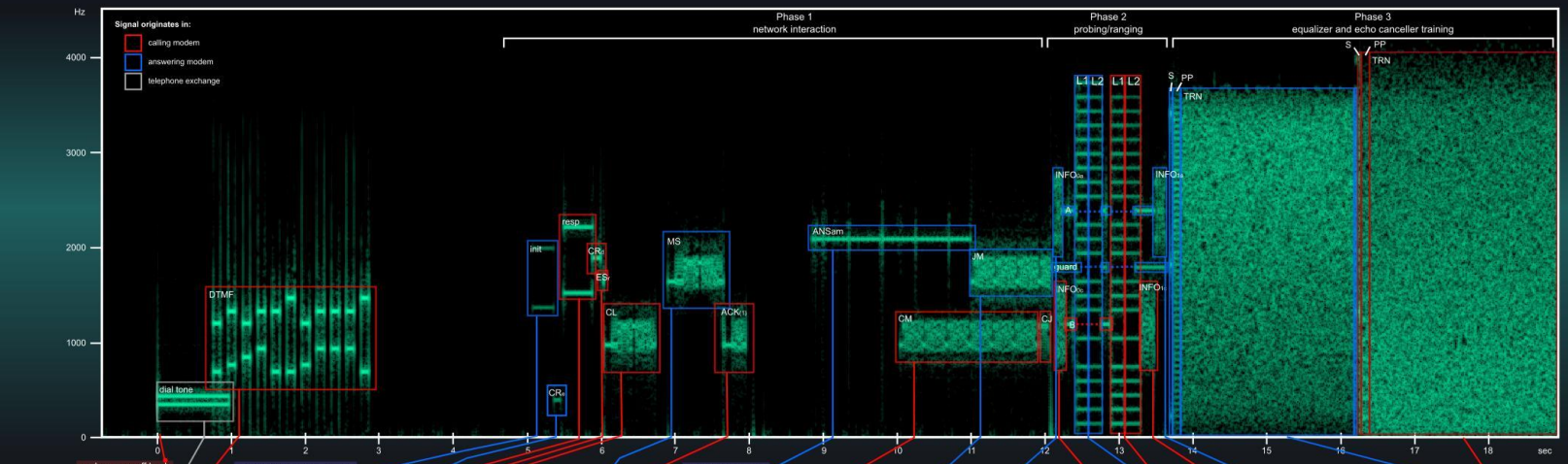
My journey into FM-RDS

Oona Räisänen

windytan.com

twitter: @windyoona

The Sound of the Dialup: an Example Handshake



modem goes off hook

telephone exchange sends a dial tone

modem dials 1-(570)234-0003, a number in Pennsylvania

answering modem initiates a V.8 *bis* transaction

answering modem asks caller to list its capabilities

caller responds to V.8 *bis* initiation, agrees to list its capabilities

caller requests to escape from telephony into information transfer mode

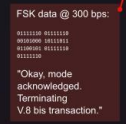
FSK data @ 300 bps:

"I'm capable of full V.8.
I can transmit ACK.
By the way,
my country is the U.S.
I was manufactured by Net2phone Inc."

FSK data @ 300 bps:

"Why don't we use V.8 then."

FSK data @ 300 bps:



"Okay, mode acknowledged.
Terminating
V.8 bis transaction."

answering modem disables echo suppressors and cancellers in PSTN

FSK data @ 300 bps:

(repeated 6 times)

"Modulation modes available:
-PCM V.90/V.92 analogue
-V.34 duplex
-V.32/V.32 bis
-V.23 duplex
-V.22/V.22 bis
-V.21

V.42 LAPM is available.

PSTN connection is over a regular landline (not cellular).
My network is analogue."

FSK data @ 300 bps:

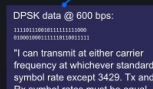
(repeated 3 times)

"Oh, I can do any of those modes as well. Except my V.90/V.92 is digital.

V.42 LAPM is available.

PSTN connection is over a regular landline (not cellular).
My network is digital."

DPSK data @ 600 bps:



"I can transmit at either carrier frequency at whichever standard symbol rate except 3429. Tx and Rx symbol rates must be equal.

I can reduce power if needed.
I can support up to 1664-point signal constellations.
My clock source is internal."

DPSK data @ 600 bps:

"I can transmit at either carrier frequency at whichever standard symbol rate except 3429. Tx and Rx symbol rates must be equal.

I can reduce power if needed.
I can support up to 1664-point signal constellations.
My clock source is external."

modems send a wide-spectrum probing signal in both directions to do measurements of the telephone line

DPSK data @ 600 bps:

"Please don't reduce your power by more than 6 dB.

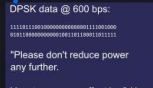
I'm not equipped to accurately measure the frequency offset of the tones you sent.

Using different symbol rates, we could achieve the following:

symrate	ur pre-emph α	bps
2400	6 dB	14400
2743	8 dB	16800
2800	8 dB	16800
3000	8 dB	16800
3200	8 dB	19200
3429	10 dB	21600

I can use the higher frequency carrier at any symbol rate."

DPSK data @ 600 bps:



"Please don't reduce power any further.

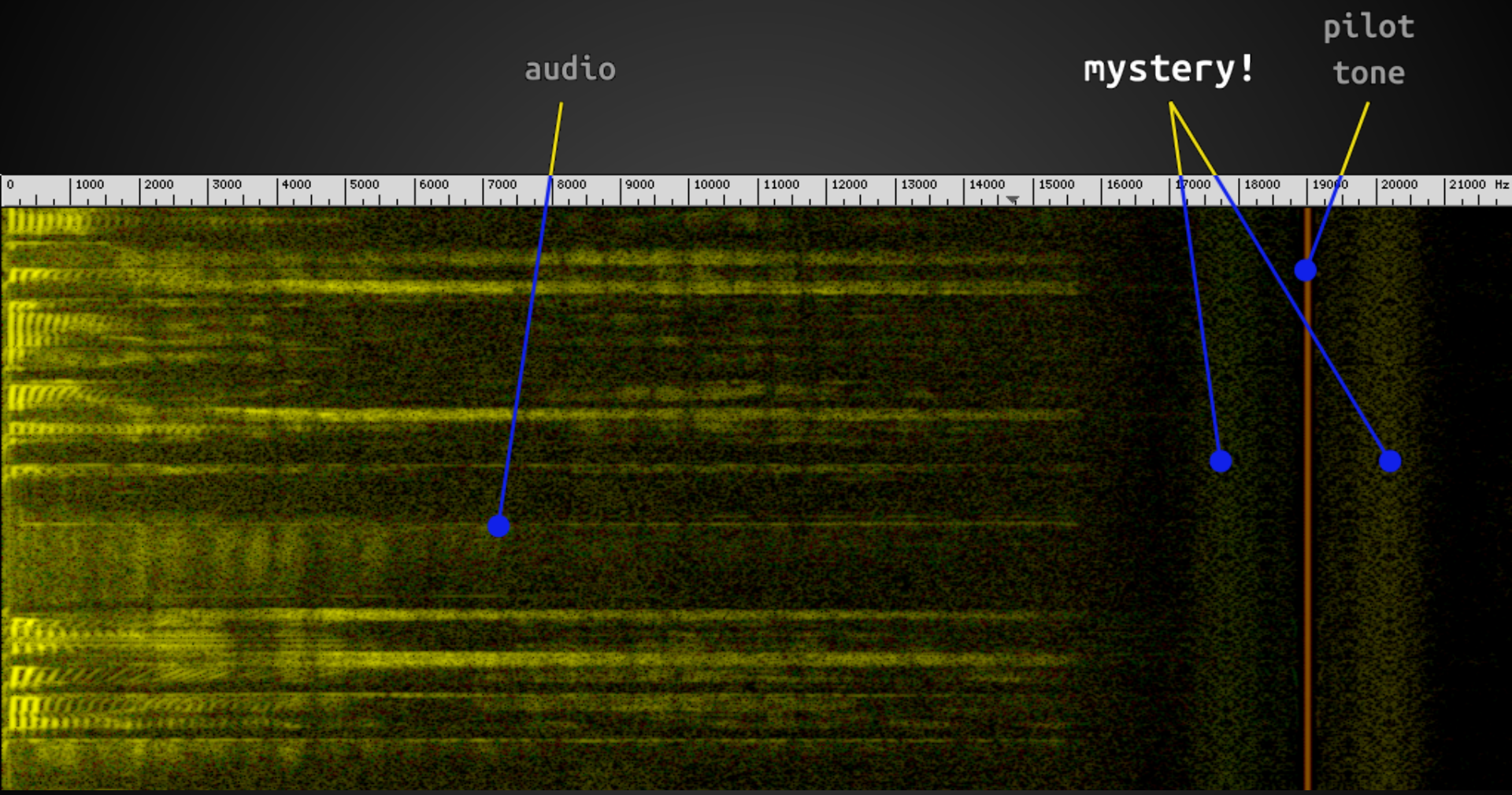
Your tones were offset by 0 Hz.

Let's use a symbol rate of 3200. We can achieve a maximum of 4800 bps. For your pre-emphasis filter, select the parameters β = 1.0 dB and γ = 2.0 dB.

Please use carrier at 1920 Hz for transmission, I'll use 1829."

Modems go to scrambled data and learn how the other modem sounds over the channel. The final bitrate and signal constellation are also decided on.

A final training phase called Phase 4 will follow, after which the modem speaker goes mute and data can be put through the connection.


audio
mystery!
pilot
tone
0
1000
2000
3000
4000
5000
6000
7000
8000
9000
10000
11000
12000
13000
14000
15000
16000
17000
18000
19000
20000
21000 Hz

(rds-mixdown.wav)


FM1 106.7 ST RDS 2:19
KBPI ROCKS THE ROCK
Back

AF CT EON PI

PS PTY RT TA/TP

TMC Pager ...

NATIONAL RADIO SYSTEMS COMMITTEE

2500 Wilson Boulevard
Arlington, VA 22201-3834
(703) 907-7500
FAX (703) 907-7501

1771 N Street, NW
Washington, DC 20036-2891
(202) 429-5346
FAX (202) 775-4981

UNITED STATES RBDS STANDARD

April 9, 1998

Specification of the radio broadcast data system (RBDS)

Descriptors: Broadcasting, sound broadcasting, data transmission, frequency modulation, message, specification

---

Sponsored by the Electronic Industries Association and the National Association of Broadcasters

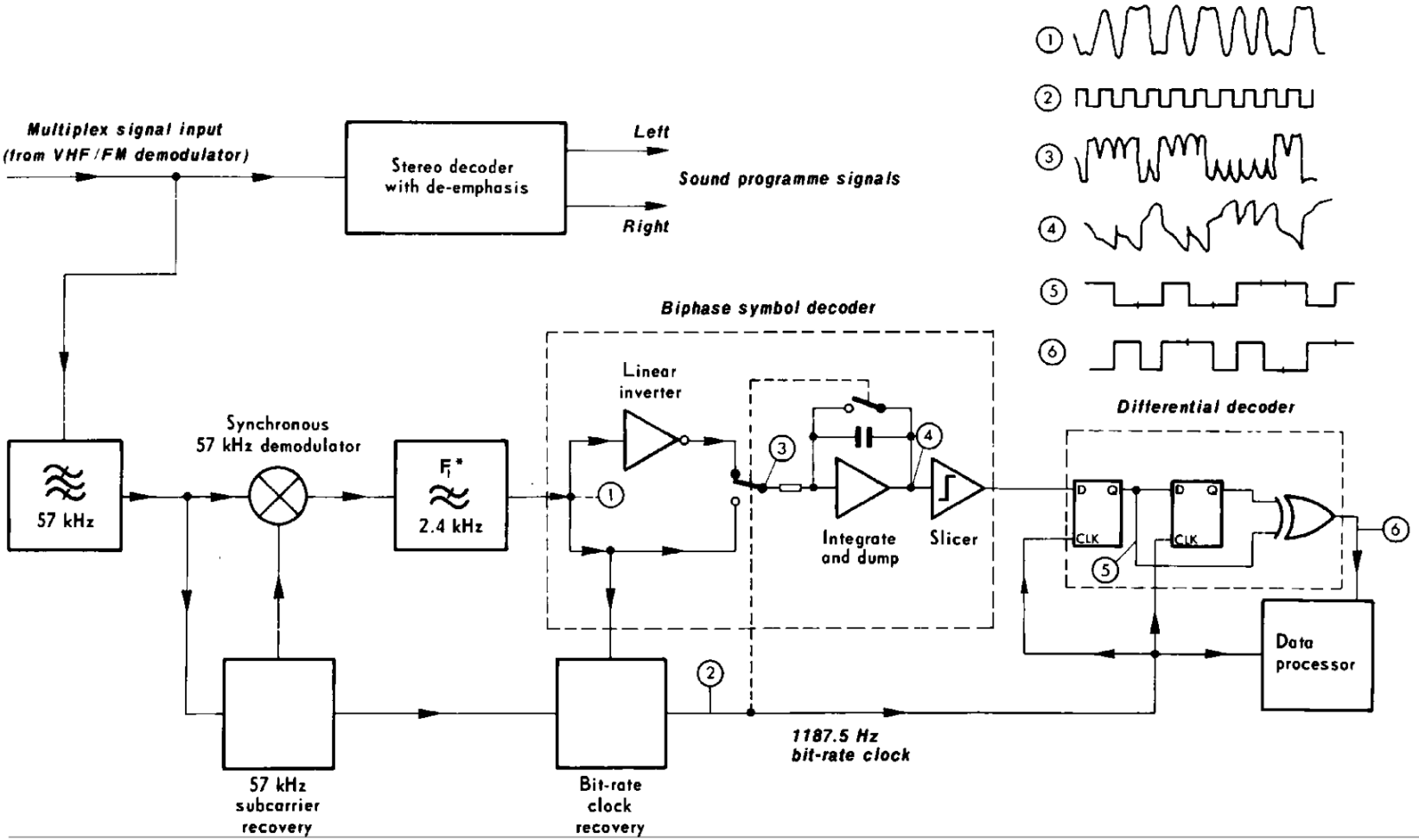
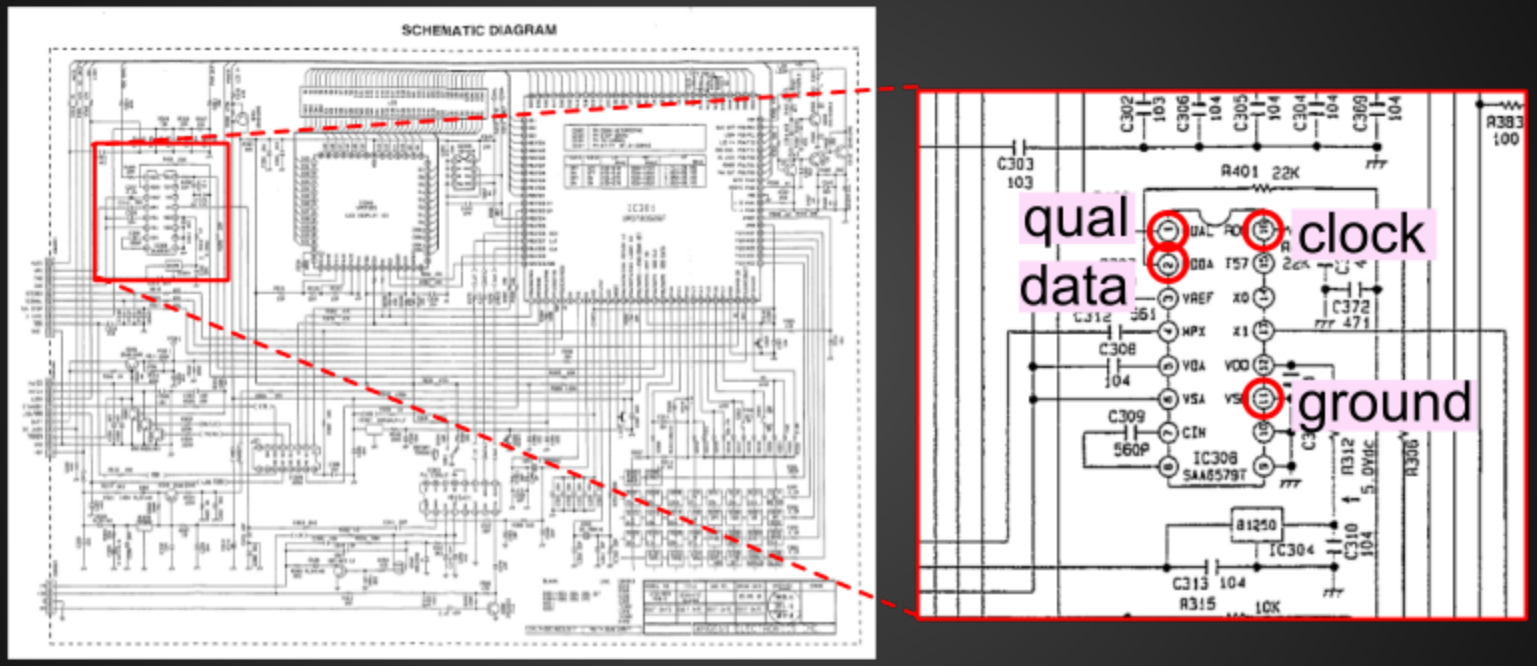
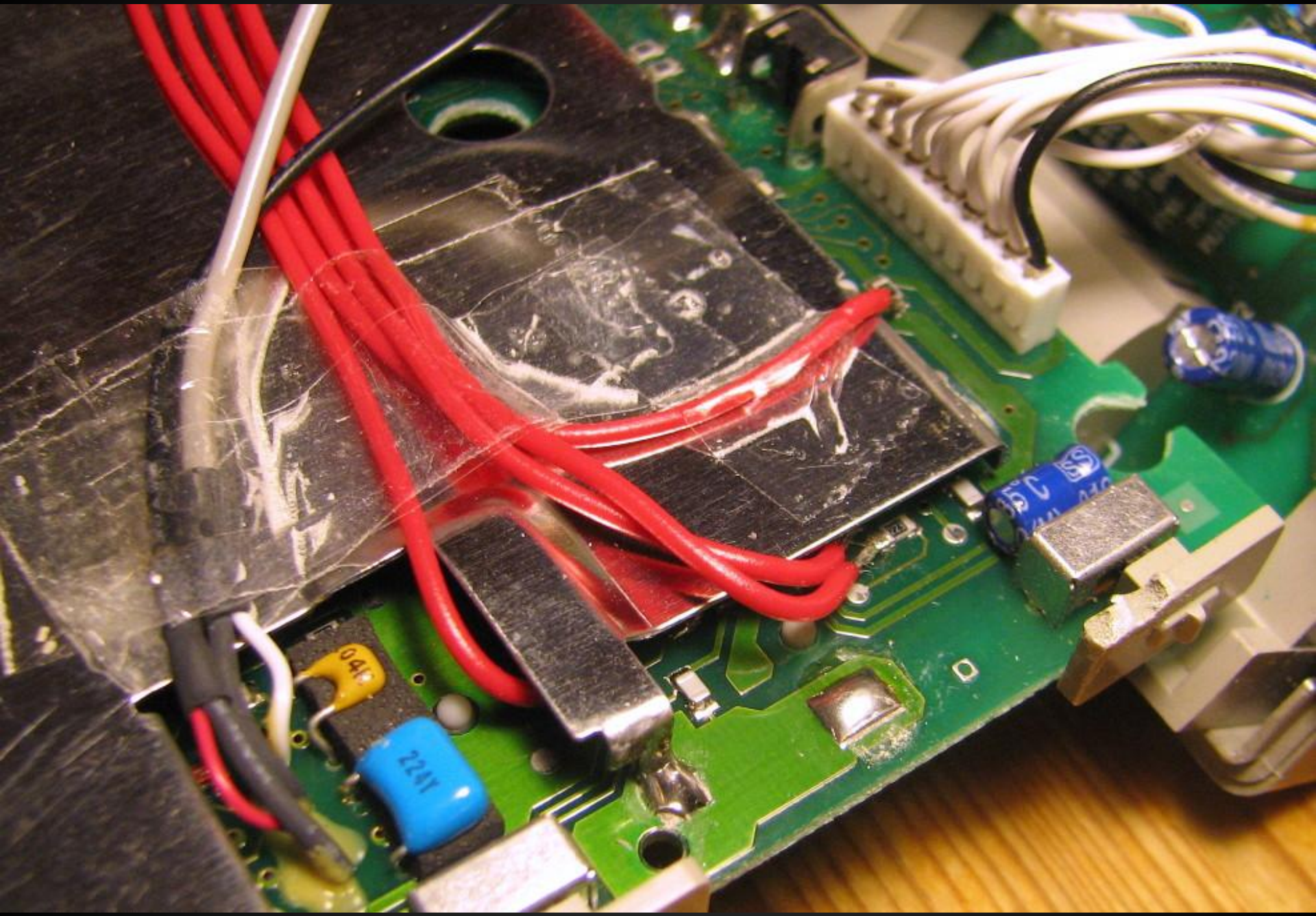


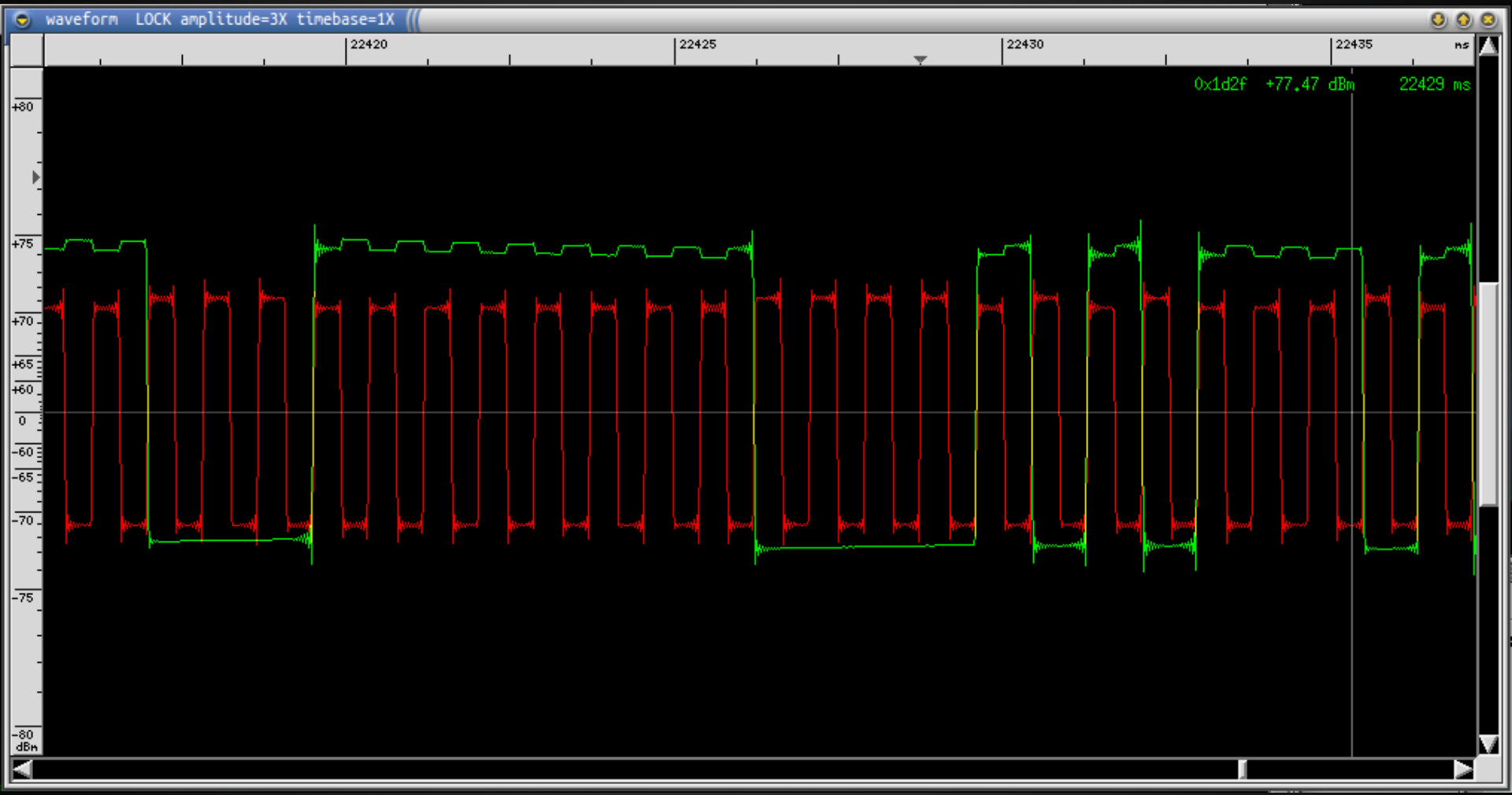
Figure 2: Block diagram of a typical radio-data receiver/decoder

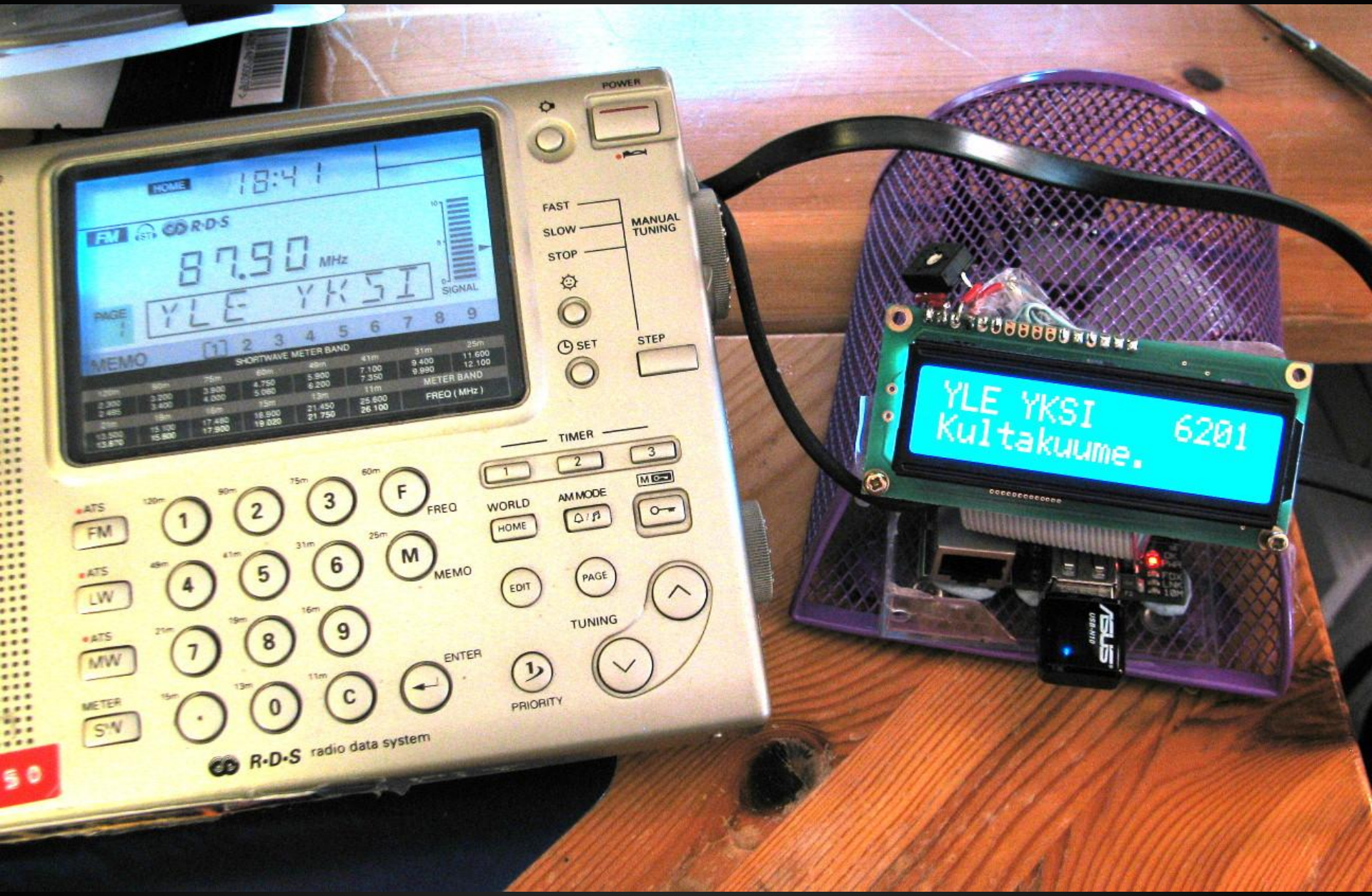

redsea
RadioText RT+ eRT EON TMC TP TA
YLESUOMI
PI 6203
RDS
ECC fi
MHz 94.0
PTY News
Päivän peili ja sää.

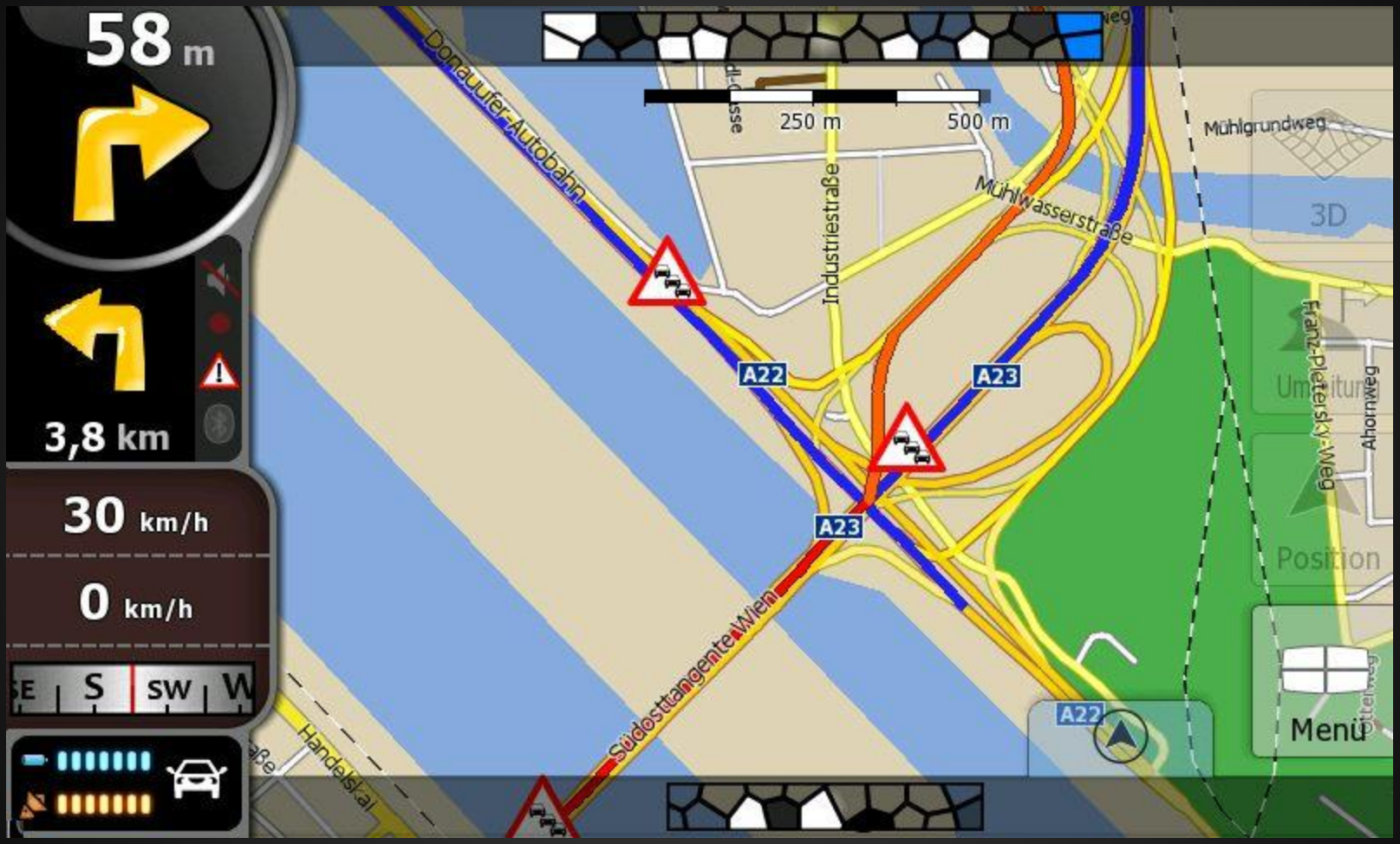

SCHEMATIC DIAGRAM
qual
clock
data
ground
C303
103
R401 22K
C372
471
C308
104
C309
560P
IC308
SAA6579T
IC304
C313 104
R315 10K


224Y


waveform LOCK amplitude=1X timebase=1X
770 771 772 773 774 775 776 777 778 779 780 781 782 783 784 785 786 787 788 789 790 791 ms
0x6710 +88.43 dBm 782 ms
+90 +85 +80 +75 +70 0 -70 -75 -80 -85 dBm


waveform LOCK amplitude=3X timebase=1X
22420
22425
22430
22435
ns
0x1d2f +77.47 dBm 22429 ms
+80
+75
+70
+65
+60
0
-60
-65
-70
-75
-80
dBm

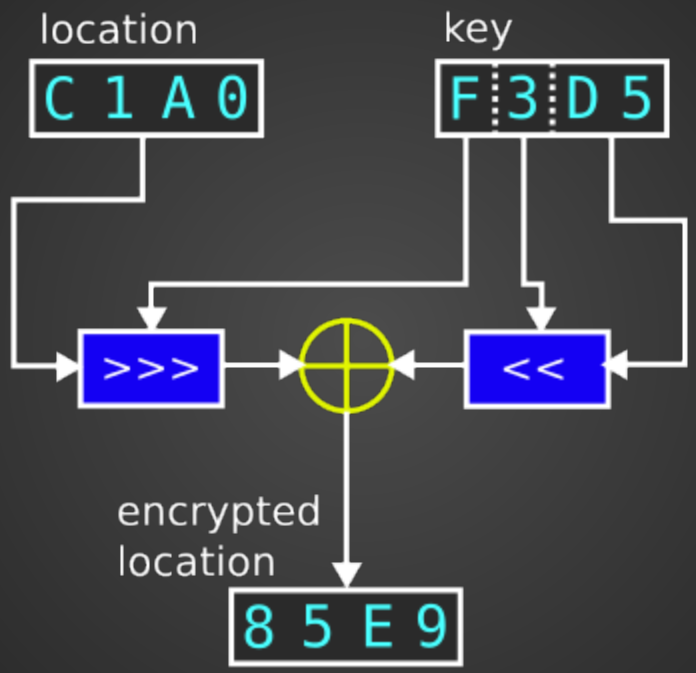

YLE YKSI 6201
Kultakuume.
POWER
HOME
18:41
R·D·S
87.90 MHz
YLE YKSI
SIGNAL
PAGE
MEMO
SHORTWAVE METER BAND
METER BAND
FREQ (MHz)
FAST
SLOW
STOP
MANUAL TUNING
SET
STEP
TIMER
WORLD HOME
AM MODE
FM
LW
MW
SW
METER
FREQ
MEMO
EDIT
PAGE
TUNING
ENTER
PRIORITY
R·D·S radio data system

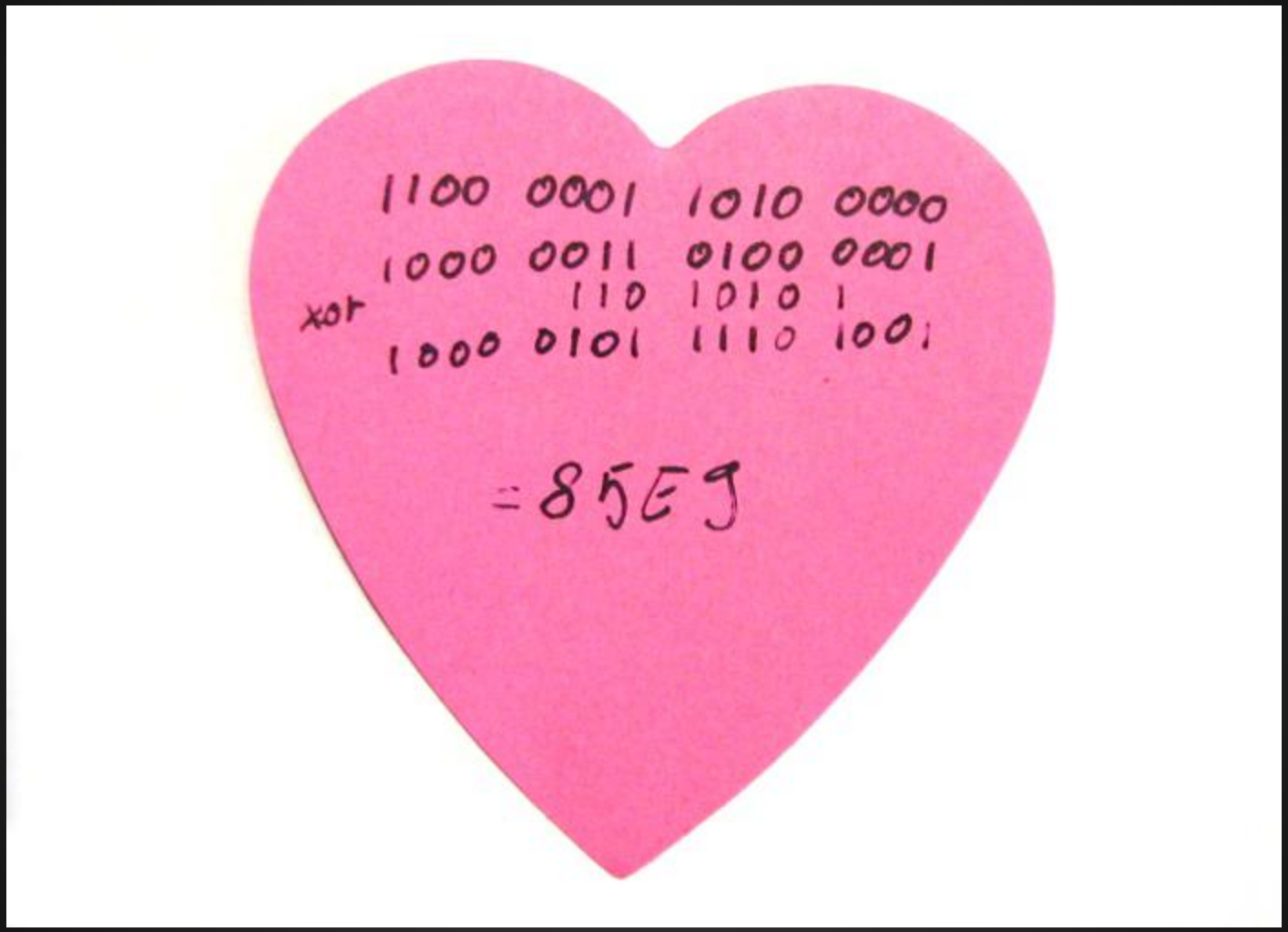

58 m
3,8 km
30 km/h
0 km/h
E
S
SW
W
250 m
500 m
Donauufer-Autobahn
Industriestraße
Mühlwasserstraße
Mühlgrundweg
3D
A22
A23
A23
Franz-Pletersky-Weg
Ahornweg
Position
Menü
A22
Südosttangente Wien
Handelskai

— ability for terminals to be activated to receive an encrypted service on an individual basis.

After calling for candidate proposals, the submission from Deutsche Telekom was judged by an expert panel to have best met the pre-determined criteria the task force had established. The method encrypts the sixteen bits that form the Location element in each RDS-TMC message to render the message virtually useless without decryption. The encryption is only 'light' but was adjudged to be adequate to deter other than the most determined 'hacker'. More secure systems were rejected because of the RDS capacity overhead that was required.

After ratification by the TMC Forum Business Group and Management Group of the decision to adopt the


location
C 1 A 0
key
F 3 D 5
>>>
<<
encrypted
location
8 5 E 9


1100 0001 1010 0000
1000 0011 0100 0001
xor 110 1010 1
1000 0101 1110 1001
=85E9

Roadworks until mid-November, neg., 3 locations, 50 km/h

ENCID	Location
3	21888
5	51448
8	267
9	3576
13	15772
18	31279
25	9280
27	46755
31	18456
-	926

Roadworks. Delays expected until end of September, 3 locations, Slow moving maintenance vehicles

ENCID	Location
5	51632
8	51013
9	13624
17	33699
18	60651
25	16366
26	20859
27	60229
31	52312
-	4575


CENSORED

:)

RDS-TMC

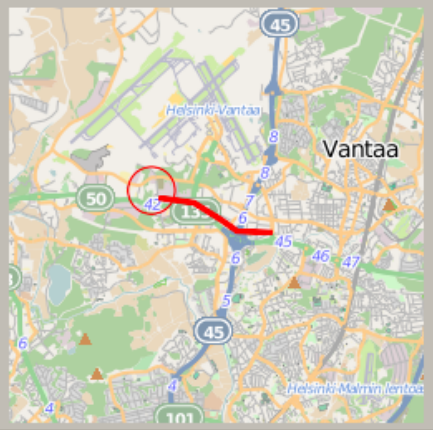
TMC Service

Service ID	1
Service provider	MMN TMC+
Location table	6/17
Encryption	Encrypted
Key identifier	5 (OK)
Mode	Basic
Scope	National, regional, urban

Received messages

	Description	Location	Until	Duration	Direction	Extent
	Maakaapelityö.	Mäntsälä	mid-October		positive	3
	Kuuraa.	Espoo	02:00		negative	10
	Kuuraa.	Nurmijärvi	02:00		negative	30
	Tietyö.	Vihti	end of October		positive	1
	Kuuraa.	Nurmijärvi	02:00		negative	29
	Maakaapelityö.	Askola	mid-October		positive	9
	Siltatyö.	Vantaa	end of October		positive	4

Message



Event	Siltatyö. Hitaasti liikkuvia kunnossapitoajoneuvoja.
LocRef	2818
Route	Tie 50 (Kehä III)
Segment	
Direction	Länteen
Location(s)	Koivuhaan liittymä ⇒ Pakkalan liittymä
Coordinates	60°17'44.9" N, 24°56'32.2" E
Speed limit	50 km/h
Lasts until	end of October
Expires in	166944
Fully received?	☑
Times received	5
Last received	2011-02-12 01:35:04

Tuomo Eloranta 06 May, 2013 17:16

Sad to request, but can you take thisoffline. It is kind of our service you hacked :)

Tuomo Eloranta,
Technology Director
Mediamobile Nordic

Reply Delete

Tuomo Eloranta 06 May, 2013 17:16

Sad to request, but can you take thisoffline. It is kind of our service you hacked :)

Tuomo Eloranta,
Technology Director
Mediamobile Nordic

Reply Delete

▼ Replies

Oona Räisänen 06 May, 2013 19:08

"Kind of"? Sure, if that's what you deem appropriate.

Please send me a cryptographically signed email (windyoona@gmail.com) with the complaint, i.e. some explanation as to how I'm infringing your IP rights, and which parts of the post are infringing and should be removed. I will replace them with [deleted as requested by Mediamobile Nordic].

Also, please provide me with a means of verifying the signature and sender, preferably a public key at a URL under your company domain.

Delete

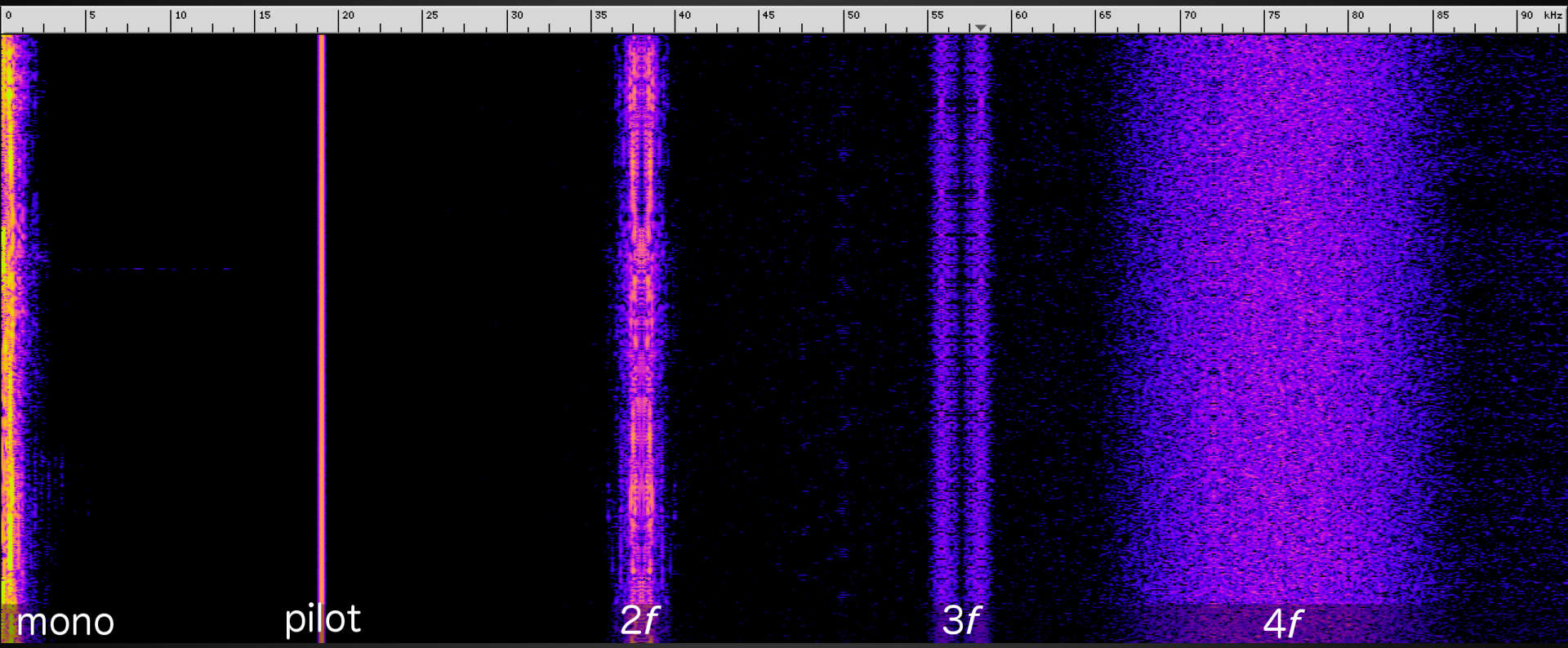
Reply

CRYPTOME

Donate for the Cryptome Archive DVDs of 74,000 files (17GB) from June 1996 to December 2012.

Search Cryptome

2013-0468.pdf	DoD Report on PRC Military-Security 2013	May 7, 2013	(2.0MB)
2013-0467.pdf	Ratcatcher Syllogism-Private Security Philosophy	May 7, 2013	
2013-0466.pdf	Tsarnaev Gets Federal Defender Program	May 6, 2013	
2013-0465.pdf	RDS-TMC Decrypted	May 6, 2013	(3.2MB)
2013-0464.htm	Syrian Electronic Army Hacks Haifa Infra Site	May 6, 2013	
2013-0463.pdf	FBI E-mail Policy	May 6, 2013	
2013-0462.htm	Cryptome Boston Bomb Photos 2X WikiLeaks Traffic	May 6, 2013	
2013-0461.pdf	Barrett Brown New Attorney Ghappour Pro Hac Vice	May 6, 2013	
2013-0460.pdf	Jeremy Hammond Hearing Postponed to May 17, 2013	May 6, 2013	
2013-0459.pdf	Strategies for Serving Our Women Veterans	May 6, 2013	
2013-0458.pdf	DoD Electronic Fingerprint Capture	May 5, 2013	


0
5
10
15
20
25
30
35
40
45
50
55
60
65
70
75
80
85
90 kHz
mono
pilot
2f
3f
4f

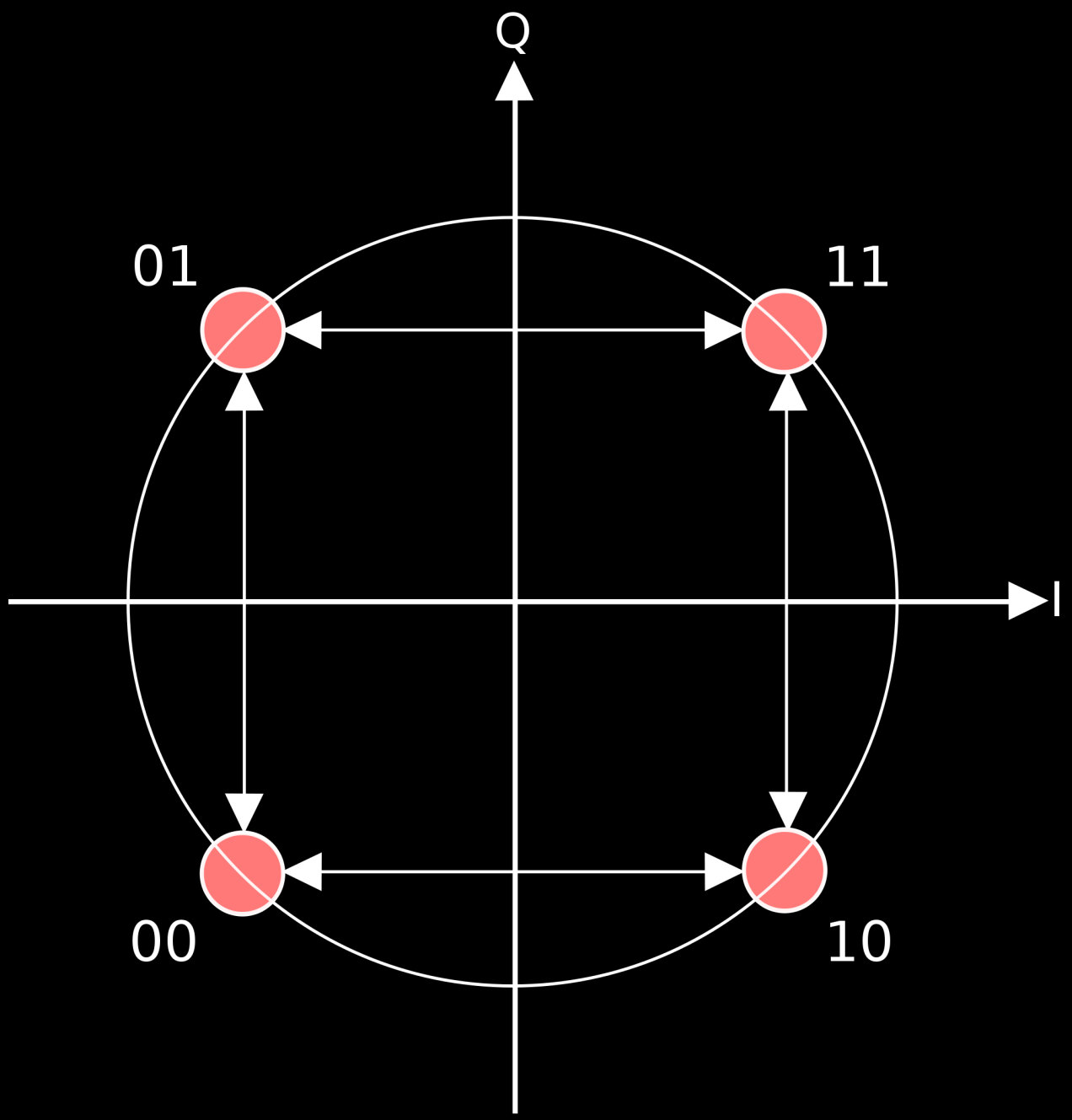
HSL:N AIKATAULUNÄYTÖT TOIMIVAT YLE 1:N TAAJUUKSILLA

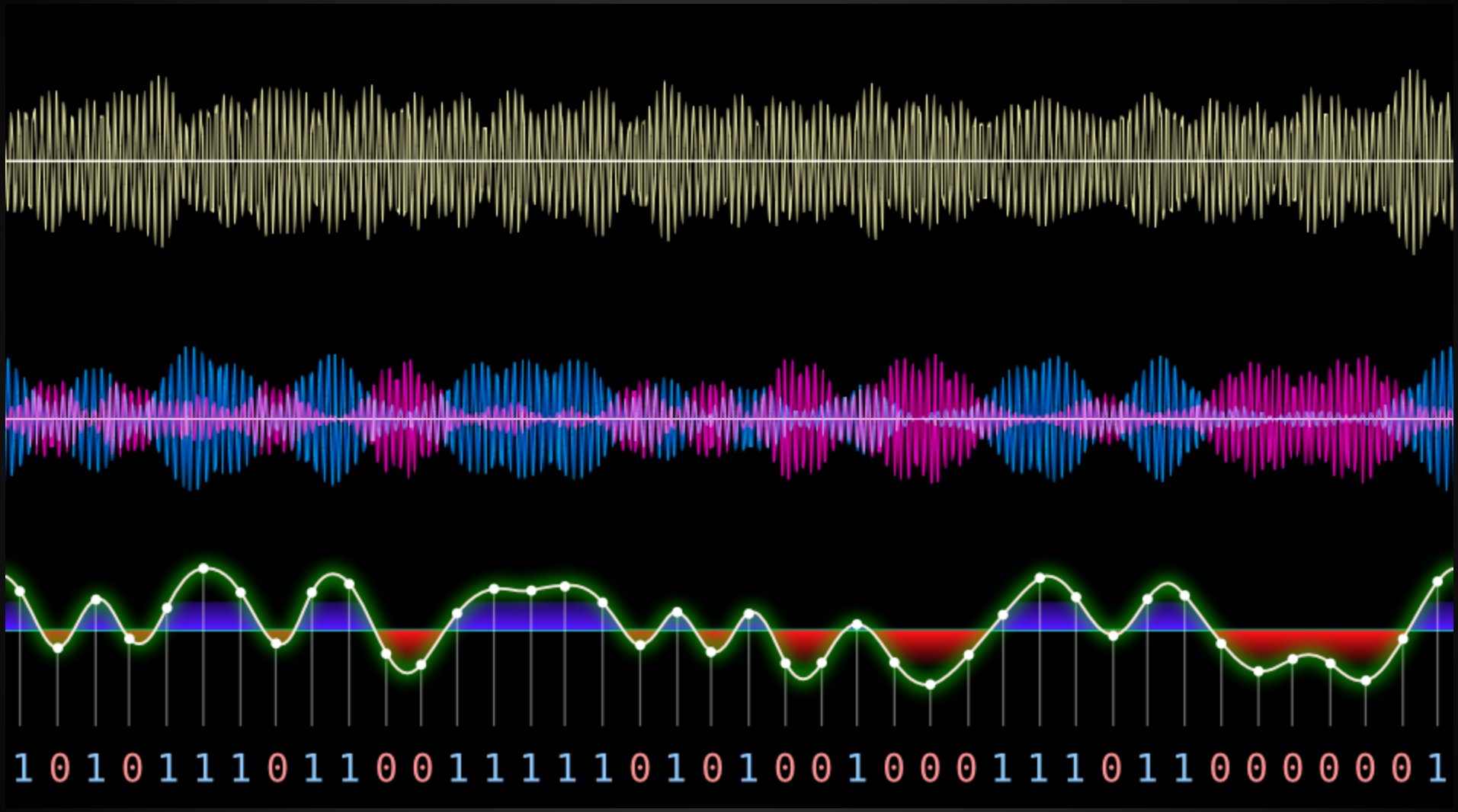
Radioaalloilla apua arkeen

Teksti: Maarit Seeling
Kuva: Susa Junnola

Helsingin bussi- ja raitiovaunupysäkkien radiosignaalia hyödyntävät aikataulunäytöt ovat erinomainen esimerkki siitä, miten radioaallot helpottavat elämäämme


HSL
HRT
55K ~ 6
FORSBY

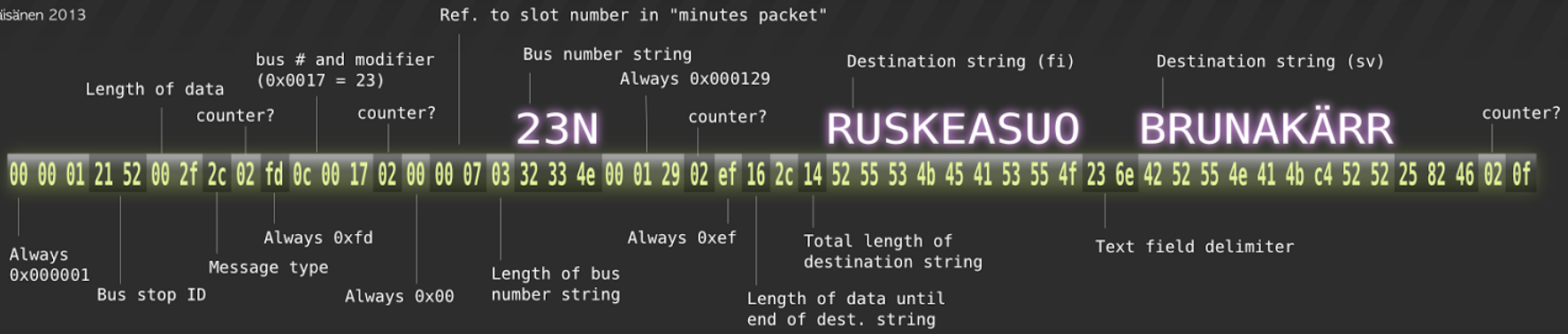

Q
01
11
I
00
10


1 0 1 0 1 1 1 0 1 1 0 0 1 1 1 1 1 0 1 0 1 0 0 1 0 0 0 1 1 1 0 1 1 0 0 0 0 0 1

```
603 # CRC with polynomials of arbitrary degree using string magic
604 # crc_general(data, init, len, clipbits, coeffs)
605 sub crc_general {
606   my $input    = shift;
607   my $init     = shift;
608   my $len      = shift;
609   my $clipbits = shift;
610   my @coeffs   = @_;
611
612   my $poly   = "0" x ($len+1);
613   substr($poly,length($poly)-$_-1,1) = 1 for (@coeffs);
614   my $data = unpack("B*",$input);
615   substr($data,-$clipbits,$clipbits) = "" if ($clipbits > 0);
616   $init = unpack("B*",$init);
617   $data .= substr($init,-$len);
618   for $a (0..length($data)-$len-1) {
619     if (substr($data,$a,1) == 1) {
620       for $b (0..$len) {
621         substr($data,$a+$b,1) = (0+substr($data,$a+$b,1)) ^ (0+substr($poly,$b,1));
622       }
623     }
624   }
625   ("0" x (8-($len % 8))).substr($data,-$len);
626 }
```

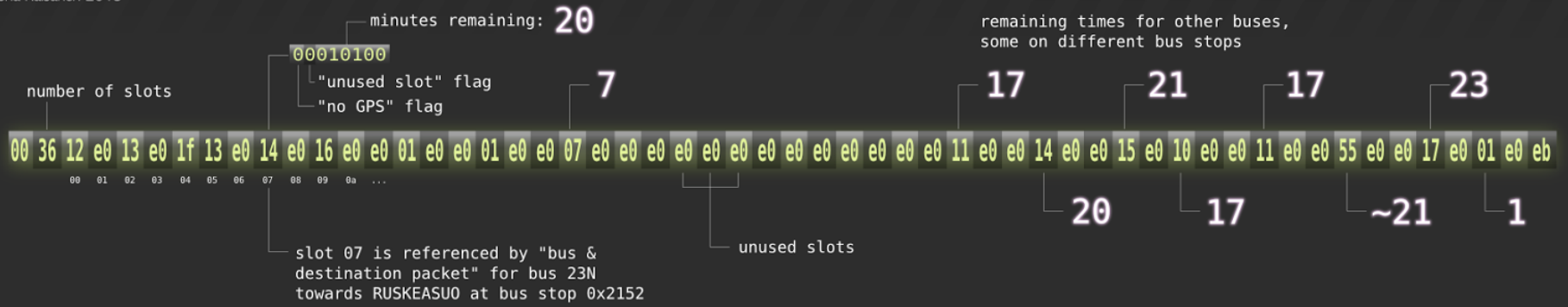
BUS & DESTINATION PACKET

Oona Räisänen 2013



MINUTES PACKET

Oona Räisänen 2013




72
°12
TAPANILA

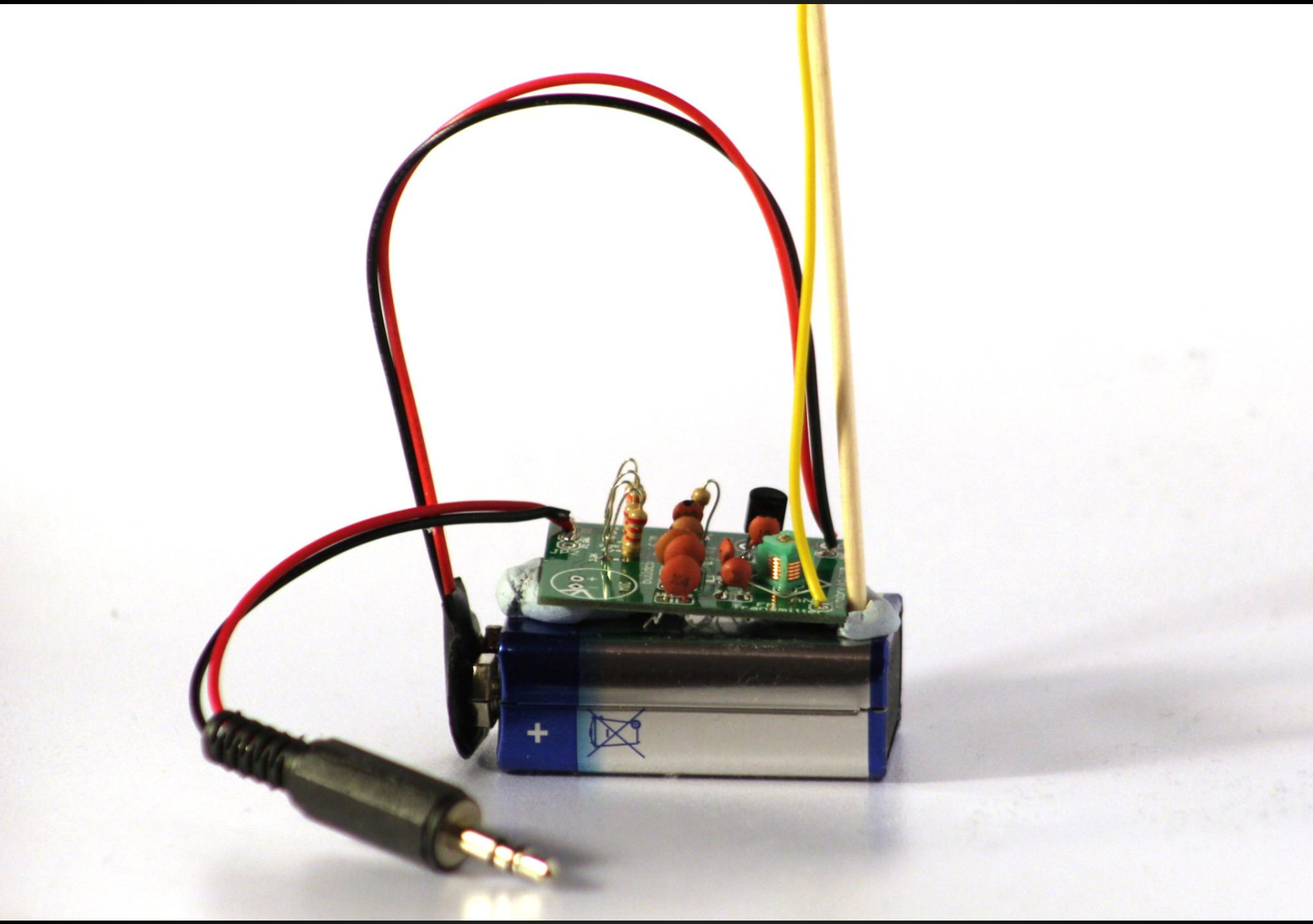
Signaalin sorkkiminen tai hassunhauskojen tekstien sommittelu nykyisiin näyttöihin ei Vanhasen mukaan hevillä onnistu.

Jos joku haluaisi muuttaa informaatiota, hän joutuisi lähettämään omaa radiosignaalia.

"Pitäisi huutaa kovempaa kuin muut, mikä vain sotkisi radiokanavan täydellisesti", Vanhanen sanoo.

Radiokanavan häirintä olisi myös laitonta.

Räisäsellä ei ole tällaisia tavoitteita.



:)

windytan.com

twitter: @windyoona