19.2.8.1 In July and August 1941, the German army tested a *Hellschreiber* line between Vienna and Athens having an SZ 40 *Schlüsselzusatz* on both ends. They transmitted 12-letter indicators preceding the message in clear language, using a spelling alphabet as shown in Fig. 159, where the resulting indicator MGLOBLCOODKQ is written by hand across the top of the W/T 'red form' sheet. The sloping text is typical for the *Hellschreiber* record, it is glued to the sheet.

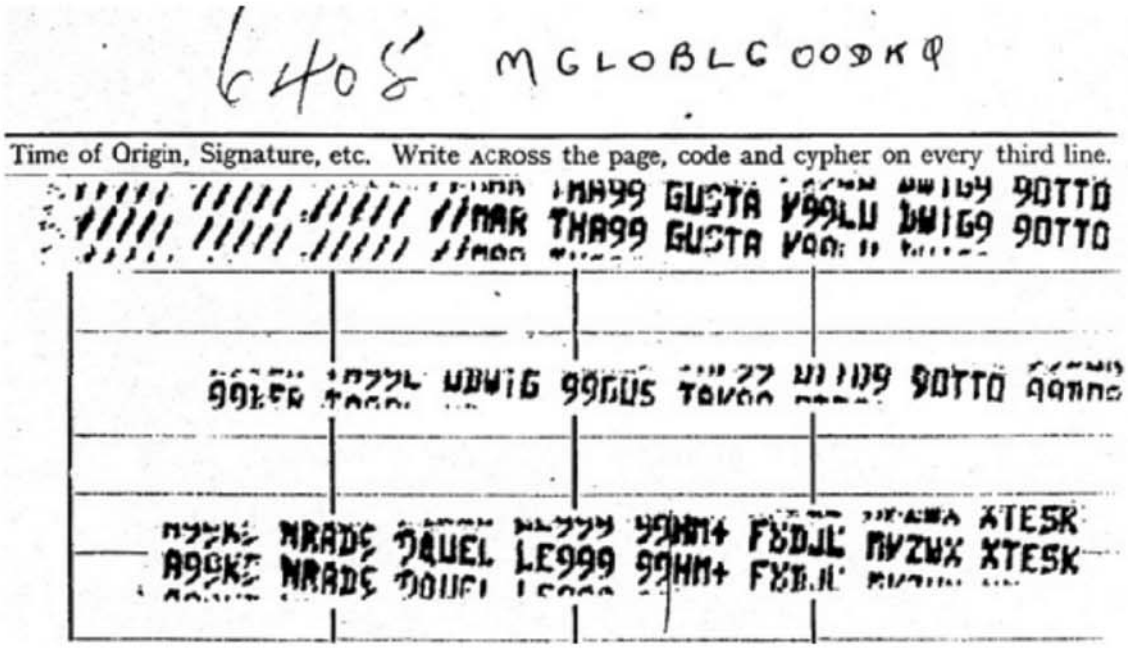
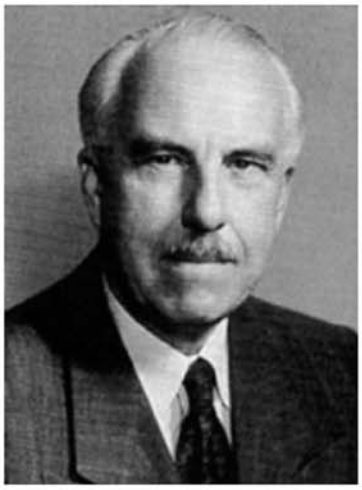


Fig. 159. Facsimile of a British *Hellschreiber* recording of a German message (08/08/1941)
Cleartext: ///// //MAR THA99 GUSTA V99LU DWIG9 9OTTO 99BER TA99L UDWIG 99GUS TAV99 OTTO9 9OTTO 99DOR A99KO NRAD9 9QUEL LE999

When the British studied these enciphered signals, they found hints that a VERNAM-type encryption based on teletype machines was involved, in particular when some of the message indicator spellings were corrupted (h0inrich for heinrich, th0o3or for theodor) in a message sent out on July 22, 1941. It was observed that the corrupted name and its correct form had 5-bit teletype representations differing only in the first bit. This could be explained by some fault in a teletype machine. Thus, it was a natural assumption that a VERNAM system was used, but not one of the Siemens machines as described in the patent of 1930, which used ten keying wheels leading to a 10-letter indicator, while the observed indicators had 12 letters.

The fact that the VERNAM system has a key group (see Sect. 19.2.1, pure encryption) considerably simplifies the cumbersome encryption and decryption process, but it also makes unauthorized decryption easier. When August Jipp and Ehrhard Rossberg applied for the *Geheimschreiber* patent in 1930 there was no indication of this danger in the unclassified literature. But several of the cryptanalytic services studied the description of this machine and it can be safely assumed that at least some British very early found out about some weaknesses even the Siemens *Geheimschreiber* offered.

19.2.8.2 A lack of crypto discipline is the enemy of good cryptography and is the hope of the unauthorized decryptor. As well as laziness, thoughtlessness is dangerous. Thus, in July and August 1941 a lot of test messages were sent on the Vienna-Athens line and since these contained no information that should be kept secret, nobody on the German side was disturbed when 'isologs' occured, that is, two messages encrypted in-phase with the same key. On July 3, 1941, a pair of isologs with the indicator DKTNFQGWAOSH (nicknamed afterwards WAOSH) was found; on July 21, 1941 another one with the indicator KONPAENGFQBZ (nicknamed afterwards GFQBZ). These isologs, starting in July 1941, were clearly evident to the British, since the identical indicator, expressing the initial setting of the wheels, was transmitted openly in front of the message. The whole SZ 40 cipher system was compromised by this error. The British recorded pairs of isologs in the hope that something like the Siemens Geheimschreiber with a letter subtractor cipher was used. By July 1941 their assumptions were confirmed. A group 33zzz11 (meaning +++), which had appeared occasionally in clear preambles, was tried as the clear at the front-end of one message, and the clear of the other message from the pair came out as seven letters of the word spruchnummer (message number), usually found at the beginning of a message. This was enough evidence that a so-called additive cryptosystem was used on the *Hellschreiber* link; it was given the codename Tunny.



John Tiltman (1894–1982)

The disaster for the Germans indeed developed much earlier than one might have expected. As reported in 1993 by Jack Good (first allusions were made in 1978 by Brian Johnson and in 1983 by Andrew Hodges), a plaintext-plaintext compromise occured even before the *Schlüsselzusatz* came into regular use, when, during tests, as a consequence of a mistake by a German telegraphist, two rather long messages p'', p' were sent with the same indicator HQIBPEXEZMUG (nicknamed ZMUG); two isologs of roughly 4000 characters, coinciding in the first seven characters, were recorded. As it turned out, the first message was corrupted by atmospheric noise and had been sent again. It should have been repeated identically, which, however, is rather difficult, and the operator made minor deviations. The compromise allowed Colonel (later Brigadier) John H. Tiltman to deduce painstakingly the two plaintexts from the difference d of the two recorded cryptotexts c', c'' (a 'depth of two'), using the fact that the difference $p' - p''$ of the plaintexts is invariant under in-phase encryption: $p' - p'' = c' - c''$. (Note, that for addition modulo 2, subtraction coincides with addition.)

19.2.8.3 As is now known, the accident happened on August 30, 1941. The first 120 characters of the two messages are shown below, together with the differences that Tiltman formed (this can be checked with the help of Table 26):