File duplicate

Return to AFSA-14

S-99

TOP SECRET "U"

TICOM/I-31 annex G

DETAILED INTERROGATIONS OF DR. HUETTENHAIN, FORMERLY HEAD OF RESEARCH SECTION OF OKW/CHI, 18TH - 21ST JUNE, 1945.

Attached are the reports of four interrogations of Regierungsrat Dr. ERICH HUETTENHAIN, carried out at OKM Signals School, FLENSBURG, on 18th, 19th, 20th and 21st June, 1945.

Preliminary interrogation reports of Dr. HUETTENHAIN have been issued as TICOM/I-2 and I-21.

Dr. HUETTENHAIN has now been brought to the U. K., with Sonderfuehrer FRICKE, for further interrogation.

TICOM
8 July, 1945

No. of Pages 21
Copy No. 30

Distribution

British
1. Director
2-3. D.D.3 (2)
4. D.D.4
5. D.D.(N.S.)
6. D.D.(MW)
7. D.D.(A.S.)
8-9. A.D.(C.C.R.)(2)
10. Lt. Col. Leathem

TICOM
11. Chairman
12-13. S.A.C.(2)
14. Cdr. Bacon
15. Cdr. MacKenzie
16. Cdr. Tandy
17. Lt. Col. Johnson
18. Maj. Seaman
19. Lt. Cdr. Manson
20. Lt. Eachus
21. Lt. Vango
22. Capt. Cowan
23. Lt. Feild
24-25. Ticom Files (2)

U.S.
26-27. CP 20-G (2)(Via Lt. Pendergrass)
28. G-2(via Lt. Col. Hilles)
29-30. S.S.A.(2)(via Major Seaman)
31. Director, S.I.D. SACSEA (via Lt.Col. Johnson).

Additional
32. Major G. W. Morgan
33. A.D.(Moh)
34-36. Lt. Col Pritchard (3)
37. Dr. Pickering

INTERROGATIONS OF DR. HUETTENHAIN FORMERLY HEAD OF THE RESEARCH SECTION OF OKW/CHI

All meetings were held in The Signals School at Flensburg.

First Interrogation. 1430 hours, 18th June, 1945.

Present: Commander DUDLEY-SMITH, R.N.
Major SEAMAN, A.U.S.
Major MORGAN, I.C.
Lt. KIRBY, A.U.S.
Lt. Cdr. FORSTER, R.N.V.R.

Career before joining OKW Chi

1. Dr. HUETTENHAIN stated that he had specialised in Mathematics and Natural Sciences and was a Doctor in Astronomy. After four years at school, he had spent nine years in the Universities of Marburg, Frankfurt and Muenster - where he assisted in the observatory. He had there worked with Professor LUDENDORFF who was interested in reconstructing the Mayan chronological system on the basis of Astronomical scripts. The reading of Mayan scripts led him to cryptographic literature.

Joins OKW Chi 1937

2. In 1937 he invented a cipher system and sent it to the local military authorities, who forwarded it to OKW Chi - it was rejected as neither new nor up to modern requirements; but as a result contact was established and he finally joined OKW Chi himself, intending to return later to his scientific studies and to combine his experience in cryptography and philology in dealing with archaeological problems. The war however intervened.

3. For the first six months he was allocated to a training section. The Spanish War was going on and low grade Spanish Government military systems in use then were worked on as practice. He had no knowledge of any work done on Italian systems used in Spain at that time.

Organises the Research Section on a mathematical basis

4. After roughly a year's initial work he became an independent member of OKW Chi, specialising on the mathematical approach to cryptanalysis. He was the first mathematician to join them, and was instructed to expand the mathematical side as he thought fit. It was not clear who was responsible for the policy behind this decision but he thought that it was Ministerialrat FENNER. (Known to have been head of OKW Chi IV (decoding) in September 1944).

5. The following mathematicians were introduced to OKW Chi by HUETTENHAIN at this time:

Professor AUMANN
Professor WITT
~~Professor FRANZ~~
Professor WEBER
Dr. SCHULTZE
Dr. AIGNER (mediziner),

and he took on a number of statisticians of clerical grades.

INTERROGATIONS OF DR. HUETTENHAIN (Continued)

First Interrogation - (Continued)

Security of German Ciphers

6. The question of the security of German Ciphers came to the fore in 1939 - 1940 because of information from Polish and Czech sources that German systems were being read. Czech PW's stated that Hoftschluessel (a sort of RASTER - "step-stencil") was being read in Prague by means of the beginning BETRIEBSSPRUCH, and in October 1939 a Polish Officer named RUZEK further confirmed this and in addition mentioned the Enigma, although it was never clearly stated that this was actually read; the Poles stated that they had worked on the machine with the French and had the instructions for its use but the Germans were never able to discover even later on in Belgium or France any evidence of success with Enigma. Nothing was learned from the Belgians or French, and when the Germans entered the Deuxième Bureau, all the materials had been withdrawn to Vichy France. When that was occupied no search was ever made.

7. It was fully realised within OKW Chi that a more efficient system was needed for dealing with German Cipher Security but it took some time for the authorities concerned to act in this respect.

Ober-Inspektor MENZER

8. The old arrangement had left the sole responsibility in such matters to Oberinspektor MENZER. He was an old Reichswehr man who had joined OKW Chi in 1935; he was not highly educated but had been attracted to these problems; he devised new systems, and his systems were usually introduced. Only occasionally did he consult HUETTENHAIN informally on security problems, when questions of probability were involved.

1940 - 41 Special Cipher Security Section

9. They knew themselves that their systems needed improvement, and were working on them. In 1940 - 41 a Special Cipher Security Section was organised within OKW Chi which was later controlled by HUETTENHAIN himself. Its function was to test new Service systems and check on old ones; this was regarded by the Services as an infringement of their rights and strongly resented. There was no direct order from above that material necessary for making tests was to be supplied, so that requests, e.g. for specimen 'live' traffic were refused, and only comparatively recently did the Services resign themselves to control in this sphere.

Machine Section Established

10. By 1941 it had become clear that machines would be necessary for the dual - offensive and defensive - task of research, but engineers were not obtained until 1942, when the following were appointed: Two Dipl. Ings: ROTSCHEIDT (formerly with Siemens) and JENSEN (who came directly from school), both telecommunications experts. (These are now thought to be in the South); three working engineers, TODT, SCHAEFFER and KRACHEL (with a Technical High School training), who were decidedly subordinate to ROTSCHEIDT and JENSEN; and twenty five mechanics.

INTERROGATIONS OF DR. HUETTENHAIN - (Continued)

First Interrogation - (Continued)

11. They decided to use Hollerith wherever possible, but it was found that Hollerith machinery was not suitable for all problems, and auxiliary deciphering machines were developed as the occasion arose. Special problems were laid before the engineers, and they were told "This is what I want to do, how would you do it?". The machines which resulted were built in a more generalised way than the immediate problem demanded so that they could be of use again.

12. The following special machines were used:

(1) BIGRAM-SUCHGERAET. For dealing with Japanese Diplomatic two-letter code plus raster traffic ('J19' or Fuji). There were 100 groups in a message, and the machine would find a solution in less than two hours. High coincidence was recorded by long strokes on an undulator strip similar to a barograph. The machine was once used for work on an English Met. cipher - figure traffic employing a stencil, when HUETTENHAIN linked with the Wetterdienst der Luftwaffe. They were allowed to use the machine. He recalled that Chef Wetterdienst was Oberst Meteologer BENCKENDORF, and he thought that the chief cryptographer was Oberinspektor NAUMANN. Messages were observed about a year ago with the same first few groups of subtractor but not continuing on the same subtractor. The traffic was never solved.

(2) FASEN-SUCHGERAETE (PERIODEN). The problem was to determine the periods in short periodic substitution by finding the distances between repeats within a message. The first machine, 'SAEGEBOCK', was built as an experiment and was subsequently used to find n -gram repeats where n is less than or equal to 10. If there were no repeats, it could count monographic coincidences. It used two strips of teleprinter tape. It could also be used to find two Enigma messages in depth. The second, 'TURMUHR', was built primarily for work on the U.S. strip cipher, when cribbing which was generally employed was impossible. The strip system in question was a Bazeries type and each link using it had its own set of strips. There were 40 - 50 sets in use by the Army, Navy and Air Force.

The machine found message parts with the same generatrices by the following method - having established a depth by finding repeats, the letter frequencies for each column were weighted. The correct generatrix for additional message parts was then found by totalling these weights. The machine gave the result as a needle graph. It ticked after each set of calculations; hence the name Turmuhr. OKH also used the machine. It could not be used after the system was modified by the withdrawal of strips. HUETTENHAIN stated that they had had no success in reading the modified Strip Cipher.

(3) DIFFERENZEN-RECHEN-GERAET. This had the same function as the 2s. 6d. machine or the N.C.R.

(4) PARALLEL-STELLEN-GERAET. A repeat finder.

(5) ZAHLENWURM-REDUZIER-GERAET. "WITZKISTE". A Key-Solving machine.

INTERROGATIONS OF DR. HUETTENHAIN - (Continued)

First Interrogation - (continued).

13. All these machines were built in three parts, and were partly mechanical but largely electrical. First, the ABTASTGERAET, A five-unit reader which finally scanned up to 70 letters a second photoelectrically, (to begin with needles had been used). Second, the RECHENGERAET. Third, the REGISTRIERGERAET--a typewriter or undulator or photograph on a film.

14. All these machines were of the 'Entzifferung' (cryptanalytic) type. There were also 'Entschluesselung' (deciphering) machines, chiefly typewriters with substitution relays. There were many more ideas for such mechanical aids than there were actual machines constructed.

15. All of the machines developed by OKW Chi were shown to the three Services and the Foreign Office; some were constructed for the other Services, particularly the Differenzen-Rechen-Geraet.

16. Hollerith was the first recourse. It was used for such processes as

1. Differencing
2. Finding repeats
3. Compiling Difference Catalogues
4. For work on Stencils; it was especially used for the solution of the Polish Stencil Subtractor (4-figure) used between LONDON and WARSAW.

Offensive work on Cipher Systems

17. JAPAN. Asked about work done on Japanese systems, HUETTENHAIN explained that cryptanalytic work in OKW Chi was organised basically in sections according to the country concerned--and that as Head of Research he saw only systems with which the individual section had failed. In this connection he mentioned the lack of entire cooperation between the philologists and the research mathematicians. He mentioned two Japanese systems which had been passed to his section.

(1) FIFIF ('KOKOK') - a local transposition of code in 19's, the code being mixed 2- and 4-letter.

(2) (FUJI) (see page 2). The cage lasted for ten days and four keys were used a day. He thought that this system went out of force about eighteen months ago.

18. FRANCE. At the beginning of the war the principal cipher used by the Ministry of War for communicating with the Southern District, and later with all important Military Commands, was completely solved cryptanalytically without the help of captures. The system was a transposed 4-figure code, an alphabetic book as were all French military books. The key was derived from the clear equivalent of a given code group of another pagination and changed for each message. Later on two groups were used. It was solved because of French mistakes. There were many re-encipherments, in which only the internal addresses were different. Because of the code group key, bookbreaking and key breaking were mutually helpful. He did not know the indicator controls.

INTERROGATIONS OF DR. HUETTENHAIN - (Continued)

First Interrogation - (continued)

19. BELGIUM. A military 3-figure code was read; this was used with substitution tables, in such a way that the first figure of each group remained unchanged and the second and third were each reciphered individually, in substitution which could be varied with each message. They studied no Belgian attache systems.

20. RUMANIA. Work was done on transposed diplomatic codes.

21. GREAT BRITAIN. Several British systems were investigated without success. Figure traffic addressed 'PRODROME' was worked on but was not read, and it was thought that OTP's were used in certain cases; indicators were recognised.

22. Asked about India Office traffic, HUETTENHAIN stated that he himself had not heard of work done on it and he thought that it would not have been covered by Pers Z-S (the Foreign Office) nor the Forschungsamt. He thought that Dr. DENKER of the English Referat should be consulted. The other Departments had no cryptanalytic sections attached to them. He thought no English systems had been solved in the last two years, with the following exception.

Double Transposition

23. A Double Transposition system was recently investigated where the same key length was used on both cages. If the first cage was too deep the problem resolved itself into that of single transposition, and although the volume of traffic was small a certain percentage was read. He did not know what the contents were, or where the messages were from.

24. Asked whether he had worked out a general theory for the solution of Double Transposition he said that he himself had not, but that the problem had been suggested as a thesis for a Doctorate to a mathematician who had not yet finished his University course--given in the first place as a single message, in the second, several messages on the same key(s). The problem was interesting partly because the German police used this system. (Here he referred to work done by a psychologist at the University of Frankfurt am Main on the time taken in the solution of substitution systems. Theses on these subjects could be kept secret by arrangement with the University.)

25. HUETTENHAIN said that he had not consulted the section responsible for the deciphering of Agent's Traffics--WNV/Fu III--on this matter.

26. U.S.A.

HAGELIN. HUETTENHAIN stated that he was interested only in the general theory involved in breaking the Hagelin machine, and not in any particular type of traffic. In 1935 Mr. HAGELIN had offered the machine to the Reich Kriegs Ministerium but on investigation it was found to be soluble on a beginner and for this reason, and because Mr. Hagelin said it would be offered to other countries, it was rejected by Germany. This was a 5-wheel machine.

INTERROGATIONS OF DR. HUETTENHAIN - (Continued)

First Interrogation - (continued)

French C 36 type

27. HUETTENHAIN's own first practical acquaintance was with the French C 36 type--fixed lugs, with no overlap. This was found to be solvable on one message without the aid of stereotyped language simply by writing out the text on a width of 17 and solving on an operative or inoperative position of the wheels, either by eye where long messages were concerned or by X^2 test for short messages. Long messages, however, were usually available. A minimum of 200 letters sufficed.

B.211

28. HUTTENHAIN described the old and the modified B.211 machine and stated that the Army worked on the modified type. He knew that traffic was not read during the 1940 Campaign. The machine was only captured very late, with the modification in damaged state; and studies in connection with it were purely academic, although he had heard an Army officer state that the machine could be broken by dragging a crib of 8-10 letters. 'W' was the missing letter, but certain traffic had some Y's turned into W's.

Russian B.211

29. This was in principle the unmodified form of the French B.211, but employed a 5 x 6 alphabet. Any information given on this machine was based purely on hearsay. - HUETTENHAIN did not know where it was used or by what authorities - SCHUBERT was the person concerned. He believed the machine was built by the Russians, not by Hagelin. He thought it was no longer in use.

Swedish

30. On one occasion the Swedish Military Attache in Moscow transmitted a message of more than 5000 letters which was not solved.

U.S. M.209

31. This failure over the Swedish message led to a similar experiment with messages enciphered by themselves on the U.S. M.209 where success was achieved with 5000 letters of text but 2500 letters failed. This method was never successfully used on actual traffic. HUETTENHAIN stated that lines of attack on the M.209 exploited depth and staggers. Firstly depth would be identified from indicators or repeats or by making a count of the distribution of individual letter differences between two messages counted in each position ((Banburismus)), using the Fasensuchergeraet. Having thus recognized depth the next step was to solve it and obtain Key. 50 to 100 letters of key would suffice to give the machine set-up.

Finnish

32. As far as he knew, no Finnish Hagelin traffic was read but he had never actually worked on it himself.

German Schluessel Geraet 41

33. He considered that the fundamental weaknesses of the M.209 were

(i) The regular movement of its wheels.

(ii) That it was a letter subtractor.

These were substantially avoided in the Schluessel Geraet 41, since the regular movement of the wheels had been avoided and the key of the machine was not solvable. Further messages could not be set even if one depth was read, and its key recovered.

INTERROGATIONS OF DR. HUETTENHAIN (continued)

Second Interrogation. At 0930 hrs. Tuesday, 19th June.

Present: Cdr. DUDLEY-SMITH, R.N.
Major SEAMAN, AUS.
Major MORGAN, IC
Lt. KIRBY, AUS.
Lt. Cdr. FORSTER, R.N.V.R.

JAPANESE SYSTEMS

34. Dr. HUETTENHAIN was asked to give all details of Japanese Diplomatic, Military and Military Attache traffic which he had dealt with. He said that these had been either small codes or machines.

35. A great number of plain codes had been used with a vocabulary of sometimes only 240 groups, limited to consonant vowel or vowel consonant (there were 20 consonants, 6 vowels, since Y counted as a vowel). Later on switch groups were introduced - e.g. 'BY' ..... indicating a new page, thus giving 2-letter and 4-letter groups. At this stage vocabularies of 2000 to 3000 groups came into use. Some were reciphered:-

(1) (FUJI) Called 'J 13' or by a 'chemical' formula 'J 2 B 4 B C Ü R U W' (= "Japanese 2-letter 4-letter Code über Raster und Wuerfel")

(2) ('KOKOK'), called by its 'chemical' formula 'J 2 B 4 B C Ü U (19)', where U = Umstellung. The key remained unchanged for weeks at a time, and the code changed more often.

(3) CIFOL VEVAZ (Discriminants). This was possibly a commercial code reciphered by a Tauschtafel.

MACHINES.

36. "SCHIEBE" This had been used years ago for Diplomatic traffic and was read. Twenty letters were printed on one "Schiebe" and six on another - originally consonants were on one and vowels on the other so that when the codes were reciphered syllables remained. Traffic was no longer read after the machine changed but work was resumed on it about nine months ago under Baurat STEINBERG, a machine expert who was connected with work on Hagelin. The Japanese machine was his first assignment in O.K.W. His specialty was machines, and he had probably worked on Hagelin. As he had only recently joined OKW - previously he was with OKH, liaising with OKW, and is now probably in the South, HUETTENHAIN could give little recent information but he thought that the same arrangement of the alphabet remained in principle in the new 'Schiebe' - that is the arrangement of six letters on one and 20 on another slide, but the six were no longer necessarily vowels. You could pick out the sixes by their frequencies. Nothing was read but the work had reached a promising stage, aided by bad usage and he thought that traffic would have been read in a few months. He had never seen an actual machine but thought that it was represented by two strips sliding against a fixed back ground, moving one and occasionally two steps at a time. Although the actual machine probably employed wheels, the same effect could be achieved with strips.

37. Attache Systems. Neither Rikugun nor Kaigun traffic was ever solved although HUETTENHAIN investigated them two years ago. The Japanese bookbreaking section was new; it was started during the war.

INTERROGATIONS OF DR. HUETTENHAIN (continued)

Second Interrogation (continued)

38. In 1942 the Germans were passing details of certain book recoveries to the Japanese via Col. HAYASHI, the JMA in BUDAPEST; they asked for details of the cipher systems used for passing this information and stated that only a secure system should be used. The Japanese refused to disclose details of their system but stated that it was unbreakable; and in spite of potential cribs in the shape of the recoveries known to be passing on the Budapest link, the Germans were unable to break into the JMA system.

39. When pressed for details of the recoveries involved, HUETTENHAIN said that this exchange of material was handled by FENNER, and emphasised that he himself had no interest in the contents of messages or in the use made of them as intelligence. He never saw any recoveries passed back in exchange by the Japanese; in any case these would have gone straight to the individual section concerned.

40. These were the only Japanese systems referred to him but he pointed out that the Japanese language section worked on others of which he had no details. He knew that a Diplomatic subtractor system was read, but was sure that no Japanese Military traffic was solved.

41. Chinese. The Japanese section also dealt with certain Chinese systems which they read, and Manchurian; but these were never referred to the Research Section.

42. U.S.A. (See preliminary field interrogation, TICOM/I-2). Besides Hagelin, the following systems were read: Strip (AM 10), a system employing 20-letter substitution on a book known as AM 8., an unreciphered book of about 100,000 groups which had been in use since 1926 and the American Military Attache Emergency Double Transposition cipher. On reflection, he thought the latter might have been an English system.

FOREIGN LIAISON.

Finnish Liaison on Strip Cipher (AM 10)

43. Close liaison had existed with the Finns over the American Strip cipher although both countries had started their work independently. Finnish cryptographers came to Berlin, and their German opposite numbers visited Mannerheim's H.Q. An Oberlt. HENDRIKSON, a physicist at Helsinki University in civil life, was remembered as one of the principal Finnish cryptographers of good ability. Later the exchanges took place by courier. The Finns were primarily interested in Baltic traffic--e.g. that passing from Washington to Copenhagen or Stockholm; but in order to read traffic on these links it was found necessary to study all American Diplomatic traffic, because the same sets of strips were used on various links. No liaison on any other systems ever took place as OKW had nothing else to offer. In the case of Russian traffic OKH might have been able to offer Army material in exchange--he did not know.

44. Asked specifically about liaison with the Finns over Swedish ciphers, HUETTENHAIN stated that the Germans themselves read plain codes only and as these had been captured he thought that no liaison took place - Swedish Hagelin was never read. He knew that the Finns gave OKW no Russian or Swedish Diplomatic traffic. He did not know if any exchange took place on British systems; the Finns were known to be interested particularly in Russia, Poland, Roumania and Sweden.

INTERROGATIONS OF DR. HUETTENHAIN (continued)

Second Interrogation (continued)

45. The Finnish bureau was small but efficient - consisting of some twenty or thirty people - and at liaison meetings a woman was always in the chair. It was not clear to what part of the Finnish General Staff the bureau was subordinated.

46. JAPANESE. It was thought that the Japanese were not informed of German work on the Strip cipher but HUETTENHAIN knew nothing about liaison with the Japanese. He thought KETTLER was mistaken about the liaison, and restated his conviction that no U.S. strip material was given to them.

47. OKW WORK ON BRITISH SYSTEMS. Asked whether he knew of any work done on a British Military high grade subtractor HUETTENHAIN said that by the time he entered OKW the division between work done on diplomatic systems (OKW) and on military (OKH) was already complete and that he himself had therefore never dealt with British High Grade Military systems.

Internal Liaison

48. He pointed out that liaison with OKH was not such as the younger men would have wished, nor such as would be natural in scientific work. But the 'Higher-ups' had a private war on and liaison between specialists was discouraged.

49. OKH. He was asked to give any details he knew of OKH Chi (Formerly Inspectorate 7/VI). He said that the following members were known to him, all of whom were mathematicians as he had no acquaintance with philologists: STEINBERG, Dr. PIETSCH, (an actuary in civil life), Dr. DOEHRING, Dr. ZUGGISCH (who was concerned with speech encipherment and joined OKW at the same time as STEINBERG), and Obltn. SCHUBERT. These had all been transferred to OKW Chi recently from OKH after the 20th July incident, when many members of the OKH communications organisation, in particular General FELIGIEBEL and Colonel HASSEL, were implicated. OKH as a result was no longer allowed to be responsible for the security and development of any German cipher systems and a large share of their former responsibility was transferred to OKW Chi.

Hollerith used by OKH

50. He stated that OKH used Hollerith machinery but the other 'Hilfsgeraete' were not employed by OKH to the same extent as by OKW. When these machines were built, all agencies except the Forschungsamt were given a demonstration and offered the use of them. It was also offered that copies should be built for them. All accepted except O.K.H., which preferred to remain independent.

51. FORSCHUNGS AMT. Owing to personal friction, political considerations and other unsavoury matters there was no liaison with the Forschungs Amt and they were not offered the machinery developed by OKW. FENNER was particularly prejudiced against GOERING'S party - in any case the general impression was that they achieved very little - they employed no mathematicians!

52. AUSWAERTIGES AMT. Over certain problems OKW had worked with the Research cryptanalytic party of the Foreign Office. The two parties did not work on the same material, but divided the work. This was a considerable achievement. In the case of the American Strip, the Auswaertiges Amt worked on the circular, and OKW the point-to-point Strip traffic. On the question of mathematicians in the Auswaertiges Amt, he said that they employed several with very good academic qualifications: but in his opinion ORR KUNZE was the most able cryptanalyst

I-31 (Hüttenhain)
Continued
- p 10 TP 52 - & end on p 11)
of TP 53

p. 4 TP 13
done?

DR. HUETTENHAIN (continued)

rogation (continued)

CHAUFFLER's papers on cryptanalytic
n asked by SCHAUFFLER to contribute
ER of OKW Chi disapproved and advised
ld cease. It was considered inaccure
of treatises on such subjects.

nese machine the AA worked on even-
anging their results. As regards
ections concerned divided up the
lly exchanges of staff.

UFFLER a true scientist and a
great opinion of his papers. They
on the other hand they were un-
orians, while the historical informa-
em was public knowledge anyway.

55. TYPEX. Asked whether Typex machines had been captured he stated that he had seen one which was captured in Normandy without drums. A standing order was issued for drums but he thought that none were captured. No captures were made as far as he knew in N. Africa.

56. Asked what initial studies were made on Typex he replied with a fairly accurate description of the machine but was uncertain whether there were five or six wheels. No mention of a plugboard was made. The Commercial Enigma was breakable with known drums and a crib. Multiplying these difficulties by 676 made them too large to be worth considering while the crowning blow was wheel orders, 5 wheels from 10 or 20. The Indicator System was not studied by OKW at all; he knew nothing of OKH's work on Typex and as far as he knew no intelligence was available purely as a result of studying the Indicator System independently of the cipher.

57. British Inter-Departmental Cipher. Asked whether he knew anything of a long subtractor system with discriminants VCVCV or CVCVC, he said that the name was familiar to him in Berlin but he knew no details of work on the system - if it was a normal Indicator system from which depths could easily be found the Book building section concerned would have been able to deal with it without reference to him.

58. OTP. An OTP of 96 pages, 70 groups to a page, found near Berchtesgaden, was produced but HUETTENHAIN stated that he had never seen such a book. It might have been similar to German weather tables. Asked if he remembered any book of 96 pages, fourteen lines to a page and five groups to a line, he stated that the Italians had a 96-group subtractor. He then recognised that he had confused groups with pages. If there were 18 (or 20) lines to the page, it could be a British Mat. subtractor.

INTERROGATIONS OF DR. HUETTENHAIN (continued)

Second Interrogation (continued)

among them. He knew of SCHAUFFLER's papers on cryptanalytic method and had in fact been asked by SCHAUFFLER to contribute articles himself, but FENNER of OKW Chi disapproved and advised that such publications should cease. It was considered insecure to circulate 30 - 40 copies of treatises on such subjects.

53. In the case of the Japanese machine the AA worked on even days and OKW on the odd; exchanging their results. As regards book building, the language sections concerned divided up the codes and there were occasionally exchanges of staff.

54. HUETTENHAIN had found SCHAUFFLER a true scientist and a calm worker but did not have a great opinion of his papers. They were mathematically trivial, and on the other hand they were unintelligible to non-mathematicians, while the historical information contained in them was public knowledge anyway.

55. TYPEX. Asked whether Typex machines had been captured he stated that he had seen one which was captured in Normandy without drums. A standing order was issued for drums but he thought that none were captured. No captures were made as far as he knew in N. Africa.

56. Asked what initial studies were made on Typex he replied with a fairly accurate description of the machine but was uncertain whether there were five or six wheels. No mention of a plugboard was made. The Commercial Enigma was breakable with known drums and a crib. Multiplying these difficulties by 676 made them too large to be worth considering while the crowning blow was wheel orders, 5 wheels from 10 or 20. The Indicator System was not studied by OKW at all; he knew nothing of OKH's work on Typex and as far as he knew no intelligence was available purely as a result of studying the Indicator System independently of the cipher.

57. British Inter-Departmental Cipher. Asked whether he knew anything of a long subtractor system with discriminants VCVCV or CVCVC, he said that the name was familiar to him in Berlin but he knew no details of work on the system - if it was a normal Indicator system from which depths could easily be found the Book building section concerned would have been able to deal with it without reference to him.

58. OTP. An OTP of 96 pages, 70 groups to a page; found near Berchtesgaden, was produced but HUETTENHAIN stated that he had never seen such a book. It might have been similar to German weather tables. Asked if he remembered any book of 96 pages, fourteen lines to a page and five groups to a line, he stated that the Italians had a 96-group subtractor. He then recognised that he had confused groups with pages. If there were 18 (or 20) lines to the page, it could be a British Met. subtractor.

INTERROGATIONS OF DR. HUETTENHAIN (continued)

Second Interrogation (Continued)

59. Work on RUSSIAN Systems. A Tigerstedt Russian R/T scrambler system was investigated by Dr. BUGGISCH who worked largely at WAPRUEF/7 where oscillographs, spectographs, etc. were available - as OKW Chi did not possess the necessary technical equipment. Traffic was intercepted and was D/F'd as passing between MOSCOW - MADRID or LISBON. The number of segments in the time transposition was not established, but the number of reading heads was very low, about four. It was apparently a type of traffic with which the Russians were experimenting, from about a year ago until the end. Fragments of text had been recovered and linguists were of the opinion that they were Russian but the validity of the solution did not satisfy HUETTENHAIN's critical sense. There were possibly other features such as "wobbulation" - wobble-modulation. He said that a strip ('Lochstreife') might have controlled the order in which the transposition was carried out; a machine would show a period, and none was observed. They would be two-level 4-letter strips. It was an interesting problem, mathematically, to key only four heads in a random manner. He thought the cycle of the four heads was about half a second.

60. Captured American Mustang apparatus of this type had remained unrecognised as such on a German airfield where everyone played with it, for six months before it reached OKW Chi. There was no difficulty in principle in deciphering this traffic; but the key changed for each flight and he thought it unlikely that a result would be produced within the two hours of a flight; it was considered as a long-term project. The same key was repeated every one or two seconds. The receiving apparatus could be adjusted progressively until the contents were extracted by the selection of the human ear - this could be done without solving the traffic. He thought there were ten or twenty heads.

61. Russian Military Subtractor (5-figure). Originally depths of 40 - 50 were available, but later only depths of 4 - 5; traffic was still read while on the same book. Later on still there appeared to be no depth at all. He thought that it was only used for high-level staff traffic. SCHUBERT should be questioned.

62. Russian T/P Machine. A Russian T/P machine was investigated by Dr. DOEHRING while at OKH; he thought that they did not get as far as reading it, but the position was obscure. It was seen to be a subtractor, each impulse reciphered by a separate wheel with some periods identical with those in SZ 40, 42. Some of their own wheels could actually be used in the model of this Russian machine. He presumed that the wheels moved regularly otherwise the cipher would not have been broken. There was apparently no transposition. The Indicator system was not described to him but he knew there was one. (His knowledge of this machine was derived only from a casual conversation with DOEHRING).

63. The machine was little used and was probably in an experimental stage. There were only two or three lines running and there was no evidence of the transfer of any other traffic to this system.

INTERROGATIONS OF DR. HUETTENHAIN - (continued)

Third Interrogation. 1530 hours 20th June

Present: Major SEAMAN, U.S. Army
Major MORGAN, I.C.
Lt. KIRBY, U.S. Army
Lt. Cdr. L.W. FORSTER, R.N.V.R.

WAPRUEF/7

64. Dr. HUETTENHAIN was asked for the names of other members of WAPRUEF/7. He mentioned Dr. LIEBKNECHT. PECHTER was the Gruppe-Fuehrer of LIEBKNECHT's section, a regular officer, without special technical knowledge. Dr. LOTZE, to whom BUGGISCH was transferred, was concerned with speech decipherment, on which work was carried out at STAATS near STENDHAL, several kilometres from PLANKEN, in buildings erected on an artillery range belonging to WAPRUEF/7.

AG/WNV/ Fu III

65. Asked for more details of AG/WNV/Fu III other than those connected with Obltn. VAUCK, HUETTENHAIN said that Wachtmeister KOEHLER was VAUCK's Assistant. There were some twenty or twenty-five people engaged on cryptanalytic work connected with Agents ciphers' at WNV/Fu III, but this was only one of the functions of Fu III.

The SZ 42 C

66. The forthcoming SZ 42 C. The objection to SZ 40 and 42 was the regular movement of several wheels. These had been built by LORENZ at MULHAUSEN (Thuringia) to the design of Dr. LIEBKNECHT. The first 30 - 40 models of SZ 42 C were built in a house called the Ingenieur Haus, BERLIN - ZAHLENDORF and production was then handed over to LORENZ in BERLIN.

67. The 42 C was externally smaller than the 42. It had only ten wheels, and Transmission and Reception were combined in one unit. The five wheels on the left were coupled - if all ten wheels had independent movement the least period of the machine was not calculable. Hence the five wheels were made all to move or all to stay still. Asked about the other five wheels he said that they had irregular movement; the wheels being numbered 1 to 10 from left to right, 5 drove 6, 6 drove 7, 7 drove 8, 8 drove 9, 9 drove 10, and 10 drove 1 to 5. There was also a device set to give the left-hand wheels a move when the machine had been in 2, 3 or 4 dead positions. The manufacturers had attempted to build the machine with wheels 6 to 10 also having common movement. This matter was still in dispute when the war ended. There was a quartz-clock synchronisation, so that two machines could run in step for twenty-four hours, only one setting being needed for the twenty-four hours. This latter was a device of VIERLING's. It was 2' x 1' x 1' and opened up like a drawer. VIERLING had previously worked on electro-acoustics at the Technical College in HANOVER and was the designer of an electric organ.

VIERLING

Work on GERMAN Systems

68. Security of German Ciphers. In working on German systems, HUETTENHAIN said that the following were assumed on the enemy's behalf:--

(1) That he had the machine (or knew the system).
(2) That he had the Instructions for use.
(3) That he had intercepted all traffic.

INTERROGATIONS OF DR. HUETTENHAIN (continued)

Third Interrogation (continued)

(4) That he had a sufficient and competent staff.

(5) That he had such machinery and other resources, including finances, as might be necessary for the solution of the system in question.

It was also assumed that the enemy would possess cipher and clear texts of the same message, re-encipherments, stereotyped beginnings and endings, repetitions within messages (limited vocabulary and numbers).

System tested, given clear and cipher

69. Given these, it was first asked, is it possible to reconstruct this system from clear and cipher? If the answer was 'no', then the system was pretty good, as this was the severest test which could be applied. Only the S.G.41 and the SZ 42 C had so far satisfied this condition. Investigations on the 52 D and E had not been completed. With these exceptions, such an assumption led in all other cases to the breaking of the system and the reading of all other messages on the same key. (In the case of the Swiss Enigma machine the wiring changed every three months, but the wheel changes at WASHINGTON were not made at the same time as those in LONDON and cribs were provided into the LONDON traffic so that it was possible to solve the LONDON wirings).

Insecurity of Swiss ENIGMA

Test of Security of Individual Messages

Secondly, is a single message solvable without a crib? This was usually true of laymen's ciphers. The section was frequently asked to criticise submitted systems, being given only one or two texts and no cribs.

Thirdly, the solution of sets of messages known to be on the same key was investigated.

Fourthly, the length of keys, the number of alphabets and the number of settings on a machine were considered. As a rule of thumb, the length of key and the number of settings were required to be of the same order of magnitude.

70. When work was started in 1941 no German systems were found to be satisfactory.

Security of T 52 A - D

71. T 52. A - D. In 1939 he had been shown the T 52 A/B, and was asked his opinion of its security - it was thought to be secure but he found that it could be solved on a hundred letters without a crib. This accounted for the successive changes to C, D and E. The machines were built by SIEMENS. OKW/Chi demanded a new T/P alphabet, a dissimilar drive, and variable patterns. SIEMENS said that these were impossible and refused to consider them. The 52 C model therefore satisfied none of the conditions required and was still solvable, although the wiring was more complicated. It could be broken on a crib of ten letters, set by a parity criterion, and was solved in three months.

72. T 52 D was not subject to the parity weakness and had irregular movement - with the D and E machines they finally set about using a dissimilar drive in the wheels. All these machines were limited to producing about 1000 alphabets which are known. ((Note by interrogators. In fact, with the A/D and D with 20 plugs many sets of 1000 alphabets can be produced.)) It was found possible to read a depth of 10 messages on the same setting without knowledge of the probable contents. They did not succeed with a depth of 5, and possibly 7 was the critical value. But if

Third Interrogation (continued)

the alphabet had been unknown and there had been more of them, then a depth of up to 30 would have been necessary.

73 He was informed that Dr. FRICKE (q.v.) had mentioned a method of reading a long message (at least 20,000 letters) on T 52 D and E; Dr. HUETTENHAIN said that he knew of no such method. He thought FRICKE had in mind the instructions for use of the SZ 40 and 42 which forbade messages over 20,000 letters in length. T 52 A/B and C went out of use. D and E they were happy about. SZ 40, 42 were due to go out of use.

T 43

42 C was considered satisfactory. There remained the T 43 which employed a One Time tape, and was secure provided that the tape was properly made. Here an attempt was made to satisfy the conditions of von MISES' 'KOLLECTIV'. In fact the key tape was produced by running a 50 metre loop of pseudo-plain language through a T 52 D.

ENIGMA

74. He considered that the Service Enigma was secure if the instructions were observed. The modified E, the Schluessel Geraet 39, of which one model only had been built by Telephonbau und Normalzeit, at FRANKFURT, was then described. LIEBKNECHT had this model at PLANKEN. It had four wheels and Umkehrwalze, each of the 3 right hand wheels causing the movement of the one to its left. In addition there were wheels of Hagelin type, periods 25, 26, 27 he thought, giving additional movement to the 3 right hand wheels. The machine was steckered and printed both texts.

75. While this machine was being developed and as a guard against future possibility and not against what they suspected at present, the Enigma Uhr and Lückenfülle Walzen were devised. The G.A.F. had introduced the pluggable UKW but the Army said it was too much trouble. With SG 39, as with all other Enigma type machines, a depth of 30 messages on the same setting could be solved element by element.

76. Asked what machine was used by the German Military Attaches he said that there were no other machines than those he had described but he did not know whether the GMA used a machine - he thought there was no machine in use by Germany which he did not know.

Amswaertiges Amt.

77. Relations with Auswaertiges Amt. HUETTENHAIN said that fierce resistance was met with from other departments at any attempt to control the security of all ciphers used. OKW/Chi was never allowed to know details of the ciphers used by the German Foreign Office. He knew that One Time Pads were used and he had once met SCHAUFFLER and HAUTHAL of the Auswaertiges Amt. Even towards the end when there was a further attempt to centralise security under OKW/Chi, the Foreign Office would not come into line. SELCHOW, the senior official was strongly opposed and preferred to remain independent.

RSHA

78. Reich Sicherheits Haupt Amt. Asked about the systems used by the RSHA, HUETTENHAIN said that their security was not under his control; HIMMLER's organisation had tried to absorb OKW/Chi after the 20th July incident - but he had only heard this second-hand from FENNER who was not at the relevant meetings. There were three other forces in the field besides OKW/Chi, RIBBENTROP's Auswaertiges Amt party, GOERING's Forschungs Amt, and HIMMLER's RSHA. RSHA Cipher Systems were probably much the same as those used by the Army: RASTER and ENIGMA.

~~TOP SECRET "U"~~

INTERROGATIONS OF DR. HUETTENHAIN (continued)

Third Interrogation (continued)

Oberinspektor MENZER

79. Oberinspektor MENZER. Asked further about MENZER whose activities he had mentioned during the first interrogation, HUETTENHAIN pointed out that MENZER had been with OKW/Chi two years (1935) before he himself joined. MENZER had had successes in cryptanalytic work and had helped devise the Hilfsgeraete used. He did no breaking for RSHA, but devised new cipher systems for them, doing on the civil side what FRICKE did on the Service. No compulsion was put on anyone to apply to OKW/Chi for security tests except where the Army was concerned (to FRICKE), and many organisations never thought of doing so. (The Luftwaffe and OKM had referred to FRICKE). To begin with MENZER had designed and tested systems but he was relieved of this with their growing complexity and technicality, and rather given a free commission. The motor drive of the SG 41 was his idea. Dr. FRICKE could give more information about his work.

SG 41

80. SG 41 (modified Hagelin). He said that traffic on this machine could be read on a depth of two but the machine could not be reconstructed and so further messages could not be read.

The weaknesses of SZ 40 and 42

81. SZ 40. He described this machine briefly but not in correct detail. The first weakness in the SZ 40 was the comparatively short combined period of the two driving wheels, 2257 (61 x 37). By writing a cipher text on this width and finding consecutive columns corresponding to the inactive position of the driving wheels, deductions could be made which lead to the complete reconstruction of the driving wheels. This was a lesser weakness and could be corrected. The second weakness was shown by writing a single impulse of the cipher on the period of the relevant regular right hand wheel. By employing the first or higher differences of these columns of cipher one could exploit the non-random character of the series produced by the left hand wheels to derive the patterns of the right hand wheels. This he had actually carried out in practice before satisfactory rules were laid down for making wheel patterns.

82. Even with these rules the machine was not entirely secure in theory, from an attack exploited the regular movement of five of the wheels. The solution was to make the wheels move independently and irregularly. He thought that within the next twenty-five years all countries would realise this and adopt some form of machine with irregular movement. And that would be the end of cryptography. He thought that mathematics was not yet sufficiently advanced to deal with the problem of 'cycles' in irregular motion. Much research is still to be done, but it is difficult to get this work done because of questions of security.

83. SZ 42. Here the movement of the left hand wheels depended on one of the regular wheels as well as the driving wheels, giving a period of movement now 61 x 37 x 43. The second weakness was not noticed in time and so persisted. When it was noticed it was guarded against by giving detailed instructions (about 1½ inches thick!) to the printers - who were given tables of pattern distribution for the left hand wheels which were dependent both on the number of pegs in the driving wheel and on the number of clusters on the left hand wheels in relation to the driving wheel. Ideally, these conditions should be satisfied by all differences of the wheel patterns. Again, FRICKE could give more details. This trouble arose because the machine was designed without an examination by cryptanalysts.

INTERROGATIONS OF DR. HUETTENHAIN (continued)

Third Interrogation (continued)

84. In 1937 MENZER and HUETTENHAIN went to PLANKEN where they met Dr. LIEBKNECHT. They discovered that a message on the old SZ 40 could be solved within two days, and from that time an association sprang up, first between LIEBKNECHT and MENZER, then between LIEBKNECHT and HUETTENHAIN himself over this work. The SZ 40 and 42 were developed by MENZER and LIEBKNECHT, with HUETTENHAIN in association. The idea for the 42C came from Dr. STEIN who was responsible under HUETTENHAIN for testing German cipher systems.

85. FRICKE's statement about the solution of the SZ 40 on 1000 letters of cipher, by exploiting the non-randomicity of series, was confirmed. They tried it out experimentally. The machine had been under way two years before the "rules for construction" came into force. These instructions took care of the series and, up to the third, differences. If they had considered the fourth difference no one could have been found able to prepare the keys. These rules were so complicated that they decided to build the 42C in order to dispense with them.

Hand Verfahren

86. GERMAN HAND CIPHERS. Asked about German hand systems he said that the following devices were used by the German Army after the last war.

(1) A simple substitution using a key word in a 5 x 5 square, where each letter was replaced by the one above it. The Army was not easily persuaded that this could be solved.

(2) A comb - Transposition (Kamm-Wuerfel)

(3) Double Transposition (Doppel Wuerfel). About 1926 - 7, Enigma was introduced as an Army cipher, then there was no change until

(4) In 1935 MENZER introduced the Heftschluessel, modified later to be with Staircase.

(5) Kaste" - Schluessel:- Playfair.

(6) Doppel - Kaste" - Schluessel:- Double Playfair. Both 5 and 6 were solvable with or without cribs; and at this stage it was clear that there was no system both secure and suitable for forward troops. They aimed to make a pocket machine still smaller than the C 36 Hagelin, but when it came

(7) The SG 41; - it was larger.

(8) MENZER's other devices as described by FRICKE were being investigated; no serious weaknesses had been found. The period was long and they might have been suitable for the Army. After the first pull on the box slide a button was released, whereas on the Schluesselscheibe the discs had to be twisted to the next position. Probably MENZER had some of them at HALLE.

(9) RASTER SCHLUESSEL. The security of this system was higher than that of the Playfair but the Army in the Field found the system and the encipherment of the Indicator most tiresome.

Luftwaffe

87. SYSTEMS USED BY THE LUFTWAFFE. In general the Luftwaffe employed the same systems as the Army together with various small systems, such as Air-Ground, which were never submitted for examination.

Third Interrogation (continued)

OKM

88. OKM. The same was true of the Navy. They used in addition, transposition and substitution systems, and a special model of the Enigma machine having four instead of three wheels.

Speech Scrambling

89. SPEECH ENCIPHERMENT. All the devices in use were invertors, giving security against maintenance parties only. Many firms worked on machines under development which were based on the principles of the TIGERSTEDT apparatus or employed wobbulation, noise admixture, a subdivision of the frequency band, and combinations thereof but either fidelity was too poor or the machine was insecure and it was not considered worth producing. They preferred to wait for the perfect machine which was to have been VIERLING's apparatus. The 'BAUSTEIN', built to replace the invertor, had the advantage that whereas the radio could pick up invertor transmission, only a BAUSTEIN apparatus could intercept BAUSTEIN transmission.

INTERROGATIONS OF DR. HUETTENHAIN (continued)

Fourth Interrogation, 1030 hours 21st June

Present: Major SEAMAN U.S. Army
Lt. NUELSON, U.S.N.R.,
Lt. KIRBY, U.S.N.R.,
(Later): Major MORGAN, I.C.

Speech Encipherment

90. Dr. HUETTENHAIN continued to describe German Speech Enciphering devices. He said that two years ago it was decided to build only two machines - an Erschwerungsgeraet (which gives internal security only); this was the BAUSTEIN, and secondly a machine for absolute secrecy - the "Keunstlichesprache". All other orders were cancelled. Both these machines were devised by VIERLING.

BAUSTEIN

91. The Baustein employed no key; it was like an invertor and required no settings at either end. Speech was divided he thought into two or three bands onto which noise was superimposed. The noise was created by a tube and was sent both through the apparatus and separately. The latter transmission was used for deciphering. There were other methods of producing noise, one or two of which were ready.

KUENSTLICHE-SPRACHE

92. He said, that no machines of the 'Kuenstlichesprache' type were completed. In this apparatus speech was divided into ten bands and each channel was separately modulated ("gewobbelt"); the 'wobbelung' was determined by an SZ 42 C machine with ten wheels, one for each channel. In deciphering, the 'wobble' was removed and the ten bands reassembled. This device was considered absolutely secure because of the security of the 42 C.

93. Asked how the 'wobble' was determined, he said that the pattern of the wheels represented an irregular curve, and this determined the curve of the wobble. Physically the pattern was sensed by a lever, this could be done electrically - the wobble curve was simply added to the voice frequency. There was a rotating invertor such that if the curve of a particular band exceeded the band maximum as a result of this addition, the band range would be subtracted from it so that it came in at both ends of the band again. The German translation of the English term for this method was "Kennwortsprache" - referring to the examination of each band to see whether it had any "value". The method was developed by a Swiss, GUANELLA, at the BROWN BOVARI Co. in Baden, Switzerland.

94. HUETTENHAIN suggested that Dr. LIEBKNECHT would be the only person who could give more details of this development. Only the flat work (wiring) was complete. The 42 C was developed simultaneously with its new methods of synchronisation.

Work on Non-morse traffic

95. Work on U.S. non-morse traffic. He said that no work had been done at OKW/Chi on U.S. non - morse traffic. HWA had a group working on the interception of special transmissions, including Multiplex, Duplex, Baudot and 'VERDUN' and the intercepts were passed to OKW/Chi in ordinary letter or digit form. OKW/Chi itself was not concerned with intercept problems.

Fourth Interrogation (continued)

32 Element Ciphers

96. Work on 32 element ciphers. Asked about work on 32 element ciphers, HUETTENHAIN said that he had never seen any other than their own. WAPRUEF/7 had issued a report on complicated transmissions about a year ago.

Shiftwork

97. He said that only the language sections worked shifts. His own section did not do so regularly, but only if there was an urgent job in hand.

POW Messages

98. He was asked about Prisoner of War codes and said that the censorship office had passed suspicious letters to OKW/Chi but that usually nothing was discovered.

OKW/Chi

99. OKW/Chi organisation. He said that KETTLER would be able to give more information on the organisation of OKW/Chi. In HUETTENHAIN's own Gruppe IV there were about ninety people, eleven in Referat A, twenty eight in Referat B, forty eight in C, none permanently in D as that was a training department. Gruppe V (languages) had at first twenty two Referate, later seventeen totalling about two hundred and twenty people.

Training

100. He said that his training Referat (D) conducted training courses for both groups IV and V. The basic course lasted two years and met two afternoons a week for anyone at all promising. An Advanced Course ran continuously for linguists if they had mathematical ability and such were expected to break some systems independently in the language sections. There were actually only about six at a time on this course. HUETTENHAIN's own group had no advanced course, as such training was not necessary in their case - they were all accomplished mathematicians and in any case informal discussions and consultations were held daily.

101. In Groups II and III there were probably two hundred people and in FRICKE's section about ten. It was difficult for HUETTENHAIN to estimate the size of other Groups than these because they were in different buildings.

POLISH SS cipher

102. HUETTENHAIN said that the Polish Stencil Subtractor cipher passed through two stages. First, a four digit, 10,000 group code was used, with a plain additive table 24 x 26, five digits to the column with spaces between the groups. The lines and columns were numbered with bigrams at random in all four margins. There were many such Tables. An Indicator was placed fore and aft and gave a Table and marginal bigram en clair. The additive could then be read off in any of the four directions. A new Indicator was used after a row or column of additive had been used.

103. The second system was introduced two or two and a half years ago. Here there was no spacing of the additive groups. There were eighty rows and a hundred figures to each row. The marginal figures appeared now only at the top and left of the Table. The unit figures ran in normal order but the tens were random. Each digit now had a column and row Indicator. The additive was read off through stencils with various numbers of windows, all 4-figure. There were from twenty eight to forty windows. The placement of the stencil was indicated by the co-ordinates of the upper left and lower right corners. Two or three additive tables were introduced each month and several were used simultaneously although there were different sets for each link. For IN traffic, passing in an opposite direction (e.g. London to Warsaw), the stencil was turned over. Later, the windows were designed so as to be read in an abnormal

Fourth Interrogation (continued)

manner (vertical, snaking, in the shape of digits, etc.) but there was only one way to begin - you always started at the upper left corner.

104. HUETTENHAIN had planned to study the problem of solving a stencil additive with variable window lengths but the occasion had never arisen. He thought that the code only changed once, the stencil changed more frequently and the tables most often. If the book, stencil and Table had changed at once then they could not have broken in again. As it was, they read most of the Polish Stencil to the end. Hollerith was used to find repetition between the message parts. The index of repeats gave the Indicator message and part. Indicators were always in clear although the units figures were later randomised. Hollerith was first used for sorting because it was fast. The 'WITZKISTE' was also used for recovering additive.

'WITZKISTE'

105. He said that he would describe the 'WITZKISTE' as far as he could (but the interrogators do not profess to have understood the explanation fully). A dark glass plate 40 cm x 40 cm was used on which the common 4-figure Code Groups were reproduced by means of light 'spots'. The pattern was repeated in each of the four quadrants and the plate was slid by hand under a frame 20 cm square a quarter the size of the plate. The plate was covered with blind strips to prevent carrying addition. The holes in the plate were 1/3 mm in diameter and there were two secondary holes for each code group, one ten places up and the other ten places over. Thus 2384 would be recorded also by 3384 and 2394. The plate was slid to a position corresponding to the cipher group, according to a scale along the edge of the frame. The frame had a solid lattice, such that for any relative disposition of the plate and frame only one light spot showed through for each code group. The lattice was made up of alternate black and white bands 2 cm wide so that 100 hole positions were exposed in each opening. After repeated exposures corresponding to the various cipher groups in the column one black dot would stand out as the correct additive. There was an idea that the plate should be moved by pushing buttons but this was not done. Recently it had been planned that it should be adapted to stripping 5-digit code where there was the possibility of dividing code groups into overlapping sets of fours. A more detailed account of this machine is being prepared.