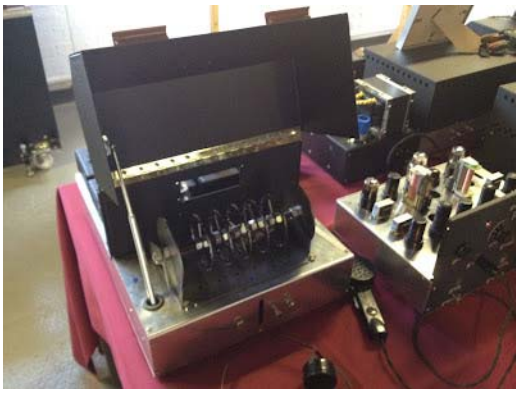
Tuesday, March 06, 2012

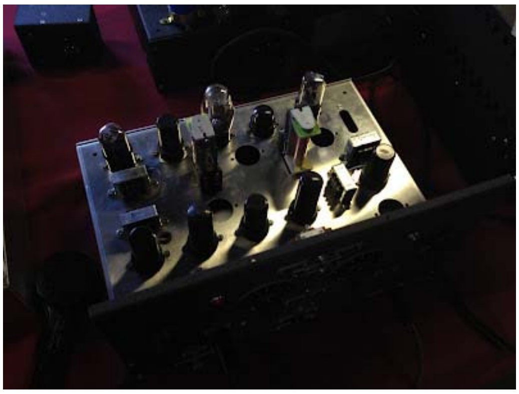
The Delilah Secure Speech System

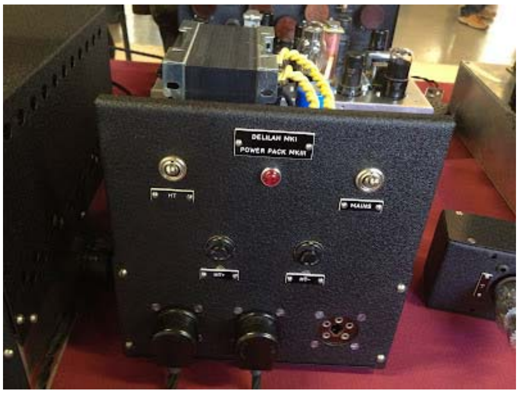
Part of the new exhibit being unveiled at Bletchley Park is the Delilah Secure Speech system that Alan Turing developed during the Second World War. Details of the system are in Andrew Hodges' excellent biography of Turing and have recently been placed in the National Archives (references FO 850/256 and HW 25/36 for people who want to go an see them for themselves).

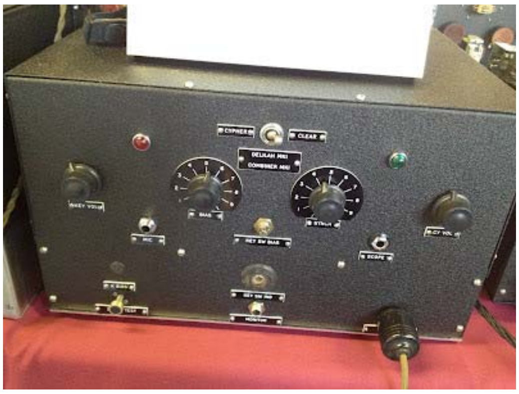
Delilah was intended to be fairly portable (unlike SIGSALY) and usable in the field (such as in a tank) and allow secure speech communication between people over radio or telephone.

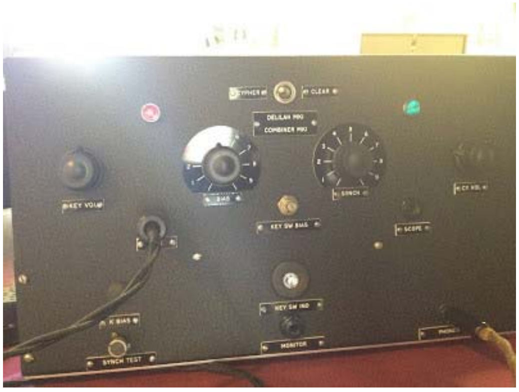
A team at Bletchley Park has been working to rebuild Delilah from the report (with some assistance from GCHQ) and I was able to see and photograph the reconstructed machine. Here are some pictures:



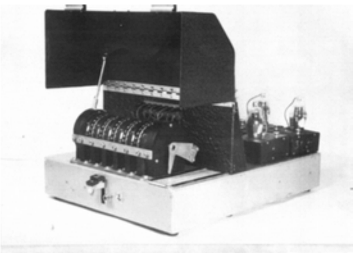


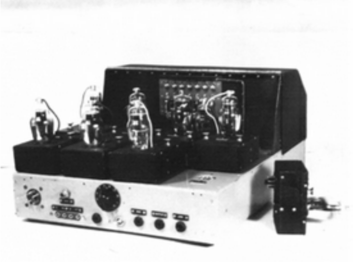

DELILAH MK1
POWER PACK MKII
HT
MAINS


CYPHER
CLEAR
DELILAH MKI
COMBINER MKI
BIAS
MIC
KEY SW BIAS
SCOPE
CY VOL
TEST
MONITOR



And here are pictures of the original machine taken from recently declassified documents:





Briefly, Delilah worked as follows. The incoming speech was limited a channel of 2kHz which was then sampled at 4kHz to produce 4,000 samples per second of the incoming waveform. These samples were normalized to a range of 0 to 1 and added using modulo arithmetic to a key stream consisting of values in the range 0 to 1.

The resulting waveform was then transmitted and at the opposite end the original waveform could be constructed by adding back (again using modulo arithmetic) the same key stream. Both ends had to be synchronized for this scheme to work (and use the same key).

The key was set on wheels visible in the photograph above that generated a stream of pseudo-random numbers which when added to the incoming signal would result in something close to pure noise being transmitted.

Labels: alan turing

If you enjoyed this blog post, you might enjoy my travel book for people interested in science and technology: The Geek Atlas. Signed copies of The Geek Atlas are available. Looking for a new job? Try UseTheSource.

posted by John Graham-Cumming at 11:53 Permalink

1 Comments:

MattyDub said...

I had no idea such a device actually existed! A fictionalized version is described in Neal Stephenon's Cryptonomicon (in which Turing is a minor character) - but this is the first I'd heard of it outside of fiction.

12:06 AM

Post a Comment

Links to this post:

Create a Link

<< Home

About

The troubled thoughts of a caustic coder. Mostly code, but sometimes rants, randomness and politics.

Available Now

The Geek Atlas

With this unique traveler's guide, you'll learn about 128 destinations around the world where discoveries in science, mathematics, or technology occurred or is happening now. Travel to Munich to see the world's largest science museum, watch Foucault's pendulum swinging in Paris, ponder a descendant of Newton's apple tree at Trinity College, Cambridge, and more. Each site in The Geek Atlas focuses on discoveries or inventions, and includes information about the people and the science behind them.

GNU Make Unleashed

230 pages of GNU Make from basics to advanced. Covering topics not covered in other GNU Make books such as: eliminating recursive make, doing arithmetic, Makefile debugging techniques and more.

Everything you wanted to know about making *real* Makefiles.

Recent Posts

- Call yourself a 'brogrammer'? Then get the hell a...
- How to break the 'rapper code'
- Programmer
- Mobile subscriber leakage in HTTP headers in the w...
- The YouPorn Chat leak revealed a lot more than ema...
- The Case for Open Computer Programs
- Alan Turing's reading list (with readable links)
- Benford's Law analysis of my own tax return
- So much for Google's Privacy Settings
- My foxhole radio

Subscribe to Posts [Atom]