receiver** but contain messages that another standard receiver will interpret **differently**"

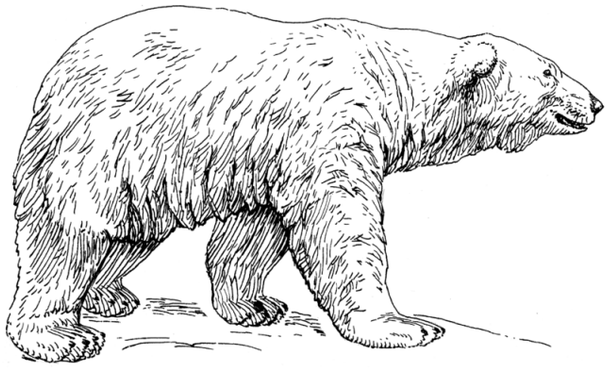
- not quite steganography: our goal is **receiver** exploration

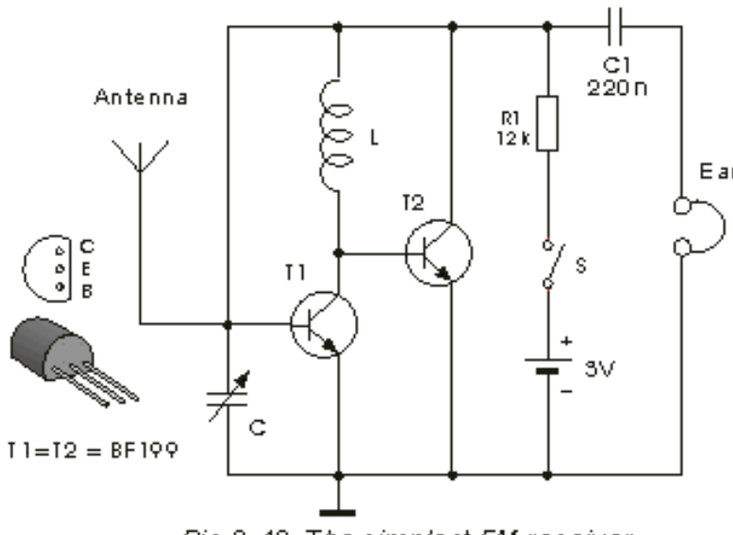
- but booklegging is also an option :)

"A Booklegging Bear"



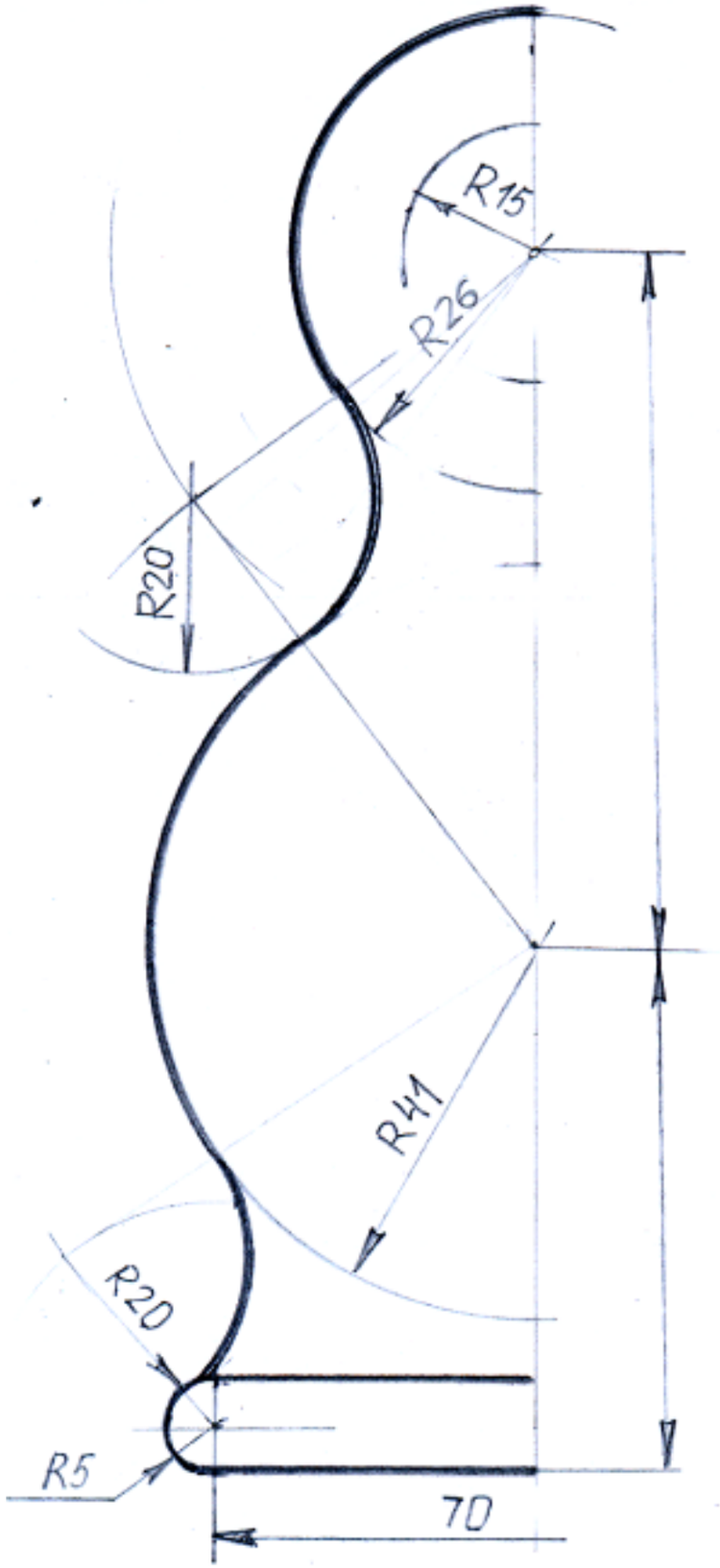






Pic.3.43. The simplest FM receiver

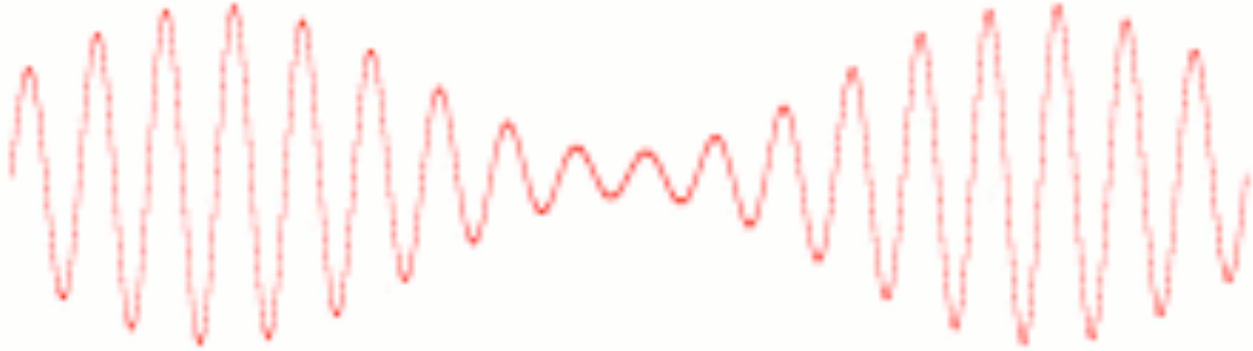
How to make a radio matryoshka?

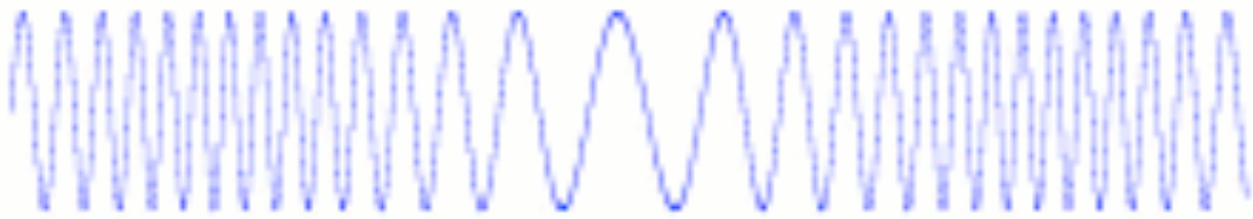


"Deeper PHY"

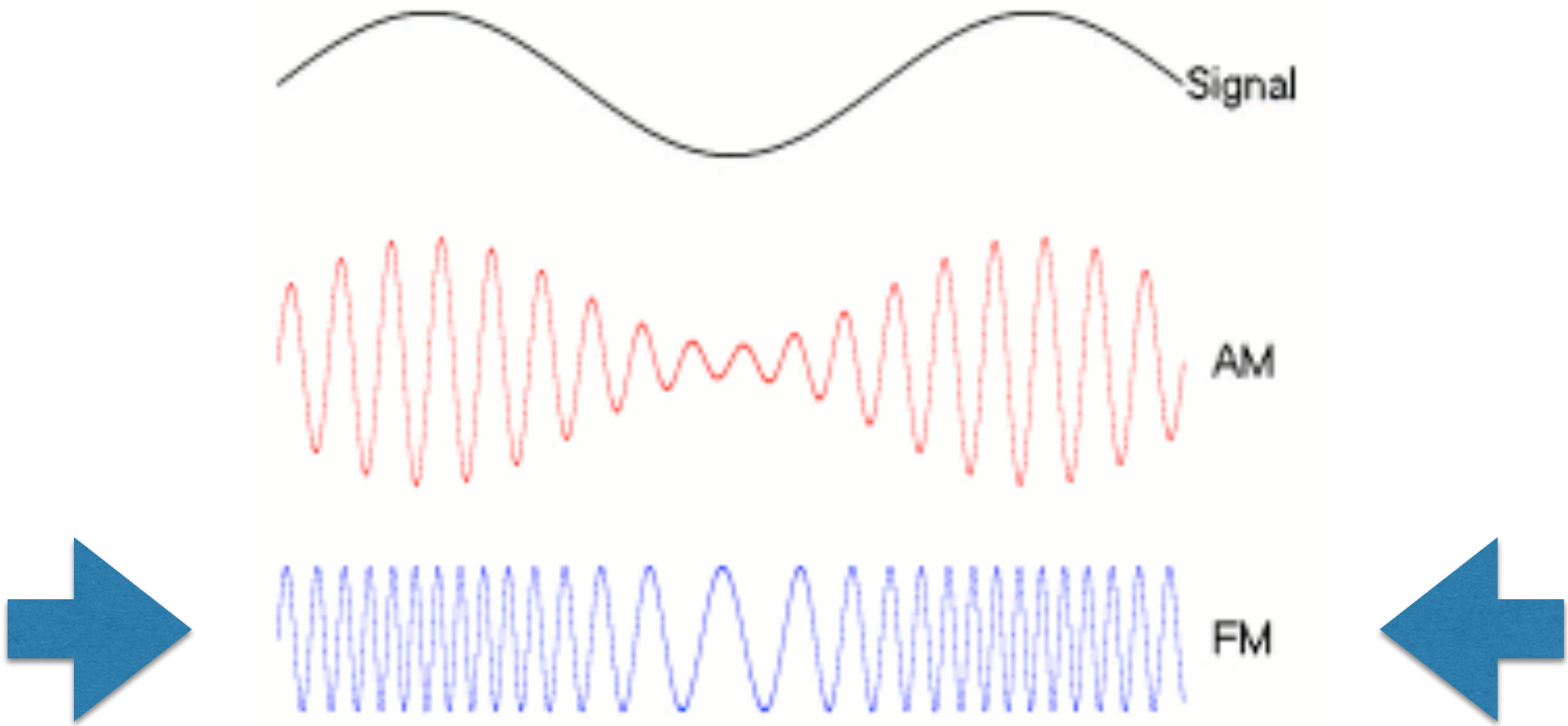
- Every receiver is built for a certain **modulation**
    - ignores all others if physics is "orthogonal"
        - **polyglot**/"schizophrenic" signals
- ...and **error correction**
    - which transparently **rewrites** the signal
- ...and **encoding**
    - for Ham protocols, loose & forgiving

Amplitude, frequency, phase

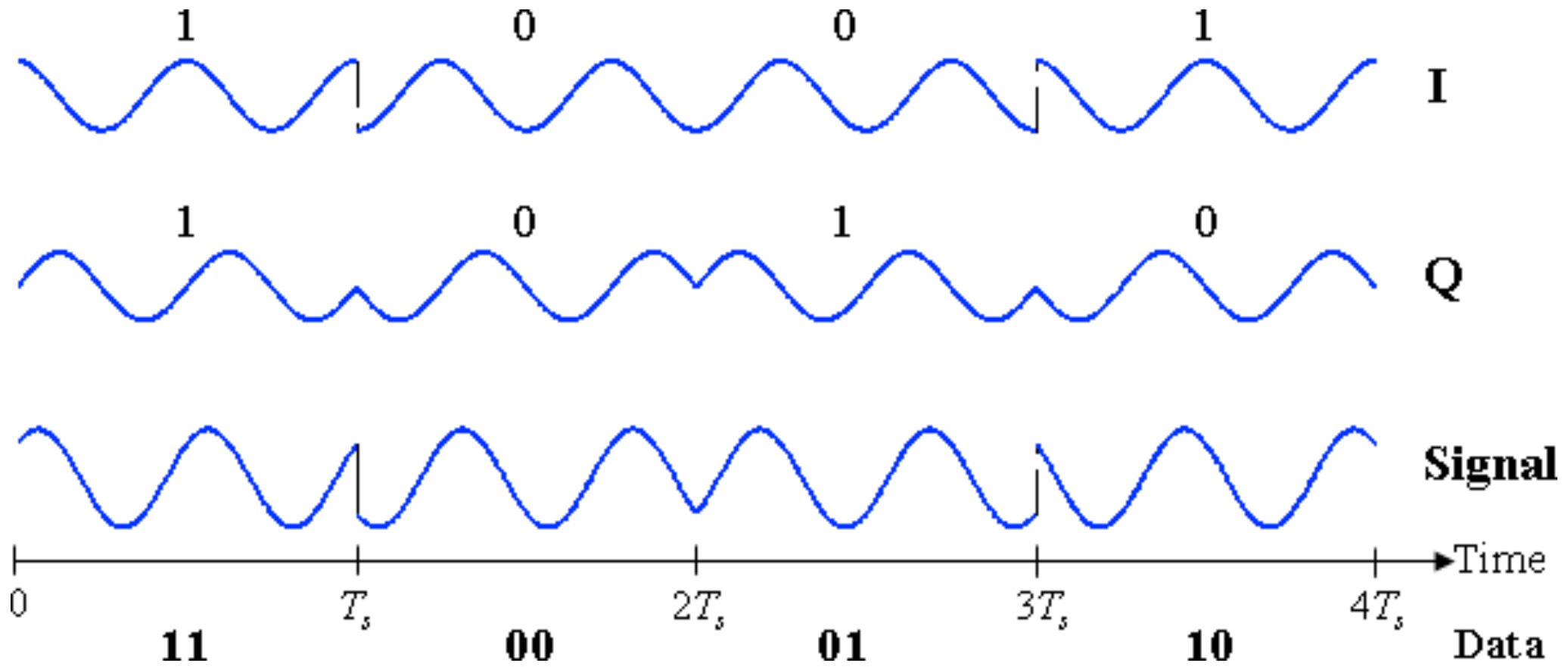




Amplitude, **frequency**, phase

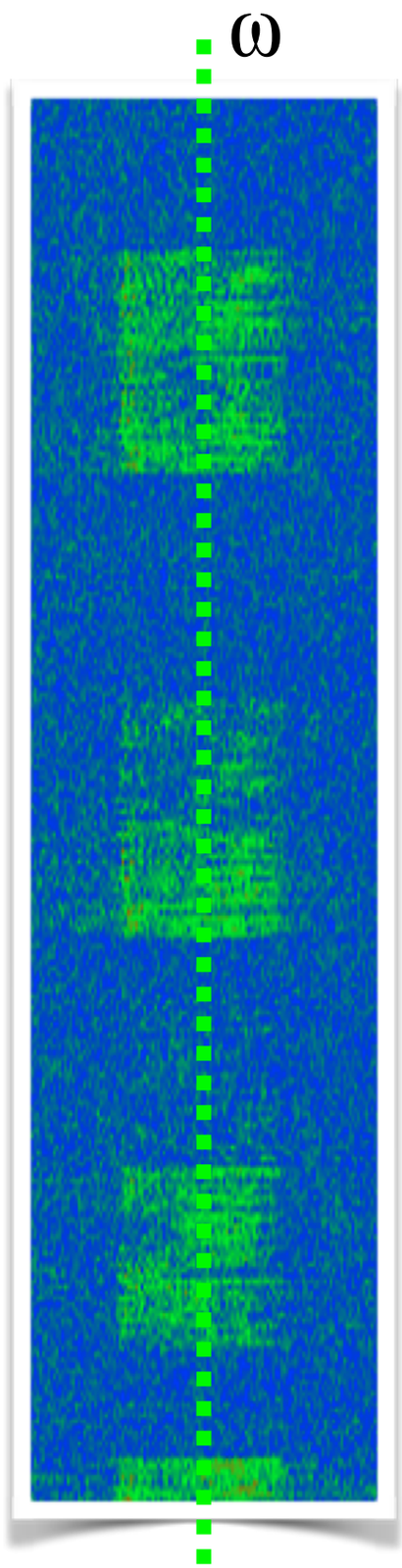


Amplitude, frequency, **phase**



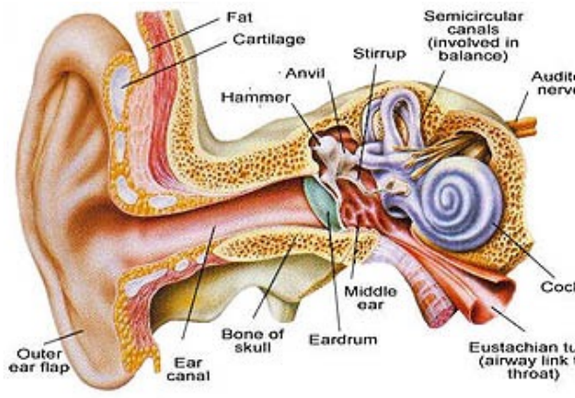
How a mathematician thinks about a signal

- "All you need is sines" (or, "All you have is sines")
- You modulate sines with your signal:
  - Amplitude: **A(t) SIN(ωt)** [∑ sines, by Fourier]
  - Frequency: **SIN((ω+*ƒ*(t))t)**
  - Phase: **SIN(ωt + α(t))** [well, in theory]
- The result is a bunch of sines anyway, extracted by the Fourier transform, between ω and +/- the fastest frequency with which the signal changes ("band")

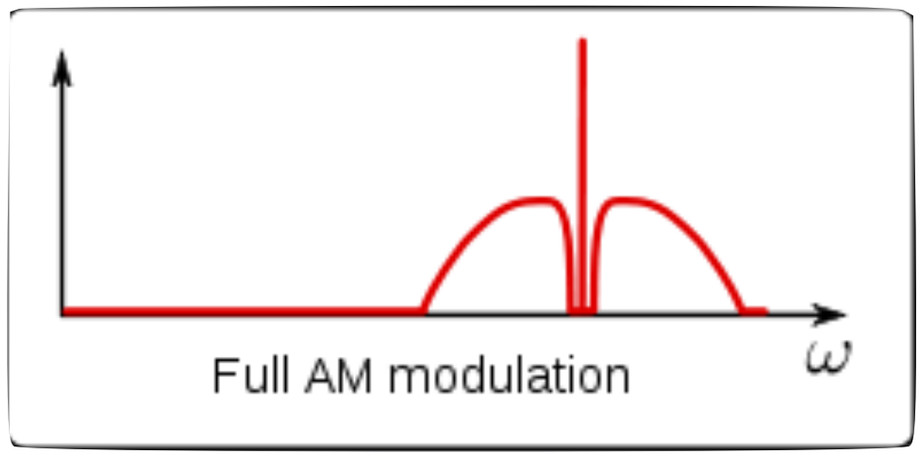


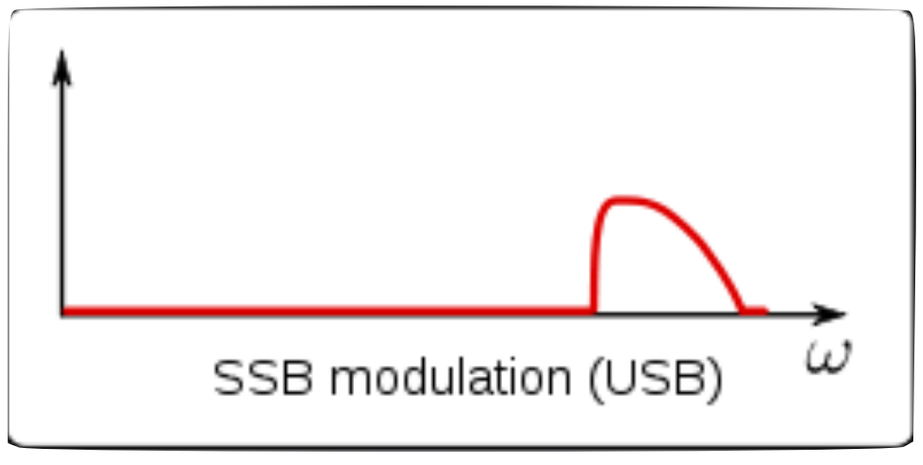
How a Ham thinks about a digital signal

- Upper Side Band
  - Radio Spectrum **downshifted** to Audio frequency
- FSK or PSK
  - The frequency or the phase changes
- Low data rate
  - The signal must fit in an audio channel



Upper Side Band:
it's a space issue



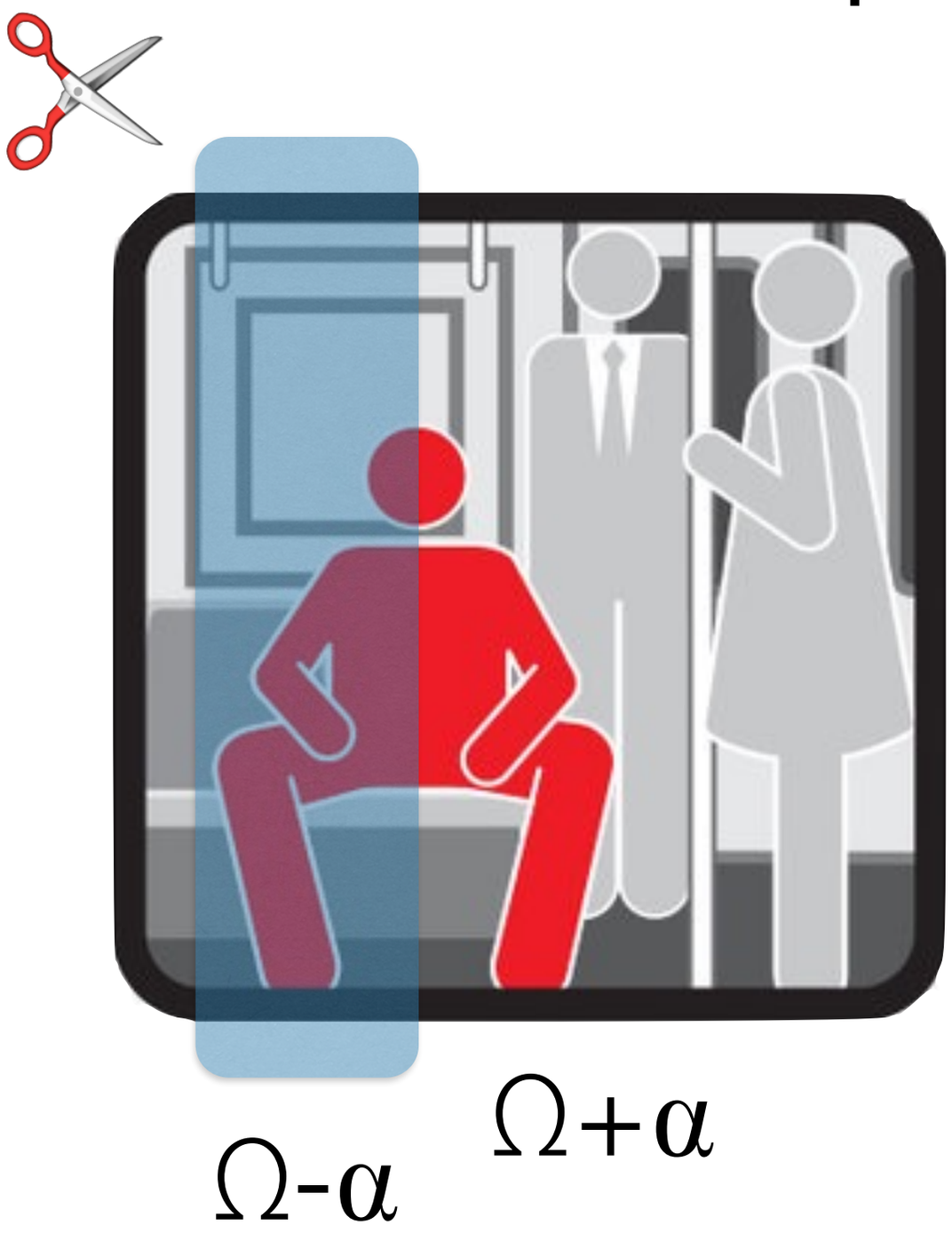


Upper Side Band:
it's a space issue

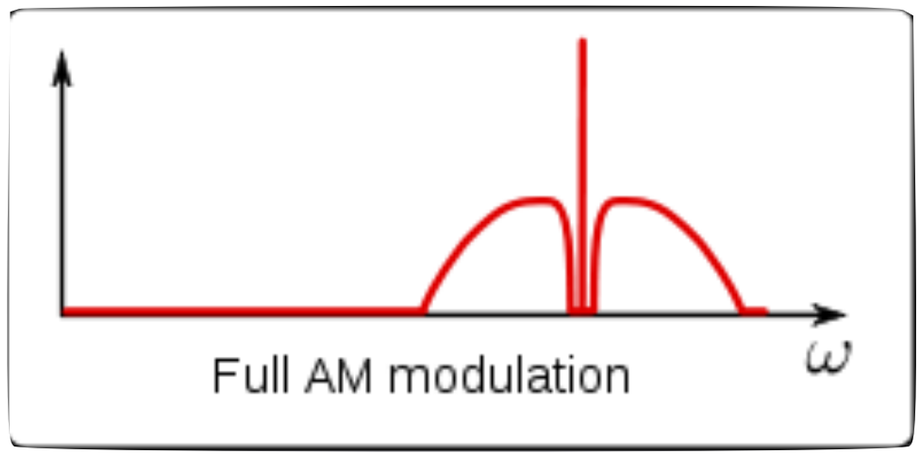
Dude...
Stop the Spread,
Please

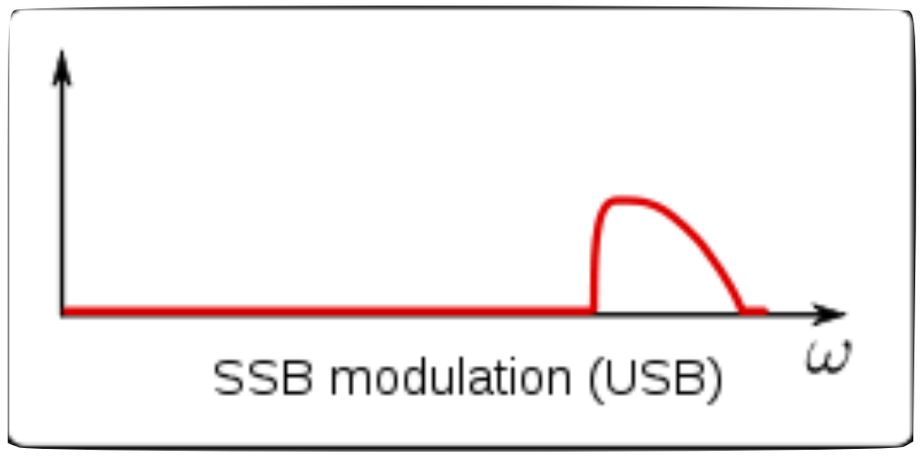
It's a space issue.

Upper Side Band: it's a space issue



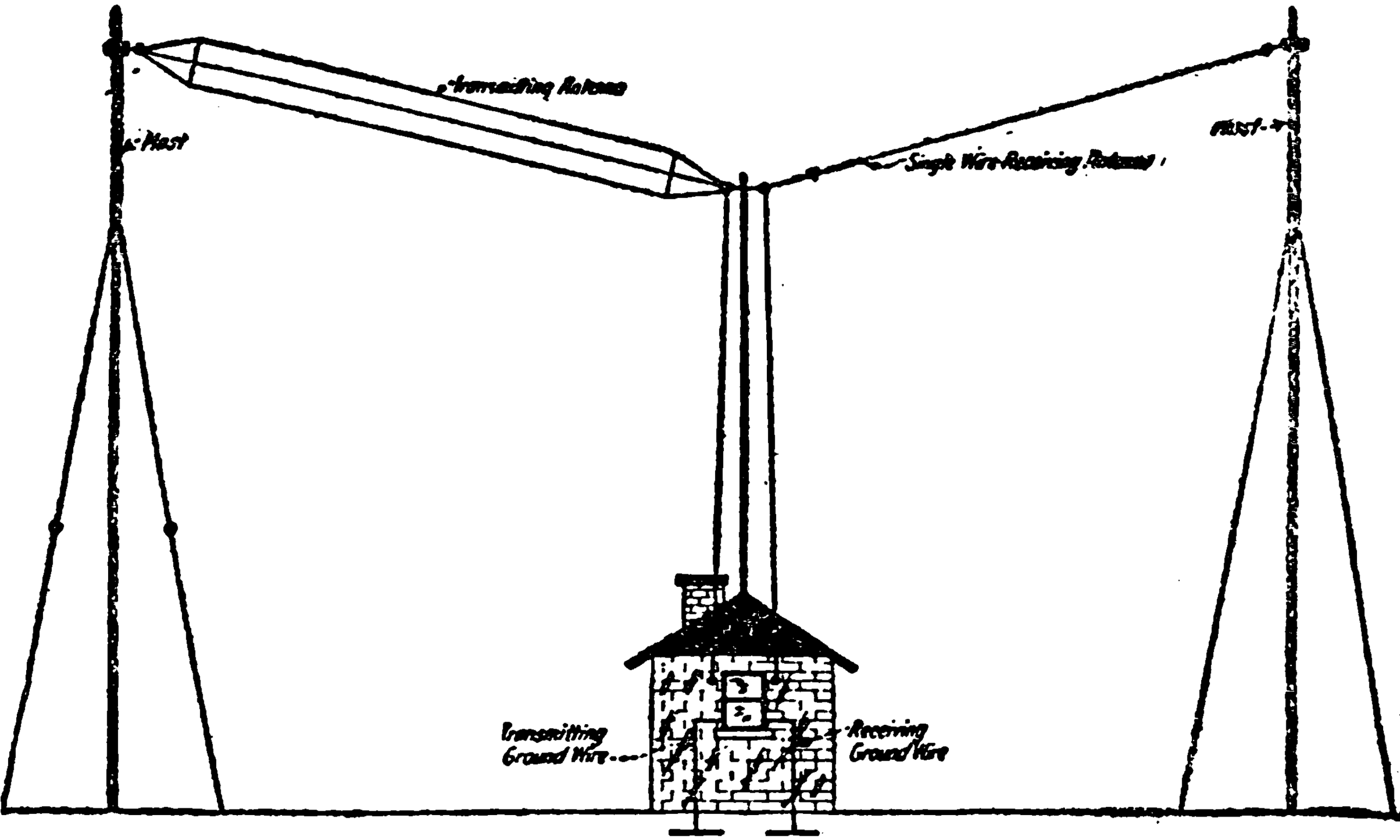
Ω-α Ω+α





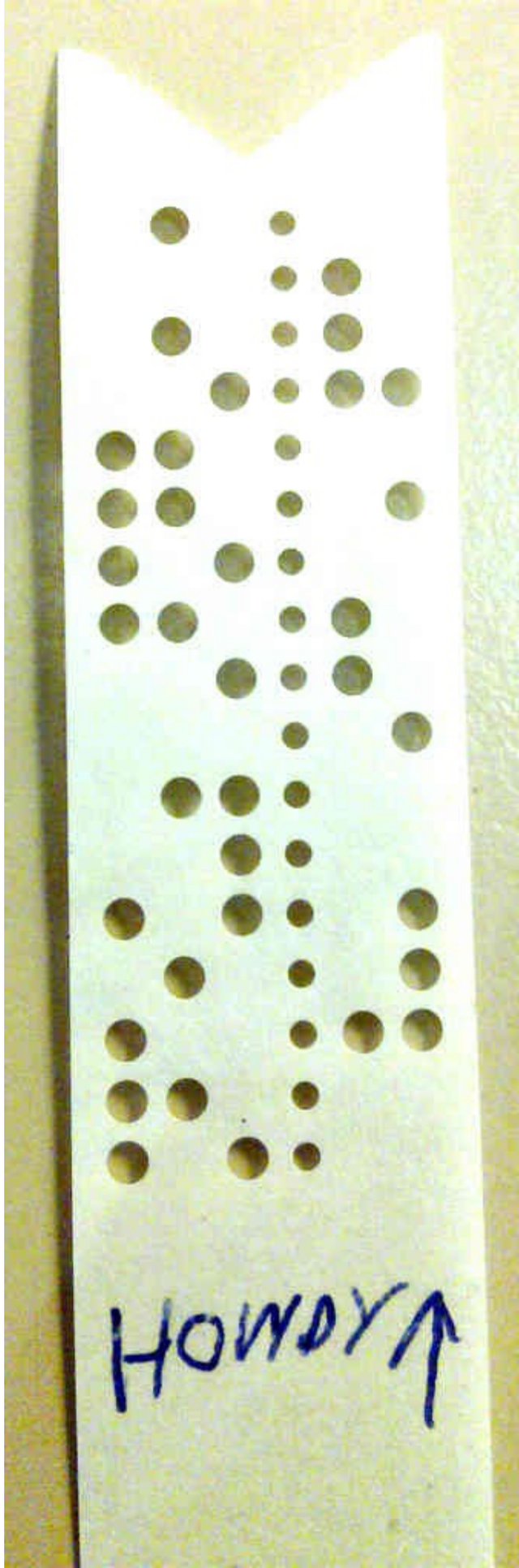
This slide intentionally left blank

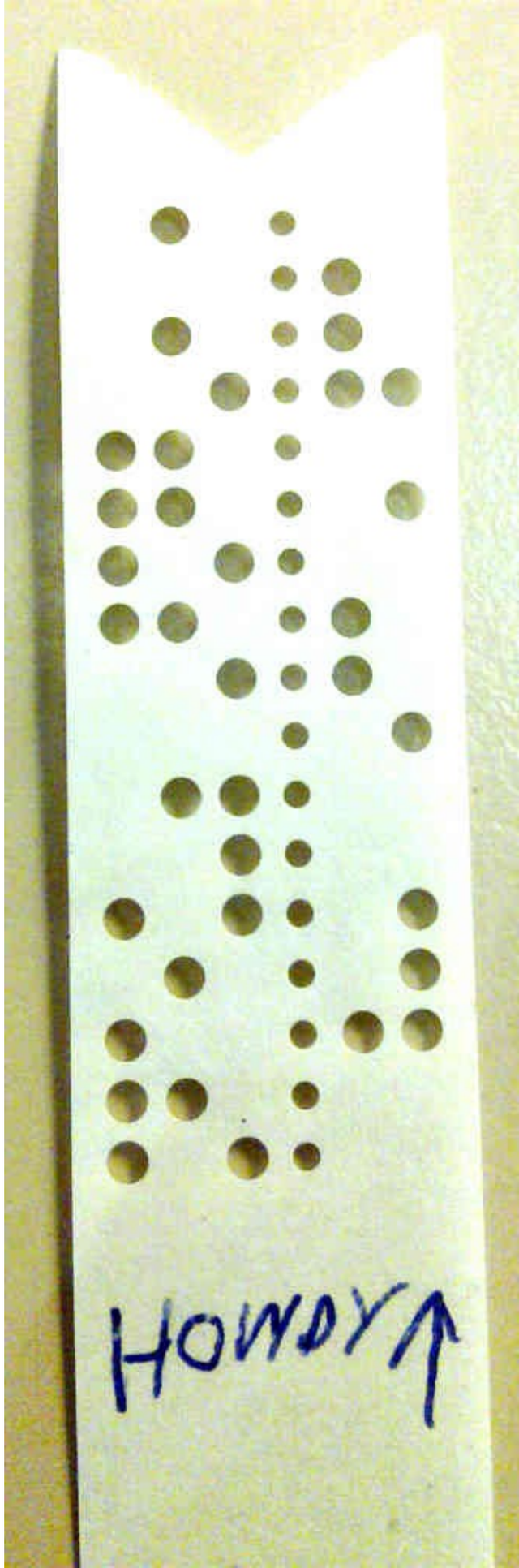
Alice, Bob, and Eve



RTTY

- Ancient military protocol (1940s), now used by amateurs (since 1970s)
- 2FSK modulation, Baudot Coding
  - Low frequency, High frequency.
  - 5/N/2 -- 5 Data Bits, No parity, 2 Stop Bits




HOWDY

fldigi - N0CALL

File Op Mode Configure View Logbook Help

Spot RxID TxID TUNE

14070.000

Frq 14071.085 On Off 0259 In Out

Call Op Az

USB 3000 Qth St Pr Loc

14072.49 V

14071.96 H

14071.13 G

14070.87 A

CQ

-6.0 Clear

CQ CQ CQ de N0CALL N0CALL N0CALL
CQ CQ CQ de N0CALL N0CALL N0CALL pse k
VT
CQ CQ CQ DE N0CALL N0CALL N0CALL
CQ CQ CQ DE N0CALL N

CQ CQ CQ de N0CALL N0CALL N0CALL
CQ CQ CQ de N0CALL N0CALL N0CALL pse k
^T

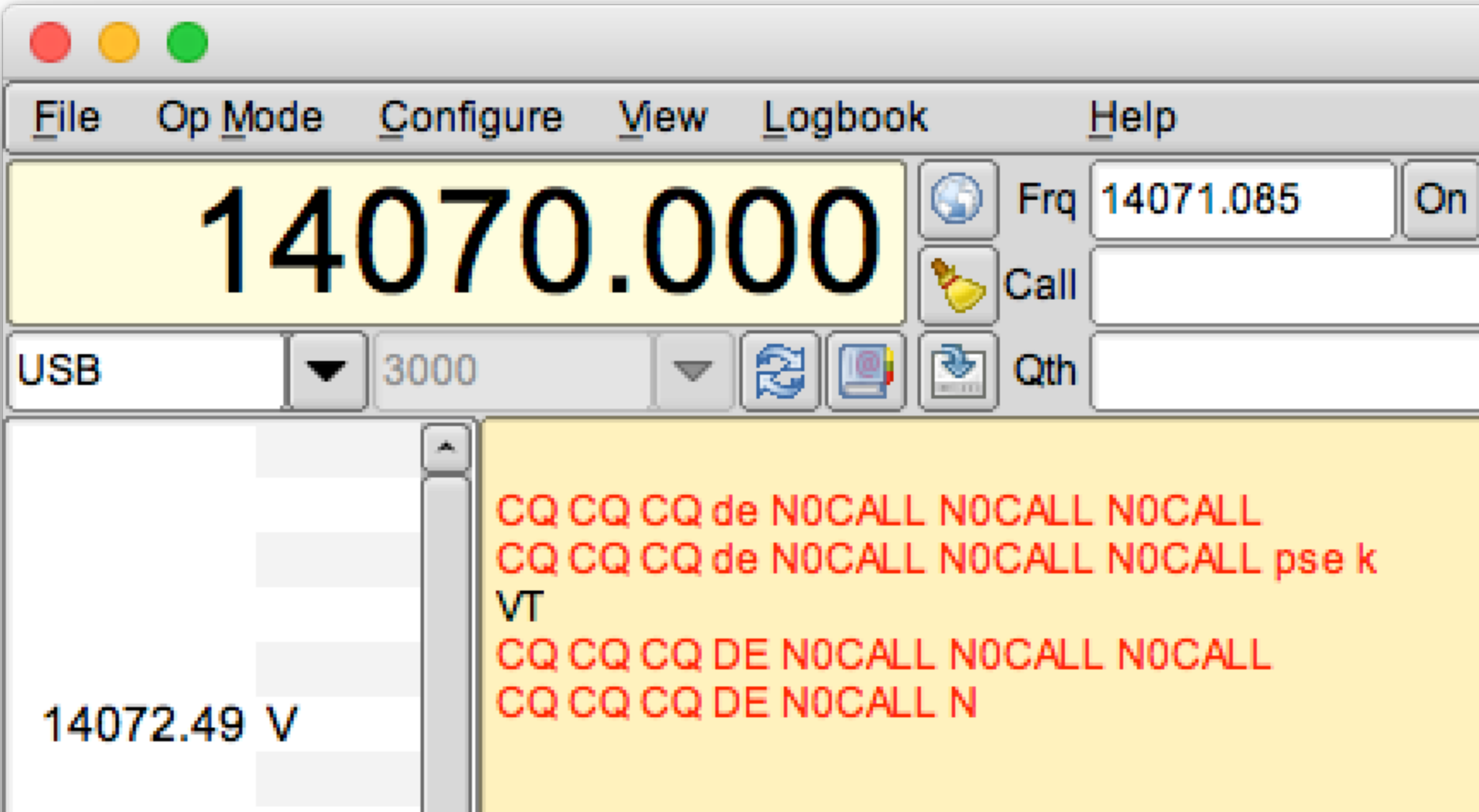
CQ ANS QSO KN SK Me/Qth Brag T/R Tx Rx TX 1

500 1000 1500 2000 2500 3000 3500 4000

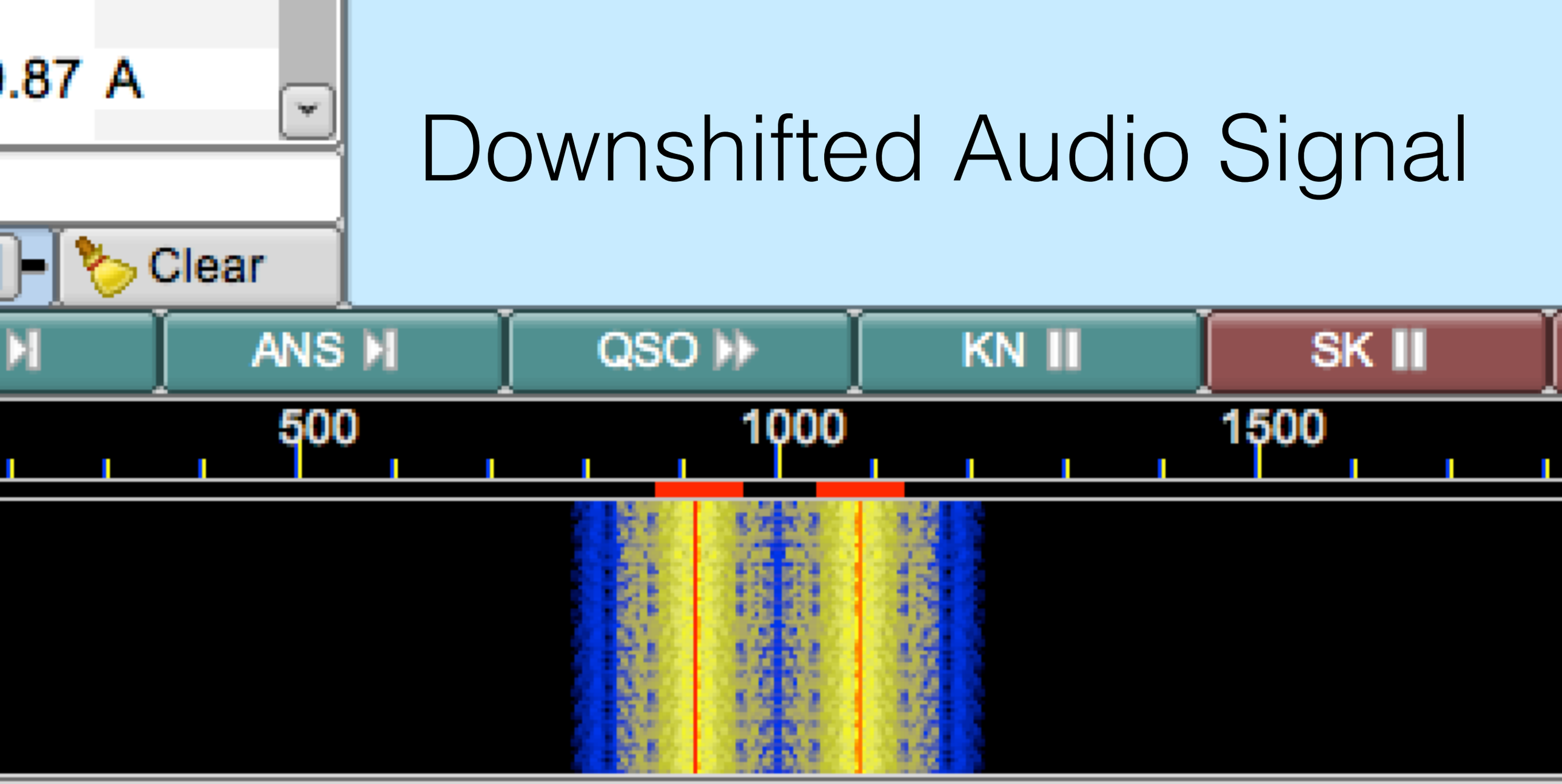
WF -20 70 x1 NORM 1000 QSY Store Lk Rv T/R

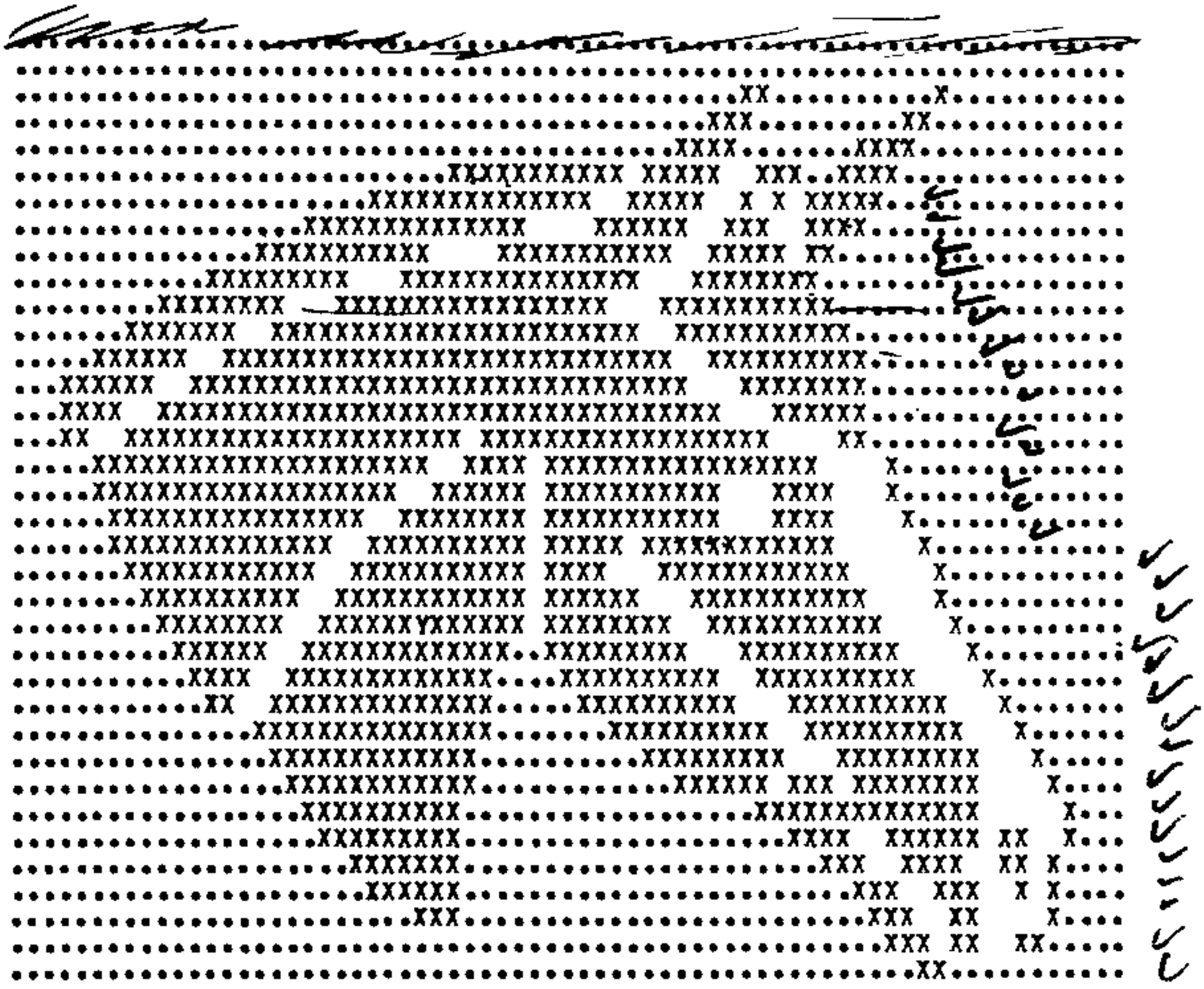
RTTY 45.45/170 s/n -23 dB -3.0 AFC SQL KPSQL

Radio Frequency (Carrier)



Downshifted Audio Signal





THE DERBY WINNER

	Letter	Figure		Letter	Figure
00000	Null	Null	11010	G	&
00100	Space	Space	10100	H	#
10111	Q	1	01011	J	’
10011	W	2	01111	K	(
00001	E	3	10010	L	)
01010	R	4	10001	Z	”
10000	T	5	11101	X	/
10101	Y	6	01110	C	:
00111	U	7	11110	V	;
00110	I	8	11001	B	?
11000	O	9	01100	N	,
10110	P	0	11100	M	.
00011	A	–	01000	CR	CR
00101	S	Bell	00010	LF	LF
01001	D	WRU?	11011	FIGS	
01101	F	!	11111		LTRS

Figure 6: RTTY’s ITA2 Alphabet

11001	B	?
01100	N	,
11100	M	.
01000	CR	CR
00010	LF	LF
11011	FIGS	
11111		LTRS

How to add vodka

LTRS

FOUR VODKAS

FIGS

!974 ;9[WRU?](-[BELL]

NULL

ФОУР ВОДКАС

LTRS, the IDLE tone

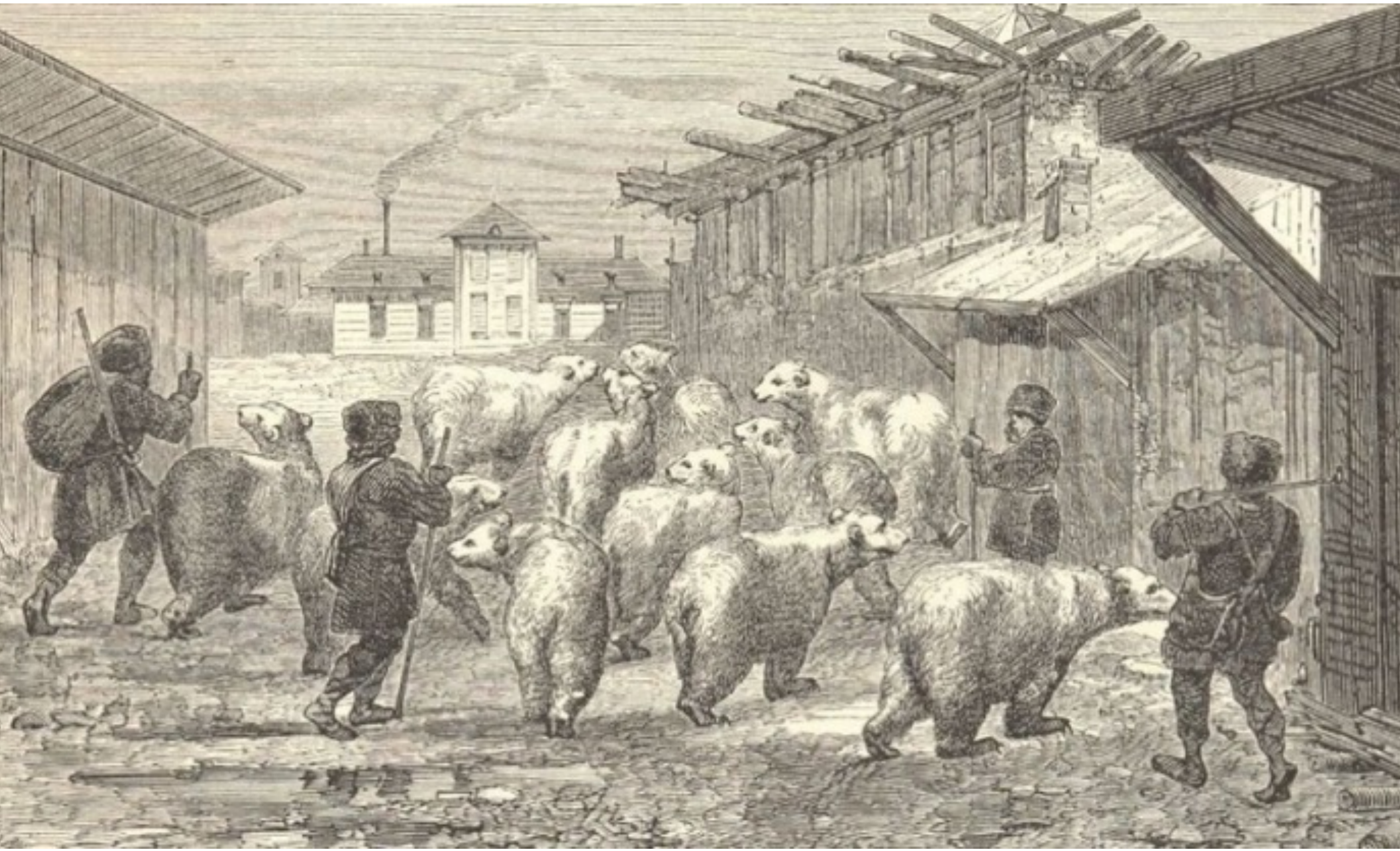
LTRS	LTRS	LTRS	LTRS
11111	11111	11111	11111

Alternate IDLE Tone!

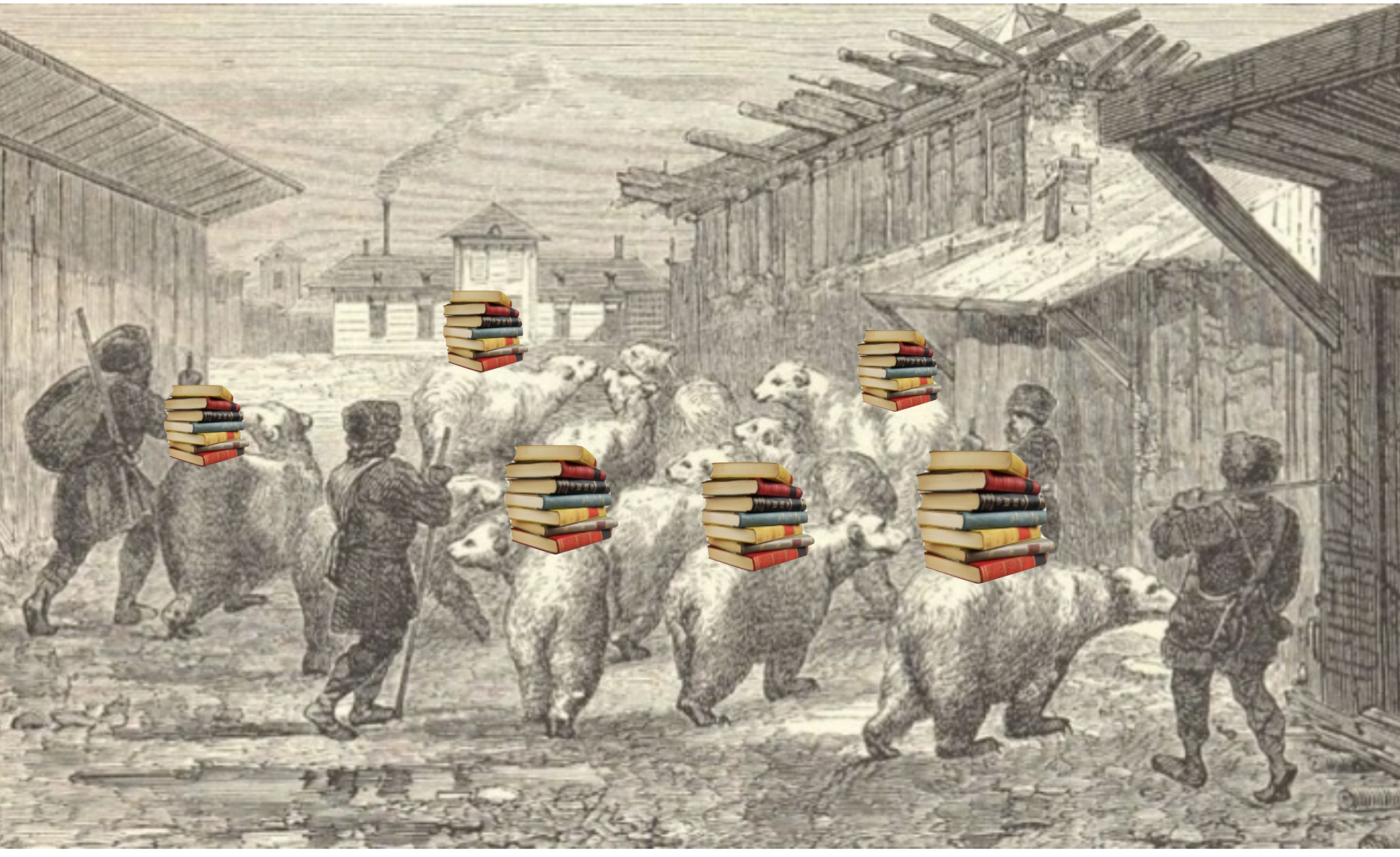
LTRS	FIGS	FIGS	LTRS
11111	11011	11011	11111

Standard receiver will **ignore** redundant shifts!

"Bears passing through a village"



"Bears passing through a village"



PSK31

- 1990's Replacement for RTTY
- 31.25 Baud
    - This is for human typing speed
- ~60Hz Wide

fldigi - N0CALL

File Op Mode Configure View Logbook Help

Spot RxID TxID TUNE

14070.000

Frq 14071.000 On Off 0258 In Out

Call Op Az

USB 3000 Qth St Pr Loc

CQ CQ CQ de N0CALL N0CALL N0CALL
CQ CQ CQ de N0CALL N0CALL N0C

CQ CQ CQ de N0CALL N0CALL N0CALL
CQ CQ CQ de N0CALL N0CALL N0CALL pse k
^[

CQ

3.0 Clear

CQ ANS QSO KN SK Me/Qth Brag T/R Tx Rx TX 1

500 1000 1500 2000 2500 3000 3500 4000

WF -20 70 x1 NORM 1000 QSY Store Lk Rv T/R

BPSK31 -3.0 AFC SQL KPSQL

File Op Mode Configure View Logbook Help

14070.000

Frq 14071.000 On

Call

Qth

USB 3000

CQ CQ CQ de N0CALL N0CALL N0CALL

CQ CQ CQ de N0CALL N0CALL N0C

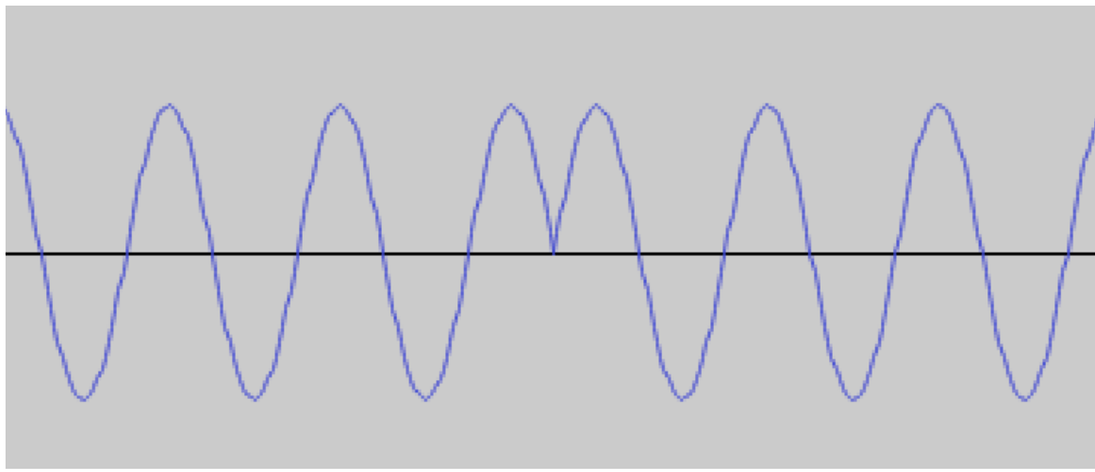
ANS QSO KN

500 1000 15

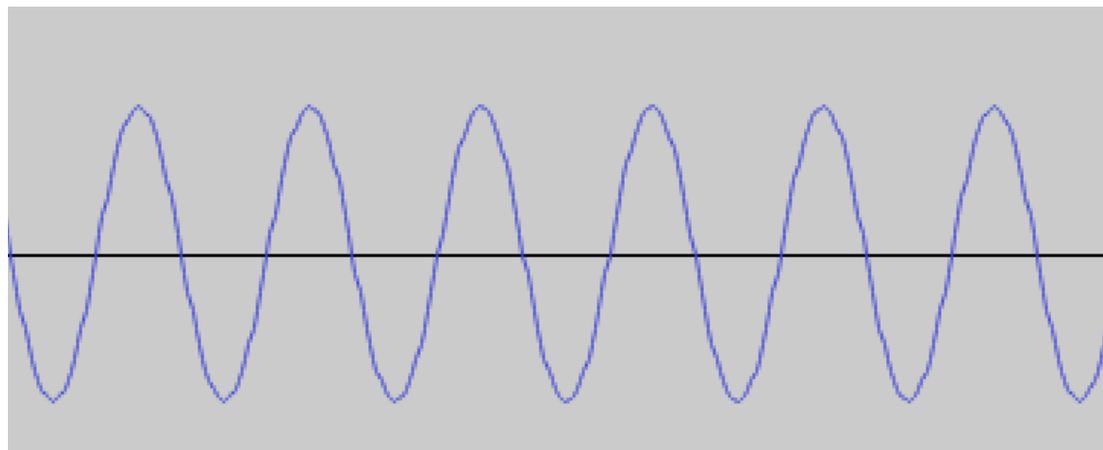
-20 70 x1

PSK31 Encoding

- Phase is Inverted to mark a Zero
  - Fancy way to say that SIN(x) becomes COS(x)
  - Or COS(x) to SIN(x)

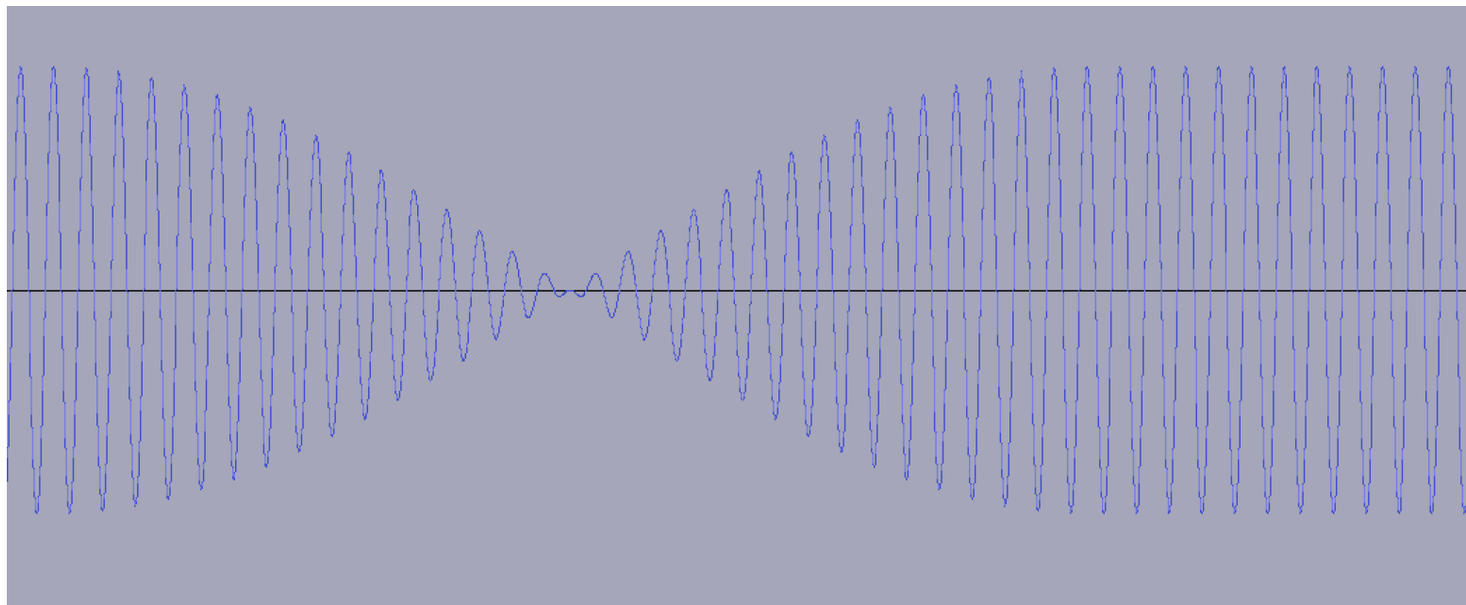


- Phase is Not Inverted to mark a One
  - No change at all



PSK31 Encoding

- You can't just abruptly invert the phase
  - This hurt your ears, hurts the speaker
- **Drop** the amplitude to zero before the shift
  - Raise it back by mid-symbol
  - So the amplitude drops
    for every Zero



PSK31 Decoding

- Recall that **+** times **+** is **+**; **-** times **-** is **+**
  - **-** times **+** is **-**
- **Multiply** signal with its **delayed** self
  - Result is only Positive when phase has changed
  - Otherwise always negative

PSK31 Varicode Alphabet

- ASCII isn't very efficient for English text
- PSK31 uses Varicode:
  - Common letters are short
  - Lowercase shorter than uppercase

11101	LF	1011	a	1111101	A
11111	CR	1011111	b	11101011	B
1	SP	101111	c	10101101	C
10110111	0	101101	d	10110101	D
10111101	1	11	e	1110111	E
11101101	2	111101	f	11011011	F
11111111	3	1011011	g	11111101	G
101110111	4	101011	h	101010101	H
101011011	5	1101	i	1111111	I
101101011	6	111101011	j	111111101	J
110101101	7	10111111	k	101111101	K
110101011	8	11011	l	11010111	L
110110111	9	111011	m	10111011	M
		1111	n	11011101	N
		111	o	10101011	O
		111111	p	11010101	P
		110111111	q	111011101	Q
		10101	r	10101111	R
		10111	s	1101111	S
		101	t	1101101	T
		110111	u	101010111	U
		1111011	v	110110101	V
		1101011	w	101011101	W
		11011111	x	101110101	X
		1011101	y	101111011	Y
		111010101	z	1010101101	Z

Figure 2: Partial PSK31 Varicode Alphabet

1011	a	1111101	A
1011111	b	11101011	B
101111	c	10101101	C
101101	d	10110101	D
11	e	1110111	E
111101	f	11011011	F
1011011	g	11111101	G
101011	h	101010101	H
1101	i	1111111	I
111101011	j	111111101	J

PSK31 Varicode Details

- Every letter begins and ends with **1**
- No letter contains more than one **0** in a row
- Two or more zeroes separate letters

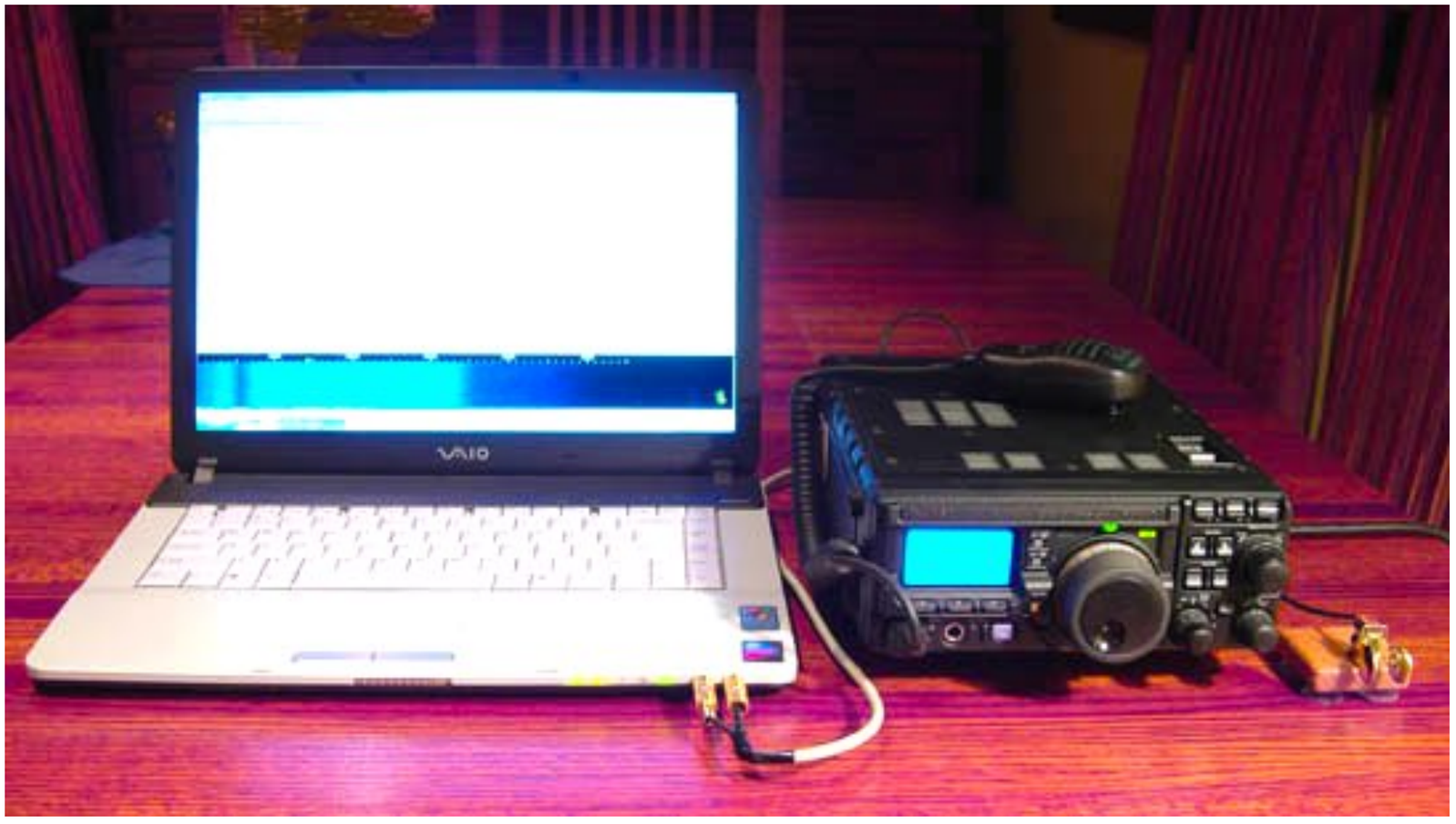
PSK31 Varicode Tricks

- Vary the Idle Count to Hide Data
  - **00** between letters is standard
  - **000** or **0000** works just as well!

- Illegally Long Letters are Ignored
  - This is how the designer added high-ASCII
  - Decoder latches only when it sees **00**

PSK31 PHY Tricks

Building PSK31 Encoder



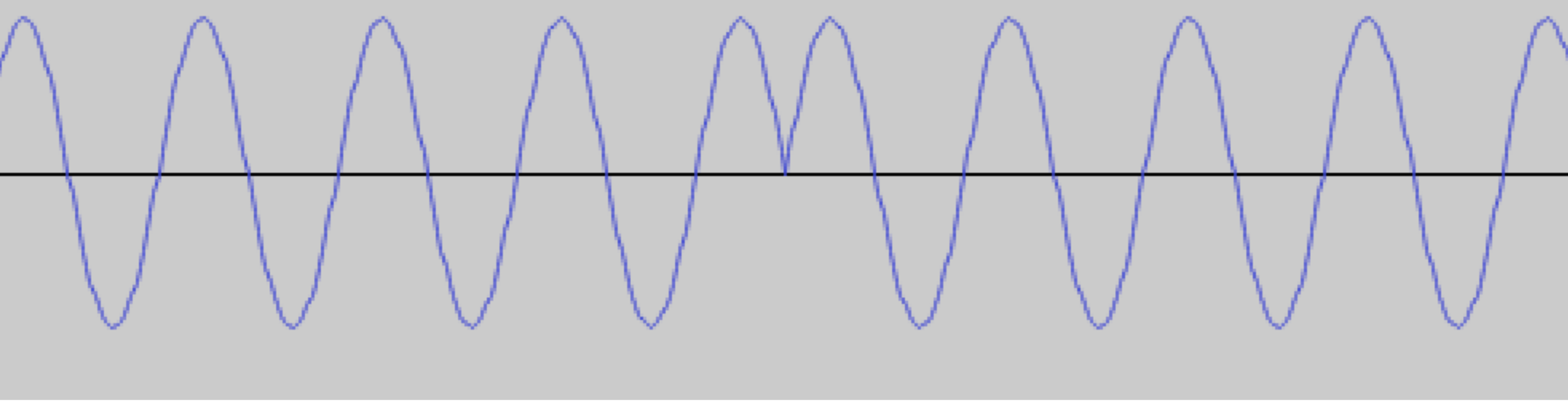
- PSK31 is generated as *__AUDIO__*
- Audio cable runs from sound card to radio

PSK31 Generator Constants

- AUDIORATE=48,000
- VOLUME=32767/2.0
  - Half the maximum amplitude
- DIVISOR=AUDIORATE/1000.0
  - 1kHz Tone
- LENGTH=INT(AUDIORATE/31.25)
  - Number of samples per symbol

PSK31 Generator Variables

- I -- Sample index within the symbol
  - 0 to length
- VALUE -- Integer audio sample at I
  - 16-bit integer
- PHASE -- 0 or 1, indicating Sin or Cos

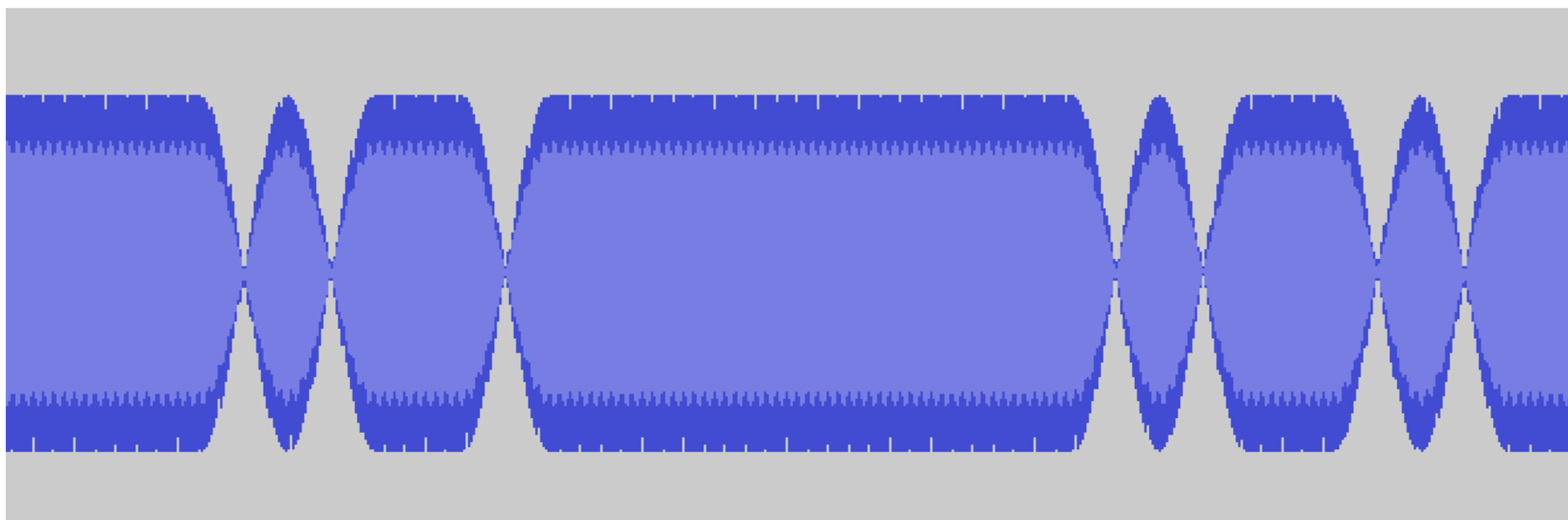


Naive PSK31
Sounds HORRIBLE!

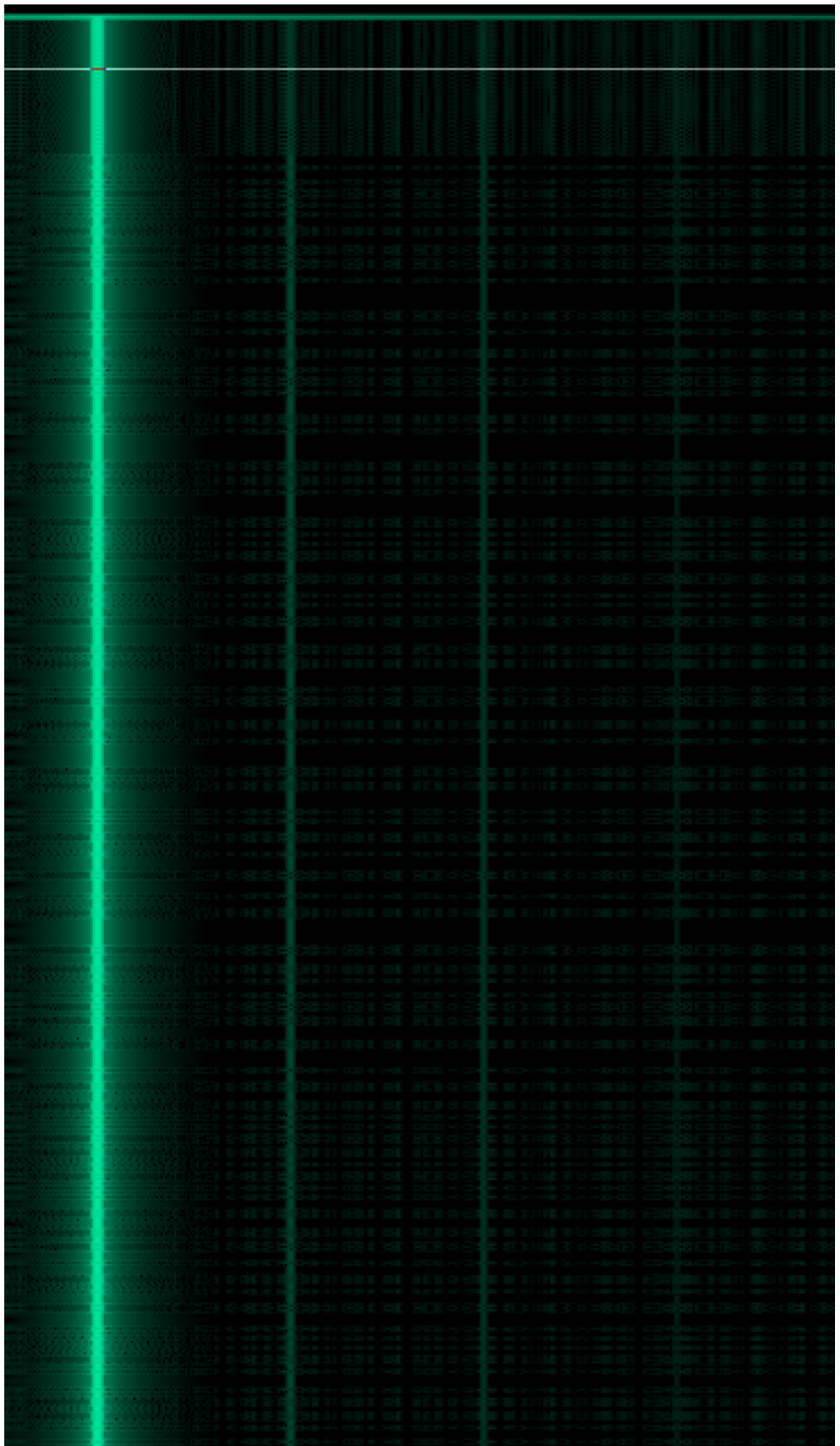
```
SAMPLE[I]=INT(

  SIN(PI*PHASE+2*PI*(I/DIVISOR))

  *VOLUME

)
```

Filtered PSK31 Sounds Good!

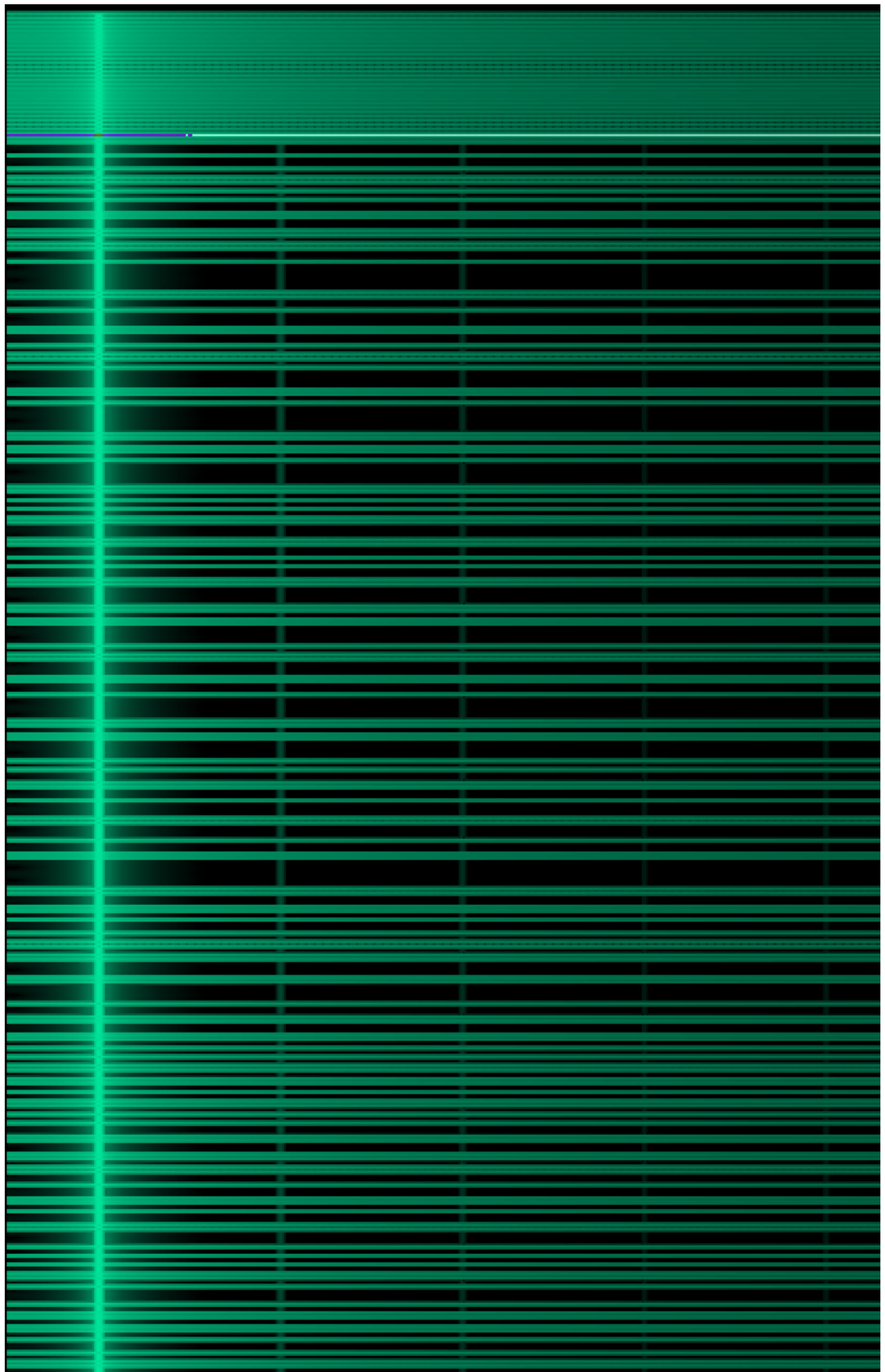
```
ATTEN[I]=SIN(I*PI/LENGTH)

SAMPLE=INT(
    SIN(PI*PHASE+2*PI*(I/DIVISOR))
   *VOLUME
   *ATTEN[I]
)
```



Filtered

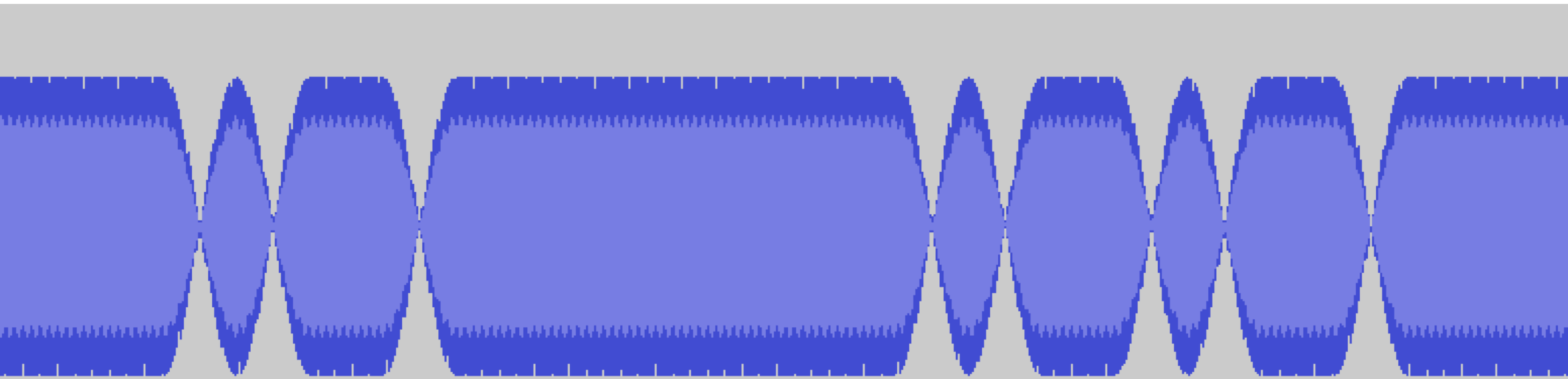


No Filter



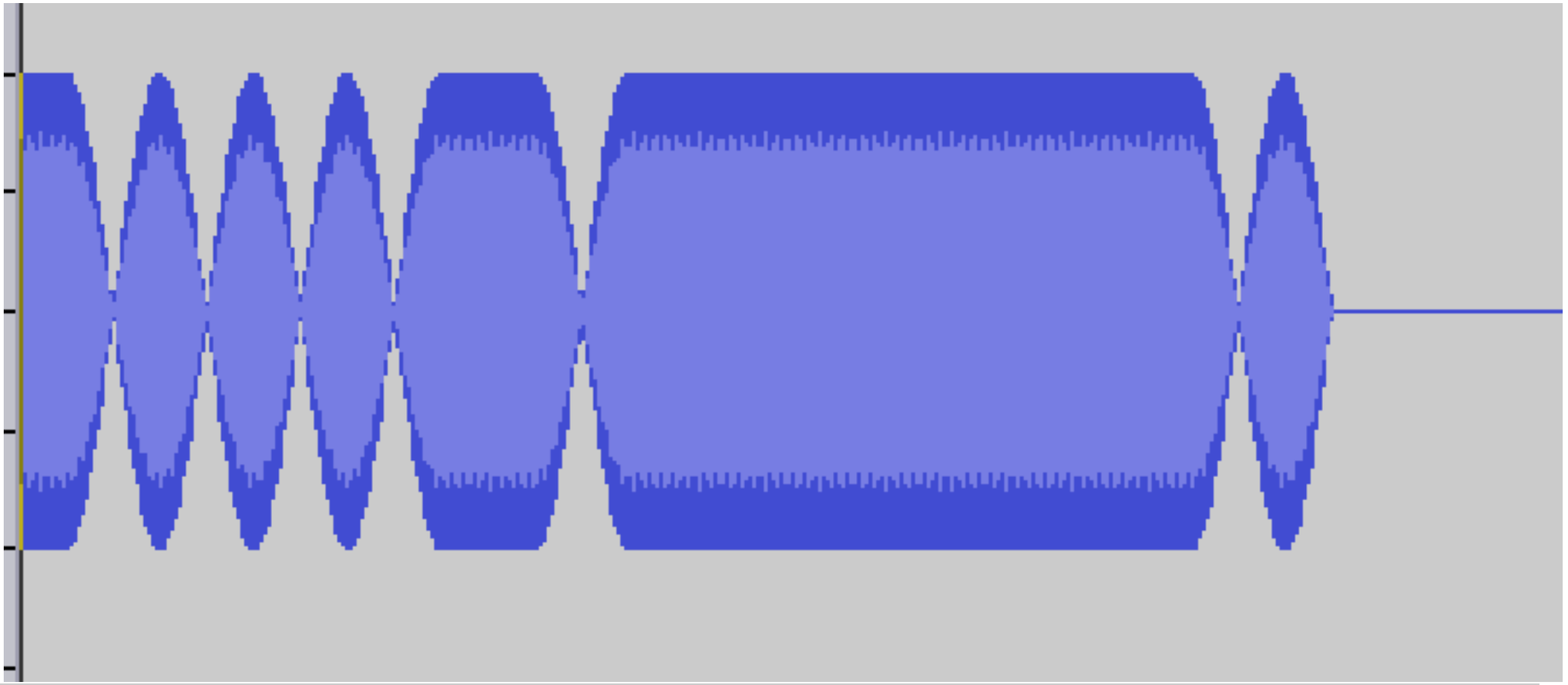
Real PSK

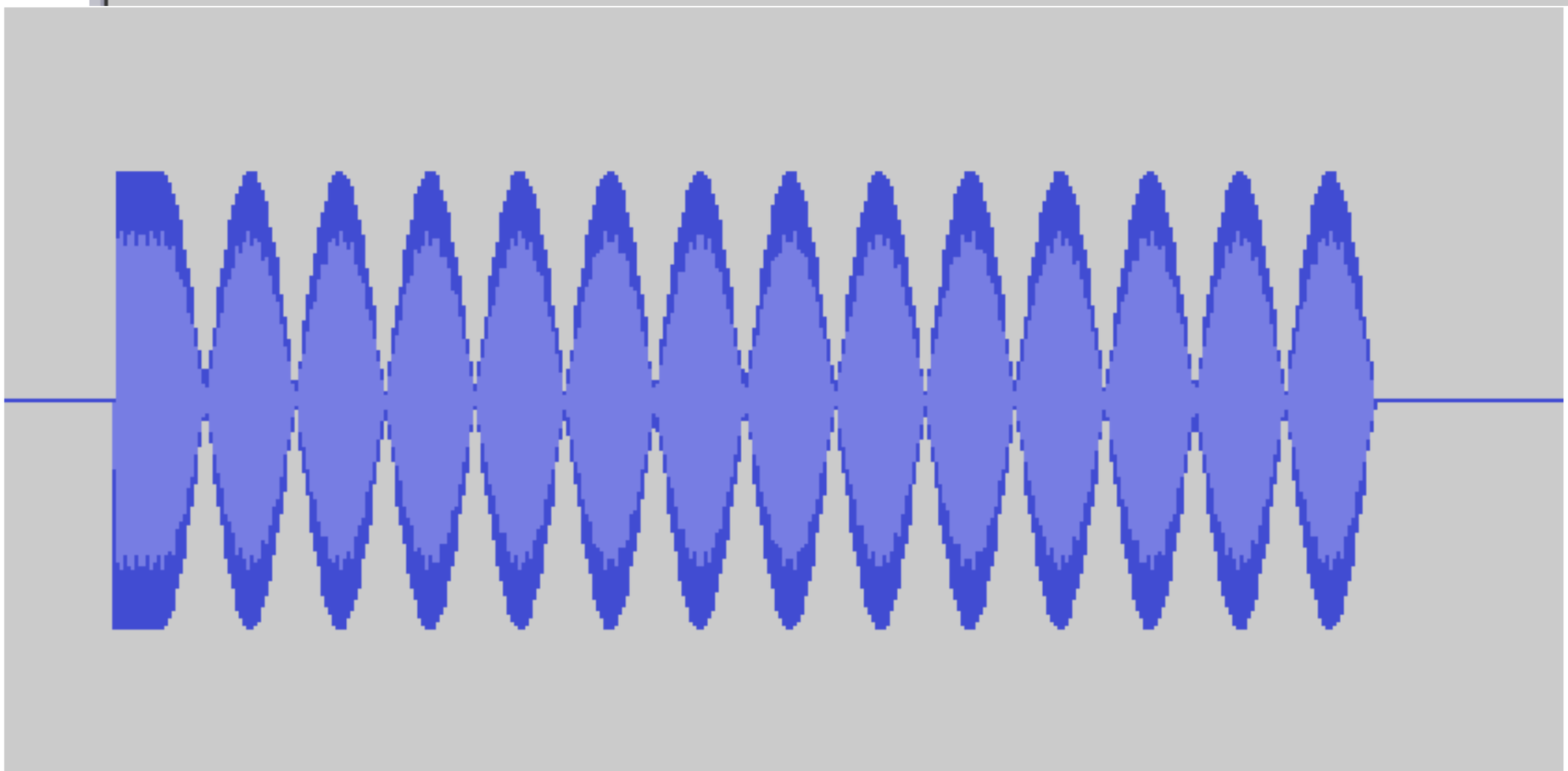
- Filter only on the side that changes phase
- No filter where the phase remains constant



PSK31 Envelope Ambiguity

- PSK31 drops amplitude inside a Zero
  - but not inside a One
    - We can drop amplitude **anyways**!
- Most receivers don't notice the difference
- But it's still measurable if you look for it
- (This trick from Craig Heffner)





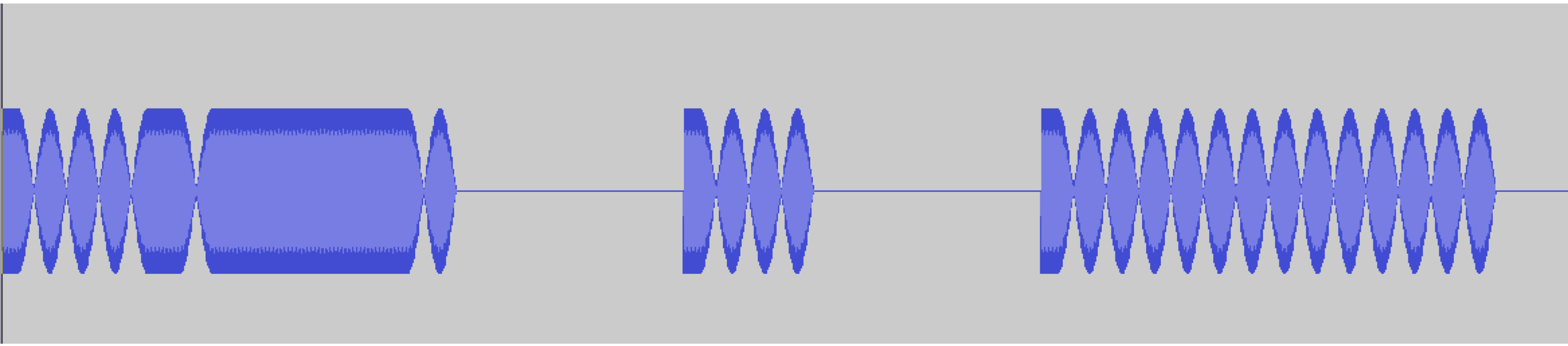
PSK31/Morse Polyglot

- PSK31 is tolerant to wild swings in amplitude
  - Remember: it's about **Phase**, not Amplitude!
- So we can send Morse with that amplitude :)
  - PSK31 remains beneath it

Morse/PSK Polyglot

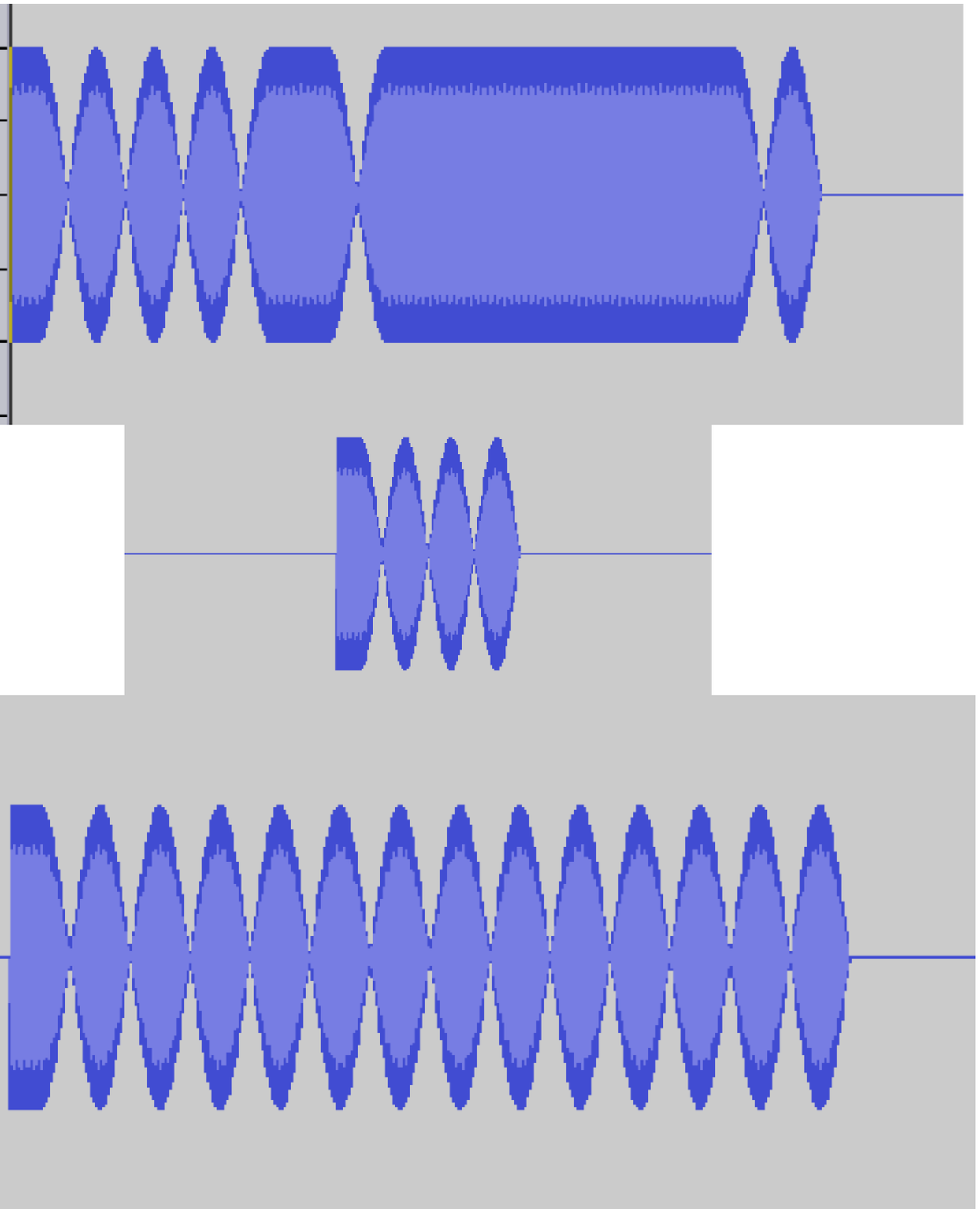
- Dahs encode letters.
- E is shorter, fits in a Dit.
- Left is waterfall of letter K.
  - Dah-Di-Dah

Morse/PSK Polyglot



Dah Di Dah

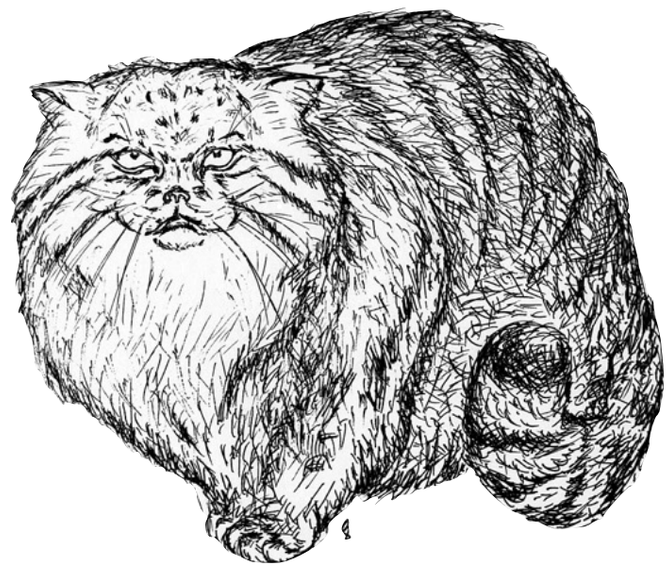
Morse/PSK Polyglot



- First Dah has K (dah-di-dah) encoded.
- Dit is all Zeroes.
- Final Dah is all Zeroes

PSK31/RTTY Polyglot

- RTTY cares about Relative Power
- PSK31 is tolerant to changes in power
  - Only cares about Phase!
- We can combine the two!



QPSK31
Error-Correcting Codes

- QPSK31 uses a Forward Error Correction Code
  - Some bits can be flipped safely
- Drapeau and Dukes did this at Defcon
  - For JT65, a heavily corrected protocol
  - LOTS of bits per bit

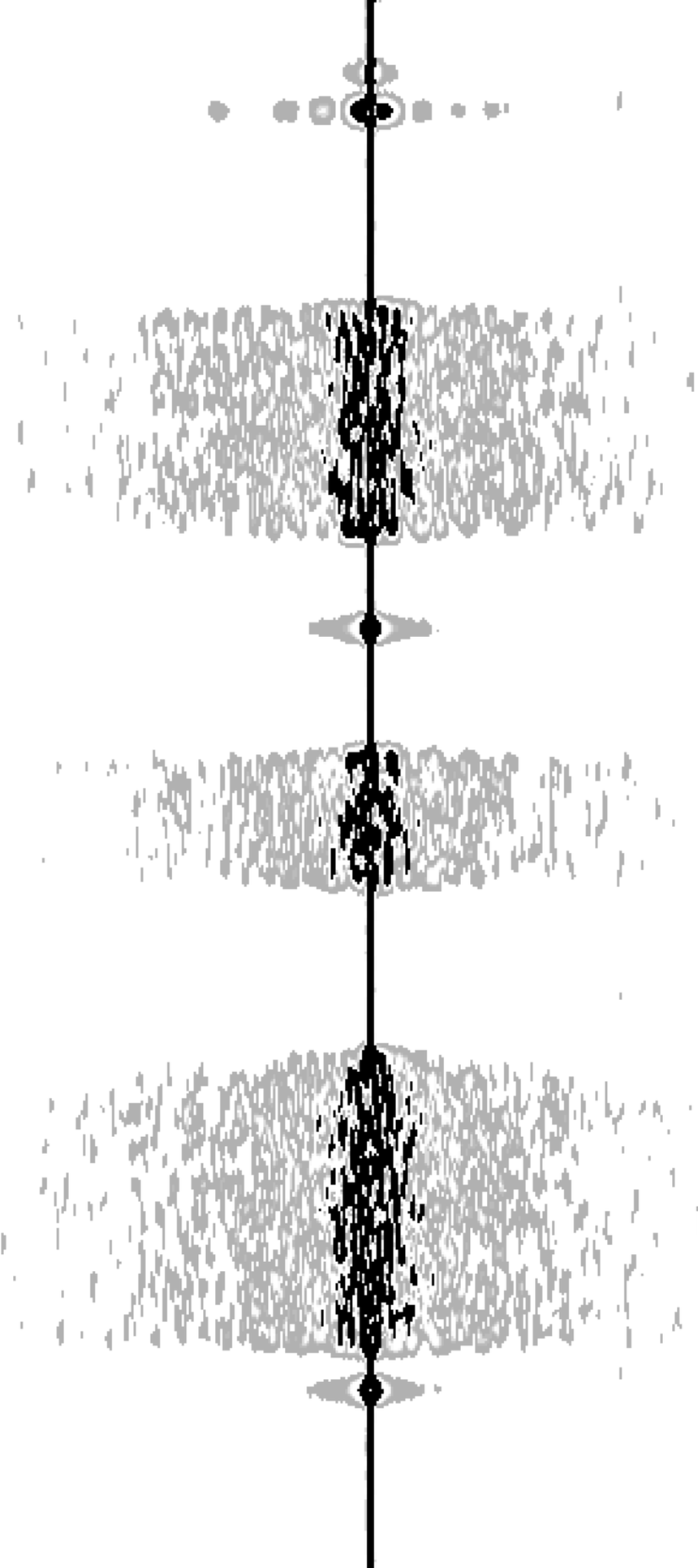
Bit Flipping in FEC

- Forward Error Correction allows bits to be flipped
  - But is this subtle?
- Good tools don't yet exist for reversing bit errors
  - Was the error intentionally transmitted?
  - "What does noise sound like & does this sound like normal noise?"

Madeline

Madeline

- Data runs over Ethernet
- You control a bit of data
    - But not very well (HTTP over Tor, for example)
- You want to exfiltrate a signal
    - THE CLIENT IS HERE, GUYS!
- If the wiring is bad, it's not that hard



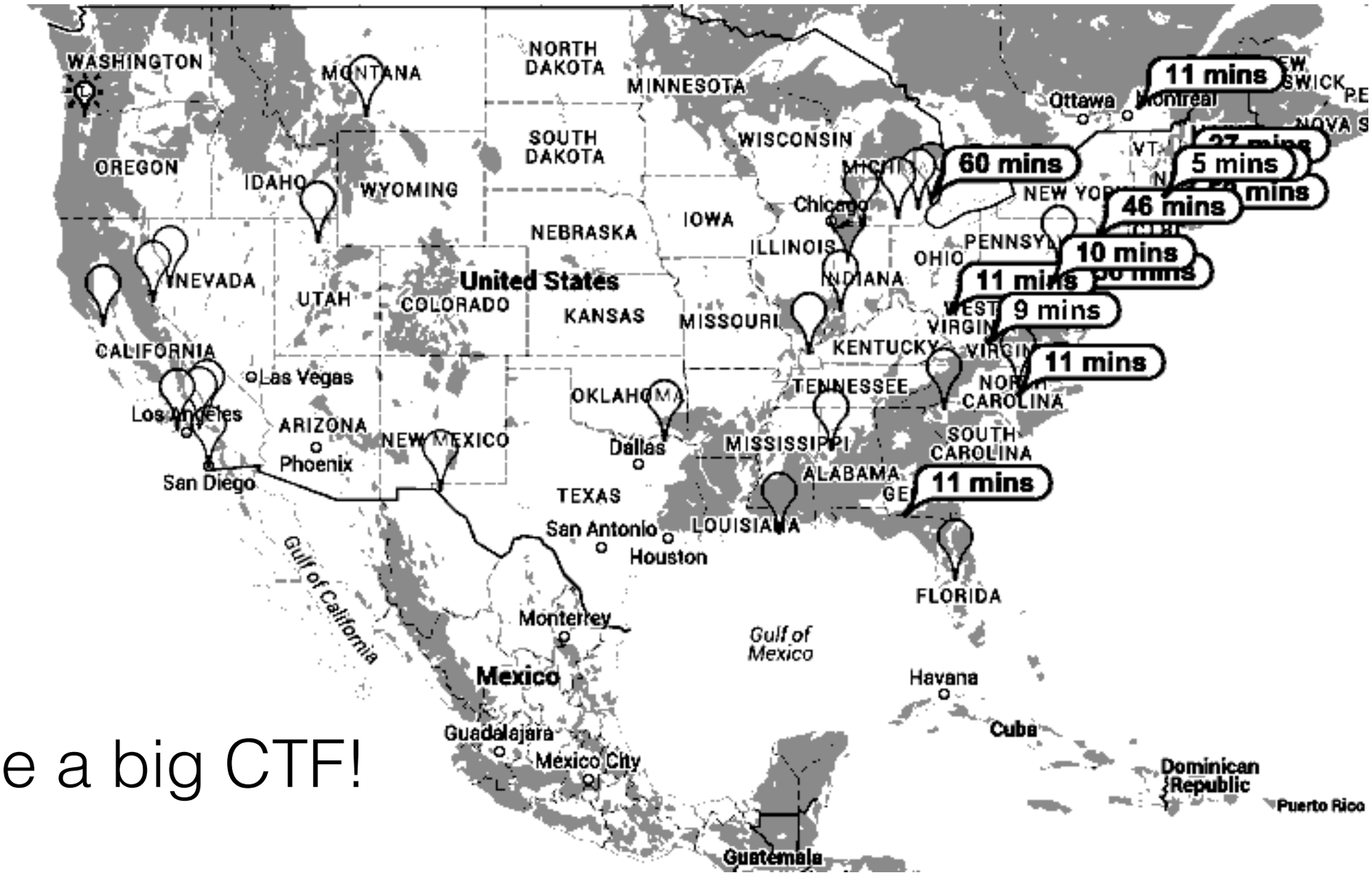
Dah

Di

Dah

Madeline

Care to play along?



- Let's have a big CTF!
  - 10 meter beacon from Northeast USA
  - Receive by USB in most of Western Hemisphere.

Conclusions

- **PHY** is pliable and should be played with
  - start with simpler protocols like PSK31, RTTY, ...
  - more complex protocols are built of similar pieces
  - parser **differentials** abound & should be understood
- Digital radio parsers allow **polyglots** with modulation, encoding, and even error correction
  - not only in PDF/ZIP/GIF/JPEG/... of PoC||GTFO ;)

Image credits

- Manul drawings by Natalia Pavlushina
  http://www.animalist.ru/?action=show_gallery&artist=pavlushina
  and Olga Zakharova
  http://www.savemanul.org/images/full/manul_3w.jpg