Turing Sources

Alan Turing's Delilah Report, 6 June 1944

Advanced speech security system in the Second World War

Transcription of document in British National Archives, HW 62/6

See the Alan Turing Home Page for a guide to this website

This is a transcription of the complete text of Turing's report dated 6 June 1944, in the (British) National Archives, box HW 62/6. I am indebted to Ralph Erskine for locating this document.

For the setting and significance of the Delilah, and a picture of it, see this page of the Alan Turing Internet Scrapbook

---

TOP SECRET

Speech System 'Delilah' - Report on Progress

Research on 'Delilah' has been in progress since the beginning of May 1943. Up to now the work has all been concentrated on the unit for combining the key with the speech to produce cipher (or scrambled speech) and for recovering the speech from the cipher with the aid of the key. We have now produced a unit for doing this; the same unit does duty both as scrambler and descrambler, changing from the one to the other on throwing a switch. The unit uses seven valves and when suitable rearranged will probably occupy a space of about 10" x 8" x 5". The greatest care has been taken to avoid using more apparatus than is absolutely essential. It is possible that if this had not been done, the present position might have been reached two or three months earlier, at the cost of having an apparatus of about twice the present size.

Proposed Future Plans

(i) The most urgent job to be done now is the design of a unit for the production of key. How long this will take is difficult to estimate, but it is hoped that it will not be so long as the making of the combining unit. Six to nine months might be taken as a reasonable estimate.

(ii) When the time comes for point to point tests, a certain amount of work will have to be done in testing the suitability of the audio stages of the wireless apparatus involved, and possibly making some corresponding alterations. Some of this could be done concurrently with work on the key unit.

(iii) The present combining unit, though reasonably satisfactory cannot be regarded as perfect. The intelligibility could probably be improved by raising the frequency from 4 Kc/s to 6 Kc/s (corresponding to changing the speech band passed from 2 Kc/s to 3 Kc/s). There will also probably be small points to consider concerning production.

(iv) Whereas there may be some difficulty in the transmission of the speech scrambled by 'Delilah' she has another application where this question does not arise, viz. the scrambling of facsimile. A facsimile scrambler would

simply be a low frequency scrambler working at a pulse frequency of about 300 cycles (say). To develop such a scrambler should be a matter of little more than changing the values in the present unit.

It will be appreciated that these lines of action can only be followed one, or perhaps two, at a time.

Ssuggested Form of Key

Some thought has been given to the problem of the form that they key should take. The original plan that a 'public key' should be transmitted, which would be so hashed up before use as to be unrecognisable, has now been abandoned, not so much for security reasons as on account of transmission difficulties. It is now proposed to produce a periodic key with a rather long period e.g. 7 x 8 x 11 x 13 x 15 x 17 = 2,031,040 pulses or about 8 minutes. The nature of the key could be set in advance by plugging to any one of a considerable number of alternative keys. There will probably be something of the order of 10^{25} different possible keys. The key chosen will be changed daily let us say, and also to some smaller extent before each conversation. Besides these changes it is hoped to introduce an automatic partial key change whenever the transmit-receive key is operated. Without this device the various pieces of conversation would be in depth, and would in theory present no difficulty to the cryptographer. For the same reason one speaker should be limited to at most 8 minutes consecutive speech.

The period of key quoted above would be obtained by means of a number of multivibrators sunchronised with the main pulse of the scrambler itself, and having frequencies which are 1/7, 1/8....1/17 of the frequency of that pulse. The outputs of these multivibrators with the networks can be altered by the plugging. The outputs of the networks then go through another set of networks, and the outputs of these are combined together with further plugging to give three different signals. These three signals are then combined by intermodulation, and the result after limiting is the key. This system has been devised to try and prevent any methods of breaking dependent on separating the effects of the different multivibrators. It is thought that by methods of the type described above a very high degree of security indeed can be obtained. There is certainly no comparison in security with any other scrambler of less than ten times the weight. For tank-to-tank and plane-to-plane work a rather less ambitious form of key will probably be adequate. Such a key unit might be of about the same size as the combining unit.

[signed] A. M. Turing

6th June 1944

Continue:

- Alan Turing Sources index page
- Relevant page of the Short Turing Biography
- Relevant page of the Alan Turing Internet Scrapbook
- Discussion on the Mind and the Computing Machine, October 1949

Quick Links: Book | Short Bio | Scrapbook | Philosophy | Publications | Sources

Alan Turing Home Page

Search

Andrew Hodges