ZCZC

QST de PI4GAZ, PI4GAZ, PI4GAZ
Afdelingsstation van de VERON in Gouda, R17, JO22IA
Uitgezonden door PA0POS vanuit Haastrecht, JO21JX
Om 11.45 uur op 145,475 MHz met RTTY (50 baud)
Om 12.30 uur op 3,580 MHz met PSK31
Aflevering no.: 589, 15 december 2002

Onderwerpen: Afdelingsnieuws, Bouwproject 80 meter ontvanger van PA0HRX, ICOM ID-1, Geluiden uit de oude doos, Coderingen en de radio luisteramateur, Gevraagd.

Afdelingsnieuws:

Afgelopen vrijdagavond 13 december 2002 was het de laatste clubavond van 2002. Bij aankomst van de vergaderruimte kon men het niet missen. Kerstverlichting was in de vlaggenmast opgehangen. In de beide vergaderruimtes was Kerstversiering opgehangen. Kortom het geheel was keurig versierd. Waarvoor dank aan diegene die daar hun inspanning voor hadden verricht. Onder het genot van koffie en een drankje was er een druk onderling QSO gaande. De opkomst was goed, een ding viel een beetje tegen, er waren deze keer maar een paar XYL's aanwezig en dat was de vorige keer duidelijk anders. Dus mijne heren de volgende keer kan wat dat onderdeel betreft het duidelijk beter.

De volgende bijeenkomst zal in de nieuwe convocaties worden vermeld die we nog in de brievenbus of per e-mail zullen ontvangen.

De vergaderingen vinden plaats aan de Goejanverwelledijk 10 te Gouda. De aanvang van de bijeenkomsten is op de vrijdagavonden is steeds om 20:00 uur.

Bouwproject 80 meter ontvanger van PA0HRX:

In het kleurrijke VERON maandblad van december blz. 548 staat een interessant artikel van een 80 meter peil/vossenjacht ontvanger met schema aangeduid als HRX80. Een echte aanrader om het eens op uw gemak te lezen. In het artikel wordt ook aangege ven dat met een eenvoudige ingreep, welke in de bouwbeschrij ving wordt beschreven, de ontvanger geschikt is te maken voor de gehele 80 meter (LSB mode) amateur-band en aan te sluiten op een draadantenne. De kosten van een compleet bouwpakket zullen ongeveer 50 euro bedragen. Voor actuele informatie kunt u terecht op: http://home.introweb.nl/(tilde)pa3fdc/kalender.htm Voor inschrijvingen e-mail naar: pa3fdc(AT)amsat.org

Ik wil hier ik nog aan toevoegen dat zo'n handzaam 80 meter peilontvangertje naast de vossenjachten op 80 meter als bijkomend voordeel ook uitstekend geschikt is om storingen te peilen die hinderlijk vaak voorkomen op 80 meter zoals,; lichtdimmers, zgn. elektronische trafo's, andere elektronische

converters en digitaal gereutel van huishoudelijke (vermaaks)apparatuur (Piet PA0POS).

Als u het artikel gelezen hebt kunt u er eens over nadenken om zo'n peilontvangertje als afdelingsbouwproject op te nemen. Het is ook een prachtig project om eens iets te maken als uw soldeerbout lange tijd niet is gebruikt, of als u nooit zelfs iets heeft gemaakt. Het geeft echt voldoening, probeer het zelfs eens uit. Laat uw stem eens horen aan het afd. bestuur of in de Goudse ronde.

ICOM ID-1:

Icom komt met een 23 cm digital transceiver op de markt. Deze kan digitaal gemoduleerde spraak (8kbps in GMSK) alsook data (128 kbps GMSK)

Bron: Funk Amateur 8/20002 blz. 772

Geluiden uit de oude doos:

Wat ouderen onder ons die de hobby zijn begonnen met alleen luisteren op HF en dus niet alleen naar HAMS zullen zich vast nog wel de zgn. "pauze tekens" herinneren. Pauze tekens zijn en waren korte muziekfragmentjes die voor elke uitzending werden uitgezonden. Elke zender had zo'n zijn eigen melodietje. Het had een functie, men had vroeger natuurlijk nog niet zulke nauwkeurige afstemmogelijkheden en daarom zond men deze herkenning uit. Ook was het een middel om de frequentie bezet te houden. Binnenlandse diensten en de buitenlandse wereldomroepen, zij hadden elk zo'n pauze teken. RNW gebruikt het nog altijd "Merck toch hoe sterck".

Al jarenlang verzamel ik stationsaankondigingen, pauze tekens en airchecks en ik ben niet de enige. Voor diegenen onder ons die het leuk vinden om weer eens de oude pingels van Radio RSA te horen, of niemand weet hoe de oude tune van Radio Moskou ging. Klik op www.intervalsignals.net en je komt er duizenden tegen uit alle landen van de wereld

Oproep
Wie heeft er nog oude opnamen liggen uit zijn luistertijd? Zend ze aan mij en ik zorg dat ze bij Dave komen, de bouwer van de site en zo kunnen we op deze wijze een stukje radiohistorie vastleggen. Het is niet de bedoeling dat we scheepsladingen Radio Veronica en ander zeezender spul op het net zetten, daar is al zo veel van bewaard gebleven dat men zelfs een radio station heeft opgericht die dat spul elke zondag in de ether zet "Radio 192" voor de liefhebbers... We zijn vooral op zoek naar materiaal uit de Pacific. Wie heeft er b.v. nog materiaal van de NIROM?
Ga eens kijken op zolder en draai de oude banden nog eens af. Kijk wel eerst even op de site zodat je kan zien wat we bedoelen. De pauze tekens en station ID's zoals dat heet, staan op landen volgorde gerangschikt.

Veel luisterplezier

Bijdrage van Rudy PA3GQW, waarvoor hartelijk dank
Reacties kunt u richten aan: R. van Dalen PA3GQW,
Kleinpolderlaan 120, 2911 PB Nieuwerkerk aan den Ijssel,
e-mail: pa3gqw(at)wxs.nl

Coderingen en de radio luisteramateur:

Met de komst van de personal-computer zijn er drastische veranderingen doorgevoerd in het radioverkeer op de HF-banden. Luistert men buiten de broadcastings-banden dan hoort men digitale signalen (telex, sitor enz.). Raadpleegt men hierover de boeken van Klingenfuss, welke signalen dit zijn, dan komt men, met Klingenfuss, tot de conclusie dat het monitoren van deze frequenties m.b.v. decoderingshardware, aangesloten op een PC, zeker de moeite waard is en een zeer interessante uitbrei ding is voor de luisteramateur. De aanschaf van deze hardware en bijbehorende software levert geen problemen op en geeft de mogelijkheid tot ca 100 gebruikte coderingen te monitoren, mits het station goed te ontvangen is en een van deze codes gebruikt. Echter veel stations zenden gecodeerde tekst uit waardoor deze tekst op de monitor wel te lezen valt, maar niet te begrijpen. Software om deze gecodeerde berichten te decoderen is niet te verkrijgen.
Om een beeld te krijgen van hoe een coderingssysteem eruit zou kunnen zien volgt hier een beperkt overzicht van een aantal systemen die in het verleden gebruikt zijn.
Let wel: dit is slechts een topje van een enorme ijsberg!

Mono-Alphabetic Substitution Ciphers:
Onder deze catagorie vallen:
1 Keyword-methode, 2 Additieve-methode (= het Caesarsysteem), 3 Multiplicatieve-methode en 4 de Affine-methode (= combinatie van 2 en 3). Met de 26 letters uit ons alfabet kunnen 26! (26 faculteit = ca. 4100000000000000000000000000) andere alfabetten gemaakt worden. Men gebruikt dus 1 van deze alfabetten als coderingsalfabet. Is het gecodeerde bericht (de zgn. Cipher-tekst) ca. 400 letters groot dan kan men m.b.v. taalkundige analyse het bericht ontcijferen, omdat de frequentie van deze letters dezelfde zijn als van het niet gecodeerde bericht (de zgn. Plain-tekst).
In het verleden heeft o.a. Maria Stuart (ca. 1648) van deze coderingsmethode gebruik gemaakt, in de veronderstelling dat haar vijanden dit niet konden ontcijferen. Toen dit wel gebeurde en men op de hoogte kwam van haar plannen is zij uiteindelijk onthoofd voordat ze haar snode bedoelingen uit kon voeren. Nu zou men het coderen geheel anders aanpakken.

Poly-Alphabetic en Poly-Graphic Substitution Ciphers:
1 Vignere-methode, 2 Hill's-methode, 3 Playfair-methode 4 Enigma-methode, 5 Vernam-mehode en nog vele anderen.
Omdat hier dezelfde letter (of combinaties van letters) van de Plain-tekst vervangen wordt door meerdere letters uit het coderingsalfabet, is de frequentie van de Cipher-letters geheel anders dan die van de Plain-letters.
Een taalkundige analyse heeft hier dus geen zin meer.
Van de Vignere-methode en de Enigma-methode zijn decoderings methodes ontwikkeld die zeer goed bruikbaar zijn.

De Enigma-methode was in WO-II, in het begin, zéér effectief totdat deze uiteindelijk door de geallieerden ontcijferd werd en men op de hoogte kwam van de plannen van de vijand. Nu nog steeds wordt de Enigma-methode door firma's gebruikt voor codering van vertrouwelijke data.

Letter-Nummer Cipher:
Hier wordt de letter van de Plain-tekst vervangen door een nummer uit de reeks 00 - 99. Het aantal nummers voor een letter wordt statistisch bepaald uit de frequentie van deze letter. De a wordt bijv. vervangen door 8 random gekozen nummers omdat de 'a' 8 procent vertegenwoordigt van alle letters in normale (Engelse) tekst. Zou de Plain-tekst uit 9 a's bestaan dan bestaat de Cipher tekst uit 8 verschillende nummers, a1 en a9 zijn dezelfde omdat de rotatie van de 8 cijfers volledig is geweest.

Symmetrische Methodes:
Deze methodes worden vooral in het dataverkeer tussen computers gebruikt. De bekendste methodes zijn: DES, RSA, IDEA, GOST en Ryndael. Hier wordt gebruik gemaakt van public en private key's voor het coderen en decoderen van de data.
De codering is gebaseerd op het product van grote priem-getallen. Zo'n getal is niet binnen afzienbare tijd, door een PC, te ontbinden in factoren, waardoor het decoderen onmogelijk wordt zonder de public en private key's te kennen.
Wil men een gecodeerd bericht, uit de HF-band, gaan decoderen, dan moet men een bitstream-file van enen en nullen maken, de data selecteren uit deze file en achter het coderingssysteem zien te komen.
Hier als voorbeeld de eerste 24 characters van dit verhaal wat u gedecodeerd heeft m.b.v. het bekende ITA2 alfabet:
0110111 0111111 0100001 0000011 0110111 0001001 0111111 0100101
0100001 0110111 0001001 0111111 0111101 0000111 0001111 0101001
0000011 0110111 0001001 0111111 0011111 0110001 0001101 0110111
Eenvoudig is te zien dat 1 startbit en 1 stopbit gebruikt wordt. De data tussen deze bits werd gedecodeerd volgens het ITA2 alfabet. De PC is momenteel, met de huidige software pakketten C++, VisualBasic enz., zo krachtig, dat software gemaakt kan worden (ook door amateurs) om dit te realiseren.

Big brother is watching you:
Om het ontcijferen van de gecodeerde berichten nog moeilijker te maken voor meelezers, codeert men het bericht met meerdere coderingssystemen bijv. met: Letter-Nummer, RSA, Nummer-Letter en vervolgens Vignere. Binnen afzienbare tijd is het bericht dan niet meer te decoderen, tenzij men het gebruikte protocol kent.
Voor de zendamateurs wil ik nog opmerken dat het uitzenden van gecodeerde berichten niet is toegestaan. Dat dit toch gebeurt en in sommige packet radio programma's mogelijk wordt gemaakt, houdt in dat 'deskundigen' meelezen.

Een zeer boeiend overzicht van coderingen en decoderingen door de eeuwen heen, wordt gegeven in het boek: 'Code' van Simon Singh. Dit boek leest als een spannende detective roman en bovendien is er geen moeilijke wiskundekennis voor nodig. Voor diegene die zich in cryptografie wil gaan verdiepen, kan

ik het boek 'Cryptological Mathematics' geschreven door Lewand aanbevelen. In dit boek vindt u zeer interessante programmeer opdrachten die in Basic of m.b.v. spreadsheets uitgevoerd kunnen worden (beter nog in de C++ taal).
Tot slot: alle 'luister'(en zend) amateurs veel plezier en succes toegewenst met het 'monitoren' van digitale signalen. Als u dit verhaal heeft gelezen is dit zeker het geval geweest. En vergeet niet de PSK31 uitzending in de HF-band te monitoren.
Bijdrage van Jaap PE1DOR, waarvoor hartelijk dank.

Gevraagd:

Ger PA3GUF zoekt een stuk messing met de volgende afmetingen: 10 mm dik bij 60 x 120 mm. Ger maakt zelf CW sleutels van diverse grootte en soort en ziet met belangstelling uit naar diegene die hem aan het gevraagde stuk messing kan helpen. Gaarne richten aan: G. Stam, Het Weense Plein 12, 3353 AS Papendrecht, tel.: 078-615 65 66

Tenslotte:

Kopij kan worden gestuurd naar P.C. van der Post, Spechtstraat 18, 2851 VL Haastrecht. Ook kan men via e-mail een bericht sturen naar pa0pos(at)amsat.org
PI4GAZ bulletin op Internet: www.veron.nl/afdeling/gouda

QSL-kaarten van luisteramateurs worden zeer op prijs gesteld en uiteraard beantwoord met een PI4GAZ QSL kaart.

Alle zend- en luisteramateurs een prettige zondag gewenst, en veel plezier met de hobby.

nnnn