Transcription of Memorandum by Parker Hitt

Demonstration of Kryha Cipher Machines

January 11th, 1930

Original Material Provided by Frode Weierud

Transcribed by Philip Marks, November 2009

INTER-OFFICE MEMORANDUM

DATE **January 11th, 1930.**

TO MR. A. K. CLOKEY

FROM COLONEL PARKER HITT

SUBJECT Demonstration of Kryha Ciphering Machine

On January 7th, Mr. Bancroft and I were given a demonstration of the Kryha Ciphering machines by Mr. G. A. Evalenko and Mr. Kryha at 545 Fifth Avenue.

The demonstration verified my previous description of the mechanical operation of the portable model which was obtained through a study of the literature on the machines (Memo of Dec. 3, 1929).

The electric machine proved to be a very simple adaptation of the portable machine, combined with two electric typewriters and the necessary connecting wires.

The usual claims of absolute indecipherability were made for messages prepared by these machines.

On the following day, Mr. Bancroft went alone to Mr. Evalenko's office and had a series of messages enciphered for test purposes. These ciphers were turned over to me on the morning of the 9th. Before noon I had deciphered ten of them. A long message in a different key was deciphered by the following morning.

The solution of these ciphers is submitted herewith for comparison with the original messages which I have not seen but which, I believe, are in your possession.

The ciphers were prepared on the electric machine which started out by making an error in the long message. There were also two other errors in the long message attributable to error by the machine.

The deciphering of these ciphers confirms my opinion expressed in my memorandum of December 3, 1929 that "the Kryha machine is dangerous and unsound and offers no safety against modern attack".

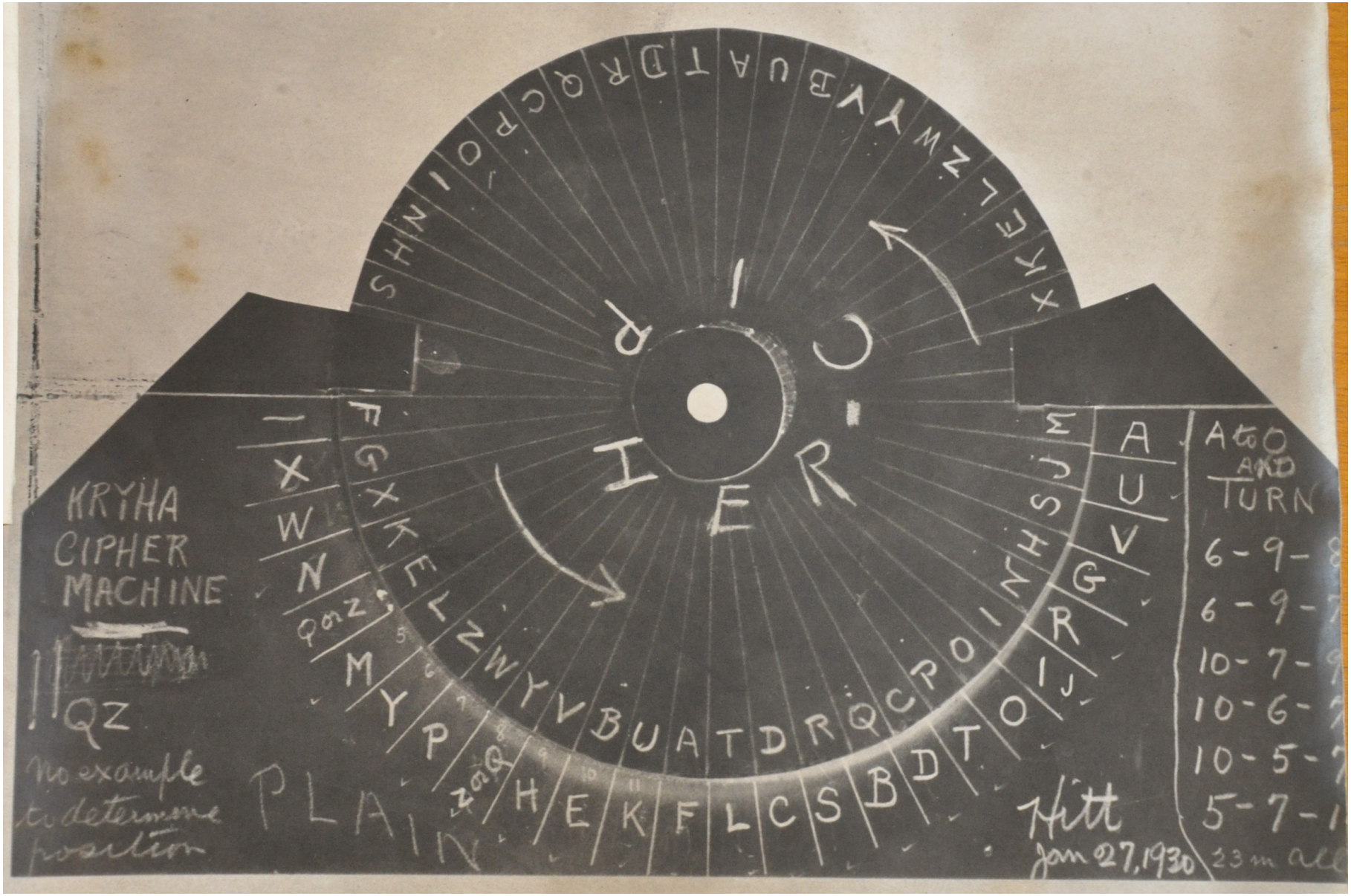
Parker Hitt

2 Incls.

Enclosures not received for file

(This notation taken from yellow copy which was destroyed) *D.J.I*

per JM


KRYHA
CIPHER
MACHINE
QZ
No example
to determine
position
PLAIN
Hitt
Jan 27, 1930
A to O
AND
TURN
6-9-
6-9-
10-7-
10-6-
10-5-
5-7-
23 m

KEY A TO O, SHIFT 6-9-8-10-6-9-7-8-10-7-9-8-10-6-7-9-10-5-7-6-5-7-10

YGJAW BICFJ BOGCB CYUHO BDGNE DFXET AHAJE TIDIS ZOXAU GRIDH UTKUK RLWCD
CLOSI NG▪DA TE▪▪A LL▪BI D▪JUL Y▪FIF TEENT H▪▪LA TE▪BI DS▪NO T▪ACC EPTED

RJCWY CGLOM PSIIK MIMJM RSFAV YNBWU RAVQL JEXMJ TFMQZ IFEAB KGHWZ OCIDB
REFER ENCE▪ ▪CONT RACT▪ GHOST —RIVE R▪PRO JECT▪ ADVIS E▪EXP ECTED COMPL

GXNBR LQOLT SAGPF BPPYG
ETION ▪DATE ▪URGE NT▪▪▪

GVJUS CRCKE SOPUB HLJAM JYIBZ YDBXW IWAXL MAYBI DXLHQ LNDYX ZTHQR OJVWT
PROCE ED▪IM MEDIA TELY▪ MILLS —CITY —REPO RTING ▪ON▪A RRIVA L▪TO▪ C▪I▪B

GJAGE SMKZN WGZOB NPUKN CBFIT
ECKET T▪HOT EL▪VI CTORI A▪▪▪▪

DTOYT WSYZO WOQCD STIFX RDWHD WIKVC WHXTN DRJWW TZAHS KJIKJ TSNSR MCPHQ
JACK▪ ▪ADVI SES▪N OTHIN G▪▪AV AILAB LE▪TH ERE▪H AVE▪Y OU▪TR IED▪▪ JONSO

IBIAA BJRLS FDZHQ
N▪OR▪ MARTI N▪▪▪▪

WJEIW BICGP SXHAE ZNUNZ KXGHE YPUVN SADDW EVZWU WWHUC BNEFT DBDSR FCYAA
LEAVI NG▪TO MORRO W▪▪SP ECIAL ▪TRAI N▪FOR ▪ST▪L OUIS▪ ▪RESE RVE▪▪ ROOMS

CMOQE PVRTK AJOYQ ZKVY
▪STAT LER▪▪ SELF▪ AND▪

YWYRY ZAVVD ALEGX ETESJ MDWMU NTQHI RDGQK EUJMS YHCHC FZIQX TFERY YPUQR
CONTR ACT▪S IGNED ▪TODA Y▪▪WI LL▪FO RWARD ▪DETA ILS▪▪ BY▪MA IL▪TO NIGHT

IDDHB CJWOV NVFYY JBNSM ZJZAG YFPED WALDE EBJWO JAAJG GFYBZ OOSNR FYWLP
▪▪HAV E▪BEE N▪ADV ISED▪ LEASE ▪▪WIL L▪NOT ▪BE▪R ENEWE D▪CAN ▪YOU▪ RETUR

IBFVA JXYSK
N▪AT▪ ONCE▪

BVMWM HJCYX VOHZE WNMLD KDWPG HIFWU UAUDD EOEFH ZVUZI GNFFK PMQCZ ENMS▪
BRIEF S▪▪AN DERSO N▪CAS E▪▪RE CEIVE D▪NOW ▪ABOU T▪HEN DRYS— AFFID AVEB▪

SKMGT AVYLT DDJRQ KBBYG
YOUEX PECTE D▪TO▪ GET▪▪

MYPBX WWGEV PEUJE MTUNP JJWSL WKEID WUIRL WVDZG LVJZI INOJK YFSMV YIRJQ
MILLS ▪HERE ▪REPO RT▪SO ME▪▪C ANCEL LATIO NS▪AN D▪GEN ERAL▪ SLOWI NG▪DO

OTGIH WMBUP CCQUL
WN▪NE W▪BUS INESS

VYSNA MPBAM WPFKK EBNKV HDWTQ MFLKZ EAQIV JSBWS CFXHH YDKUL PLDPR OCIGF
SITUA TION▪ SHAFT ▪SEVE N▪▪BA D▪SOM E▪CAV ING▪A ND▪▪M UCH▪W ATER▪ COMIN

TBOFW JSQHK UJFVB BHPYG
G▪THR OUGH▪ CEILI NG▪▪▪

TFCCG GSEVI XQIAK ELJQH KCWSB HTVJA IEURW HFDHY UOLHX ETWNI OZWWR SFMBR
OFFIC IAL▪R EPORT ▪ELEV EN▪▪O CLOCK ▪THIR TY▪SE VEN▪K ILLED ▪ONE▪ TWENT

SBZUG IOSVK
Y▪MIS SING▪

NVNJX WIBIN OCSXO ECHJF AYYUX YJGUG TTHMG RNGGI RBCHN CIJAP DZUJQ LXWYT
XRBXS ▪GOKG X?G?K ▪GKTX OIXCK UKX▪ OXIZS KXLIG XXS▪? PI?XS ROPXX ▪?TXB

METCQ QFNDE
?*IF*▪? *KXXXX* (? indicates indeterminate Q or Z)

RAIZT HWUQE XAOCU VGUMI BJXSV BBOXW IJHQG HITIU DXFDC BIANY YTSFM LTMEW
RUSH▪ SHIPM ENT▪▪ MY▪OR DER▪T WENTY ▪FIRS T▪ALL ▪OUT▪ ▪ITEM S▪ONE ▪SEVE

IBFIK LXDQT
N▪AND ▪NINE

KEY A to I
NVNJX WIBIN etc
**IS*C ARTER* etc

FWKPT MYEON TYZCU EABJV ONXQL PBWBG OGXD▪ HWYBY LVTZG CFMNK PEGCE RRRFV
YOUR▪ TELEG RAM▪▪ ▪DATE ▪PROC EED▪▪ AS▪OU TLINE D▪KEE P▪ME▪ ADVIS ED▪OF

CLUZB PCVTK
▪*RESU LTS*▪▪

RJINF MTCAP BVFZU FDESM OTHSG VWFJO EKXEH MEDKC YAJHV KFVNX ULCWR SCIFP
RESUL TS▪NO T▪AS▪ GOOD▪ ▪AS▪E XPECT ED▪HE RE▪GO ING▪T O▪SEA TTLE▪ TOMOR

AKKCA
ROW▪▪

~~16.~~ LTUST FBCGY XVGBP JJLMX OIFNA YFXES PWABU MEDFN JEXRJ XIMLP UWPSB
KAY▪▪ OF▪TH E▪▪OP INEON ▪YOUR ▪▪FIG URESA RE▪OV ER▪OP TOMIS TIC▪R

RAJCU XBFIK LJUBS AJZHQ.
ECHEC K▪AND ▪ADVI SE▪▪▪

~~17.~~ IQJPJ WLAXN TOQZL WCUZD PZGAK WDYKH DMYNR DELWQ QOLDS BFMEJ KTVWP
▪WORK ▪PROG RESSI NG▪▪S ATISF ACTOR ILY▪N EED▪T WENTY ▪▪MOR E▪MEN

LBVXA VBIKA WVEJK.
▪FIRS T▪OF▪ WEEK▪

~~18.~~ VJYDT NCINO VOEVL KYUGV FWXRC YFEVM VHXAU VIFZP GWSZC VKUUI PPKOM
SEND▪ CONFI DENTI AL▪RE PORT▪ ▪▪CAU SE▪DA M▪FAI LURE▪ AND▪D AMAGE

LRYBW CLMZN LMITO.
▪DONE ▪RUSH ▪▪▪▪B

~~19.~~ IDNPW JIGVD MKRGZ EVZQV EDKQI PFQBF RWGJY DIWDY VYIZC XNOLZ YTGCD
▪▪BRI DGE▪S PICER ▪CREE K▪GON E▪▪▪A RRANG E▪OPE RATE▪ TRAIN S▪VIA

LJIGR LOUEA SPHQK SDZOO.
▪▪MIT CHEL▪ TOWN▪ ▪▪▪VN

~~20.~~ QVEDW BICVQ UAUCU VRJQM HYBWV DFQMO EHRNM KDLWK YHAHZ MBCNZ UOESR
GRADI NG▪▪D ONE▪▪ MILE▪ NINET Y▪▪ST EEL▪L AID▪M ILE▪S SEVEN TY▪▪▪

IYACF CLMZN LIOWQ ADLMW WPAPQ.
SEVEN ▪RUSH ▪RAIL S▪AND ▪TIES

CLOSING DATE ALL BIID JULY FIFTEENTH LATE BIIDS NOT ACCEPTED

REFERENCE CONTRACT GHOST RIVER PROJECT ADVISE EXPECTED COMPLETION DATE URGENT

PROCEED IMMEDIATELY MIILLS CITY REPORTING ON ARRIVAL TO C II BECKETT HOTEL VICTORIA

JACK ADVISES NOTHING AVAILABLE THERE HAVE YOU TRIED JONSON OR MARTIN

LEAVING TOMORROW SPECIAL TRAIN FOR ST LOUIS RESERVE ROOMS STATLER SELF AND

CONTRACT SIGNED TODAY WILL FORWARD DETAILS BY MAIL TONIGHT

  HAVE BEEN ADVISED LEASE WILL NOT BE RENEWED CAN YOU RETURN AT ONCE

BRIEFS ANDERSON CASE RECIEVED HOW ABOUT HENDRYS AFFIIDAVIIT YOUEXPECTED TO GET

MILLS HERE REPORT SOME CANCELLATIONS AND GENERAL SLOWING DOWN NEW BUSINESS

SITUATION SHAFT SEVEN BAD SOME CAVING AND MUCH WATER COMIING THROUGH CEILING

OFFICIAL REPORT ELEVEN OCLOCK THIRTY SEVEN KILLED ONE TWENTY MISSING

 IS CARTER PREPARED TO LEAVE AT ONCE FOR CANYON CIITY AND SPOKANE

RUSH SHIPMENT MY ORDER TWENTY FIIRST ALL OUT ITEMS ONE SEVEN AND NINE

18-20-1 Đ23 wheel.
mixed alphabet.

FEB 28 1930

Steps in Analyzing the 20 Kryha Ciphers Prepared with a Single Key.

1. Write messages so that initial letters, second letters, third letters, etc. are in column.
2. Prepare frequency table for each column.
3. Combine obviously equivalent columns.
4. Tentatively choose space, E, and common consonants.
5. Apply to text.
6. Prepare messages in blocks of 14 to 25 columns.
7. Analyze for identical cipher letters having probable meanings as found in 4.
8. Pick out the block best meeting this analysis. (This determines number of groups of teeth on gear wheel).
9. Using this Block, begin to pick out words through use of 2 and 4.
10. As words develop, start a two way similarity table.
11. Continue 9 and 10 simultaneously until 10 is practically completed. This will give most of the gear tooth spacing.
12. Make up a cipher disk with letters running according to horizontal similarity lines and a plain text disk with available letters chosen from vertical similarity (Method 7).
13. Using these disks, determine all gear tooth spacing through trial on proved words.
14. Complete plain text disk and translation of messages.

PH: FIS

Transcription Notes

- *Original material was in the form of a monochrome photocopy (white letters on black background) and in places is hard to read (especially the page headed (1)), so there is a possibility of transcription errors. Transcription was from digital images of the original photocopies. Some pages were cut off on the right hand side and a small amount of material may have been lost.*
- *No particular attempt has been made to exactly reproduce the layout of the original document.*
- *The stepping pattern has been reconstructed by combining information from the image of Hitt's "paper analog" of the Kryha machine, information at the top of the page headed (1), and analysis of the sample messages (to determine the value of the 23rd step, which is not completely visible on either page).*
- *The first set of initials at the bottom of the first page may be "D.T.J" rather than "D.J.I.".*
- *The range of displacement values in the Kryha stepping pattern shown in this document (5 through 10) seems much closer to what one would expect from examination of machines and other historical documents than the stepping pattern shown in Hitt's memorandum of 2-3 December, 1929. This reinforces the impression that the December solution used simulated messages that were constructed based on an understanding of the machine from documents rather than messages encoded on the machine itself. The introductory memorandum on the first page makes it clear that Hitt did not see the actual machine until January, 1930, and the paper analog on the second page is dated January 27th.*
- *There must have been an operator or machine error when rendering message 8 on the page headed "(1)" - one character is missing from the short group "ENMS". It has been transcribed with an extra spacing character at the end of the group so as to most closely resemble the original, but a more likely value for the group is "ENSMS". A similar problem occurs in message 14 in the group "OGXD".*
- *There is a handwritten error in the decoded plaintext of message 16 of the page headed "(3)". The word "OPINION" decodes correctly from the ciphertext, rather than yielding "OPINEON" as shown – the error has been retained in the transcript.*
- *The fair copy of the decrypted messages on the page beginning "CLOSING DATE" shows odd typing errors where the letter I does not print clearly – this may be because the same position in the plaintext alphabet is used to represent both the letters I and J. The resulting character has been rendered as II.*