844

TOP SECRET

[redacted]

EO 3.3(h)(2)
PL 86-36/50 USC 3605

REPORT ON VISIT TO FRENCH "SECTION DU CHIFFRE"

On 21st May 1951, I went with Cdr, G.Chiles, U.S.N., to the French Combined Forces Headquarters (Etat-Major Combiné des Forces Armées)) at 51, Boulevard de la Tour Maubourg in Paris. We had been instructed to report to Colonel VEYRON LA CROIX, to witness a demonstration of the French modification of the M-209-B Hagelin. Most of our subsequent discussions were carried out with Commandant ARNAUD at the Ministry of War. The evidence leads us to believe that he may be the head of the French Army cryptanalytic bureau, and that our meetings took place within the walls of that organisation. The atmosphere was very friendly throughout, and we gained the impression that they would have liked to tell us more than they were allowed. It is probable that Arnaud would welcome technical collaboration both on cryptography and cryptanalysis.

2. A summary of our conclusions is given below. Part II of this report contains a personal record of the visit, Part III a description of the French modification with some comments on its practicability and implications, Part IV an outline of an electrical keyboard modification of which we were given some details.

3. After careful study of the French modification to the M209, we reached the conclusion that it is a practical proposition. They have gone to considerable trouble to circumvent the practical snags. The changing of the alphabets is no more tedious than the normal change of pin- and lug-settings, and can be completed in about 10 minutes. The danger of error is probably less than in the pin-settings, and is counteracted by the carrying out of a 26-letter check. They claim that after a little practice encypherment with a hatted wheel is no slower than the present system; while experiments will be needed on this, we consider that this estimate may prove to be fair.

4. As a result of this, it follows that a frequent change of alphabet is quite practicable, and the French in fact propose to change at least every other day and possibly daily. This means that the alphabet may be regarded as uncompromised, and considerably alters our previous misgivings on security. A detailed security study must now be made of the implications of this modification.

5. The French will have 1800 machines by the end of this year, and will presumably introduce it throughout their Army shortly afterwards. The modification of these machines will take about 8 months, at a cost of £8 per machine. It is thus comparatively quick and cheap to introduce.

6. Whatever the result of our final security evaluation, it seems likely that the modified machine will provide an adequate solution to the problem of French internal military traffic. It also seems probable that it will prove sufficiently secure for third-level NATO traffic, at least until some better machine is available. It is therefore recommended that it should be given serious consideration as one possible solution to this problem.

PL 86-36/50 USC 3605

[redacted]

TOP SECRET

~~TOP SECRET~~

PART II. RECORD OF EVENTS.

At Combined Forces Headquarters, we were kept waiting an hour until Colonel Veyron La Croix returned from lunch at half past three. During part of this time, we were entertained by his Adjutant, Commandant Lignac, who claimed to know nothing about cyphers. From his conversation and the diagrams on the walls, it appeared that we were probably in the French equivalent of the [redacted] and that the section was mainly concerned with such matters as frequency allocation. Cdt. Lignac spoke English moderately well and had often been in London, and had had contacts with [redacted]

2. When the Colonel finally arrived, he did little more than introduce himself and arrange for a car to take us to the Ministry of War, where the modified machine was to be demonstrated by Commandant ARNAUD (whose name was familiar as the French representative on the NATO cypher committee). The Colonel did not speak English. He was enthusiastic concerning the modified machine, of which he said that 1800 would be available by the end of 1951. He said that the modification could also be applied to another machine called the "Aigline"; when asked about this latter machine, he said that ARNAUD would be able to give us full details.

3. We then had to wait about 20 minutes in the courtyard while a car was found for us. We left Headquarters not particularly impressed by the efficiency of the arrangements which had been made for our reception.

4. At the Ministry of War (231, Boulevard Saint-Germain), we were conducted up to the "Section du Chiffre" on the third floor. At no time during our visit were we asked for any proof of identity. Our way to the Section du Chiffre was blocked by a door marked "No entry except to authorised personnel". A number of factors combined to make us believe that we were in the French Army cryptanalytic bureau:- (a) French Sigint was known as "Section du Chiffre" before the War; (b) the books in Arnaud's library included all the standard cryptanalytic works ; Baudouin, Givierges, Yardley, etc.; other volumes included an ABC Telegraph Code, Bentleys, and Swedish and Spanish dictionaries; (c) there was a general air of secrecy and great care was taken to ensure that no doors were left open for our inspection; (d) one piece of evidence during the visit suggested that Germans were employed in the section, and the French Army is known to have recruited certain German cryptanalysts for work in their Sigint organisation. If this theory is correct, Cdt. Arnaud, as Chef de Section, is presumably the successor of Colonel BERTRAND.

5. The remainder of the time was spent in Arnaud's office, and we were not introduced to any of his subordinates. He began by saying that he knew insufficient English to expound his subject, and the discussions were carried on entirely in French. As Cdr. Chiles does not know French, I acted as interpreter throughout. It was apparent, however, that Arnaud understood most of what we said in English. He was obviously master of his subject, very shrewd, with a dry wit; we left with a very favourable impression of his efficiency.

6. He began by asking what we were experts in. I said that we represented the users, and had come to investigate the practicability of the modification which had been described to us. He expressed himself disappointed, as he had hoped that we should be in a position to discuss the security implications. I replied that we were not qualified to do this, although we should probably be able to understand any such points which he wished to put across.

[redacted]

~~TOP SECRET~~

~~TOP SECRET~~

7. He said that they had undertaken the modification owing to the basic security weakness of the present machine, by which three messages with the same indicator can be read "and theoretically, even two". It seems almost certain that he in fact knows that a depth of two is readable; he referred to depths of two later in the conversation; and, if he employs Voegele, who was a German expert on the M209, he must certainly be aware that the Germans exploited such depths. His reticence may be an indication that the French are currently exploiting this weakness, and do not therefore wish to broadcast the possibilities.

8. He then showed us the modified machine, and gave us ample opportunity to experiment with it, change the alphabets, etc. Possibly owing to the fact that the modification has been patented, he refused to let us have a modified wheel to take away, but allowed us to make rough drawings. He said that the alphabet should be changed according to traffic load (he refused to commit himself on what should be regarded as a safe load); he thought it should be changed every other day at Division, and that it might be desirable to change it daily. As a result of our investigation, we reached the conclusion that they had done a very nice job, and that a daily change should be a perfectly practicable proposition. A detailed description of the modification, production, cost, etc. will be found in Part III.

9. Arnaud emphasised that he considered the security of the modified machine very high. Depths of two or three could not be read, and even if users employed the wrong alphabet or made mistakes in setting it up, he did not think that security would be jeopardised. He thought, in any case, that such mistakes would be of rare occurrence, since a 26-letter check is printed with the keylists; if this check is carried out, any mistake will be immediately obvious.

10 He was prepared to issue a separate wheel with the normal straight alphabet as well as the modification, and gave three reasons for this :- (a) if the U.S. Army refused to adopt the modification, they would require to talk to the Americans in the less secure machine; (b) they might not wish to give the modified machine to countries whose security arrangements were in question; (c) they might use the machine unmodified in dangerous areas where there was risk of capture.

11. When we had fully discussed the modified machine, Arnaud volunteered that they were designing an electrical version to work with a keyboard. This would use the same principle as the modified machine, and many of the same parts, so that one type could work with the other. We expressed considerable interest in this, particularly in view of the speed which he claimed for it, and he finally produced a drawing for our inspection. I suspect that he had reason to regret this afterwards, as the drawing contained two noteworthy features :- (a) The German word "Klartext" on the plain-language tape suggests that the machine was designed by a German; (b) The appearance of numbers on some of the wheels suggests that the cycle has been increased, and that it would certainly not work with the present machine. The wheel-periods would appear to be 29 31 .. .. 35 ..

12. A reconstruction of the drawing from memory, together with any details which Arnaud gave us, will be found in Part IV. I asked Arnaud whether he proposed to include the figure substitution system as for the present modification (see Part III), and in that case whether the machine

would print figures on the tape or only their letter equivalents. He replied that he was including the substitution system, but that only letters would be printed. I suggested that, as in any case he had to modify the printer-head to print two tapes, he might consider a shifting printer so that the numbers could be printed direct on to the tape instead of substituted afterwards. He agreed that this would be a useful facility, and said that he would consider the possibility.

13. I then asked Arnaud about Colonel Veyron La Croix's statement concerning "Aigline". He appeared rather annoyed and said that the Colonel must be thinking of the other French machine, the B211. This worked on a different principle, and was quite unsuited to the modification. The Colonel was not a cypher expert, and did not know what he was talking about. The following morning, he asked the Colonel what he meant, and it finally emerged that "Aigline" was the Colonel's pronunciation of Hagelin; he had merely meant that the modification could be included in Hagelin models other than the M209. The subject of B211 was thus introduced accidentally, and against Arnaud's will.

14. At the end of the day, we were asked to return the following morning, as the Colonel would like to see us before our departure. The Colonel was at a meeting when we arrived, and was again half an hour late for the appointment. During this time, we were able to ask more questions, and do a time test on the changing of the alphabets.

15. When the Colonel arrived, he began by stating that the modified machine was eminently suitable for use at levels where speed of encypherment was not the first consideration, but where weight and lack of power supply were the main factors. He therefore envisaged that it would be used only at the third level - forward of Division; he thought that the electrical model, when it was ready, might well be suitable for the second level.

16. He then asked whether we knew what Hagelin models other than M209 were available to the various NATO countries. Arnaud had previously stated that he believed M209 was available to all NATO countries except Norway and Italy. I replied rather guardedly that the Hagelin machine was of course produced in a number of models by the Swedish firm, but that we did not know how far such models might be used by other countries.

17. He then asked us what we had decided. We replied that it was not up to us to decide, but merely to report back in detail what we had been shown and told. Acceptance of their modification would depend upon a study of the security implications, on which we were not in a position to comment, and upon what other systems were available as an alternative solution. On the practical side, we should put it forward as our personal opinion that they had made a very good job of the modification, that frequent changing of the alphabet in the way they proposed seemed to be an entirely practicable proposition, and that for this reason we should recommend that their machine deserved serious consideration as one possible solution to the problem of third-level NATO communications. They both expressed themselves very satisfied with this statement; Arnaud said that they had of course done a full security appreciation of the machine themselves, but that naturally each country must make up its own mind on such a matter. He expressed himself willing to go to Washington to demonstrate the machine if required, and the Colonel supported this.

~~TOP SECRET~~

[redacted] EO 3.3(h)(2)
PL 86-36/50 USC 3605

18. Several times during the morning meeting, the Colonel pointed to Arnaud's safe and suggested that he had some interesting documents which he ought to show us, whereupon Arnaud would reply that there was nothing of interest. At one stage, quite a voluble argument proceeded between them as to whether or not we should be shown these exhibits, in which - unfortunately for us - Arnaud prevailed. We had the impression throughout that he regarded the Colonel as a thorn in his side.

19. We felt, however, that Arnaud would have been very willing to co-operate on a reciprocal basis. Both men were fairly forthcoming, and there is little doubt that if we had been prepared to enter into any discussions on security we should have been given a considerable insight into their methods and organisation.

20. We parted on very friendly terms; we thanked them for the way in which they had answered all our questions and allowed us to go into details on the machine; they expressed their appreciation that our Governments had made us available for such a discussion; and Arnaud stated that he was fully at our disposal if we wished to follow up the meeting in any way.

[redacted]

PART III. M209 MODIFICATION.

Two main alterations are involved in the French modification - replacement of the printer alphabet by removeable segments, and replacement of the alphabet on the setting-wheel by removeable segments. In addition, a new setting-wheel containing the numbers in fixed numerical order has been added outside the normal wheel, which has the double purpose of locking the alphabet segments in position, and providing a letter-figure simple substitution. The space-mechanism, and consequently the letter Z on the two alphabets, has remained unaltered, and the Z segments are locked in position.

2. The modification is issued as a complete unit and is easily detachable from the machine. (Fig. 7) Reference should be made to the accompanying diagram. The shaft on the normal M-209-B convertor has been cut about half way between the gear wheel and the printer wheel; a notch (g) is cut on one side of the stump, and brass bushing installed inside the hollow. (Fig. 8). The modified unit is fitted with a projecting lug (f), which fits exactly into the notch; it is then locked into position by inserting a butterfly screw (h) through the hollow shaft of the unit, and screwing it into the brass bushing. When screwed up, the butterfly lies flat with the surface of the outer knob.

3. On the print-wheel,(Fig. 4) the type segments are replaced by a narrow taut spring (e), attached to each side of the fixed Z segment. Each type segment (Fig. 5) has a hook at the inner end, which is inserted by holding the segment vertically and sliding it under the spring (Fig. 6); the type face is then lowered into its normal position, where it is held by the spring. To remove it, pull it into the vertical position with a pair of pincers, and slide out the hook from under the spring.

4. On the setting-wheel (Fig. 3), the alphabet is again replaced by a spring (d), and beds for the letter-segments are hollowed out. The segment is slid horizontally into its bed (Fig. 9), where it is held lightly in position by the spring. Very little pressure is required to slide the segment in either direction, but the spring holds it sufficiently to prevent it from falling out while the remaining segments are inserted.

5. Finally, there is a removeable annulus (Fig. 2) containing the figures 0-9, 0-9, 0-4 in order, with one blank segment coloured red. Inside the rim of the annulus are three short slots, which fit over three shallow knobs (a) on the face of the setting-wheel (Fig. 1). The annulus is then rotated slightly, so that the three knobs are held in the slots, and a spring on the face of the annulus (b) falls into position behind one of the knobs to hold the annulus in position. The annulus is removed by raising this spring clear of the knob, and rotating until the slots are released. It will only fit against the setting-wheel in one position, which throws the red segment against the fixed letter Z on the setting-wheel.

6. In order that the machine should decypher, it is essential that the alphabet on the print-wheel should be in reversed order from that on the setting-wheel. In the machine as shown to us, the alphabet employed was reciprocal, so that the machine would have decyphered equally well with the printer alphabet in the same order. Arnaud was apparently unaware of this unnecessary feature, which would be a slight weakness if used in practice.

~~TOP SECRET~~

7. The purpose of the numbered annulus, in addition to holding the setting-wheel segments firmly in position, is to provide a means of encyphering digits without spelling them out. A letter such as W is taken to indicate "numbers follow", and the user then encyphers any of the alternative letters opposite the figures on the annulus; in decyphering, these are printed as letters, which must be substituted manually, by reference to the setting-wheel. When encyphering important numbers, or when there is danger of corruption, numbers will either be spelt out in full, or the substituted letters repeated.

8. The machine which was demonstrated is the only one at present available. 1800 machines have been contracted out to a firm (which they have security vetted) for modification, and these are expected to be ready at the end of 1951, i.e. eight months from the time of placing the order. The cost of modifying each machine is about 8000 francs (£8). The modification is thus quick and cheap.

9. Although Arnaud was the inventor of the modification, it has been patented by the man responsible for development. If it should be adopted by other countries, it is their intention that those countries should modify their own machines, and they would have to purchase the patent rights. Arnaud offered to put us in touch with the development authority if we should be interested, and was obviously anxious that the question of the patent should not stand in the way.

10. When the 1800 machines are ready, they will be sufficient to satisfy the needs of the French Army, but not of course of other NATO nations.

11. Together with the modified unit, they are supplying special boxes, containing two drawers each divided into 25 segments lettered A to Y. These will be used to store the setting and printer alphabets, and it is intended to issue three sets of each with every machine. This means that if a segment is lost there is a replacement immediately available; it also enables the user to employ a different set of type when setting up the new key on the print-wheel, with consequently less trouble from inky fingers.

12. After experimenting with the alphabets for some time, we both reached the conclusion that changing the alphabets is comparatively quick and simple. It is slightly "fiddly", but no more so than resetting the pins and lugs. It took us 13 minutes to effect a complete change of alphabet key; this was without previous practice, and without the help of the lettered boxes, which enable the correct letter to be found more quickly. Arnaud estimated that the change could easily be done in 10 minutes with practice, and we endorsed this view. The conclusion is that this extra process takes no longer and is no more liable to error than the existing changes of key, and cannot be regarded as in any way an intolerable burden.

13. Arnaud had also carried out tests on the speed of encypherment using a hatted setting-wheel. He found that an average operator was slightly slower than usual for the first half hour after the change; but that he soon became used to the new alphabet, and used it as quickly as the present system. While we did not experiment with this at length, we found that it was unexpectedly easy to find the correct letter, and we believe that his estimate is not far wrong.

[redacted] EO 3.3(h)(2)
PL 86-36/50 USC 3605

14. He had had no opportunity to carry out prolonged tests on the print-wheel. He expressed himself confident that the strain on the spring was very small, and that no trouble would be experienced from this source.

15. It appears that the greatest danger from the changing alphabets is the possibility of setting them up wrong; if operators carry out the 26-letter check as ordered, the mistake will immediately be spotted; and the danger is probably less than that of making a mistake in the pin-settings.

16. If we accept that the modified M209 is a practicable proposition, it remains to assess its security. It seems likely that the French have not gone further than to decide that depths are unreadable. Our previous security doubts were based on the assumption that it would be impracticable to change the alphabet very often, and it must therefore be assumed compromised. If it can be changed frequently, however, and the French are prepared to change it at least every other day and possibly daily, it can be assumed uncompromised, and our security view must be very different.

17. Attacks based on depth are defeated, and similarly cribbing attacks, unless the enemy has a cribbed depth of two. An investigation must be made, however, as to how far statistical attacks are still possible, and what will be the effect of the additional busts which may occur if the 26-letter check is not enforced. It seems likely that our conclusion will be that it is not as good as we would like for our own use, but that (a) it solves the problem of French military traffic, and (b) it may be acceptable as an interim system for third-level NATO traffic until something better is available.

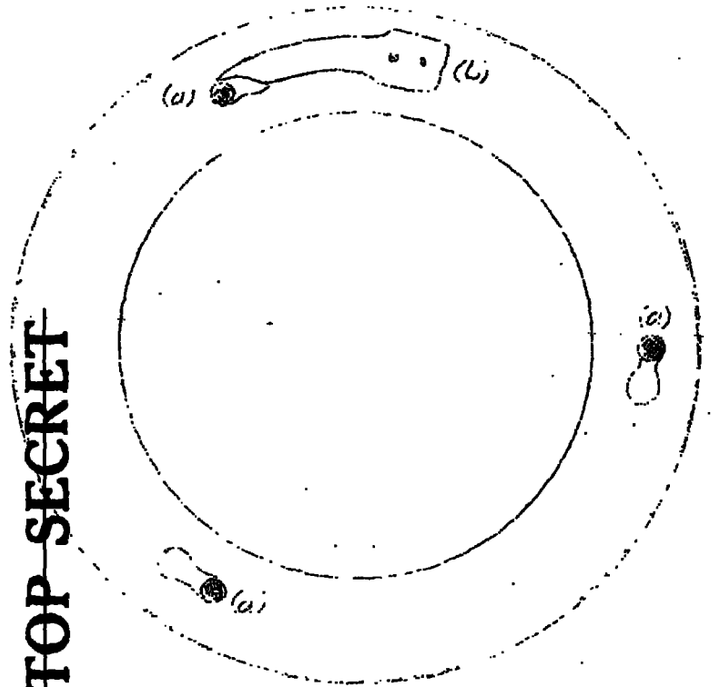


Fig 1

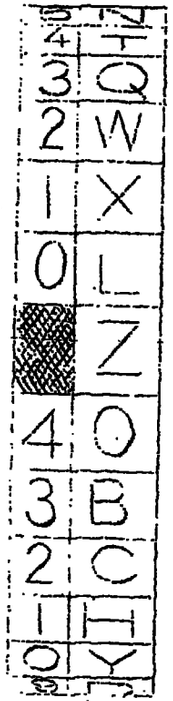


Fig 2

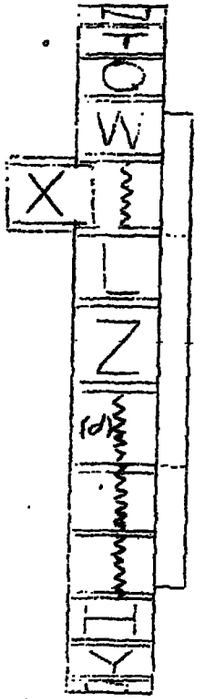


Fig 3

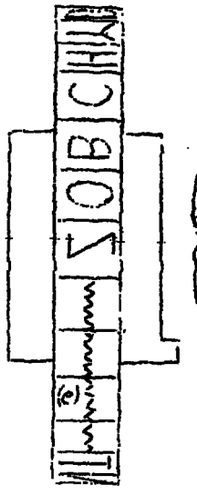


Fig 4

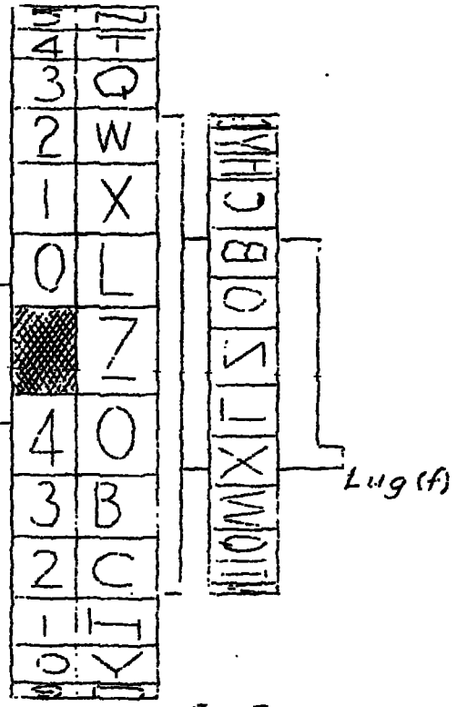


Fig 7

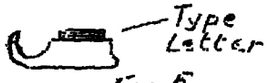


Fig 5

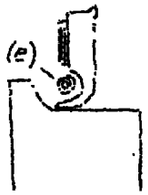


Fig 6

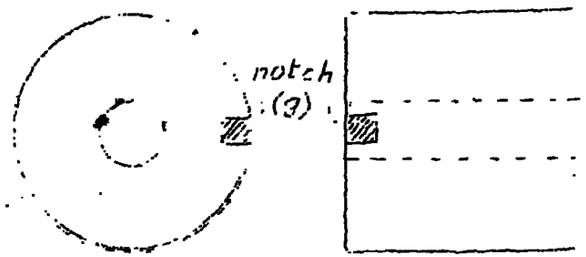


Fig 8

Fig 9

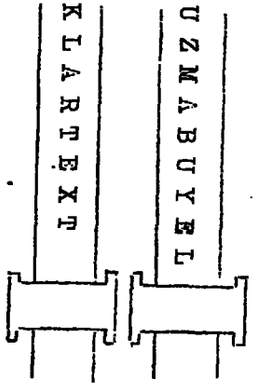
ROUGH DIAGRAM OF FRENCH
M.209 MODIFICATION

IV. ELECTRICAL M.209

According to Arnaud, the French are in the development stage of an electrically-operated keyboard version of the M.209, based mainly on the same parts, and designed to work with the present modified machine. This statement is inconsistent with the design which we were shown, which is reproduced from memory on the right; it will be seen that figures as well as letters appear on the wheels, which must thus apparently have a larger cycle than the present machine. This cycle would appear to be 29 31 .. .. 35 ..

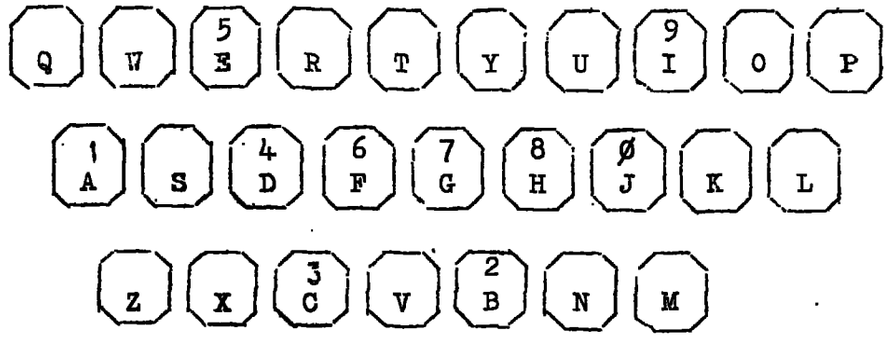
2. The dimensions of the machine will be 26 x 23 x 9 cm. It will weigh about 8 Kg. (18 pounds). Details of voltage, etc., are not settled. It will be capable of hand as well as electrical operation. It will print in plain-language as well as a cypher tape. As at present planned, numbers will be printed as their letter equivalents; he will consider the possibility of including a shifting print-wheel. He claimed that it will operate up to 4-5 characters per second.

3. It is clear from the diagram that, quite apart from the fact that it would not even work with the unmodified M.209, no provision has been made for variable alphabets. Arnaud did not make it clear how he proposed to achieve this, and it was thought better not to press him further at this stage.



2	2	U	N	7	Q
3	3	T	M	8	P
Z	4	S	L	9	O
Y	5	R	K	Z	N
X	Z	Q	J	Y	M
W	Y	P	I	X	L
V	X	O	H	W	K
U	W	N	G	V	J
T	V	M	F	U	I
S	U	L	E	T	H

X
Y
Z
A
B
C
D
E



Sketch from memory of electrical keyboard machine. (Some details doubtful.)

TOP SECRET

TOP SECRET