Doc ID: 6587345 Other Ref ID: A2972105

A-15
Annex D
Copy 4

~~TOP SECRET~~

TICOM/I-181

HOMEWORK BY DR. WERNER WEBER OF OKW/CHI

Attached is a complete translation of a report written at our request by Dr. WERNER WEBER, of OKW/Chi. The report is in three parts:

1) Movements of OKW/Chi after leaving HALLE on 10th April, 1945.

2) Report on U.S. Diplomatic Traffic worked on by Dr. WEBER during 1941.

3) Report on Japanese Diplomatic Traffic worked on by Dr. WEBER between 1941 and 1943.

This homework was written during October, 1945, and was received from Director S.I.D., U.S.F.E.T.

Trans. KCK, WRL, and JME.

TICOM

5th January, 1946 No. of Pages: 36

Distribution

British

D.D.3
H.C.G.
~~D.D. (N.S.)~~
D.D. (M.W.)
D.D. (A.S.)
C.C.R.
Cdr. Tandy
Major Morgan.

U.S.

Op-20-G (4) (Via Lt. Cdr. Manson)
G-2 (via Lt. Col. Hilles)
A.S.A. (4) (via Capt. Collins)
Director, S.I.D. USFET
Col. Kunkel, USAAFE.

TICOM

S.A.C. (3)
Cdr. Bacon
Lt. Cdr. Manson
Major Cowan
Capt Collins
Ticom Files (4)

Extra

Capt. Thornett, Berkeley Street.

Do NOT Destroy Return to the NSA Technical Library when no longer needed
Copy No. 2

Approved for Release by NSA on 07-25-2017, FOIA Case # (66109)

Doc ID: 6587345 Doc Ref ID: A2972105

The Further Fate of the Elements of OKW Stationed at Halle

Since the beginning of March 1945, a considerable section of OKW, including service personnel and male and female civilians, were accommodated at the Army Signals School HALLE. Most of them belonged to the cipher department (Chi); but other departments were represented, including the Fu. Department. Hauptmann GROTZ was in charge of organisation , but the cipher department, for example, remained subordinated to its former head, Oberst KETTLER, who was not at HALLE. When the Western front came nearer, it was decided to transfer the whole organisation to PRIEN on the CHIEMSEE (Upper BAVARIA). An advance detachment went there at the beginning of April and was still able to use the shorter railway route to the South. The remainder was to follow in two separate transports. The ladies were however given the choice of not undertaking the arduous journey (in goods trucks) and of leaving OKW, especially as the accommodation at PRIEN was said to be very primitive (barns as sleeping quarters). A number of ladies made use of this offer and went home, while others declared themselves willing to make the journey.

In order not to overload the train, all out-of-date papers were burnt. AMMENDORF station, south of HALLE, was chosen as the point of departure of the first transport in which I was, as the goods station at HALLE had been badly damaged in air attacks. After haversack rations for 5 days had been issued we were able to leave HALLE on the 10th April. There was M/T to AMMENDORF, but only for official luggage,some of the private luggage, the ladies and the infirm. The rest had to walk. In consequence of air-raid damage the tram only went as far as the market-place, and then again from the entrance to AMMENDORF as far as the station.

I do not know whether the second train ever left HALLE. I only know that a few stragglers left behind from the first train came along in time to overtake it en route (some by FALKENBERG). They related that in the meantime the precincts of the Army Signals School, which had so far remained undamaged, had been hit by bombs and a hut previously belonging to OKW had been burnt down. Neither did I hear anything more ot the members of the second transport later on (e.g. at WERFEN).

Command of the first train was taken over by Hauptmann HEIN (later promoted to Major at WERFEN), who had had command in HALLE of the "EINSATZKOMPANIE CHI" belonging to OKW . The route proposed was the south-bound railway line via MERSEBURG. But there were so many technical difficulties (too much traffic on the track? shortage of train crews?) that the departure was delayed by another two days. During this period we slept in goods trucks, which had been fitted out quite comfortably. We still had plenty of time to do our shopping at AMMENDORF. Some of us took refuge in the public air-raid shelters during the numerous air-raid alarms; many however remained in the trucks. Just before we left, the neighbouring labour service camp was broken up and distributed its stocks among the population. The members of the transport, although officially only the service personnel, therefore received a number of items of clothing and linen from these stocks.

Doc ID: 6587345 Doc Ref ID: A2972105

Then in the afternoon of 12th April the transport moved off in two separate goods trains. But in the meantime the front had come so near that it appeared doubtful we should still be able to reach our destination via MERSEBURG. Consequently it was decided to make a wide detour to the east and we went via the goods station at HALLE now open again, and then via EILENBURG - TORGAU to FALKENBERG, where the trains arrived during the night 12 - 13 April. Although it was night-time, a hot meal was issued. At no time on the journey did the rumour - which we first heard in HALLE - that we should only travel by night owing to low-flying attacks, prove to be true.

On the morning of 13 April, when the trains were still at FALKENBERG, Hauptmann HEIN surprised the transport with the announcement that the Russians were attacking 25 km away. I don't believe this was true. The Hauptmann then explained that because of this we should have to proceed during the next few hours along the south-bound stretch of line, which crosses the East-West line at FALKENBERG. But there was only one locomotive available, so we should have to join up the two trains, it would be necessary to leave a few trucks behind so as not to make the train too long. He went on to say that all male members of the transport would have to help reload the official luggage in these trucks into the other trucks. This was immediately done, but still the train did not get away until about 1800 hours. As a result of a low-flying attack, in which the train Flak and the heavy Flak position near the station both went into action, the departure was then made very suddenly, but there were no casualties. As the journey progressed, the train was split up again into two parts, at least for a time, as a second locomotive became available; but it usually proceeded as one unit of 122 axles (61 trucks). In consequence of the reduced number of trucks, the goods trucks containing the official luggage were grossly overloaded, the springs being bent quite flat.

We went through DRESDEN in the early hours of the morning on 14 April, and PIRNA during the morning. We entered the Reichsgau SUDETENLAND about 1300 hours. There was a short stop at TETSCHEN - BODENBACH owing to an air-raid warning. AUSSIG was reached in the afternoon. Several members of the party had a look at the town, as the line was not clear for the train to proceed yet and it would therefore stop for several hours.

The journey now continued under phantastic difficulties. As a rule all the tracks were blocked and there were often several trains in front of the OKW train waiting to go on. General surprise was caused by the fact that the OKW train did not receive preference. The stops at some places became so long that many members of the party made long excursions into the towns and villages, sometimes to buy or exchange goods. If they were taken by surprise by a sudden departure signal, it often happened that some of them missed the train. Then they always followed on by passenger train and still had plenty of opportunity of catching up with the transport. To make things easier a notice board was introduced and hung up on the outside of the command truck, giving the earliest possible time that the train could proceed.

Doc ID: 6587345 Doc Ref ID: A2972105

Stops of several hours were quite normal. There was quite a number of low-flying attacks, but not too frequently, occasionally we sought protection under the trucks. But no bombs were dropped near the train.

An extremely colourful individual existence developed in the separate trucks. In this connection it should be noted that this was not an exclusively OKW transport; for at an early stage a number of Flak units had been taken on to the train, and in addition some of the members of the transport had brought their wives with them. In fact even civilians who were perfect strangers, and children, are said to have been picked up en route. And rations, too, were given out to all these guests as a rule in just the same way as to the members of the transport themselves. When the first haversack ration had been exhausted, it had to be replenished at the various stations. And this was always managed in good time. After FALKENBERG we only had a hot meal once, in PRAGUE; but a lot of cooking was done in the trucks, as we had stoves too. The washing arrangements at the stations were in great demand. With effect from 14 April, the whole OKW transport was subordinated to GENERAL OF SIGINT SOUTH, BÖTZEL and from then on formed a part of OKH.

The train left AUSSIG late in the afternoon of 14 April. We did not travel far in the night; DUCHKOW was passed on the morning of 15 April, and the train reached the frontier via ZATEC and PODBORANY, in a relatively short time. Disturbing rumours were current about the attitude of the Czechs: there was said to be considerable danger from guerillas in the Protectorate, a danger which of course did not exist in the SUDETENGAU, which is only inhabited by Germans. There were however no clashes at all with the Czech population at any time on the journey through the Protectorate.

The Protectorate frontier was then crossed in the direction of PILSEN, soon afterwards, however, the train was held up for a whole night and proceeded a few kilometres the next morning, as far as MLADOLICE. There it was announced that the railway station at PILSEN had been almost totally destroyed the night before in an air attack and that there was no possibility of proceeding further for 3 or 4 days. We were told that in consequence of low-flying attacks, which were very frequent in this neighbourhood, we would have to set up communal quarters for ourselves outside the station. We took them over and put in straw, however, many members of the transport continued to sleep in the train, although some slept out in the open among the near-by haystacks. All sorts of successful barter was carried on with the Czech peasants in the village.

After a few days the station at PILSEN was still not open. Those in charge of the transport therefore decided to turn back and to proceed via PRAGUE. So the train went north again into the Reichsgau SUDETENLAND. What had happened before on the sharp left-hand curve just before reaching the Protectorate, and had been treated as a joke, now became serious after a few kilometres: on a sharp gradient, the (one!) locomotive proved inadequate for the over-long train and the latter had to be pushed by the male members of the party.

Doc ID: 6587345 Doc Ref ID: A2972105

The day brought several more long delays, it was not until the following morning that the train was able to turn off north of PODBORANY from the north-south line to the east and then enter the Protectorate for the second time, just before LOUNY. From there we made quick progress to PRAGUE - KOHLFELDEN, where we arrived early in the evening. We stayed a few days and nights in PRAGUE owing, it was stated, to lines being cut. Although the centre of the town was a long way off, we had in these circumstances time enough by day to have a thoroughly good look at the town.

It was early morning when the train moved off and proceeded via PRAGUE main station. We went via TABOR and C. BUDEJOVICE to the southern boundary of the Protectorate, and the only long stop during the day made on this line was at SUDOMERICE - NEMYSL. Just after leaving BUDEJOVICE we entered the Reichsgau UPPER DANUBE. We got near to the DANUBE the next day, and crossed the river in the night near STEYR, by-passing LINZ. We made another fairly long stay at PREGARTEN. The train then went along the ENNS through the LOWER DANUBE area into STYRIA and then turned West, along the upper course of the ENNS, through the GESAUSE. Late in the afternoon of 27 April we reached the Reichsgau SALZBURG. The transport reached the little station of WERFEN during the course of the evening - via BISCHOFSHEFEN station, which is said to have been badly damaged - and stopped there.

The next morning (28 April) Hauptmann HEIN (i/c Transport) announced that everyone was to prepare to resume his official duties in WERFEN, and not in PRIEN after all: this was because a bridge had been destroyed on the line to the north via SALZBURG. In the event of an air raid warning, the train would go into a tunnel. (There were incidentally no further air attacks on WERFEN). As far as possible we were to procure serviceable quarters for work and accommodation away from the train. The transport was now subordinated to the neighbouring Army or Army Corps H.Q. at SALZBURG. General BCRK was in command here, or assumed command at that time: he also had addressed an appeal to soldiers and civilians at the beginning of May and also took over the large reception depot which grew up here as "Corps Group BORK". Hauptmann HEIN, who had just been promoted to Major, then was soon made Town Major of WERFEN. Oberstleutnant KAEHLER took over the section of Chi department which was here but we did not get as far as starting work.

About May 1st what had been the advance detachment also arrived at WERFEN, from PRIEN, having now left there again and come to WERFEN along the Tirol line. It is possible that our own transport also arrived at WERFEN in two separate parts, thus having covered the last part of the route divided again, and that stragglers were still coming in.

In the first days of May several members of the transport went into private quarters, some in the village, some in near-by alpine huts. In view of the military situation, preparations were made for burning papers, and to some extent carried out. One night about midnight we heard the bells ringing in the village.

Doc ID: 6587345 Doc Ref ID: A2972105

As this was alleged to be the agreed signal for "enemy alarm", orders were immediately issued to destroy all material at once. This order was however immediately rescinded. In fact no enemy troops were seen. Not until about May 6th, when Americans were in the immediate vicinity, were all documents burnt.

The entry of the Americans (about May 8th) was preceded by the very widely spread rumour that the Chi Department would now take service with the Americans, presumably against the Soviet Union. The statement of Grossadmiral DÖNITZ that the fight against Bolshevism would be continued was probably partly the cause of this, but the rumour became pointless after the capitulation.

On the order of the American occupation authorites private billets were immediately vacated, communal quarters were set up which each had to accommodate at least 50 persons. The train could also continue to be used as quarters, many made use of this. Some wagons of the train had wireless and by means of loud-speakers the political events were regularly made known.

The "News Sheet of Corps Group BORK" (originally called "Listen Comrade!"), censored by the occupation authorities, also contributed in this direction.

The provisioning of the transport in WERFEN was at first still fairly good, all the more since numerous foodstuff transports of the Southern Army were then streaming back and Major HEIN confiscated them for the transport. Remaining stocks of clothing and linen could also be distributed to the members of it. At the end of May the food situation became gradually worse because GAU SALZBURG was itself already an area requiring supplies. On the orders of the Americans preparations were nevertheless made for the transfer at the end of the month of the whole of Corps Group BORK to UPPER BAVARIA. In the middle of May, the 20th of May at the latest, Abteilung Chi officially disbanded itself.

In preparation for the transfer Corps Group BORK was split up into several "March Regiments". There were at least three, they were designated by the letters A,B and C. The regiments consisted of battalions and the battalions of companies. The battalions and companies were numbered within the whole of the Corps Group. The women were naturally not included in this dividing-up process, the male civilians, however, were put together in a "civil service company", the 18th company. A section of the personnel remained as an HQ outside the company. The soldiers from the previous Chi Abteilung, who were known to me, all belonged to one and the same company as far as they were not employed in this HQ. It was either the 16th or 17th and was also called the "Teleprinter Company"; this name did not have any actual signification. The 16th, 17th and 18th companies together formed the VI battalion which belonged to regiment C. The third of these companies was probably called the "Telephone Company".

Doc ID: 6587345 Doc Ref ID: A2972105

On 22nd of May both companies, in which the previous Abteilung Chi was combined, went into new quarters outside WERFEN in the village of HUNDSBACH situated high up in the mountains, 12 kilometres distant. Only the HQ stayed behind in WERFEN. The remaining parts of the VI Battalion which did not originally come from WERFEN (i.e. the "Telephone Comapny" and the battalion HQ) also appeared on the scene in HUNDSBACH. Quarters there were, for the most part, communal quarters in barns. Food was pretty bad. Yet, for the first time since HALLE, there was a field kitchen available.

In place of the name HUNDSBACH, the designation WERFENWENG may appear in other reports. It was the name in general use then but actually referred to a neighbouring place or part of a place outside the village of HUNDSBACH. On 26th May the VI Battalion was sent to WERFEN, this time for the most part on foot, and from there it was despatched further by railway. The old goods train of the OKW Transport was still standing on the rails; the HQ of the Corps Group, which included numerous members of the previous transport, was still in WERFEN too, the women likewise. The departure fixed for 12 o'clock noon took place almost punctually at about 12.10. The transport was taken via BISCHOFSHOFEN and thence through the TIROL, that is via St.JOHANN - KITZBÜHEL - WÖRGL. Leaving KUFSTEIN behind the train arrived in BAVARIA towards 9 o'clock in the evening. During the night it reached ROSENHEIM where the railway branches. As the section to the originally intended destination station of HEUFELD was temporarily unusable, the transport branched off at ROSENHEIM in the other direction and at roughly 4 o'clock in the morning the alternative destination of OSTERMÜNCHEN was reached. In the course of this twenty-seventh day of May the participants were brought, partly on foot and partly by lorry, to that part of the village of WILLING called WESTERHAM where the whole of the VI Battalion went into its new quarters. There were communal quarters in barns here also.

Other parts of Corps Group BORK also removed to neighbouring places at this time. The other (V) battalion of regiment C, for instance, came to MITTERHAM (District of WILLING) and battalion B to HEUFELD or close by. Finally the HQ had also arrived by June 1. This should have originally left WERFEN at 1600 hours on 26th May in sections, the departure was postponed yet again and only one part of the transport probably arrived in OSTERMÜNCHEN on the morning of 27th May, a few hours after the VI battalion. The remainder of the HQ and the women were conveyed from WERFEN to HEUFELD railway station a few days later; the journey did not proceed as smoothly as that of the VI battalion but lasted for about 2 days. The quarters for this transport, for a large part individual quarters, were in HEUFELD itself where the orderly room of the new reception camp was set up under the name "Abschnittskommando A, Lager 2". Major HEIN became the Ic ((Intelligence)) officer of the camp. During the first days of June all male civilians were withdrawn from the camp directorate and transferred to WESTERHAM to the 18th company.

Doc ID: 6587345 Doc Ref ID: A2972105

About the 1st of June the first American release regulations appeared. For the purpose of carrying out the release the women were collected together in special camps on about the 4th of June. The release of the men was similarly started in the week commencing the 4th of June. From each company of the VI battalion a few men were almost daily ordered to the neighbouring release camp of GÖTTING and were there released within 24 hours. GÖTTING was also valid for units stationed further away. The transport home of released persons took place from WESTERHAM. Since quarters for one night were needed for them there, the VI battalion was transferred on about the 10th of June to MITTERHAM (District of WILLING). Other release camps, among them LAMPFERDING, were valid for the HQ stationed in HEUFELD and the other units there. Food at the reception camp, which at first was rather meagre, improved noticeably, more particularly as the strength became smaller and smaller on account of releases in spite of some new arrivals from the south, including civilians even ! Some took the opportunity of helping the peasants with the hay-making and of thereby earning additional food. A general roll-call of the camp only took place once in HEUFELD. All other instructions were issued through the medium of camp or battalion orders. At the beginning of June the office of welfare officer was introduced in all regiments. Following on these measures English and Russian language courses, in particular, were organized in HEUFELD.

At that time releases were only effected to the American or French zones of occupation. As a result of the increasing number of releases the companies shrank more and more and were accordingly amalgamated. Already at the time of the transfer to MITTERHAM the VI battalion had thus been merged with the V battalion, the location of which was in MITTERHAM as heretofore. The companies received new numbers (few higher than number 10) and a few days later they were completely amalagamated with each other and with other companies. In WESTERHAM also the strength had already dropped owing to numerous soldiers of the 16th and 17th companies having been called away to construct signals communications; this did not happen to any of the previous members of OKW who were known to me. In the middle of June the camp deposited all those who wished to be released into the, still barred, Russian zone of occupation in the area of REGENSBURG, this party was only very small (in V battalion there were 13 men, among them not one previous member of OKW). At this time the V battalion was merged in the III battalion, the HQ of which was in UNTERHEUFELD. The quarters in MITTERHAM were retained.

On the 18th or 19th of June, when the releases to the American and French zones were almost finished, those persons who wanted to be released into the still unopened British occupation zone and who did not belong to the HQ were despatched to a hastily prepared transit camp in UNTERHEUFELD. Only very few previous members of OKW were in this group, however, I among them. On the 21st of June we were sent to HEUFELD and from there by lorry to the release camp at SONNDORF in the Bavarian Forest. The further history of HEUFELD camp is therefore not known to me.

10th October, 1945

(Signed) Dr. WERNER WEBER.

(Trns. KCK & WRL)

Doc ID: 6587345 Doc Ref ID: A2972105

PART TWO

The U.S. Cypher.

In May and June 1941, numerous U.S. telegrams of the years 1940 and 1941 were submitted to me, they were in a letter system. The groups were 5-letter, usually consonants stood in the first, third and fifth positions and vowels in the second and fourth. In exceptional cases, a consonant might be in the fourth, a vowel in the fifth position. These characteristics corresponded to the groups of a familiar and already broken U.S. code. It was therefore suspected that the groups of the system under examination were formed from the other code, or from a similar code, by using substitution tables. In that code, only the first ten consonants of the alphabet (b,c,d,f,g,h,j,k,l,m) occurred as the first and third letters of each group. It was observed in many telegrams that a typical indicator group stood at the beginning, which was constructed exactly like the other groups. The search for repeats among messages having the same indicator led only to slight success, but it could at least be assumed that messages with the same indicator were on the same key, if they belonged to the same period of time. It was noticeable that identical groups in the same message only occurred at even intervals. It was therefore assumed that different substitution tables were used for the groups in the uneven positions. In many indicator-groups, there appeared as initial letters of the first 50 groups or so only 10 different consonants for groups standing in the odd positions and a further ten consonants for the groups in the even positions. It could therefore be assumed that this time also the code only used 10 consonants as initial letters, but that in those indicator groups the first letter of each group was encyphered independently. It was presumed that two further substitution tables were used: one for the bigram formed by the 2nd and 3rd letters and one for the bigram formed by the 4th and 5th letters (type: 1-2-2). For other indicator-groups the type 2-1-2 emerged; so, for the third letter of each group the code could only amount to ten consonants. The type 2-2-1 never appeared. The code groups therefore probably ended with any consonant. Indicator groups which conformed neither to the 1-2-2 nor to the 2-1-2 type could be ascribed to the 2-2-1 type.

With many indicator groups of the 1-2-2 type the ten consonants used were the same for the even as for the odd groups. Such indicator groups could be regarded as having identical meaning, i.e. the substitution tables used were the same. The 2-1-2 type had corresponding characteristics. In the case of 2-2-1, the identity of certain indicator groups could be assumed from the distribution of the initial bigrams, but I dropped this investigation.

Why the regularity in the ten first or third letters always stopped by about the 50th group can only be explained as follows: the key changed after about 50 groups. This assumption was supported by the following observation:

Doc ID: 6587345 Doc Ref ID: A2972105

In many telegrams having the same indicator group (for example BAMEL), the same group (GALEK for example) was found again as group 50 or thereabouts and again (as HEFAM, for example) as group 100.

It was therefore assumed that we were dealing with a second, third etc., indicator-group, which applied in each case to the 50 groups following it. As these new indicator-groups never appeared at the beginning of a message, it was obvious that each was encyphered by means of the indicator preceding it. If GALEK were then followed by 50 groups which began with the 10 consonants observed previously in connection with the indicator MOWIN (naturally a different ten for the odd positions to the even positions), GALEK would represent the group MOWIN encyphered on the BAMEL substitution tables. Whether the tables used were for the odd or the even positions was decided by the setting of the group GALEK, which was in fact either odd throughout or even throughout.

It was therefore to be assumed that the substitution tables contained the following:

Letter	1:	M	replaced by	CG
"	2 + 3:	OW	"	"	AL
2	4 + 5:	IN	"	"	EK

There is still an element of uncertainty here, however, because an equivalent (gleichwertig) indicator-group could be used in place of MOWIN. In the case of a large quantity of material being available, however, it would presumably have been possible to make a decision one way or another. By these means one could hope gradually to penetrate the details of the substitution tables. A prerequisite for this, however, was the finding of many such cases as the above. Each message had therefore to be compared with all messages having the same or an equivalent indicator-group. When possible, too, all messages had to be divided into sections of about 50 groups each, and the appropriate indicator-group allocated to each section according to distribution of letters (for example, of the ten initial letters, when the 1-2-2 type was produced). If the indicator-group were encyphered, one had to find it by comparative methods; for each message there must be another message in which the same two indicator-groups followed each other.

I had no staff available for this statistical work, however, so I was obliged to abandon both the remainder of the work and the evaluation of what had already been accomplished.

Whether the traffic was military or diplomatic I cannot remember.

8th October, 1945.

(Signed) Dr. WERNER WEBER.

Doc ID: 6587345 Doc Ref ID: A2972105

PART THREE

The Japanese Cipher

(20 Appendices Attached)

1) The "Old Code".

At the end of July, 1941, Japanese diplomatic telegrams were submitted to me. They were mainly in 5-letter traffic, and contained at the beginning-after an early comprehensible number-group or something of the kind - an obvious indicator-group. This changed daily. Messages with the same indicator could be assumed to be on the same key. Examination of messages with the indicator JEVUC, of 12th June, 1941, revealed 16 split repeats between two messages (of the VICHY/TOKIO traffic), each of which consisted of three separate sections, excepting the fifth, which contained only two.

This is set out schematically in Appendices 1 and 2. Moreover the gaps between two parts of the same repeat were of the same length in both messages, except in the case of the eleventh repeat, where the gap in the earlier message (Appendix 1) was longer by one than the gap in the later message (Appendix 2). If one ignores these irregularities, the picture is typical of a repeat in phase in a transposition system, and must consist of three separate parts. (Explanation of the word "transporition" (Würfel) in Appendix 3). Underlying this one might expect two texts of the type given in Appendices 4 and 5, in which the order of the vertical columns would be altered, but altered in both cases in the same way. It is true that a correction would have to be made to column 11: the gap between the two sections of the repeat in the first message (see Appendix 4) would have to be shortened by 1. Instead of this, one could have lengthened the gap by 1 in the later message, but that would not have been expedient, because it was to be suspected that the later message was a correction to the earlier one. The insertion by mistake of a letter into the cypher text means that, owing to it being a transposition system, the recipient would not be able to read it. How was it, however, that the cypher-clerk did not notice the mistake? When the text was split up into 5-symbol groups, there must have been one left over at the end, although the cypher clerk must have so arranged it that the text was divisable by five. Explanation: a letter must have been lost in some other position. This position was certainly in the fifth column, because that was where the third section of the repeat was missing. In the earlier message this third section was probably copied in error from a neighbouring column, one letter being lost in the process. In fact where one could expect the third section, Appendix 1 contains the letters RWIEEZ, with which column 16 is concluded. So it is probable that column 5 was adjacent to column 16, and that the 5 letters WIEEZ of column 5 in Appendix 1 took the place of the 6 correct letters, while the preceding R was correct. The correction was already made in Appendix 4.

Doc ID: 6587345 Doc Ref ID: A2972105

A short distance in front of the first part of each of the split repeats, Appendices 1 and 2 show further repeats (designated I in Appendices 4 and 5), but with different column order in each case. For instance what is contained in column 1 of Appendix 1 is contained in column 6 in Appendix 2, i.e. the letters VIA.

Formula: 1 → 6. On the other hand, what is contained in column 6 of Appendix 1 is contained in column 15 in Appendix 2, i.e. the letters YI. Formula: 6 → 15, etc. Combination produces the following chains:

1 → 6 → 15 → 14 → 1
2 → 9 → 16 → 3 → 2
4 → 5 → 13 → 10 → 4
7 → 12 → 11 → 5 → 7

A further repeat (designated III in Appendices 4 and 5) gave the following chains:

1 → 3 → 14 → 16 → 15 → 9 → 6 → 2 → 1
4 → 12 → 10 → 7 → 13 → 8 → 5 → 11 → 4

A later repeat still (designated V in Appendices 4 and 5) gave the following chains:

1 → 9 → 14 → 2 → 15 → 3 → 6 → 16 → 1
4 → 8 → 10 → 11 → 13 → 12 → 5 → 7 → 4

A last short repeat (designated VI in Appendices 4 and 5) gave the following chains:

1 → 2 → 6 → 9 → 15 → 16 → 14 → 3 → 1
4 → 11 → 5 → 8 → 13 → 7 → 10 → 12 → 4

The explanation of all these chains was easily found. If the cages of two transpositions on the same key contain a repeat out of phase, which starts in the second cage "k" columns to the right of the position in the first cage (in Appendix 6, k = 3) the relevant text belonging to the repeat, from column 1 of the first transposition, is found in the column of the second transposition lying "k" columns to the right of column 1 (in Appendix 6, for example, column 5, so that in accordance with the above, one would write 1 → 5). That is to say that in the above example the columns 1,6,15 and 14 would follow one another at equal intervals ("k"), likewise columns 2,9,16,3 etc., but (with a different "k") also columns 1,3,14, 16,15,9,6,2 etc. Result: the transposition key over the cage would have to contain one of the four following figure sequences in either the odd or the even position:

1 3 14 16 15 9 6 2
1 16 6 3 15 2 14 9
1 9 14 2 15 3 6 16
1 2 6 9 15 16 14 3

or else a figure sequence obtained therefrom by "cyclic substitution," i.e. retaining the order of figures, but starting at a different point, for example:

14 16 15 9 6 2 1 3.

Doc ID: 6587345 Doc Ref ID: A2972105

In the intermediate positions above the transposition cage, one of the following figure -sequences would have to stand:

4 12 10 7 13 8 5 11
4 7 5 12 13 11 10 8
4 8 10 11 13 12 5 7
4 11 5 8 13 7 10 12

or else a sequence obtained therefrom by cyclic substitution.

Only a few of these sequences appear impossible. The repeat marked III, for instance, contains a "thin" section consisting, in Appendix 4, of columns 4,5,9,11,15 and 16, but in Appendix 5 of columns 4,6,9,11,12 and 15, comprising two lines in each case, and of a "thick" section, consisting of the remaining columns and comprising three lines in each case. In each repeat, however, the "thin" columns must lie adjacent to one another, likewise the "thick" columns. That means that the only possible transposition keys in (1) are those in which the figures 9,15 and 16 and, simultaneously, 6,9 and 15 are adjacent, i.e. the following:

1 3 14 16 15 9 6 2
1 2 6 9 15 16 14 3

Similarly, from (2), only those transposition keys are admissable in which 4,5,11 and 4,11,12 are adjacent, i.e. only the following:

4 12 10 7 13 8 5 11
4 11 5 8 13 7 10 12

Thirdly, however, the figures 9,15 and 16 from (3) must lie adjacent to the figures 4,5 and 11 from (4), likewise the figures 6,9 and 15 from (3) must lie adjacent to 4,11 and 12 from (4). So the transposition key on top of the cage must be one of the following:

1 13 3 8 14 5 16 11 15 4 9 12 6 10 2 7
1 7 3 13 14 8 16 5 15 11 9 4 6 12 2 10
1 10 2 12 6 4 9 11 15 5 16 8 14 13 3 7
1 7 2 10 6 12 9 4 15 11 16 5 14 8 3 13

or one obtained therefrom by cyclic substitution.

Appendices 4 and 5, however, show that we are not dealing with the usual type of rectangular cage, because the height of the columns varies considerably. The following assumption arises: in the upper part of the cage (before the start of the repeat) there must be "forbidden" spaces in which nothing may be written, a so-called stencil. In Appendices 4 and 5, they have all slipped upwards, as it were, the picture presented can, however, still contain a mistake. It is assumed in Appendix 4 that the last line of the cage is filled up completely. If the following transposition key stands on top of the cage:

1 13 3 8 14 5 16 11 15 4 9 12 6 10 2 7

Doc ID: 6587345 Doc Ref ID: A2972105

which is admissable, and if one assumes that the last complete line is followed by one more letter, then column 1, which is right at the left, must be extended by one letter. This letter, therefore, does not appear at the top of column 2. The relative heights of the 16 columns (in the above order) no longer, as in Appendix 4 have the values

2 4 5 5 4 5 4 3 3 1 6 5 3 4 4 5

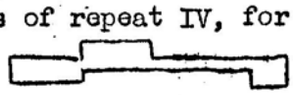
but

2 4 5 5 4 5 4 3 3 1 6 5 3 4 3 5

If a second letter is added to the last line, it comes in column 13, so that column 14 loses it at the top. The relative heights of the 16 columns are now:

2 4 5 5 3 5 4 3 3 1 6 5 3 4 3 5

Continuing along those line, one obtains 16 possible systems of relative heights, which are all reproduced in Appendix 7. Appendices 8 - 10 show the other three types of transposition keys according to (5). If one takes Appendix 5 as a basis, not Appendix 4, entirely different relative heights result, which are reproduced in Appendices 11 - 14. Messages with the same indicator group, however, must have the same stencil, i.e. they must produce the same relative column-heights. If, for instance, the first of the four transposition keys (5) is the right one, Appendices 7 and 11 must have a line in common, whose position also provides information on the number of letters in the last line of each message. If the second, third or fourth transposition key from (5) is correct, Appendices 8 and 12, 9 amd 13, 10 and 14 must contain a common line. In reality, however, Appendices 8 and 12 have no line in common, nor have Appendices 9 and 13, so that the only possible figure - sequences from (5) are the first and fourth. In fact, Appendices 7 and 11 do contain a line in common, but only one. In both Appendices it is underlined in red, and indicates: if the first figure-sequence from (5) is the correct one, the last line of the first message (Appendix 4) comprises 7 letters, and of the second message (Appendix 4) four letters. Apperdices 10 and 14 similarly contain one and only one line in common. It has been underlined in red in both cases and indicates: if the fourth transposition key from (4) is the correct one, the last line of the first message comprises 13 letters, and of the second message 10 letters.

Distinction between the first and the fourth transposition keys is easily made by trial and error. If the first key were correct, the message given is Appendix 4, for instance, would take the form given in Appendix 15, as its last line would have to contain 7 letters. It is true that the picture could still be somewhat modified by vertical sliding of the columns against each other, but it will never be possible to make full use of the contents of the seven repeats. The letters of repeat IV, for instance, will always appear in the order  (Appendix 15) or a similar order,

Doc ID: 6587345 Doc Ref ID: A2972105

or if one wishes to avoid this by dropping columns 5,11,14,15 and 16 by one line, and raising column 7 by one line, other different repeats, as in II would occur in a new but equally unusable form. One must therefore regard the fourth transposition key from (5) as the correct one. On top of the cage there will be the following key:

1 7 2 10 6 12 9 4 15 11 16 5 14 8 3 13

or else one obtained therefrom by cyclic substitution. There can be no cyclic substitution, however, as this is a stencil. It only means the addition of a few new "forbidden" spaces, not beginning the first line of the cage at the extreme left (Ex. Appendix 16). One can therefrom confidently accept the transposition key (6) as the correct one. Then the repeats I - VII are made best use of if the messages are written out as in Appendices 17 and 18. The last lines must consist of 13 or 10 letters. The only thing lacking now is the fixing of the stencil. What is noticed at first in Appendices 17 and 18, is that the repeat I could be lengthened quite considerably if, in Appendix 17, the "c" of line 10 were not in column 4. So we can try raising the "e" further replacing it by a "forbidden" space, the result is that repeat I will already begin with the letters TZOWDAAFM ... Naturally, the space at line 10 column 4 must also be left empty in the other message, the "i" in that position is therefore shifted up.. The repeat I is at once lengthened again, and now starts with VANTZOWDAAFM... (In connection with all these operations, comparison should be made with the later Appendices 19 and 20). This confirms the accuracy of the method of approach adopted. So one continues further along these lines, attempting so to fix the upper part of the stencil that many short repeats are formed. This is most successful when a stencil is chosen such as in Appendices 19 and 20. This stencil is therefore obviously the right one. The cypher-clerk, however, will not have chosen a transposition key beginning with 1. The consequent cyclic substitution will alter the stencil; for example, if one starts the transposition key with 3, the many "forbidden" spaces in the first line would be eliminated; that is much more encouraging. The text is not affected, and columns 5 and 16 are in fact adjacent, as was originally surmised.

The two messages thus solved were, as it appeared, in a readable code, composed of 20 letter groups, and unrecyphered. It could be recognized by the fact that all of its cypher texts (as in Appendices 19 and 20) began with CA. Next, the 16 other messages with the same indicator JEVUC were decyphered (entschlüsselt) by means of the same figure-sequence and the same stencil. Only four of these messages were in the "CA" code, the other 12 were in an unknown code whose elements were likewise obviously 2-letter. That is how the presence of this code was discovered. In contrast to the CA code, which contained about 40% vowels, this one showed only 20-25% vowels.

Doc ID: 6587345 Doc Ref ID: A2972105

2) The "New Code".

The telegrams referred to above had a number of "pronouncable" indicator-groups: the first, third and fifth letter of each indicator-group was a consonant, the second and fourth a vowel. In addition the indicators followed an alphabetical arrangement, during the first days of March, they always began with F, later with G, H and J. The sequence was broken on 30th June 1941, but already on 23rd June, four new series of indicator-groups appeared alongside the others, also in diplomatic traffic. Each series corresponded to a particular traffic network viz.

Series I: Circular messages
" II: N and S. AMERICA/TOKYO
" III: EUROPE and NEAR EAST/TOKYO
" IV: MIDDLE and FAR EAST

These telegrams too were composed of letters. In the daily-changing indicators, the first and third letters were always consonants, the second always a vowel, while the fourth and fifth could be chosen at random. In each series the indicator-groups again followed an alphabetical arrangement. On 1st September however, the initial letters of the indicators moved back in the alphabet; Series I, which had reached F, now started with B, Series II with G, Series III with LE and Series IV with V. They continued in alphabetical order until the old indicators were reached on 23rd June, 1942. The following picture was formed: from 1st September to 31st August.

Series I began with B,C,D,F;
" II began with G,H,J,K,LA;
" III began with LE, LI, LO, LU, LY, N,P,Q (M was absent)
" IV began with V,W,X,Z (R,S and T absent).

On 1st September, therefore, each series joined on to the preceding series alphabetically.

I only examined these messages more closely from February, 1942. According to our experience with JEVUC, a transposition was again to be suspected. This suspicion was in fact confirmed on the basis of two messages of 18th July 1941, with the indicator-group GICXA. These revealed between them 23 split repeats of exactly the same type as shown in Appendices 1 and 2. The first repeat began this time with the first letter of each message, so that the fact was even more striking, owing to identical message-beginnings. After proceeding exactly as before, it became apparent that we were dealing with a transposition with a key-length of 23, the upper lines of which again contained a stencil. The messages were in quite a difficult code to what they were in before, but it too was a 2-letter system. That was how we discovered the presence of the "new code".

Doc ID: 6587345 Doc Ref ID: A2972105

3. Identification of the daily key. Messages with other indicator-groups whether in the old or the new code, I solved in the same manner (the CA code, recognisable by its 40% vowels, hardly ever occurred):

a) Search for adjacent columns. Two lengths of text must be sought when written perpendicularly next to each other produce as many as possible of the most frequent bigrams of the code actually in force. In cases when the width of the cage (number of columns) is supposed to be an odd number, each second line can be ignored when doing this. If almost all the bigrams are equally frequent, the length of the cage is certainly an even number.

This was the most important, but also the most arduous part of the work. It was made easier for me by the allocation to me, as assistant, in September 1941, of a few male service personnel and women, with whom I worked until February on the old code, later on the new one.

b) Identification of the transporition key. If a message has undergone a certain amount of investigation, the approximate depth of each column and the number of columns, i.e. the width of the cage, can be established. Should the width of the cage be an odd number, the key can also be established, because each column A must have a certain"left-hand neighbour" B and a "right-hand neighbour" C, with which it alternately forms good bigrams in the individual lines; BAC must therefore occur in the transpcsition key. In the case of the cage-width being an even number, the problem was more difficult. Success was often achieved, however, by means of the striking repeats obtained by appropriate arrangement of the column-pairs into which a message was divided. If not enough progress could be made with one message, a second message with the same indicator-group was brought in, and so on. The 4-letter groups were of great assistance. In each of the two codes there were two series of bigrams which had no significations of their own, but simply occurred in the form of coupled pairs, of which the first pair indicated one series, the second the other series. If, for instance, a column-pair contained four bigrams of the "first" series at intervals of 2,5 and 3 lines, immediately to the right of this a column-pair must occur containing four bigrams of the "second" series at the same intervals. The ((2nd column-pair)) could generally be unambiguously established by these means. In the case of a large number of messages, such a favourable situation always occurred somewhere. Thus, the whole key was got out.

Doc ID: 6587345 Doc Ref ID: A2972105

c) Length of last line.
The last letter of the cypher text was at the same time the last letter of column W, when W = width of cage. In a horizontal direction, it could not be followed in the cage by more than W-1 letters. How many letters there really were, i.e. at which column the last line came to an end, could be decided in principle exactly as in Appendices 7 - 14, two messages being required for the purpose. A more elegant solution, however, was as follows: Let P_1 be the length (number of letters) of the shorter message, P_2 the length of the longer one. Let $P_2 - P_1$ be divided (leaving a remainder) by the width of the cage W:
$P_2 - P_1 = qw + r$, $0 \leq r < w$
Even assuming $r > 0$, which is usually the case, then the last ((long)) column of the longer message must be r columns further to the right than in the shorter message. Let columns a and b ($a < b$) be adjacent. Let one of the bigrams formed by them in the first message consist of two letters which, in the cypher text, are separated by S_1 letters. Then let one of the bigrams formed by columns a and b in the second message consist of two letters separated in the cypher text by S_2 letters. Evidently, then
$S_2 - S_1 = q(b-a) + t$
where t represents the number of those columns from the series a, a + 1, a + 2 . . . b - 2, b - 1 which fall within the r columns (from the last ((long)) column of the first message to the right as far as the last ((long)) column of the second message, the latter being already excluded).
If one now selects at random two adjacent columns a and b, it is possible to calculate S_1 and S_2, thus

$$t = S_2 - S_1 - q(b - a).$$

This will not, however, produce many intervals of r columns into which fall exactly t columns from the series a, a + 1 ..., b - 1 (no more and no less). One of them must be correct, i.e. the column on the extreme left must be the last column of the first message. It can quickly be seen plainly which is the column by bringing in further column-pairs a and b or further messages.

d) Obtaining the stencil.
It is only now that the length of the last line has been determined for one (i.e. for every) message that the relative depth of each column can be given, i.e. that the message can be given the form shown in Appendices 17 or 18. There are, however, still certain letters of the upper lines which must be slid upwards. The resultant stencil was always clearly established by the formation of as many short repeats as possible, also between different messages with the same indicator-group (as in Appendices 19 and 20).

Doc ID: 6587345 Doc Ref ID: A2972105

Thus the messages with that particular indicator were solved.

4) Results.

The fact that the system was a new one meant that the solution of new indicator-groups proceeded at first very slowly. Consequently the amount of material read in the old code up to February 1942 was so slight that the code became unreadable. After work had been switched on to the new code, progress improved as the time passed. A few months later, the new code became readable. By Autumn 1943, several hundred indicator-groups of the new code had been solved, the most frequent series (I and III) being finally solved almost completely.
No particular system appeared in the transposition keys, they were evidently chosen quite at random. It was only the width of the cages that was confined within certain limits; in the old code, only widths of 16 and 18 were observed, and in the new code only those between 19 and 25. On the other hand, there was a close connection between the stencils of the indicators of the same period of ten days. In each period of ten days (1st of the month to the 10th, 11th to 20th, 21st to 30th or 31st) only one stencil was used, which was, more-over, common to all four series. If the width of the cage were less, the last columns of the stencil were omitted. In the case of the new code, for instance, this basic stencil always contained 25 columns; for messages with a cage-width of 21, the four last columns on the right-hand side were to be deleted. It was, therefore, often unnecessary to determine the form of the stencil, if one already knew the basic stencil of the same 10-days period. Each new month, of course, produced three new basic stencils.
No further evidence of any system appeared in the stencils, but there was a preference for horizontal and vertical chains of "forbidden" spaces.
After conclusion of the first year (23rd June, 1942) the old indicator-groups were repeated in the new code until 31st July, 1942. During the months of August, September, October, November, December 1942 and January 1943, the indicators of the appropriate dates in July, June, May, April, March and February were used again. From 1st February till 30th June 1943, the indicator-groups used from March to July appeared again, in sequence, except for that part of I and IV traffic which was confined to the FAR EAST (excluding the MIDDLE EAST), Where the normal indicators appeared, i.e. those in force from February to June.

Doc ID: 6587345 Doc Ref ID: A2972105

On 30th June, 1943, use of the system was discontinued almost everywhere. It only remained in force in the traffic (belonging to series III) between TOKYO and the stations of the SOVIET UNION (MOSCOW and KUIBYSHEV) and occasionally in I traffic, and in July and August it used the indicator-groups for February and March. At the end of August, the system ceased in this traffic too.

From 23rd to 30th June 1942, the messages were encyphered according to the same indicators of the preceding year. After 1st July 1942, the following alterations appeared:

a) Up till the end of January, 1943, in each message the first two groups (i.e. the first ten letters) read vertically off the columns of the transposed text were set at the end of the message. Before decyphering, therefore, one had to set the two last groups of the message at the beginning.

b) During the same period, the transposition key underwent the following modification: the starting point was given by the key belonging to the identical indicator of the previous year. One took first the first figure, then the last, then the second, then the last but one, etc. In the case of the cage being an uneven length, the uneven central section was placed at the end. The width remained consequently unchanged.

c) Up till 30th September 1942, the first line of the stencil which had been used with that particular indicator was omitted, i.e. the second line became the first, the third the second, etc., so that the total number of stencil lines became one less.

d) From 1st October 1942 till the end of January 1943, procedure c) only continued to be followed in Series IV and in an unidentifiable section of Series I traffic. In the other traffics, the lines of the stencil were transposed: the 5th line came first, then what used to be the first four lines, finally the former sixth and all following lines.

e) From 1st February to 30th June, 1943, the majority of the messages were encyphered with a completely different transpposition key, which had only its length in common with the previous key. No connection could be established between the new key.
("Key B") and the old one ("Key A"). In July and August, 1943, a "Key C" came into force, which similarly had nothing in common with keys "A" and "B" except length.

Doc ID: 6587345 Ref ID: A2972105

f) The stencil used for "B" was formed from the basic stencil of the appropriate 10-day period for "A", by starting the latter at the 11th column and transferring the columns remaining on the left-hand side to the right-hand side. Similar procedure was followed for "C", but starting with the 16th column.

g) The FAR EASTERN sections of traffics I and IV did not introduce keys "B" and "C", but continued up to 30th June 1943 to use "A", incorporating the alterations listed above under a) b) and c). After 1st February 1943, the same thing still occasionally took place in the other traffics, but such messages bore the prefix "STRAD", set in front of the indicator-group.

(Signed) Dr. WERNER WEBER

10th October, 1945.

Doc ID: 6587345 c Ref ID: A2972105

APPENDICES

1 in Appendix 1 = Original Text in Old System.

jevŭo reŭev viaby rkyia vhwpŭ eiehf volap nzyli fnmtm igisw
1 1 1 2
iygai fgsnf dhfŭt oyazi kfoqz ifgdw idzib sipia bxhsz qomyo
2 2 3 3 3
zeaŭa iplpe bzpoe afpfa ŭkinj lwhml yfsfy ownyy ooygf otqho
4 4 4 5 5
rwiee zyaqz zjzyi iŭmga omcai amyvo idcky jcmiy pevaa fifpŭ
6 6 6 7
pwnpp ŭoiss anike fmlgl mywwy ŭholk dbepl epnar onoaz ŭenis
7 7 7 8 8 8
hmvoo zihlw ŭzpca qpiba imwho giwiq ppqyp oqnyg typtw fnmxf
9 9 9 10
ihyge jtekx lktty niapt anbxs terii iseyi xeydp fbnji irtaa
10 10 11 11 11
prxox eespx eqatp fnine rmnyy eoahk hkmar pmyrf impgr ooete
12 12 12 13 13
psent wabvy yygmy mywer syyok zmxaq rzygŭ xsqhe dhiyn druac
13 14 14 14 15
hoipq winŭa miyŭm sinuv aefwi yavoc oazgm nidys aexkr wieez
15 15 15 16 16 16

2 in Appendix 2 = Original text in new system.

jevŭo rgail bmyby rkywi yhwps aebhf volak oipwu kzpsa zimig
1 1 1 2
isomo gafaq iefdh fŭtjd scvih qeejg avggd wiiav bsija mzxhs
2 2 2 3 3 3
zqoam yrmom iypai plpii rpols scraŭ kinjf eyrnn wwyav waŭwn
3 4 4 4 5
yylep gfogi nydge xiŭgs slzzi fhvia iŭmga ibeai jpisn idcky
5 5 6 6 6
joaac yvhzn ygjol fpŭpw xfiŭo itqhs ikefm ljffl ypahk mggan
6 7 7 7
bdbep pgrna riafo zŭeni scayh mvzeh aŭmnm tpcaq ppqoi mkuev
8 8 8 9 9
pwiqp pqpmw yyoap iwhpm twfnm qathy jonan kxlkt tŭkeg alyaa
9 10 10 10
zxexs teroy seyne jpfpf bnjie iolet yeimz afies pxeeb ppfxt
11 11 11 12 12

etemn yyeoi hnamy qlvxz fylrf immpp ooeax eaent wabwc feyik
12 13 13 13

ffidr ŭersy dzizm xhhox yguxs gnaur dfwoe tyiac hojmn winqf
14 14 14 15 15

ggiŭm sinuj hmroy ygvao ŭzcoa zyoki dyvmy iyrwi eezvŭ
15 16 16 16

Appendix 3:-

Transposition System

Clear Text: Die Methoden der Mathematik haben um die Jahrhundertwende einen Umbruch erlebt.

Transposition cage. (Width 8):

3	8	6	1	4	2	5	7
d	i	e	m	e	t	h	o
d	e	n	d	e	r	m	a
t	h	e	m	a	t	i	k
h	a	b	e	n	ŭ	m	d
i	e	j	a	h	r	h	ŭ
n	d	e	r	t	w	e	n
d	e	e	i	n	e	n	ŭ
m	b	r	ŭ	o	h	e	r
l	e	b	t				

Cypher text: (Read off the columns vertically, taking the columns in numerical order).

mdmea riŭtt rtŭrw ehddt hindm leean htnch mimhe

neene bjeer boakd ŭnŭri ehaed ebe

Effect of a Split Repeat in Phase

I

Die Gesellschaft für experimentelle Zoologie hielt heute eine Sitzung in der Festhalle der Stadt ab.

Transposition cage:

3	8	6	1	4	2	5	7
d	i	e	g	e	s	e	l
l	s	c	h	a	f	t	f
ŭ	e	r	e	x	p	e	r
i	m	e	n	t	e	l	l
e	z	o	o	l	o	g	i
e	h	i	e	l	t	h	e
ŭ	t	e	e	i	n	e	s
i	t	z	ŭ	n	g	i	n
d	e	r	f	e	s	t	h
a	l	l	e	d	e	r	s
t	a	d	t	a	b		

II

Heute sprach ein bekannter Biologe in der Gesellschaft für experimentelle Zoologie. Am Anfang dieser Sitzung in der Festhalle der Stadt wurde ein Bericht verlesen.

3	8	6	1	4	2	5	7
h	e	ŭ	t	e	s	p	r
a	c	h	e	i	n	b	e
k	a	n	n	t	e	r	b
i	o	l	o	g	e	i	n
d	e	r	g	e	s	e	l
l	s	c	h	a	f	t	f
ŭ	e	r	e	x	p	e	r
i	m	e	n	t	e	l	l
e	z	o	o	l	o	g	i
e	a	m	a	n	f	a	n
g	d	i	e	s	e	r	s
i	t	z	ŭ	n	g	i	n
d	e	r	f	e	s	t	h
a	l	l	e	d	e	r	s
t	a	d	t	w	ŭ	r	d
e	e	m	n	b	e	r	i
c	h	t	v	e	r	l	e
s	e	m					

Doc ID: 6587345 Doc Ref ID: A2972105

Cypher text:

ghbne eeufe tsfpe otngs ebdlu | tenog henoa eufet nvsne esfpe ofegs euerh

ieeui datea xtlli nedae telgh eitne | akidl uieeg idate oseit geaxt lnsne dwbep

creoj ezrld lfrli esnhs isemz httel | briet elgar itrrr luhnl rcreo mizrl ditnr

a | elnlf rlins nhsdi eecao esemz adtel aehe

Appendix 4

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
									h							
			o		l		c	g	m			ii				
		p	y		w		m	l	v	y		r	a	v		v
		n	a		h	y	i	m	o	p	y	t	h	y	e	a
	r	z	z		m	a	y	y	o	o	nn	a	k	y	d	e
	e	y	i	m	l	q	p	w	z	q	i	a	h	y	h	f
	u	l	k	y	y	z	e	w	i	n	a	p	k	g	i	w
	e	i	f	o	f	z	v	y	h	y	p	r	m	m	y	i
	v	f	o	z	s	j	a	u	l	g	t	x	a	y	n	y
I	v	n	q	e	f	z	a	h	w	t	a	o	r	m	d	a
I	i	m	z	a	y	y	f	o	u	y	n	x	p	y	r	v
I	a	t	i	u	o	i	i	l	z	p	b	e	m	w	u	o
II	b	m	f	a	w	i	f	k	p	t	x	e	y	e	a	c
II	y	i	g	i	n	u	p	d	c	w	s	s	r	r	c	o
II	r	g	d	p	y	m	u	b	a	f	tt	p	f	s	h	a
II	k	i	w	l	y	g	p	e	q	n	e	x	i	y	o	z
II	y	s	i	p	o	a	w	p	p	m	r	e	m	y	i	g
III	i	w	d	e	o	o	m	l	i	x	i	q	p	o	p	m
III	a	i	z	b	y	m	p	e	b	f	i	a	g	k	q	n
III	v	y	i	z	g	c	p	p	a	i	s	t	r	z	w	i
IV	h	g	b	p	f	a	u	n	i	h	e	p	o	m	i	d
IV	w	a	s	o	o	i	o	a	m	y	y	f	o	x	n	y
IV	p	i	i	e	t	a	i	r	w	g	i	n	e	a	u	s
V	u	f	p	a	q	m	s	o	h	e	x	i	t	q	a	a
V	e	g	i	f	h	y	d	n	o	j	e	n	e	r	m	e
VI	i	s	a	p	o	v	a	o	g	t	y	e	p	z	i	x
VI	e	n	b	f	r	p	n	a	i	e	d	r	s	y	y	k
VII	h	f	x	a	.	i	ii	z	w	k	p	n	e	g	u	r
VII	f	d	h	u	.	d	k	u	i	x	f	n	n	u	m	w
VII	v	h	s	k	.	c	e	e	q	l	b	y	t	x	s	i
VII	o	f	z	i	.	k	f	n	p	k	n	y	w	s	i	e
VII	l	u	q	n	.	y	m	i	p	t	j	e	a	q	n	e
VII	a	t	o	j	.	j	l	s	q	t	i	c	b	h	u	z

Doc ID: 6587345 Doc Ref ID: A2972105

Appendix 5

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
									y							
			s		y		a	f	h			o				
		i	c		m		c	l	m	w	i	i	n	f		m
		p	y		n		y	y	v	y	e	e	a	e		r
		w	i		n	l	v	p	z	y	g	t	m	y	r	o
	r	ŭ	h	y	w	z	h	a	e	o	a	y	y	i	d	y
	g	k	q	r	w	z	z	h	h	a	l	e	q	k	f	y
	a	z	e	m	y	i	n	k	a	p	y	i	l	f	w	g
	i	p	e	o	a	f	y	m	ŭ	i	a	m	v	f	o	v
	l	s	j	m	v	h	g	g	m	w	a	z	x	i	e	a
	b	a	g	i	w	v	j	g	n	h	z	a	z	d	t	o
I	m	z	a	y	a	i	o	a	m	p	x	f	f	r	y	u
	y	i	v	p	ŭ	a	l	n	t	m	e	i	y	ŭ	i	z
	b	m	g	a	w	i	f	b	p	t	x	e	l	e	a	c
	y	i	g	i	n	ŭ	p	d	c	w	s	s	r	r	c	o
II	r	g	d	p	y	m	ŭ	b	a	f	t	p	f	s	h	a
	k	i	w	l	y	g	p	e	q	n	e	x	i	y	o	z
	y	s	i	p	l	a	w	p	p	m	r	e	m	d	i	y
	w	o	i	i	e	i	x	p	p	q	o	e	n	z	m	o
III	i	m	a	i	p	b	f	g	q	a	y	b	p	i	n	k
	y	c	v	r	g	e	i	r	o	t	s	p	p	z	w	i
	h	g	b	p	f	a	ŭ	n	i	h	e	p	o	m	i	d
IV	w	a	s	o	o	i	o	a	m	y	y	f	o	x	n	y
	p	f	i	l	g	j	i	r	k	j	n	x	e	h	q	v
	s	a	j	s	i	p	t	i	ŭ	o	e	t	a	h	f	m
V	a	q	a	s	n	i	q	a	e	n	j	e	x	o	g	y
	e	i	m	e	y	s	h	f	v	a	p	t	e	x	g	i
VI	b	e	z	r	d	n	s	o	p	n	f	e	a	y	i	y
	h	f	x	a	g	i	i	z	w	k	p	n	e	g	ŭ	r
	f	d	h	ŭ	e	d	k	ŭ	i	x	f	n	n	ŭ	m	w
	v	h	s	k	x	c	e	e	q	l	b	y	t	x	s	i
VII	o	f	z	i	i	k	f	n	p	k	n	y	w	s	i	e
	l	ŭ	q	n	ŭ	y	m	i	p	t	j	e	a	q	n	e
	a	t	o	j	g	j	l	s	q	t	i	c	b	n	ŭ	z
	k	j	a	f	s	o	j	o	p	ŭ	e	i	w	a	j	v
	o	d	m	e	s	a	f	a	m	k	i	h	c	ŭ	h	ŭ

Doc ID: 6587345 Doc Ref ID: A2972105

Appendix 6:

Effect of a split repeat out of phase in a transposition.

I

Clear Text:

Die Gesellschaft für experimentelle Zoologie hielt heute eine Sitzung ab.

Transposition cage:

3	8	6	1	4	2	5	7
d	i	e	g	e	s	e	l
l	s	c	h	a	f	t	f
u	e	r	e	x	p	e	r
i	m	e	n	t	e	l	l
e	z	o	o	l	o	g	i
e	h	i	e	l	t	h	e
ŭ	t	e	e	i	n	e	s
i	t	z	ŭ	n	g	a	b

Cypher text:

ghexo eeusf peoin gdlui eeuie
1 2 3 4

axtll inete lghea eoreo iezlf
4 5 6 7

rlies bisem zhtt
7 8

II

Im Festsaale der Gesellschaft für experimentelle Zoologie sprach heute ein bekannter Gelehrter.

3	8	6	1	4	2	5	7
i	m	f	e	s	t	s	a
a	l	e	d	e	r	g	e
s	e	l	l	s	c	h	a
f	t	f	ŭ	e	r	e	x
p	e	r	i	m	e	n	t
e	l	l	e	z	o	o	l
o	g	i	e	s	p	r	a
c	h	h	e	ŭ	t	e	e
i	n	b	e	k	a	n	n
t	e	r	g	e	l	e	h
r	t	e	r				

edlui eeeeg rtrcr eopta liasf
7 2 3

peoci trses emzsu kesgh enore
3 4 5

nefel frlih breae axtla enhml
6 7

etelg hnet
8

The following chain is formed

1→5→8→4→7→6→2→3→1

Doc ID: 6587345 Doc Ref ID: A2972105

Appendices 7 - 15 inclusive.

Spalte = column
Relative Höhe = relative height.

Appendix 7

Spalte:	1	13	3	8	14	5	16	11	15	4	9	12	6	10	2	7
Relative Höhe:	2	4	5	5	4	5	4	3	3	1	6	5	3	4	4	5
	2	4	5	5	4	5	4	3	3	1	6	5	3	4	3	5
	2	4	5	5	3	5	4	3	3	1	6	5	3	4	3	5
	2	4	5	5	3	5	4	3	3	0	6	5	3	4	3	5
	2	4	5	5	3	5	4	3	3	0	5	5	3	4	3	5
	2	4	5	5	3	5	4	3	2	0	5	5	3	4	3	5
	2	4	5	5	3	5	4	3	2	0	5	5	2	4	3	5
	1	4	5	5	3	5	4	3	2	0	5	5	2	4	3	5
	1	4	5	5	3	5	4	3	2	0	5	4	2	4	3	5
	1	4	5	5	3	5	3	3	2	0	5	4	2	4	3	5
	1	4	5	5	3	4	3	3	2	0	5	4	2	4	3	5
	1	4	5	5	3	4	3	3	2	0	5	4	2	3	3	5
	1	3	5	5	3	4	3	3	2	0	5	4	2	3	3	5
	1	3	5	5	3	4	3	3	2	0	5	4	2	3	3	4
	1	3	5	5	3	4	3	2	2	0	5	4	2	3	3	4
	1	3	4	5	3	4	3	2	2	0	5	4	2	3	3	4

Appendix 8

Spalte:	1	7	3	13	14	8	16	5	15	11	9	4	6	12	2	10
Relative Höhe:	2	5	5	4	4	5	4	5	3	3	6	1	3	5	4	4
	2	5	5	4	4	5	4	5	3	3	6	1	3	5	3	4
	2	5	5	4	4	4	4	5	3	3	6	1	3	5	3	4
	2	5	5	4	4	4	4	5	3	3	6	0	3	5	3	4
	2	5	5	4	3	4	4	5	3	3	6	0	3	5	3	4
	2	5	5	4	3	4	4	5	2	3	6	0	3	5	3	4
	2	5	5	4	3	4	4	5	2	3	5	0	3	5	3	4
	1	5	5	4	3	4	4	5	2	3	5	0	3	5	3	4
	1	5	5	4	3	4	4	5	2	3	5	0	2	5	3	4
	1	5	5	4	3	4	3	5	2	3	5	0	2	5	3	4
	1	5	5	4	3	4	3	5	2	3	5	0	2	4	3	4
	1	5	5	4	3	4	3	5	2	3	5	0	2	4	3	3
	1	5	5	4	3	4	3	4	2	3	5	0	2	4	3	3
	1	4	5	4	3	4	3	4	2	3	5	0	2	4	3	3
	1	4	5	3	3	4	3	4	2	3	5	0	2	4	3	3
	1	4	4	3	3	4	3	4	2	3	5	0	2	4	3	3

Doc ID: 6587345 Doc Ref ID: A2972105

Appendix 9

Spalte:	1	10	2	12	6	4	9	11	15	5	16	8	14	13	3	7
Relative	2	4	4	5	3	1	6	3	3	5	4	5	4	4	5	5
Höhe :	2	4	3	5	3	1	6	3	3	5	4	5	4	4	5	5
	2	4	3	5	3	1	6	2	3	5	4	5	4	4	5	5
	2	4	3	5	3	1	6	2	3	5	4	5	4	4	4	5
	2	4	3	5	3	1	6	2	3	5	4	5	4	3	4	5
	2	4	3	5	3	1	6	2	3	5	4	5	4	3	4	4
	2	4	3	5	3	1	6	2	3	4	4	5	4	3	4	4
	2	3	3	5	3	1	6	2	3	4	4	5	4	3	4	4
	2	3	3	4	3	1	6	2	3	4	4	5	4	3	4	4
	2	3	3	4	3	1	6	2	3	4	3	5	4	3	4	4
	2	3	3	4	2	1	6	2	3	4	3	5	4	3	4	4
	1	3	3	4	2	1	6	2	3	4	3	5	4	3	4	4
	1	3	3	4	2	1	5	2	3	4	3	5	4	3	4	4
	1	3	3	4	2	1	5	2	2	4	3	5	4	3	4	4
	1	3	3	4	2	1	5	2	2	4	3	5	3	3	4	4
	1	3	3	4	2	0	5	2	2	4	3	5	3	3	4	4

Appendix 10

Spalte:	1	7	2	10	6	12	9	4	15	11	16	5	14	8	3	13
Relative	2	5	4	4	3	5	6	1	3	3	4	5	4	5	5	4
Höhe :	2	5	3	4	3	5	6	1	3	3	4	5	4	5	5	4
	2	5	3	4	3	5	6	1	3	3	4	5	4	4	5	4
	2	5	3	4	3	5	6	1	3	3	4	5	4	4	4	4
	2	5	3	4	3	5	6	1	3	2	4	5	4	4	4	4
	2	4	3	4	3	5	6	1	3	2	4	5	4	4	4	4
	2	4	3	4	3	5	6	1	3	2	4	5	4	4	4	3
	2	4	3	3	3	5	6	1	3	2	4	5	4	4	4	3
	2	4	3	3	3	5	6	1	3	2	4	4	4	4	4	3
	2	4	3	3	3	5	6	1	3	2	3	4	4	4	4	3
	2	4	3	3	3	4	6	1	3	2	3	4	4	4	4	3
	1	4	3	3	3	4	6	1	3	2	3	4	4	4	4	3
	1	4	3	3	2	4	6	1	3	2	3	4	4	4	4	3
	1	4	3	3	2	4	6	1	2	2	3	4	4	4	4	3
	1	4	3	3	2	4	5	1	2	2	3	4	4	4	4	3
	1	4	3	3	2	4	5	0	2	2	3	4	4	4	4	3

Doc ID: 6587345 Doc Ref ID: A2972105

Appendix 11

Spalte:	1	13	3	8	14	5	16	11	15	4	9	12	6	10	2	7
Relative Höhe:	1	4	5	5	4	5	4	3	2	1	6	5	2	4	4	5
	1	4	5	5	4	5	4	3	2	1	6	5	2	4	3	5
	1	4	5	5	3	5	4	3	2	1	6	5	2	4	3	5
	1	4	5	5	3	5	4	3	2	0	6	5	2	4	3	5
	1	4	5	5	3	5	4	3	2	0	5	5	2	4	3	5
	1	4	5	5	3	5	4	3	1	0	5	5	2	4	3	5
	1	4	5	5	3	5	4	3	1	0	5	5	1	4	3	5
	0	4	5	5	3	5	4	3	1	0	5	5	1	4	3	5
	0	4	5	5	3	5	4	3	1	0	5	4	1	4	3	5
	0	4	5	5	3	5	3	3	1	0	5	4	1	4	3	5
	0	4	5	5	3	4	3	3	1	0	5	4	1	4	3	5
	0	4	5	5	3	4	3	3	1	0	5	4	1	3	3	5
	0	3	5	5	3	4	3	3	1	0	5	4	1	3	3	5
	0	3	5	5	3	4	3	3	1	0	5	4	1	3	3	4
	0	3	5	5	3	4	3	2	1	0	5	4	1	3	3	4
	0	3	4	5	3	4	3	2	1	0	5	4	1	3	3	4

Appendix 12

Spalte:	1	7	3	13	14	8	16	5	15	11	9	4	6	12	2	10
Relative Höhe:	1	5	5	4	4	5	4	5	2	3	6	1	2	5	4	4
	1	5	5	4	4	5	4	5	2	3	6	1	2	5	3	4
	1	5	5	4	4	4	4	5	2	3	6	1	2	5	3	4
	1	5	5	4	4	4	4	5	2	3	6	0	2	5	3	4
	1	5	5	4	3	4	4	5	2	3	6	0	2	5	3	4
	1	5	5	4	3	4	4	5	1	3	6	0	2	5	3	4
	1	5	5	4	3	4	4	5	1	3	5	0	2	5	3	4
	0	5	5	4	3	4	4	5	1	3	5	0	2	5	3	4
	0	5	5	4	3	4	4	5	1	3	5	0	1	5	3	4
	0	5	5	4	3	4	3	5	1	3	5	0	1	5	3	4
	0	5	5	4	3	4	3	5	1	3	5	0	1	4	3	4
	0	5	5	4	3	4	3	5	1	3	5	0	1	4	3	3
	0	5	5	4	3	4	3	4	1	3	5	0	1	4	3	3
	0	4	5	4	3	4	3	4	1	3	5	0	1	4	3	3
	0	4	5	3	3	4	3	4	1	3	5	0	1	4	3	3
	0	4	4	3	3	4	3	4	1	3	5	0	1	4	3	3

Doc ID: 6587345 Doc Ref ID: A2972105

Appendix 13

Spalte:	1	10	2	12	6	4	9	11	15	5	16	8	14	13	3	7
Relative Höhe:	1	4	4	5	2	1	6	3	2	5	4	5	4	4	5	5
	1	4	3	5	2	1	6	3	2	5	4	5	4	4	5	5
	1	4	3	5	2	1	6	2	2	5	4	5	4	4	5	5
	1	4	3	5	2	1	6	2	2	5	4	5	4	4	4	5
	1	4	3	5	2	1	6	2	2	5	4	5	4	3	4	5
	1	4	3	5	2	1	6	2	2	5	4	5	4	3	4	4
	1	4	3	5	2	1	6	2	2	4	4	5	4	3	4	4
	1	3	3	5	2	1	6	2	2	4	4	5	4	3	4	4
	1	3	3	4	2	1	6	2	2	4	4	5	4	3	4	4
	1	3	3	4	2	1	6	2	2	4	3	5	4	3	4	4
	1	3	3	4	1	1	6	2	2	4	3	5	4	3	4	4
	0	3	3	4	1	1	6	2	2	4	3	5	4	3	4	4
	0	3	3	4	1	1	5	2	2	4	3	5	4	3	4	4
	0	3	3	4	1	1	5	2	1	4	3	5	4	3	4	4
	0	3	3	4	1	1	5	2	1	4	3	5	3	3	4	4
	0	3	3	4	1	0	5	2	1	4	3	5	3	3	4	4

Appendix 14

Spalte:	1	7	2	10	6	12	9	4	15	11	16	5	14	8	3	13
Relative Höhe:	1	5	4	4	2	5	6	1	2	3	4	5	4	5	5	4
	1	5	3	4	2	5	6	1	2	3	4	5	4	5	5	4
	1	5	3	4	2	5	6	1	2	3	4	5	4	4	5	4
	1	5	3	4	2	5	6	1	2	3	4	5	4	4	4	4
	1	5	3	4	2	5	6	1	2	2	4	5	4	4	4	4
	1	4	3	4	2	5	6	1	2	2	4	5	4	4	4	4
	1	4	3	4	2	5	6	1	2	2	4	5	4	4	4	3
	1	4	3	3	2	5	6	1	2	2	4	5	4	4	4	3
	1	4	3	3	2	5	6	1	2	2	4	4	4	4	4	3
	1	4	3	3	2	5	6	1	2	2	3	4	4	4	4	3
	1	4	3	3	2	4	6	1	2	2	3	4	4	4	4	3
	0	4	3	3	2	4	6	1	2	2	3	4	4	4	4	3
	0	4	3	3	1	4	6	1	2	2	3	4	4	4	4	3
	0	4	3	3	1	4	6	1	1	2	3	4	4	4	4	3
	0	4	3	3	1	4	5	1	1	2	3	4	4	4	4	3
	0	4	3	3	1	4	5	0	1	2	3	4	4	4	4	3

Doc ID: 6587345 Doc Ref ID: A2972105

Appendix 15

1	13	3	8	14	5	16	11	15	4	9	12	6	10	2	7
		t	l		j					h	i				j
	c	c	g		l	ŭ				n	i		q		c
	a	y	l	v	w	v	t			v	r		y	p	m
	h	a	m	y	h	a	y	e		o	t	y	p	n	i
r	k	z	y	y	m	e	n	d		o	a	a	o	z	y
e	h	i	w	y	l	f	i	h	m	z	a	q	q	y	p
ŭ	k	k	w	g	y	w	a	i	y	i	p	z	n	l	e
e	m	f	y	m	f	i	p	y	o	h	r	z	y	i	v
v	a	o	ŭ	y	s	y	t	n	z	l	x	j	g	f	a
v	r	q	h	m	f	a	a	d	e	w	o	z	t	n	a
i	p	z	o	y	y	v	n	r	a	ŭ	x	y	y	m	f
a	m	i	l	w	o	o	b	ŭ	ŭ	z	e	i	p	t	i
b	y	f	k	e	w	c	x	a	a	p	e	i	t	m	f
y	r	g	d	r	n	o	s	c	i	c	s	ŭ	w	i	p
r	f	d	b	s	y	a	t	h	p	a	p	m	f	g	ŭ
k	i	w	e	y	y	z	e	o	l	q	x	g	n	i	p
y	m	i	p	y	o	g	r	i	p	p	e	a	m	s	w
i	p	d	l	o	o	m	i	p	e	i	q	o	x	w	n
a	g	z	e	k	y	n	i	q	b	b	a	m	f	i	p
v	r	i	p	z	g	i	s	w	z	a	t	c	i	y	p
h	o	b	n	m	f	d	e	i	p	i	p	a	h	g	ŭ
w	o	s	a	x	o	y	y	n	o	m	f	i	y	a	o
p	e	i	r	a	t	s	i	ŭ	e	w	n	a	g	i	a
ŭ	t	p	o	q	q	a	x	a	a	h	i	m	e	f	s
e	e	i	n	r	h	e	e	m	f	o	n	y	j	g	s
i	p	a	o	z	o	x	y	i	p	g	e	v	t	s	a
e	s	b	a	y	r	k	d	y	f	i	r	p	e	n	n
h	e	x	z	g	.	r	p	ŭ	a	w	n	i	k	f	i
f	n	h	ŭ	ŭ	.	w	f	m	ŭ	i	n	d	x	d	k
v	t	s	e	x	.	i	b	s	k	q	y	c	l	h	e
o	w	z	n	s	.	e	n	i	i	p	y	k	k	f	f
l	a	q	i	q	.	e	j	n	n	p	e	y	t	ŭ	m
a	b	o	s	h	.	z									

II

IV

Doc ID: 6587345 Doc Ref ID: A2972105

Appendix 16

Modification of a Stencil by Cyclic Substitution of the Figure-Sequence

Clear text: Über komplexe Funktionen zweier Variabeln ist noch wenig bekannt.

Transposition with Raster:

I							
3	8	6	1	4	2	5	7
ü	e	.	b	e	r	k	o
m	p	.	l	e	x	.	e
f	ü	n	k	.	.	.	t
i	o	n	e	n	z	.	w
.	e	i	e	r	v	a	r
i	a	b	e	l	n	i	s
t	n	o	c	h	w	e	n
i	g	b	e	k	a	n	n
t							

II							
2	5	7	3	8	6	1	4
.	.	.	ü	e	.	b	e
r	k	o	m	p	.	l	e
x	.	e	f	ü	n	k	.
.	.	t	i	o	n	e	n
z	.	w	.	e	i	e	r
v	a	r	i	a	b	e	l
n	i	s	t	n	o	c	h
w	e	n	i	g	b	e	k
a	n	n	t				

Cypher text:

blkee ecerx zvnwa ümfii
titee nrlhk kaien nnibo
boetw rsnne püea ng

Doc ID: 6587345 Doc Ref ID: A2972105

Appendix 17

1	7	2	10	6	12	9	4	15	11	16	5	14	8	3	13
						h							g	c	
	c				i	n					l		l	y	a
	m	p	y		r	v				v	w	v	m	a	h
	i	n	p	y	t	o		e	y	a	h	y	y	z	k
r	y	z	o	a	a	o		d	n	e	m	y	w	i	h
e	p	y	q	q	a	z	m	h	i	f	l	y	w	k	k
ŭ	e	l	m	z	p	i	y	i	a	w	y	g	y	f	m
e	v	i	y	z	r	h	o	y	p	i	f	m	u	o	a
w	a	f	g	j	x	l	z	n	t	y	s	y	h	q	r
v	a	n	t	z	o	w	e	d	a	a	f	m	o	z	p
i	f	m	y	y	x	u	a	r	n	v	y	y	l	i	m
a	i	t	p	i	e	z	u	ŭ	b	o	o	w	k	f	y
b	f	m	t	i	e	p	a	a	x	c	w	e	d	g	r
y	p	i	w	u	s	c	i	c	s	o	n	r	b	d	f
r	ŭ	g	f	m	p	a	p	h	t	a	y	s	e	w	i
k	p	i	n	g	x	q	l	o	e	z	y	y	p	i	m
y	w	s	m	a	e	p	p	i	r	g	o	y	l	d	p
i	n	w	x	o	q	i	e	p	i	m	o	o	e	z	g
a	p	i	f	m	a	b	b	q	i	n	y	k	p	i	r
v	p	y	i	c	t	a	z	w	s	i	g	z	n	b	o
h	ŭ	g	h	a	p	i	p	i	e	d	f	m	a	s	o
w	o	a	y	i	f	m	o	n	y	y	o	x	r	i	e
p	i	i	g	a	n	w	e	ŭ	i	s	t	a	o	p	t
ŭ	s	f	e	m	i	h	a	a	x	a	q	q	n	i	e
e	s	g	j	y	n	o	f	m	e	e	h	r	o	a	p
i	a	s	t	v	e	g	p	i	y	x	o	z	a	b	s
e	n	n	e	p	r	i	f	y	d	k	r	y	z	x	e
h	i	f	k	i	n	w	a	ŭ	p	r	.	g	ŭ	h	n
f	k	d	x	d	n	i	ŭ	m	f	w	.	ŭ	e	s	t
v	e	h	l	c	y	q	k	s	b	i	.	x	n	z	w
o	f	f	k	k	y	p	i	i	n	e	.	s	i	q	a
l	m	ŭ	t	y	e	p	n	n	j	e	.	q	s	o	b
a	l	t	t	j	c	q	j	ŭ	i	z	.	h			

I

Doc ID: 6587345 Doc Ref ID: A2972105

Appendix 18

1	7	2	10	6	12	9	4	15	11	16	5	14	8	3	13
						h							l	c	
	c				i	m					m		y	v	a
	y	p	y		e	v				r	n	e	p	i	m
	v	w	y	l	t	z		r	g	o	n	y	a	h	y
r	h	ŭ	o	z	y	e		d	a	y	w	i	h	q	q
g	z	k	a	z	e	h	r	f	l	y	w	k	k	e	l
a	n	z	p	i	i	a	m	w	y	g	y	f	m	e	v
i	y	p	i	f	m	ŭ	o	o	a	v	a	f	g	j	x
l	g	s	w	h	z	m	m	e	a	a	v	i	g	g	z
b	j	a	h	v	a	n	i	t	z	o	w	d	a	a	f
m	o	z	p	i	f	m	y	y	x	ŭ	a	r	n	v	y
y	l	i	m	a	i	t	p	i	e	z	ŭ	ŭ	b	g	l
b	f	m	t	i	e	p	a	a	x	c	w	e	d	g	r
y	p	i	w	ŭ	s	c	i	c	s	o	n	r	b	d	f
r	ŭ	g	f	m	p	a	p	h	t	a	y	s	e	w	i
k	p	i	n	g	x	q	l	o	e	z	y	y	p	i	m
y	w	s	m	a	e	p	p	i	r	y	l	d	p	i	n
w	x	o	q	i	e	p	i	m	o	o	e	z	g	a	p
i	f	m	a	b	b	q	i	n	y	k	p	i	r	v	p
y	i	c	t	e	p	o	r	w	s	i	g	z	n	b	o
h	ŭ	g	h	a	p	i	p	i	e	d	f	m	a	s	o
w	o	a	y	i	f	m	o	n	y	y	o	x	r	i	e
p	i	f	j	j	x	k	l	q	n	v	g	h	i	j	a
s	t	a	o	p	t	ŭ	s	f	e	m	i	h	a	a	x
a	q	q	n	i	e	e	s	g	j	y	n	o	f	m	e
e	h	i	a	s	t	v	e	g	p	i	y	x	o	z	a
b	s	e	n	n	e	p	r	i	f	y	d	y	z	x	e
h	i	f	k	i	n	w	a	ŭ	p	r	g	g	ŭ	h	n
f	k	d	x	d	n	i	ŭ	m	f	w	e	ŭ	e	s	t
v	e	h	l	c	y	q	k	s	b	i	x	x	n	z	w
o	f	f	k	k	y	p	i	i	n	e	i	s	i	q	a
l	m	ŭ	t	y	e	p	n	n	j	e	ŭ	q	s	o	b
a	l	t	t	j	c	q	j	ŭ	i	z	g	n	c	a	w
k	j	j	ŭ	o	i	p	f	j	e	v	s	a	a	m	c
o	f	d	k	a	h	m	e	h	i	ŭ	s	u	y	y	f
i	f	s	e	a	n	w	y	m	o						

Doc ID: 6587345 Doc Ref ID: A2972105

1	7	2	10	6	12	9	4	15	11	16	5	14	8	3	13
.	.	.	.	.	.	.	.	.	.	.	.	.	.	o	a
r	c	p	y	.	i	h	m	e	.	.	l	v	g	y	.
e	m	.	.	.	r	n	y	.	y	v	w	y	l	.	.
.	i	n	p	y	t	v	o	d	.	.	.	.	m	a	h
ŭ	y	z	.	.	a	o	.	.	n	a	h	.	y	z	k
.	p	y	o	a	.	o	z	.	.	e	m	y	w	i	h
.	.	.	q	q	a	z	e	h	i	f	l	y	w	k	k
.	e	l	n	z	p	i	.	i	a	w	y	g	y	f	m
e	v	i	y	z	r	h	.	y	p	i	f	m	ŭ	o	a
v	a	f	g	j	x	l	.	n	t	y	s	y	h	q	r
w	a	n	t	z	o	w	.	d	a	a	f	m	o	z	p
i	f	m	y	y	x	ŭ	a	r	n	v	y	y	l	i	m
a	i	t	p	i	e	z	ŭ	ŭ	b	o	o	w	k	f	y
b	f	m	t	i	e	p	a	a	x	c	w	e	d	g	r
y	p	i	w	ŭ	s	c	i	c	s	o	n	r	b	d	f
r	ŭ	g	f	m	p	a	p	h	t	a	y	s	e	w	i
k	p	i	n	g	x	q	l	o	e	z	y	y	p	i	m
y	w	s	m	a	e	p	p	i	r	g	o	y	l	d	p
i	n	w	x	o	q	i	e	p	i	m	o	o	e	z	g
a	p	i	f	m	a	b	b	q	i	n	y	k	p	i	r
v	p	y	i	c	t	a	z	w	s	i	g	z	n	b	o
h	ŭ	g	h	a	p	i	p	i	e	d	f	m	a	s	o
w	o	a	y	i	f	m	o	n	y	y	o	x	r	i	e
p	i	i	g	a	n	w	e	ŭ	i	s	t	a	o	p	t
ŭ	s	f	e	m	i	h	a	a	x	a	q	q	n	i	e
e	s	g	j	y	n	o	f	m	e	e	h	r	o	a	p
i	a	s	t	v	e	g	p	i	y	x	o	z	a	b	s
e	n	n	e	p	r	i	f	y	d	k	r	y	z	x	e
h	i	f	k	i	n	w	a	ŭ	p	r	.	g	ŭ	h	n
f	k	d	x	d	n	i	ŭ	m	f	w	.	ŭ	e	s	t
v	e	h	l	c	y	q	k	s	b	i	.	x	n	z	w
o	f	f	k	k	y	p	i	i	n	e	.	s	i	q	a
l	m	ŭ	t	y	e	p	n	n	j	e	.	q	s	o	b
a	l	t	t	j	c	q	j	ŭ	i	z	.	h			

Doc ID: 6587345 Doc Ref ID: A2972105

Appendix 20

1	7	2	10	6	12	9	4	15	11	16	5	14	8	3	13
.	.	.	.	.	.	.	.	.	.	.	.	.	.	c	a
r	c	p	y	.	i	h	r	r	.	.	m	e	l	v	.
g	y	.	.	.	e	m	m	.	g	r	n	y	y	.	.
.	v	w	y	l	t	v	o	d	.	.	.	.	p	i	m
a	h	ŭ	.	.	y	z	.	.	a	o	n	.	a	h	y
.	z	k	o	z	.	e	m	.	.	y	w	i	h	q	q
.	.	.	a	z	e	h	i	f	l	y	w	k	k	e	l
.	n	z	p	i	i	a	.	w	y	g	y	f	m	e	v
i	y	p	i	f	m	ŭ	.	o	a	v	a	f	g	j	x
l	g	s	w	h	z	m	.	e	a	a	v	i	g	g	z
b	j	a	h	v	a	n	.	t	z	o	w	d	a	a	f
m	o	z	p	í	f	m	y	y	x	ŭ	a	r	n	v	y
y	l	i	m	a	i	t	p	i	e	z	ŭ	ŭ	b	g	l
b	f	m	t	i	e	p	a	a	x	c	w	e	d	g	r
y	p	i	w	ŭ	s	c	i	c	s	o	n	r	b	d	f
r	ŭ	g	f	m	p	a	p	h	t	a	y	s	e	w	i
k	p	i	n	g	x	q	l	o	e	z	y	y	p	i	m
y	w	s	m	a	e	p	p	i	r	y	l	d	p	i	n
w	x	o	q	i	e	p	i	m	o	o	e	z	g	a	p
i	f	m	a	b	b	q	i	n	y	k	p	i	r	v	p
y	i	c	t	e	p	o	r	w	s	i	g	z	n	b	o
h	ŭ	g	h	a	p	i	p	i	e	d	f	m	a	s	o
w	o	a	y	i	f	m	o	n	y	y	o	x	r	i	e
p	i	f	j	j	x	k	l	q	n	v	g	h	i	j	a
s	t	a	o	p	t	ŭ	s	f	e	m	i	h	a	a	x
a	q	q	n	i	e	e	s	g	j	y	n	o	f	m	e
e	h	i	a	s	t	v	e	g	p	i	y	x	o	z	a
b	s	e	n	n	e	p	r	i	f	y	d	y	z	x	e
h	i	f	k	i	n	w	a	ŭ	p	r	g	g	ŭ	h	n
f	k	d	x	d	n	i	ŭ	m	f	w	e	ŭ	e	s	t
v	e	h	l	c	y	q	k	s	b	i	x	x	n	z	w
o	f	f	k	k	y	p	i	i	n	e	i	s	i	q	a
l	m	ŭ	t	y	e	p	n	n	j	e	ŭ	q	s	o	b
a	l	t	t	j	c	q	j	ŭ	i	z	g	n	c	a	w
k	j	j	ŭ	o	i	p	f	j	e	v	s	a	a	m	c
o	f	d	k	a	h	m	e	h	i	ŭ	s	ŭ	y	y	f
i	f	s	e	a	n	w	y	m	o						