(d) Depths

Each QKP number, and each QKP list, should only be used once. However sometimes the same QKP number and settings are used for two (usually consecutive) transmissions. As long as a limitation involving P_5 is not being used the key generated will be the same for both transmissions and they will be in DEPTH.

If the Tunny machine is switched out and a new transmission started without resetting, there is said to be a FOLLOW-ON. 11B (k) shows that the decodes of the two parts of a follow-on will be divided by two blanks for which nothing will have been transmitted.

(e) Change of keys

Once a day (usually between 0600 and 1200), some or all of the wheel patterns are changed. The sender sends out QZZ (usually in clear) and this tells the receiver that he is changing over to the new day's patterns, and that the receiver's incoming Tunny must also be changed.

Before Summer 1944 motor patterns were changed daily but chi patterns were changed monthly and psi patterns monthly or quarterly (see 11E(a)). During the summer changes became more frequent, and after August 1st there was a daily change of all wheel patterns on all links.

Wheel patterns were issued for a month at a time. A day's wheel patterns - as issued - are shown in Fig.11 (III) where + = Hooks and O = Knims.

11E THE TUNNY NETWORK

(a) The period of experiment.

The Tunny machine (SZ40 with no limitation) made a first and experimental appearance in June 1941 on the link Berlin - Athens - Saloniki. At first it was used crudely enough.

(i) Wheel patterns were not chosen so that $\Delta\Psi = \frac{1}{2}$, and there was a regular excess of dots over crosses in the $\Delta\Psi$ stream.

(ii) The QKP indicating system had not been introduced and wheel settings were chosen by the sender, and sent out in a simple substitution of letters for settings which changed every month and was different for each wheel.

(iii) Motor patterns were changed daily, chi patterns monthly, and psi patterns every three months.

(iv) The machine was not wired to a tone transmitter, but the cipher text was recorded and sent by facsimile (Hellschreiber).

Until October, 1942 there was still only one Tunny link, but the procedure gradually improved with the introduction of $\Delta\Psi = \frac{1}{2}$ and of Tone Transmission before March, 1942.

The replacement of the single link by two links - Codfish from Berlin to Saloniki, and Octopus from Koenigsberg to South Russia - using the QKP system and with monthly change of chi and psi patterns signified the end of the German experimental period and the start of the general expansion of the Tunny system.

(b) The period of expansion

SZ42A was first introduced on Codfish in February 1943, and gradually replaced SZ40 on all links.

SZ42A was fitted with a P_5 attachment which was used experimentally on Herring (Rome-Tunis) in March 1943, but only made a general appearance after December 1943 on Western European links.

At the time of the allied invasion of the continent in 1944, Tunny had reached its most widespread and stable level of organisation. There were 26 links and two main central exchanges.

STRAUSSBERG near Berlin - the terminus for the 9 Western links and
KOENIGSBERG the terminus for the 10 Eastern links.

41A EARLY TRAFFIC

(a) A first analysis

The first messages on the "Tunny" link (the name "Tunny" was first given to this traffic in the summer of 1942) to be studied cryptographically were sent out shortly after the German invasion of Russia. They passed between Vienna and Athens. The Hellschrieber method of transmission was used. Some earlier traffic, apparently practice transmissions, had been intercepted in May. This had been sent out in the form of a five-unit code, so it was suspected that a teleprinter was being used. This was confirmed by a preliminary examination of the later traffic, which showed that an alphabet of 32 characters was being employed. These characters were the 26 letters of the normal alphabet, and the six extra symbols 3, 4, 8, 9, + and /.

Each message began with a clear preamble in which there appeared first the serial number, repeated several times, and then a set of 12 letters, in the form of names (Anton, Bertha etc.) which was clearly a 12-letter indicator. The symbol 9 was used as a separator in this preamble, and a group of five 9's separated the clear preamble from the cipher text. Immediately after the cipher text there appeared a sequence of 8's. The serial number was given in letter form by means of a simple keyboard substitution the digits 1,2,3,4,5,6,7,8,9,0, being represented by the letters Q,W,E,R,T,Y,U,I,O,P, respectively.

(b) Meanings of teleprinter letters

On the assumption that a teleprinter machine was being used, two problems presented themselves. First, was the correlation of the 26 letters of the normal alphabet with teleprinter signs the same as that of the international convention, and second, what teleprinter signs corresponded to the symbols 3,4,8,9,+ and / ?

Both these questions were answered by the study of a a series of corrupt messages which were sent out on July 22nd. Only sixteen different letters appeared in these messages, and those letters of the normal alphabet which appeared were those whose first impulse was conventionally a dot. Clearly, owing to some fault in the machine, the first impulse of each letter had been transmitted as dot, even when it should have been cross. This effect finally confirmed the hypothesis that a teleprinter machine was being used and answered the first of the above questions in the affirmative.

The second problems was then solved by a study of the corrupt clear preambles. For example the sequence H / I N R I C H and T H / O 3 O R would be recognised as corruptions of H E I N R I C H and T H E O D O R respectively. Hence it would be deduced that for each of the pairs (E,/) and (D,3) the teleprinter signs differed only in the first impulse. But by convention E is (x...) and D is (x..x.). Hence it was deduced that / corresponded to the teleprinter sign (.....), and 3 to the teleprinter sign (...x.). By this sort of argument the teleprinter sign corresponding to each of the letters 3, 4, 8, 9, +, and /, was determined.

41B TUNNY SHOWN TO BE A LETTER SUBTRACTOR

The next advance to be made was the demonstration that the cipher was a letter subtractor cipher, and the determination of the law of addition used.

This was made possible by the occurrence of a number of "depths of two", that is, of messages having the same 12 letter indicator. Usually the two messages of such a pair were consecutive, as though an operator had failed to reset his machine between the two messages, but instead had made use of some device for returning all the wheels to their starting points.

The simplest assumptions to make seemed to be that a letter subtractor cipher was being used. The law of addition was fairly