

~~SECRET~~

Chairman, Ad Hoc Committee on Harvest  
Evaluation

25 June 1957

R. E. Lyons

Declassified by D. Janosek,  
Deputy Associate Director for Policy and Records  
on 21-10-2010 and by JP

Statement of Problem Being Evaluated

## 1. Given:

a. A code book with the meaning of  $26^3$  (17,576) values from AAA through ZZZ (three letter code, 26 letter alphabet). The codebook is stored in 26 records, densely within a record, on X100 tape, 34 characters per code group (4 character frequency, 30 character meaning).

b. A message tape (729 tape). This tape contains the messages (in unenciphered code) which are to be decoded. The messages are placed on tape in a card-to-tape conversion process resulting in 80 character records. The card format is as follows:

1 Heading card, heading in columns 1-20, the remainder blank.

N Line ( $N=50$ ) cards, columns 30-59 contain 10 three-character groups, remaining columns blank.

c. Average message length - 200 code groups  
Maximum " " - 500 code groups  
Average number of messages per 729 tape - 75.

d. Memory size: 4 x 512 core words @ 0.5  $\mu$ /sec; 8 x 8192 core words @ 2.0  $\mu$ /sec; 16 words @ 0.1  $\mu$ /sec; unlimited tape (X100 and 729) and disc.

## 2. The problem:

To produce an output 729 tape which has 80 characters per record, one record per code group, in the following format: characters 1-20, message heading; 21-23, code group number; 24-26, code group; 30-59, meaning; remainder blank.

## 3. Procedure:

At least two basic procedures will be tried.

- a. Read a segment of the code book into core memory. Decode part of message(s). Repeat until all the code book segments are used.
- b. Convert code book to disc memory. Do not use core memory for the book, but always refer to the disc.

~~SECRET~~

~~SECRET~~

**4. Extensions:**

As time allows, further consideration will be given to:

- a. File maintenance of code book.
- b. Deciphering before decoding using known key.

**ROBERT E. LYONS  
CHIEF, MPRO-4**

~~SECRET~~