THE ENIGMA BULLETIN
Edited by Zdzisław Jan Kapera
No. 2 - May 1997 ISSN 0867-8693
The Enigma Press, ul. Borsucza 3/58, 30-408 Kraków, Poland; E-mail: zjkapera@vela.filg.uj.edu.pl

RALPH ERSKINE
Belfast

THE DEVELOPMENT OF TYPEX

Introduction

The advent of radio dramatically increased the difficulty of maintaining the secrecy of civil and military communications, but the experiences of the major powers in World War I showed that no protagonist in a major conflict could maintain radio silence. They also proved that all practical manual methods of encrypting signals were much too vulnerable to attack by a skilled enemy. After the war, book codes were improved by the use of additive tables for super-encipherment, but were slow and cumbersome. Many governments therefore investigated typewriter-based cipher machines in the hope that they would solve the problems of communications security, but recognised that they faced major difficulties until they came into service, which was a slow process in peacetime. In a counsel of despair, the British Government even went so far as to decree that messages should be transmitted by radio in peacetime only in cases of „extreme urgency", but inevitably that precept was quickly abandoned.[1]

In 1926, the British Government set up an Inter-Departmental Cypher Committee to investigate the possibility of replacing the book systems then used by the armed forces, the Foreign Office, the Colonial Office and the

[1] Minutes of committee 27 July 1921 and of Imperial Communications Committee, 23 February 1922: CAB 35/1 (files are at the Public Record Office, Kew, London, unless otherwise stated). For further background on the development of British cipher machines, including Typex, see John Ferris, *The British 'Enigma': Britain, Signals Security and Cipher Machines, 1906-1946*, "Defence Analysis", 3(2) (1987), p. 157.

India Office by cipher machines.[2] But as late as 1933 the Committee had not been able to find a satisfactory machine, despite testing numerous models and various prototypes and spending the then quite considerable sum of £10,000. The Committee evidently decided not to proceed with development of „O'Brien & Gardner machines" and did not make any progress with advanced machines.[3] However, Wing Commander O. G. W. Lywood, in the Signals Division of the Royal Air Force („RAF"), believed that it would be possible to develop an improved version of commercial Enigma, in conjunction with parts from Creed teleprinters, in order to produce printed text.[4] Fortunately for the United Kingdom, although the Inter-Departmental Committee appears to have refused to proceed on those lines, the RAF decided to go it alone in 1934 and authorised Lywood to proceed.[5]

„The RAF Enigma"

Lywood was appointed the chairman of a small committee consisting of Flight Lieutenant J. C. Coulson, Sergeant A. P. Lemmon and E. W. Smith, foreman of the WT workshop at Kidbrooke, Oxfordshire. On 25 June 1934, the Government Code and Cypher School („GC and CS") arranged to lend Lywood one of the two commercial Enigma machines that it had bought in 1928. Lywood's group began work in August 1934, with the print unit being designed and made by Creed Ltd., and the cipher unit at the Kidbrooke workshops. The first experimental model of Lywood's machine was delivered to the Air Ministry on 30 April 1935. Modifications and service tests were

[2] F. H. Hinsley, with E. E. Thomas, C. F. G. Ransom and R. C. Knight, *British Intelligence in the Second World War: Its Influence on Strategy and Operations*, vol. 2, London 1981, p. 631.

[3] Wing Commander O. G. W. Lywood, minute, 9 February 1937, „Report of Mechanical Machine Informal Producing Committee", 9 February 1937: AVIA 8/356; R. S. Archer, minute, 12 March 1937 (ibid); Ferris, *op. cit.*, p. 157. Little seems to be known about the O'Brien and Gardner machines, but see „Reports on O'Brien Cipher Machine": National Archives (NA), RG 457, NSA Box CBKI 62, NSA Accession No. 6826a.

[4] On commercial Enigma, which lacked a plugboard and was insecure, see Cipher Deavours and Louis Kruh, *Machine Cryptography and Modern Cryptanalysis*, Dedham 1985, p. 94. On Lacida, a Polish rotor machine which was also insecure, see Krzysztof Gaj, *Polish Cipher Machine - Lacida*, "Cryptologia" 16 (1992), p. 73.

[5] Minute, Archer, 29 December 1937; contrast Hinsley et al., *op. cit.*, vol. 2, p. 631.

carried out, with the results of the tests being sent to the Air Ministry on 16 May 1936.[6]

It is very difficult to reconcile the above chronology with the British official history's statement, =apparently quoting from an unnamed source, that „the [Inter-Departmental Cypher] Committee recommended in January 1935 that the Air Ministry should arrange for the construction of `3 sets of cypher machines of an improved „Enigma" type through the agency of so-called „Type X" attachments'" (hence „Typex").[7] However, since the present account is based on relatively contemporaneous accounts by Lywood himself and others, and the history does not cite its source, its version must be regarded as somewhat suspect. Apart from anything else, it would have been almost impossible in practice for a first working model to have been developed during peacetime on a part-time basis in the three months between January and April 1935.

As a result of trials with the second experimental model, the Air Ministry decided to put Typex Mk. I into production. By 9 February 1937, two Mk. I machines were installed at the Air Ministry and two at Coastal Command. A further 25 machines were then in the course of installation, mostly at RAF Home and Overseas Command Headquarters and the Air Ministry. Three machines were supplied to the War Office and one lent to the Foreign Office, with two being kept in reserve.[8] Lessons learned during the 1935 Abyssinia crisis were probably a factor contributing to the RAF order. The RAF had then found that its manual cipher systems were almost overwhelmed by the growth in signals traffic. The number of cipher groups handled by the Air Ministry jumped from 6,000 to 72,000 per month, requiring an increase in staff from five to 25. After Typex Mk. I was installed, 75,000 groups a month could be handled by 10 people.

[6] Lywood, minute, 9 February 1937; Archer, minute, 12 March 1937. The letter from GC and CS agreeing to the loan is set out in John Terraine, *The Right of the Line: The Royal Air Force in the European War 1939-1945*, London 1988, pb. ed., p. 40, which contains a brief account of the very start of Typex. See also James Rusbridger, *Betrayal at Pearl Harbor: How Churchill Lured Roosevelt into World War II*, London/New York 1992, Appendix 8 (Development of Enigma and Typex).

[7] Hinsley et al., *op. cit.*, vol. 2, p. 631, whose wording suggests that it is derived from a post-war internal history.

[8] Lywood, minute, 9 February 1937.

Preliminary design work on a Mk. II machine had already been started on 1 February 1937. The final design was agreed with Creed Ltd. on 29 July 1937. The first working model of Mk. II Typex was delivered by Creed on 28 May 1938 and demonstrated to the Inter-Departmental Cypher Committee on 14 June 1938. The Committee was clearly impressed, since at the same meeting it authorised the Air Ministry to order 350 machines at £107-8-0 each, of which 30 went to the Army for trials. By September 1939, the War Office had asked for a further 177 machines. The Defence Departments in the Dominions also decided to adopt Typex. So did the Royal Navy, but that is another story.

In 1939, Typex was still closely based on commercial Enigma. However, because of the Creed teleprint attachments, the early Mk. II model was much larger than Enigma, measuring 75 x 55 x 35 cms. and weighing 55 kgs., compared to Enigma's size of 35 x 28 x 10 cms. (without lid) and weight of 12 kgs. Instead of military Enigma's plugboard, Typex Mk. II included two entry stators (stationary rotors, which could be set but did not rotate during the course of a message), in addition to three stepping rotors (see Figures 1 and 2). Typex's stepping action was also much more irregular than that of Enigma, due to a simple pawl mechanism devised by Smith (see top of Figure 2) and the inclusion of nine notches in Typex rotors - Enigma had only one notch in rotors I to V and two in rotors VI to VIII. Each electrical contact in the rotors was duplicated in order to improve reliability. Apart from these changes and the inclusion of the printer units, there were no other significant differences between Typex and commercial Enigma. Plugboards were not installed in Typex until relatively late in the war.

Typex production

The demand for Typex from all branches of the forces and government, and from the Dominions, was always far in excess of supply throughout World War II. Moreover, Typex production was slow, at times painfully so, even after a second production line was established by Creed at Treforest, in Wales. For 1943, the total planned production was 2,452, giving a forecast deficiency of 1,800 machines. The forecast shortfall had increased to 4,000 in 1944.

Some of the reasons for the low production rate are clear. Any rotor-based machine tends to be very complex mechanically. Figures 3 and 4 illustrate just how many different parts a Typex machine included. Typex's relative complexity proved too much for the British machine tool industry.

Overloaded as the industry was with the demands of the war economy generally, it took almost two years to obtain the machine tools required to manufacture Typex, despite the priority that would have been accorded to it. Only 2,300 Typex machines had been made by the end of 1942, 4,000 by December 1943 and 5,016 by May 1944. About 8,200 Mk. II machines and perhaps 3,000 Mk. VI Typexes were made before August 1945. The total number of Typex machines of all models (which may have included the adaptation of Typex known as the Combined Cipher Machine („CCM")) built by the war's end was therefore probably around 12,000.

Production problems may have been exacerbated by the inability of the services to forecast their needs accurately. In December 1943, for example, their requirement for 1945 was estimated at 2,550 machines, but by May 1945 this had almost trebled, to about 7,500.[9] Actual production of the Mk. II machine did not increase significantly after 1943. Even with both production lines operating, it seldom exceeded 250 machines per month, despite optimistic forecasts of 490 per month.[10] Staff shortages and the difficulties of obtaining skilled labour, plus problems with defective components were major factors in the low production rates.

As with most war materials, the United Kingdom was desperately short of Typex machines, which were not available in sufficient numbers to meet the needs of the British forces - to which those of the civil departments and the Dominions' armed forces had to be added. Typexes were in such short supply in the Middle East in 1941 and 1942 that the British Army had none available for operational messages, which had dire results for signals security.[11] Even GC and CS did not have enough machines. Due in part to a lack of Typex machines, one of its outposts at Kilindini (near Mombasa) did not receive all the assistance the parent organisation at Bletchley Park could have given to it in Kilindini's work against the Japanese naval code, JN-25-D.[12]

[9] Minutes, Typex Committee, 6 December 1943 and extrapolated from minutes, Typex Committee, 8 May 1944, 2 May 1945: AIR 20/1473.

[10] For forecasts by Creed Ltd., which were much higher than the more realistic forecasts of the overseeing Government department, see minutes, Typex Committee, 7 February 1944, para. 3: AIR 20/1473.

[11] John Ferris, The British Army, Signals and Security in the Desert Campaign, 1940-42, "Intelligence and National Security" 5(2) (1990), p. 263 passim.

[12] "Report on Special Intelligence, Kilindini", 9 December 1942, vol. 40, A. Hillgarth and R. T. Barrett, "Far East and Pacific": ADM 223/297.

Typex models and rotors

The two most common models of Typex were the Mk. II and the more mobile Mk. VI, of which production began around November 1943.[13] The main difference between the two models was that the Mk. VI used a six volt battery instead of mains electricity. A rotating handle drove the print unit. Figure 5 gives details of the main models. Nothing is known about Mk. IV, V and VII machines, which may have been experimental or have had only limited production runs.[14] The British continued to develop Typex during the war. A plugboard was brought into service with some models around 1943, although by no means all machines had been issued with plugboards even by February 1945. Development also continued after the war. The incorporation of a pluggable reflector, whose wiring was changed as part of a key, into Typex Mk. 22 (a development of Mk. II) suggests that it was a post-war machine, since the Germans only introduced a pluggable reflector for Enigma, Umkehrwalze D (Dora), towards the end of the war. The Mk. 22 was held down to destroyers in the Royal Navy (which also suggests that it was a post-war machine), to Brigade Headquarters in the Army and to Group Headquarters in the RAF.[15]

Seven rotors (or "drums", in Typex terminology) were required to give reasonable security, but at least 10 drums were issued from about January 1941 onwards.[16] Drums were at first solid, but were redesigned so as to consist of an outer casing or shell, and an inner removable insert, which contained the wiring. Mk. VI machines were issued with 14 inserts, five of which were used in the machine at any one time. Inserts were reversible which, in effect, doubled the number of rotors. 13,000 to 20,000 rotors inserts, each taking about two and a half hours to wire, were being made monthly in the first four months of 1945.

[13] Rusbridger, *op. cit.*, p. 231, errs (as in some other details), in stating that Typex Mk. VI did not enter production.

[14] On Typex models, see "Maintenance of Typex machines IB, II, III and VI by Code and Cypher Personnel" CD 0281: FO 850/134.

[15] Cryptographic Data Sheet Typex Mark 22. I am indebted to Kirk Kirchhofer for a copy of this document. On Umkehrwalze D, see "Uncle D", NA RG 457/ CBCB 54/7403A.

[16] "Type X Machine, Mark III" - vol. 1, para. 16. I am grateful to Kirk Kirchhofer for a copy of this document.

During the first 18 months of the war, higher units in the RAF used Mk. I drums and other units Mk. II drums. By December 1944, there were nine different sets of rotors or inserts, including at least one inter-service set, for RAF Typex. There were therefore about 90 to 126 different wirings for the RAF alone. Because inserts could be reversed, they were probably equivalent to between 120 and 168 rotors.[17] If, as is probable, the Army, like the RAF, had nine sets of rotors or inserts, the equivalent of from 180 to 336 different Typex rotors were probably in service with the Army and RAF at the end of the war.[18] Moreover, these figures do not take account of different inserts for the Typex machines used by the civil departments, such as the Foreign Office, or those in service with the Dominions.

RAF Typex keys

The RAF's Mk. I and II drums used the same keys until February 1941, when four keys were introduced for the Mk. II drums: „general", „home", „middle east" and „empire". Users in each area had the key for that area, plus the general key. If a message was being sent to addressees in more than one area, the general key had to be used. Later, additional keys were introduced for the middle east, India (which had two), Australia (again two), Canada and VIP and ferry movements. At the end of 1944, there were at least 30 different keys for RAF Typex - and seven keys for the CCM (probably for RAF-shared nets and not including separate CCM ciphers for the army or naval). Surprisingly, the 30 RAF Typex keys used only 10 different plugboard settings (although some of the shortfall may be because machines on some nets did not have plugboards). Indicators for RAF nets, which at first seem to have been chosen by operators, were later selected from an indicator book (as were indicators for Kriegsmarine Enigma[19]). This led to

[17] „Security of RAF Signals Communications", 9: AIR 20/1531. Since not all wirings took the form of inserts, the figures of 120 and 168 are reached by deducting an arbitrary one-third from the theoretical maximum number of inserts (that is from 180 (2(9x10)) or 252 (2(9x14)) for the RAF), to allow for some wirings possibly being solid rotors.

[18] The Navy is known to have had at least two sets of rotors in 1941 („code" and „cypher"), but is excluded from this reckoning, since comparatively few Typexes, as such, as distinct from the CCM, came into service with the Navy. Again, one-third has been deducted - from 240 (2(12x10)) and 504 (2(18x14)).

[19] On the indicator system for Kriegsmarine Enigma, see Ralph Erskine, *Naval Enigma - A Missing Link*, "International Journal of Intelligence and Counter-

a trade-off against ciphering efficiency. Encipherment and decipherment became much slower and signals were more often corrupt, requiring corrections. The rate at which Typex work was done in the RAF fell to only 25 per cent. of that at the beginning of the war. But at from four to eight groups per minute for Mk. II Typex, that was still two or three times better than the average speed with complicated book ciphers.[20] However, even with the aid of Typex, one of Isaiah Berlin's lengthy essays to the Foreign Office on wartime politics in Washington, which Prime Minister Winston Churchill found fascinating, took no less than 13 hours to encipher.[21]

Comparison with Enigma

It has been said that the British, like the Germans, relied mainly on a single cipher machine in World War II.[22] However, the statement completely ignores the CCM, which was used by the British in large numbers.[23] Even when comparing Typex to Enigma, as was probably intended, the statement is very misleading. Military Enigma was a standard machine, which was in part its undoing. There were virtually no variations between the Enigma machines issued to all three branches of the Wehrmacht - even down to their five identical rotors. Only the Kriegsmarine had additional rotors (VI to VIII) and two settable reflectors for the Kriegsmarine's four-rotor Enigma, M4.[24] The position with Typex was very different, with a minimum of 120 different rotors or inserts being in service.

intelligence", 3(4) (1989), p. 501; David Kahn, *Seizing the Enigma: The Race to Break the U-boat Codes*, Boston 1991, p. 285.

[20] "Security of RAF Signals Communications", 12.

[21] Ferris, *op. cit.*, p. 159. 13 hours implies that the reports were about 5,000 words long.

[22] Peter Calvocoressi, quoted in *The ULTRA Conference*, in David Kahn, *Kahn on Codes: Secrets of the New Cryptology*, New York 1983, p. 97. The use of several machines (mainly Typex, the CCM and Sigaba) by the Allies has been put forward as one of the reasons for the German lack of success against those machines (David Kahn, *Codebreaking in World Wars I and II*, in *Kahn on Codes*, p. 114). However, if any one of those machines had been as weak as Enigma or as poorly used, the German cryptanalytical agencies should, by concentrating their efforts against that machine, have had virtually as good a chance of breaking it as the British did with Enigma.

[23] Hinsley et al., *op. cit.*; vol. 2, p. 639.

Moreover, five rotor inserts could, in effect, be selected from a set of 28 (2x14 - because inserts could be reversed) for a Mk. VI machine, instead of Enigma's choice of three rotors from five, or three from eight for the Kriegsmarine's three-rotor machine, M3.[25] A single set of 14 rotor inserts could therefore be arranged inside the machine in a staggering 7,687,680 (28x26x24x22x20) different ways, compared to a mere 60 for German Army or Air Force Enigma or 336 for M3.[26]

Typex was consequently a significantly more refined system than Enigma. Wehrmacht Enigma had only two sets of rotors (one set for the land model and the other for the Kriegsmarine's M3 and M4) with about 50 per cent. commonality between all three machines, since they shared five rotors. In sharp contrast, Typex had 20 or more completely different sets of rotors. In addition, the rotors in one set had no common wiring with those in any other set. Thus the rotors in the „inter-service" set were not mixed with those used on other nets. Any penetration of one Typex net would therefore not have weakened the security of another net. In order to solve Enigma as used by the German Army and Air Force, the Allies had first to reconstruct or acquire the wiring of a mere five rotors. For the Germans to have been on an equal footing with Typex, as used by the British Army and the RAF, they would have had to find the wirings of from 120 to 252 rotors.[27] Even Marian Rejewski or Alan Turing might have blanched at that Herculean task. It is scarcely surprising that, although various German cryptanalytical agencies

[24] The Enigma Uhr (which made the plugboard non-reciprocal) and reflector D came into service comparatively late in the war and did not operate on all Enigma ciphers. It may also be that a few Enigma ciphers, such as that used by the Oberkommando der Wehrmacht („OKW" - the German High Command) to communicate with Hitler, used specially wired rotors. M4 was only slightly different from other Enigma machines, to allow for the fourth „rotor".

[25] As to the preceding part of this paragraph, see minutes, Cypher Security Committee, 7 February 1945, para. 38: DEFE 1/38.

[26] Enigma M4 is left out of account, since it was not a true four-rotor machine. The fourth „rotor" was really a settable reflector, which could not be used instead of rotors I to VIII. M4 had two such „rotors" (beta and gamma): Ralph Erskine and Frode Weierud, *Naval Enigma: M4 and its Rotors*, "Cryptologia", 11 (1987), p. 235.

[27] 120 rotors assumes, somewhat unrealistically, that the Army only had three sets of rotors, and that each RAF and Army set contained only 10 rotors. 252 is based on the Army also having nine sets and both services having 14 rotors in a set.

attacked Typex, they made little progress and that it was never broken by them.[28]

How secure was Typex? Two civilian experts have put its security at around the same level as that of Air Force and Army Enigma, but below that of four-rotor naval Enigma.[29] However, they were not aware of the addition of plugboards to Typex or of the huge number of rotors issued with Typex, which invalidates their comparison. Even without a plugboard, the multiplicity of rotors faced the German cryptanalysts with an almost impossible task. It is significant that the Germans never really began to penetrate Typex, although they captured a machine, without its rotors, and the keylists for about two months for one cipher net during the retreat to Dunkirk in 1940.[30] Typex was also used much more carefully than Enigma. In particular, the method for indicating message-settings (the rotor starting position for specific signals) was considerably improved as time went on.[31]

The supreme irony is, of course, that Typex infringed several patents on Enigma held by the German company, Chiffriermaschinen Aktiengesellschaft („AG").[32] Under section 29 of the Patents and Designs Act 1907, the British Government was entitled to use any patent, subject to the payment of royalties to the patent owners. However, in practice the British could not pay royalties during peacetime, since their use of the patent had to remain secret, while in wartime payment was clearly out of the question. It may therefore be that no payment was ever made to the patent owners. A secret British patent was granted to E. W. Smith for his improvements to the Chiffriermaschinen patent.[33]

[28] "German Success Against British Codes and Cyphers"; cf Hinsley et al., *op. cit.*, vol. 2, p. 641. Typex machines, again without rotors, were also captured in North Africa: memorandum by NID [Naval Intelligence Division] 10, 10 October 1945: ADM 223/505. However, Dr Otto Leiberich, a former member of OKW Chi IV, states that Typex was never attacked by his section.

[29] Cipher Deavours and Louis Kruh, ***The Typex Cryptograph***, "Cryptologia", 7(2) (1983), p. 163. See also "Cryptographic Description, Type X Machine": NA RG 457/CBTC 46/17428a.

[30] "German Success Against British Codes and Cyphers".

[31] "Security of RAF Signals Communications", 9.

[32] Patents 267,472, accepted 11 August 1927 and 343,146, accepted 16 February 1931, "Patent Application by Ernest William Smith, 24 May 1938, improvement in cipher machines": AVIA 8/355; minute, 3 December 1937: AIR 2/2720.

[33] "Patent Application by Ernest William Smith".

The development of Typex cost the British very little, largely because a major part of its research and development costs had been indirectly met by Chiffriermaschinen AG in evolving commercial Enigma! Initially, Typex was little more than a private venture by four individuals in the RAF, although with some official blessing. Eventually, around 1940, Lywood was awarded £500, Coulson £50, Lemmon £100 and Smith £250 (in present day terms about £15,000, £1,500, £3,000 and £7,250, respectively).[34] The total cost (£900) of those payments was a mere fraction of the £30,000 awarded in arbitration in the 1930s to a Mr O'Brien for inventing the very basic, and far from secure, Syko machine, which was little more than a holder for cards which embodied a series of mixed alphabets.[35] Once Typex entered volume production it was relatively cheap to produce - initially costing about £108 per machine in early 1939, which fell to about £90 in 1940. Syko machines cost about £4 or £5 each but provided such poor protection to signals that message security was actually increased when they were dropped and the RAF relied on cards alone („Rekoh").[36]

Why did the British take such pains to improve Typex? The knowledge that GC and CS was breaking Enigma is likely to have been the main reason. The contrast with the German approach to Enigma, which underwent very little development, is marked. Unlike Enigma with its mere eight rotors, the British did not, with Typex, put all their eggs into one very confined basket. Perhaps the clearest moral when comparing Enigma and Typex is that one should not adopt a single cipher system as a standard. That lesson is as relevant to cipher practice today, especially in the commercial world, as it was during World War II.

[34] Minute, 12 September 1941, PAS (E) MAP Chairman: AVIA 8/356. Coulson's award was later increased by £50, minute, 3 March 1942: ibid.

[35] Archer, minute, 12 March 1937; "Security of RAF Signals Communications", 12. On Syko, see "Syko Machine: Cryptanalytic Study, 1942": NA RG 457/ZEMA 180/10415a; "Study of the "Syko Machine": NA RG 457/ZEMA 22/2341a; "Enciphering Cards for the Syko System, circa 1944": NA RG 457/ZEMA 181/13050a; David Kahn, *The Codebreakers: The Story of Secret Writing*, New York 1967, p. 463.

[36] Under Rekoh, the cards were no longer reciprocal: „Security of RAF Signals Communications", 12.

Conclusion

Typex undoubtedly made a major, albeit little appreciated, contribution to the British war effort, which could not have been pursued efficiently without a secure cipher machine. As it was, producing and distributing subtractor tables in adequate numbers for the codes being used presented an almost intractable problem until mid-1943 when a new system, the stencil subtractor, seems to have allowed tables to be used more efficiently.[37] The nature of the predicament facing the authorities due to heavy cipher traffic is illustrated by figures from the RAF's Telecommunication Centre, Middle East („TME"), which on a peak day in May 1943 had to encipher 106,421 groups - one-sixth using codebooks and the balance (about 89,000 groups) with Typex. TME reckoned that, at that time, a cipher clerk could handle 21,000 groups of super-enciphered book code a month and about 50,000 groups in Typex. TME therefore requested 26 sergeants for book ciphers and 54 sergeants for Typex work: the same number would, of course, have been needed for decoding purposes at the receiving end of the traffic.[38]

RAF signals traffic rose from 2.5 million groups per month in February 1941 to about 22.5 million in October 1944, although not all of it was handled by Typex.[39] In October 1944, the British military and civil authorities enciphered 45 million groups on Typex. By April 1945, the figure had increased to 49 million groups in 413,000 messages.[40] Without Typex, thousands more men and women would have had to be employed in the British forces on high-level cipher work.[41] Training them would have been a major problem. More cipher errors would have been made and radio communica-

[37] Hinsley et al., *op. cit.*; vol. 2, p. 632, 638.

[38] AIR 2/4853. I am grateful to Frode Weierud for this information.

[39] „Security of RAF Signals Communications", 10.

[40] Minutes, Cypher Security Committee, 4 July 1945, para. 288: DEFE 1/38.

[41] By January 1944 the Army employed 2,000 cipher operators, not all on high-level traffic: Major L. E. Clark, „Stencil Subtractor Frame", memorandum of 7 January 1944: FO 850/132.

[42] The only completely secure system would have been one-time tables. However, it would have been completely impracticable to have used them for the volume of traffic enciphered on Typex. On the difficulties of using one-time tables for high-volume traffic, see Kirk Kirchhofer, *Cryptology: Part 2 - The 'Unbreakable' System*, "International Defense Review" 9(3) (June 1976); letter from Howard Campaigne, "Cryptologia" 7 (1983), p. 129. Campaigne was formerly the head of mathematical research at the National Security Agency.

tions would probably have been hampered, with incalculable consequences, since book codes were slow and difficult to use. Signals security would have been gravely imperilled, since British codes and tables could not possibly have dealt safely with the volume of traffic.[42] The war machine as a whole would have been seriously impeded. There can therefore be no doubt that the United Kingdom owes an immense, but largely unrecognised, debt to Wing Commander Lywood and his small amateur team since, by indirectly assisting to shorten the conflict, their work, like that of the GC and CS codebreakers, helped to save many lives.

Acknowledgments

I am, as ever, grateful to Gilbert Bloch for comments.

Figures 1 to 4 (from AIR 10/4051, 4052 and AVIA 8/355), which are Crown copyright, are reproduced with the permission of the Controller of Her Majesty's Stationery Office.

S.D.0336 (1)

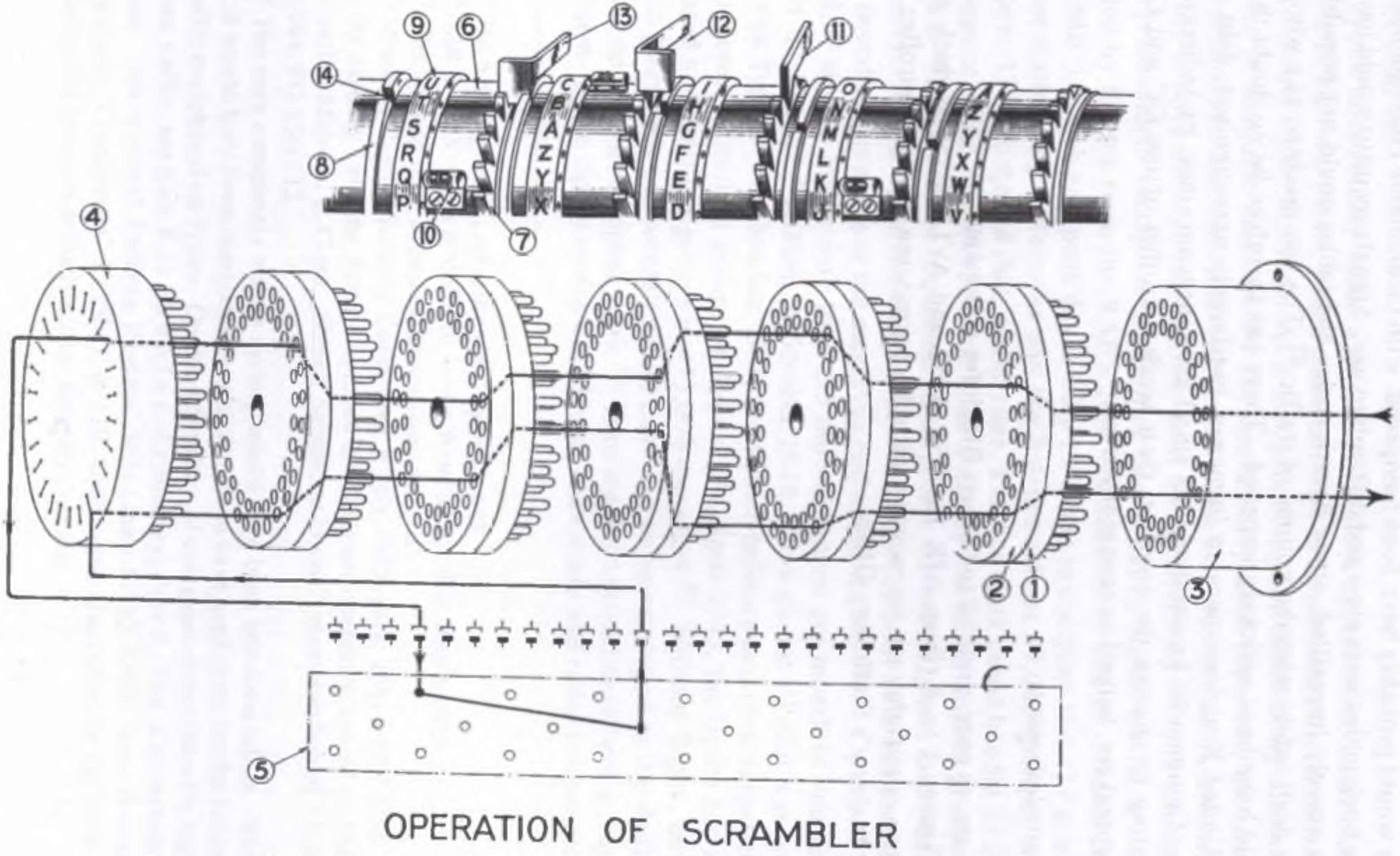


Figure 1: Typex: Operation of Scrambler and Pawls. [AIR 10/4051]

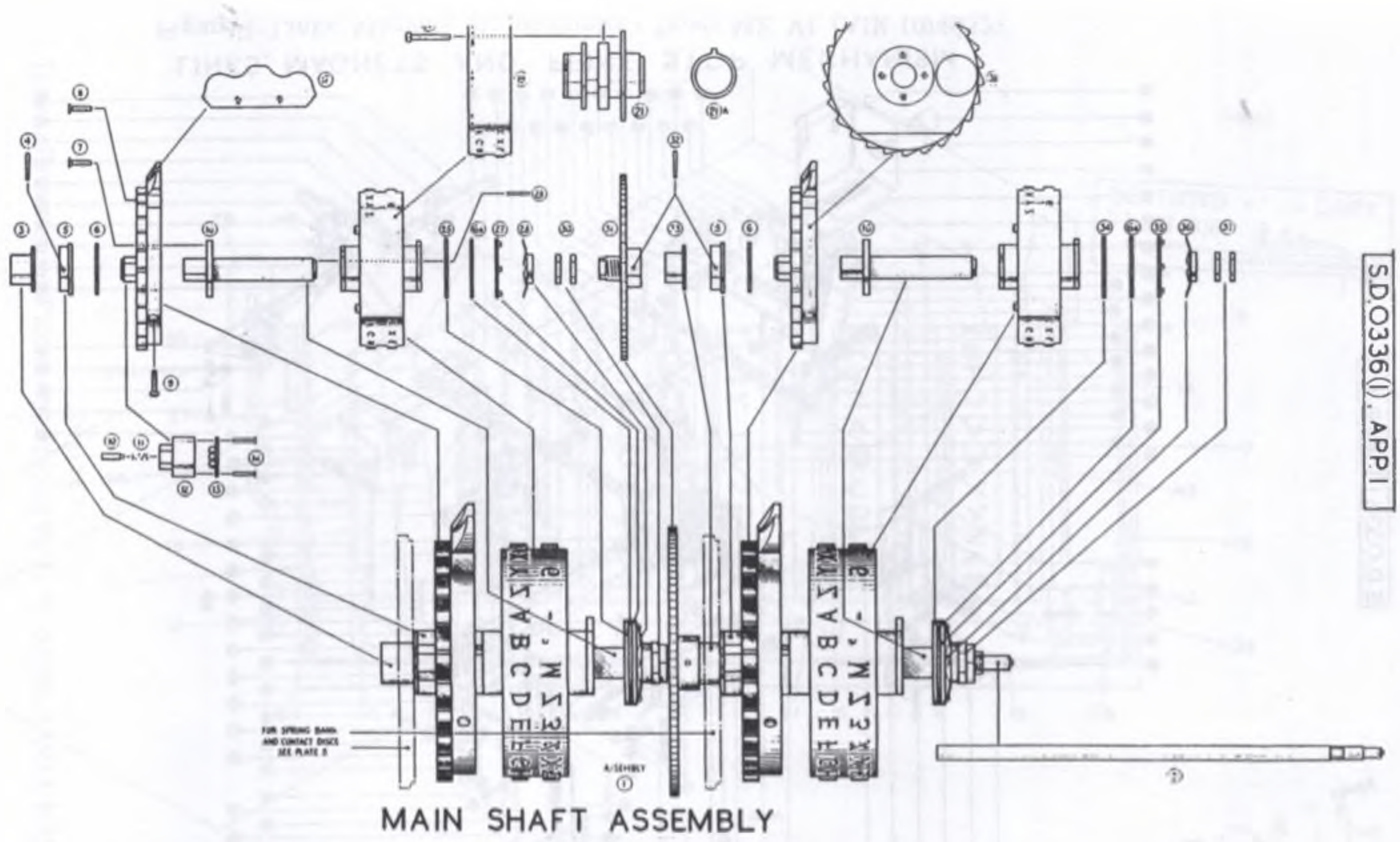
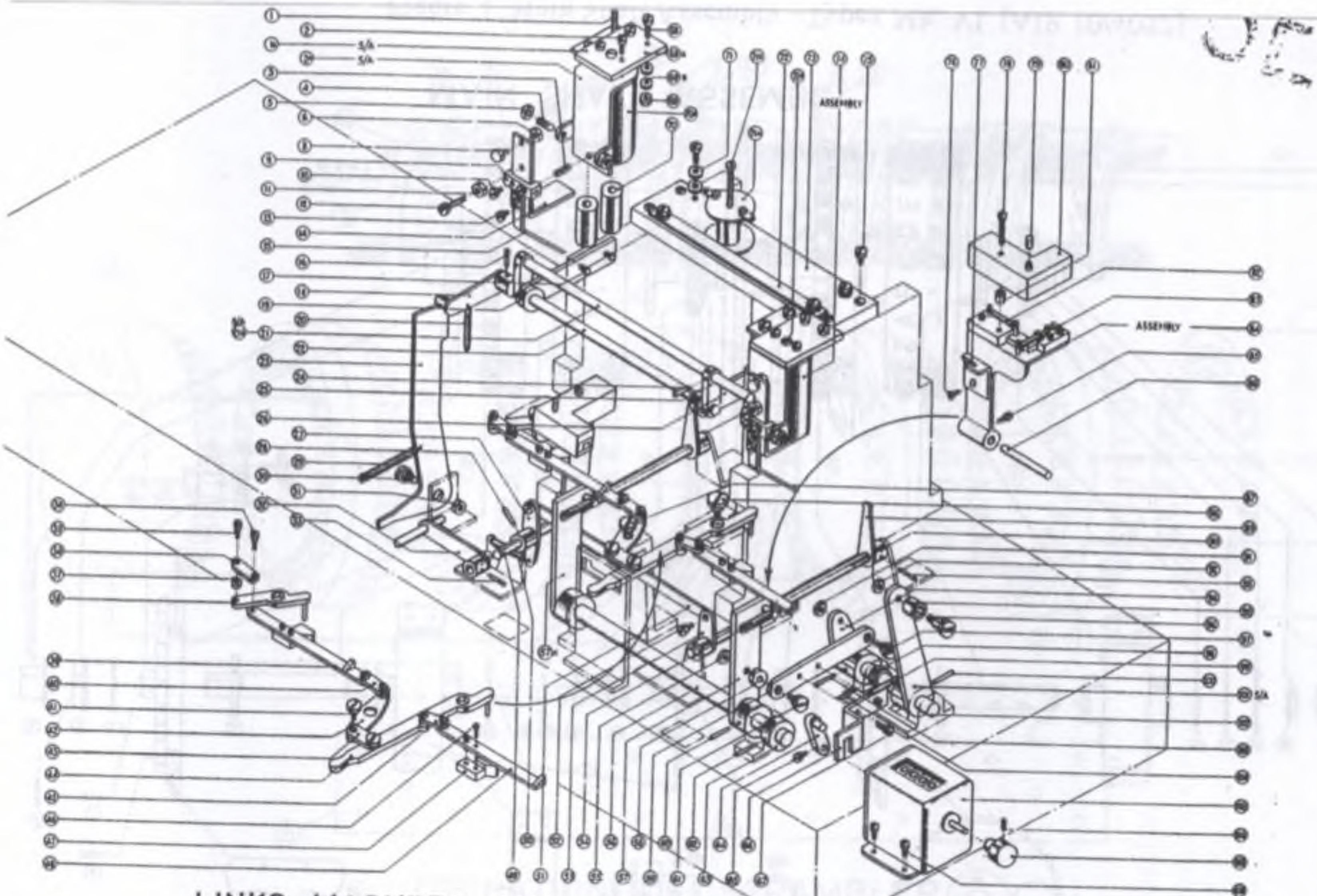


Figure 2: Main Shaft Assembly - Typex Mk. VI. [AIR 10/4052]



LINKS, MAGNETS AND PRINT STOP MECHANISM

Figure 3: Links, Magnets, etc. of Printer - Typex Mk. VI. [AIR 10/4052]

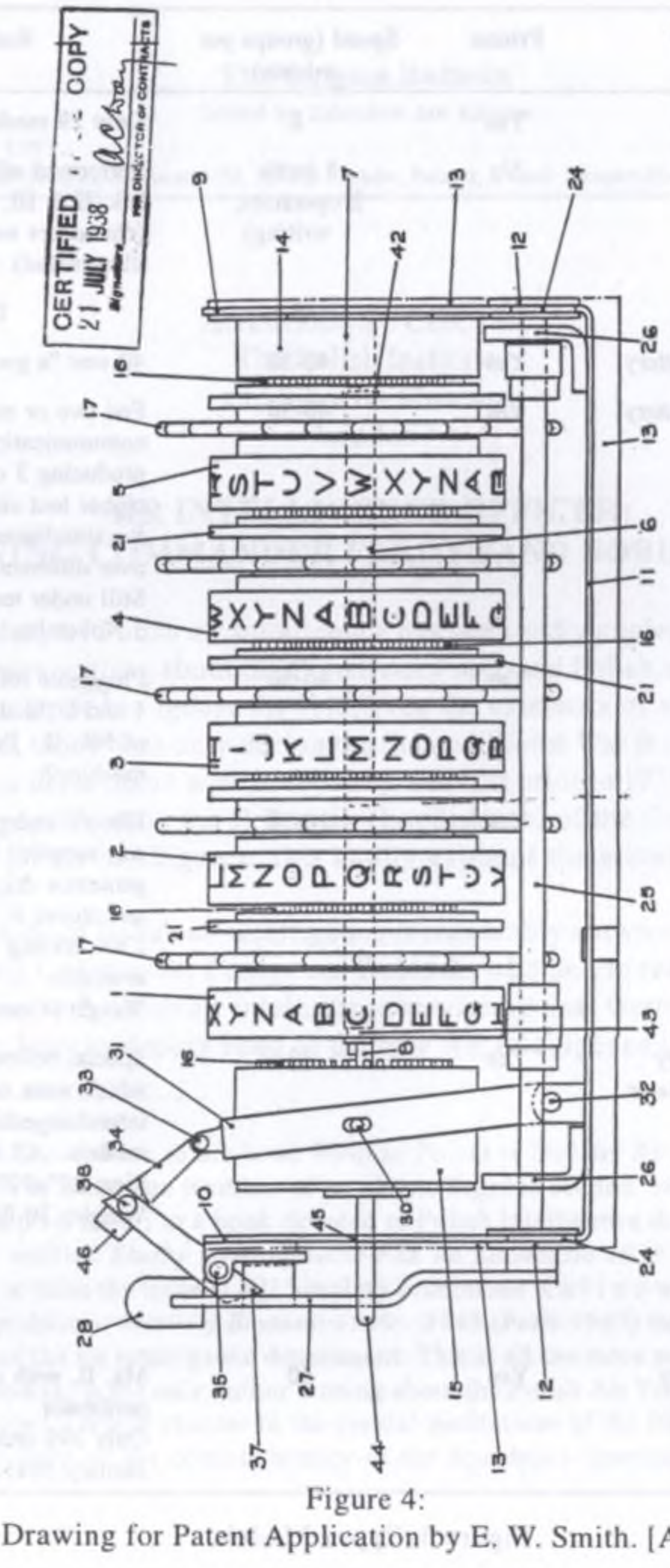


Figure 4:
Typex: Drawing for Patent Application by E. W. Smith. [AVIA 8/355]

Mark	Power	Printer	Speed (groups per minute)	Remarks
I	230v	Yes	8	Only 29 made.
IA	230v	No	8 (with 2 operators; 1 writing)	Performed all functions of Mk. II & III, except printing (characters were illuminated).
IB	230v	No	8	Do.
II	230v or battery	Yes	40-50	40 was "a good high speed".
IIA	230v or battery	Yes	40-50	Fed two or more communications channels, producing 3 or 4 copies of cipher text simultaneously, for simultaneous despatch over different WT links. Still under test at 3 November 1944.
22	230v	Yes	40-50	Pluggable reflector. Rotors 1 and 5 fixed. Development of Mk. II. Post-war machine?
III	Hand	Yes	16-18	Electric energy for printing was supplied by impulse generator driven by handle and stored in condenser. 230v driving unit was available. Weight in case: 65 lbs.
VI	6v battery or accumulator	Yes	12	Special hollow drums used, which were not interchangeable with other models. All inserts useable. Size: 20"x12"x9". Weight: 30 lbs.
VIA				
VIB				
VIII	230v or battery	Yes	50	Mk. II, with morse perforator. Only 398 ordered at 10 January 1945.

Figure 5: Typex Models.