Transcription of Handwritten Notes by Parker Hitt

Notes on Decipherment of Kryha Ciphers
Progress of the Attack

2nd – 3rd December, 1929

Original Material Provided by Frode Weierud

Transcribed by Philip Marks, November 2009

Notes on Decipherment of Kryha Ciphers
Progress of the Attack

1. First 26 letters of each intercepted message prepared to give 26 columns of letters (Page 1)
2. Frequency table for each column prepared (Pages 2 & 3)
3. Messages scanned for repetitions and underlined (P 4)
4. Note made of the HW, HWJ, HWJG in first columns. Try TH, THE, THE-. Appears OK.
5. Other assumptions made as noted on Pages 4 to 7 in colors and assumed letters entered in Frequency tables Pages 2 and 3.
6. Noted that P. 2 & 3 columns 2 and 12, 3, 13 and 24, 5 and 15, 6, 16 and 26, 9 and 19, 10 and 20 were identical. This added letters to all these columns which did not appear in them. Also verified or suggested many of the assumptions. (Page 2 & 3)
7. Order of letters for plain text plotted with intervals (Page 8) and a general decision reached as to the order of the letters in the plain text alphabet. (bottom of Page 8)
8. Letters of the cipher alphabets placed against corresponding plain text letters as determined by frequency tables. (Page 9) After six of these cipher alphabets had been so superimposed, the whole cipher alphabet was indicated and also the first five increments of shift to the right.
9. Preparation of sliding plain text – cipher alphabet. Determination of the whole series of ds. (Page 10).
10. Verification of results by decipherment of the whole of Message No. 1. (Page 11)

Parker Hitt
2 Dec 1929.

Nineteen messages (first 26 letters only) in KRYHA cipher and assumed to have been intercepted from a radio station controlled by the State Department.

```
1.  R S C G D G P M Y A Z Z T Q E G T P K Y B L X J K O
2.  S M J D E G D O P A R Z S A A S C S K B C U S Z N Z
3.  H R L H R Z E Q Y V K B J R E P K C Y K V I E G U Z
4.  H W J G Y G X B U W B L Q F R Y R D E K K H L F E F
5.  T V H N M X F R K G R F H Q C F P T P B R Q K G N B
6.  E F H T B B F O Y W R O P D E K K D Y W I I J E Y B
7.  Q L B B A D N Z K Y K I H F Z F H I J T B C J F K O
8.  F T C H J Z D M C N J U P K A F H X J K Q C J M V N
9.  O L X M A Z Y O M B R E H R D P P D Y C F C Y H B G
10. H W J G N X F N A U K F S A Y I K D Q W J L U O Q Z
11. Q L D H B X L X S B U S H L S F B V P L F U Z G U O
12. E F H M A W Y O H B U S H F U G E F L W V I T H T C
13. H W J M A F E B I B P L J D R N N P Q Y H G C J U I
14. C R S H E Z D O P A R Z S R R Y K X D B P U S Z D N
15. H W P F R P I M P R S S E D R P P P K Y E I K H D V
16. O L R H B P A Z U N N P J R D D E L U O N L D Q C I
17. I U J M S F K Q Q N S G H D A U T W L A B Q J P T F
18. F L X Y E I M X Y G H O N N K G Y B E I K G K X V D
19. S Z J C T X Y M A O S A H V T T R P R N B G J K Q B
```

The plain text letters in colors were determined from frequency, from assumptions on pages 4 to 7 and from column similarities.

Kryha Cipher
Frequency table of first 13 Columns

	1	2	3	4	5	6	7	8	9	10	11	12	13	
A	A	S			E IIII		L I		I II	P III		S I		**A**
B		C	Q I	U I	R III	D I		A II		- IIII	M I	C I	Q	**B**
C	L I		R II	P I	F				I				R	**C**
D			F I	A I	T I	S I	- III		M				F	**D**
E	I II	F	O		S III		H II		L			F I	O I	**E**
F	D II	N II		S I		- II	E III					N II		**F**
G			S	- III		E III				I II		I	S	**G**
H	T IIIII		- III	E IIIII					D I		S I		- IIIIIII	**H**
I	I	M				I I	F I		S I			M I		**I**
J			E IIIIII		C I						I		E III	**J**
K			M			U	I		T II	S	E III		M	**K**
L		E IIIII	K I				I I		A			E II	K	**L**
M		L I		R IIII	I I		O I	T IIII	Y I			L		**M**
N				D I	P I	N	T I	S I		E III	Q I		I	**N**
O	S II	-	H					R IIIII		O I		- II	H	**O**
P		U	I I			A II			E III		B I	U I	I II	**P**
Q	R II		N					E II	C I				N I	**Q**
R	F I	A II	V I		- II			C I	B	R I	O IIIII	A	V	**R**
S	P II	O I	T I		I				G I		N I	O III	T III	**S**
T	B I	I I	P	O I	A I	V						I	P I	**T**
U		I							R II	D I	T II	I		**U**
V		Y I								N I		Y		**V**
W		H IIII				G I				T II		H		**W**
X			C II			R IIII	P I	N II					C	**X**
Y				I I	D I	F	A III		- IIII	H I				**Y**
Z		R I				T IIII		- II			U I	R III		**Z**
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	
		12	*13*		*15*	*16*			*19*	*20*		*2*	*3*	
			24			*26*							*24*	

The plain text letters in colors were determined from frequency, from assumptions on pages 4 to 7 and from column similarities.

Kryha Cipher

Frequency table of second 13 Columns

	14	15	16	17	18	19	20	21	22	23	24	25	26	
A	- II	E III				I	P I							**A**
B		R	D	I	I		- III	E IIII			Q	I	D IIII	**B**
C		F I		I	Y I		I	I	III	G I	R	I	I	**C**
D	N IIII	T II	S I		E IIII	M I				I	F	II	S I	**D**
E		S III	.	- II		L II		R I		P I	O I	I		**E**
F	T III		- IIII		M I			II			II		- II	**F**
G			E III				I		N III		S III		E I	**G**
H				II		D		A I	I		- III			**H**
I			I I		I	S	I	H I	E IIII				I II	**I**
J		C				II		S I		- IIIII	E II			**J**
K	I	I	U I	R IIII		T III	S III	- II		E III	M I	II	U	**K**
L	I				F I	A II	I		- III	I	K			**L**
M		I				Y					I			**M**
N	I	P	N I	O I			E I	M I				I II	N II	**N**
O							O I				H I		III	**O**
P			A III	T III	- IIII	E II		I			I I		A	**P**
Q	O II					C II		I	R II		N I	A II		**Q**
R	S IIII	- IIII		E II		B I	R	P I			V			**R**
S		I	I		I	G				II	T			**S**
T		A I	V I	S II	H I		I			R I	P	II	V	**T**
U		H I	I			R I	D		III	T I		- III		**U**
V	H I				I		N	T II				E III	I	**V**
W			G		I		T III						G	**W**
X			R		O II					II	C I		R	**X**
Y		D I	F II	I		- III	H III			I		I	F	**Y**
Z		O I	T							I	I		T III	**Z**
	14	**15**	**16**	**17**	**18**	**19**	**20**	**21**	**22**	**23**	**24**	**25**	**26**	
		5	*6*			*9*	*10*				*3*		*6*	
			26								*13*		*16*	

Black – underline
Orange – 1st assumption
Green – 2nd "
Blue – 3rd "

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
				_		*E*																				
1.	R	S	C	G	D	G	P	M	Y	A	Z	Z	T	Q	E	G	T	P	K	Y	B	L	X	J	K	O
			E			*E*	_	*R*			*O*															
2.	S	M	J	D	E	G	D	O	P	A	R	Z	S	A	A	S	C	S	K	B	C	U	S	Z	N	Z
	T			*E*		*T*																				
3.	H	R	L	H	R	Z	E	Q	Y	V	K	B	J	R	E	P	K	C	Y	K	V	I	E	G	U	Z
	T	*H*	*E*	_		*E*																				
4.	H	W	J	G	Y	G	X	B	U	W	B	L	Q	F	R	Y	R	D	E	K	K	H	L	F	E	F
			_								*O*		_													
5.	T	V	H	N	M	X	F	R	K	G	R	F	H	Q	C	F	P	T	P	B	R	Q	K	G	N	B
	I	*N*	_					*R*			*O*															
6.	E	F	H	T	B	B	F	O	Y	W	R	O	P	D	E	K	K	D	Y	W	I	I	J	E	Y	B
		E			*E*								_													
7.	Q	L	B	B	A	D	N	Z	K	Y	K	I	H	F	Z	F	H	I	J	T	B	C	J	F	K	O
				E		*T*	_																			
8.	F	T	C	H	J	Z	D	M	C	N	J	U	P	K	A	F	H	X	J	K	Q	C	J	M	V	N
	S	*E*	*C*	*R*	*E*	*T*	*A*	*R*	*Y*	_	*O*	*F*	_													
9.	O	L	X	M	A	Z	Y	O	M	B	R	E	H	R	D	P	P	D	Y	C	F	C	Y	H	B	G
	T	*H*	*E*	_																						
10.	H	W	J	G	N	X	F	N	A	U	K	F	S	A	Y	I	K	D	Q	W	J	L	U	O	Q	Z
		E		*E*						_	*T*	*O*	_													
11.	Q	L	D	H	B	X	L	X	S	B	U	S	H	L	S	F	B	V	P	L	F	U	Z	G	U	O
	I	*N*	_	*R*	*E*	*G*	*A*	*R*	*D*	_	*T*	*O*	_													
12.	E	F	H	M	A	W	Y	O	H	B	U	S	H	F	U	G	E	F	L	W	V	I	T	H	T	C
	T	*H*	*E*	*R*	*E*	_				_																
13.	H	W	J	M	A	F	E	B	I	B	P	L	J	D	R	N	N	P	Q	Y	H	G	C	J	U	I
				E		*T*	_	*R*			*O*															
14.	C	R	S	H	E	Z	D	O	P	A	R	Z	S	R	R	Y	K	X	D	B	P	U	S	Z	D	N
	T	*H*																								
15.	H	W	P	F	R	P	I	M	P	R	S	S	E	D	R	P	P	P	K	Y	E	I	K	H	D	V
	S	*E*		*E*																						
16.	O	L	R	H	B	P	A	Z	U	N	N	P	J	R	D	D	E	L	U	O	N	L	D	Q	C	I
			E	*R*		_							_													
17.	I	U	J	M	S	F	K	Q	Q	N	S	G	H	D	A	U	T	W	L	A	B	Q	J	P	T	F
		E	*C*																							
18.	F	L	X	Y	E	I	M	X	Y	G	H	O	N	N	K	G	Y	B	E	I	K	G	K	X	V	D
			E				*A*						_													
19.	S	Z	J	C	T	X	Y	M	A	O	S	A	H	V	T	T	R	P	R	N	B	G	J	K	Q	B

1. Typed. Previous work.
2. Red – 4th assumption.
3. Orange – 5th assumption.
4. Green – 6th assumption.
5. Blue – 7th assumption.

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
		O		_		E			_	P		R														
1.	R	S	C	G	D	G	P	M	Y	A	Z	Z	T	Q	E	G	T	P	K	Y	B	L	X	J	K	O
	P	L	E	A	S	E	_	R	E	P	O	R	T													
2.	S	M	J	D	E	G	D	O	P	A	R	Z	S	A	A	S	C	S	K	B	C	U	S	Z	N	Z
	T	A	K	E	_	T	H	E	_				E	S		A			_							
3.	H	R	L	H	R	Z	E	Q	Y	V	K	B	J	R	E	P	K	C	Y	K	V	I	E	G	U	Z
	T	H	E	_		E		A				E			_			E								
4.	H	W	J	G	Y	G	X	B	U	W	B	L	Q	F	R	Y	R	D	E	K	K	H	L	F	E	F
			_			R					O		_				T									
5.	T	V	H	N	M	X	F	R	K	G	R	F	H	Q	C	F	P	T	P	B	R	Q	K	G	N	B
	I	N	_		R			R	_		O			N				E	_							
6.	E	F	H	T	B	B	F	O	Y	W	R	O	P	D	E	K	K	D	Y	W	I	I	J	E	Y	B
	R	E			E								_													
7.	Q	L	B	B	A	D	N	Z	K	Y	K	I	H	F	Z	F	H	I	J	T	B	C	J	F	K	O
				E		T	_																			
8.	F	T	C	H	J	Z	D	M	C	N	J	U	P	K	A	F	H	X	J	K	Q	C	J	M	V	N
	S	E	C	R	E	T	A	R	Y	_	O	F	_	S	T	A	T	E	_							
9.	O	L	X	M	A	Z	Y	O	M	B	R	E	H	R	D	P	P	D	Y	C	F	C	Y	H	B	G
	T	H	E	_		R							T					E								
10.	H	W	J	G	N	X	F	N	A	U	K	F	S	A	Y	I	K	D	Q	W	J	L	U	O	Q	Z
	R	E	F	E	R	R	I	N	G	_	T	O	_													
11.	Q	L	D	H	B	X	L	X	S	B	U	S	H	L	S	F	B	V	P	L	F	U	Z	G	U	O
	I	N	_	R	E	G	A	R	D	_	T	O	_													
12.	E	F	H	M	A	W	Y	O	H	B	U	S	H	F	U	G	E	F	L	W	V	I	T	H	T	C
	T	H	E	R	E	_	H	A	S	_	B	E	E	N	_											
13.	H	W	J	M	A	F	E	B	I	B	P	L	J	D	R	N	N	P	Q	Y	H	G	C	J	U	I
	L	A	T	E	S	T	_	R	E	P	O	R	T	S	_											
14.	C	R	S	H	E	Z	D	O	P	A	R	Z	S	R	R	Y	K	X	D	B	P	U	S	Z	D	N
	T	H			_				E					N	_	A	T									
15.	H	W	P	F	R	P	I	M	P	R	S	S	E	D	R	P	P	P	K	Y	E	I	K	H	D	V
	S	E		E	R								E	S	T											
16.	O	L	R	H	B	P	A	Z	U	N	N	P	J	R	D	D	E	L	U	O	N	L	D	Q	C	I
			E	R		_		E					_													
17.	I	U	J	M	S	F	K	Q	Q	N	S	G	H	D	A	U	T	W	L	A	B	Q	J	P	T	F
		E	C		S			N	_																	
18.	F	L	X	Y	E	I	M	X	Y	G	H	O	N	N	K	G	Y	B	E	I	K	G	K	X	V	D
	P	R	E			R	A						_													
19.	S	Z	J	C	T	X	Y	M	A	O	S	A	H	V	T	T	R	P	R	N	B	G	J	K	Q	B

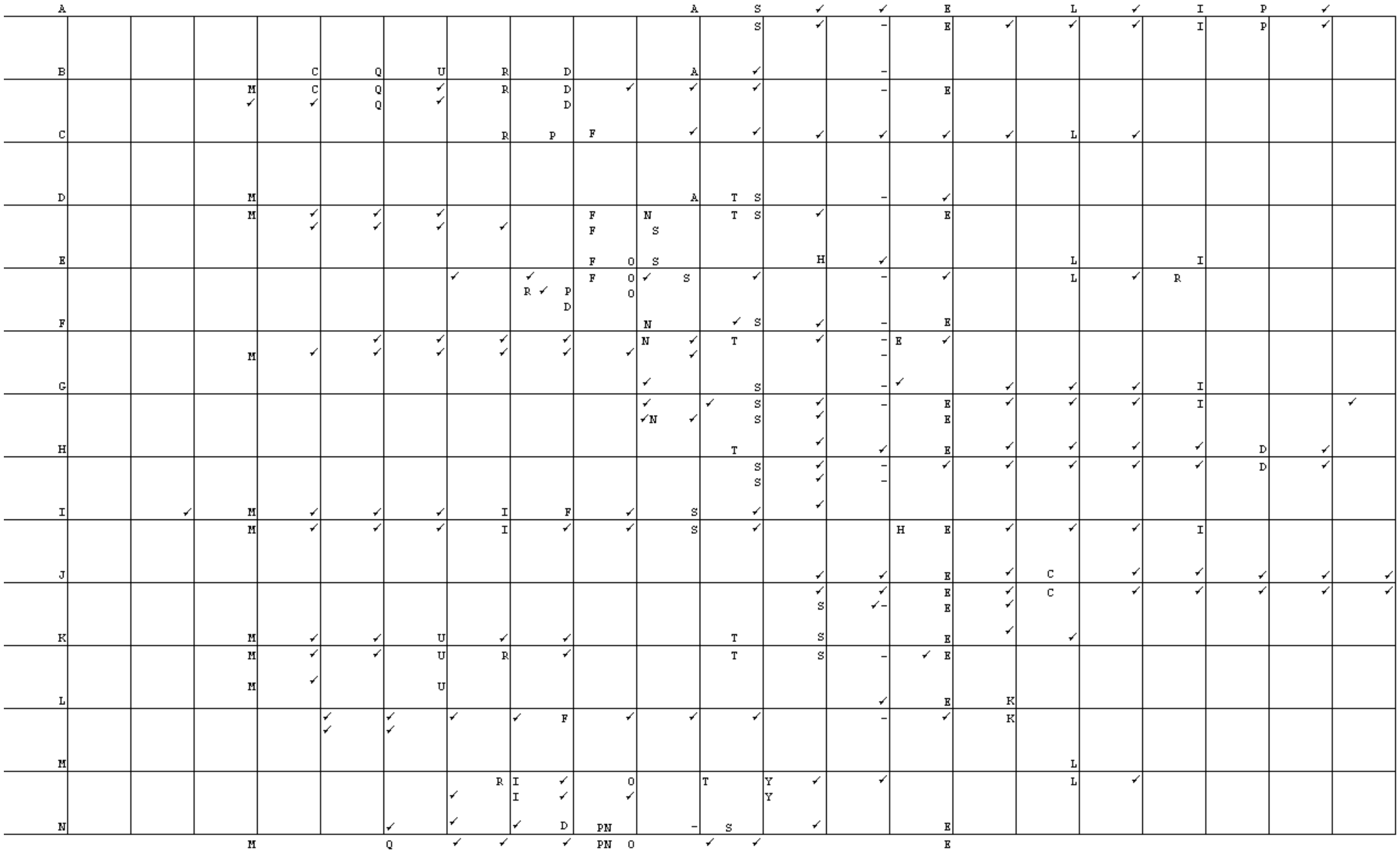
1. Typed. Previous work.
2. Red – 8th assumption.
3. Orange – 9th assumption.
4. Green – 10th assumption.
5. Blue – 11th assumption.

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
	F	O	*R*	_	*T*	E		*T*	_	P	*U*	R	*P*	*O*	*S*	*E*	*S*	_	*T*	*H*	*E*	_		*E*		
1.	R	S	C	G	D	G	P	M	Y	A	Z	Z	T	Q	E	G	T	P	K	Y	B	L	X	J	K	O
	P	L	E	A	S	E	_	R	E	P	O	R	T	_	*E*				*T*	_						
2.	S	M	J	D	E	G	D	O	P	A	R	Z	S	A	A	S	C	S	K	B	C	U	S	Z	N	Z
	T	A	K	E	_	T	H	E	_	*N*	*E*	*C*	E	S	*S*	A	*R*	*Y*	_	*S*	*T*	*E*	*P*	*S*	_	
3.	H	R	L	H	R	Z	E	Q	Y	V	K	B	J	R	E	P	K	C	Y	K	V	I	E	G	U	Z
	T	H	E	_	*D*	E		A		*T*		E			_	*F*		E		*S*						
4.	H	W	J	G	Y	G	X	B	U	W	B	L	Q	F	R	Y	R	D	E	K	K	H	L	F	E	F
	B	*Y*	_	*D*	*I*	R	*E*	*C*	*T*	*I*	O	*N*	_	*O*	*F*	_	T	*H*	*E*	_			*E*	*S*		
5.	T	V	H	N	M	X	F	R	K	G	R	F	H	Q	C	F	P	T	P	B	R	Q	K	G	N	B
	I	N	_	*O*	R	*D*	*E*	R	_	*T*	O	_	*I*	N	*S*	*U*	*R*	E	_	*T*		*E*		*O*		
6.	E	F	H	T	B	B	F	O	Y	W	R	O	P	D	E	K	K	D	Y	W	I	I	J	E	Y	B
	R	E			E			_	*T*	*H*	*E*		_			_					*E*					
7.	Q	L	B	B	A	D	N	Z	K	Y	K	I	H	F	Z	F	H	I	J	T	B	C	J	F	K	O
	D	*I*	*R*	E	*C*	T	_	*T*					*I*		*E*	_		*O*		*S*						
8.	F	T	C	H	J	Z	D	M	C	N	J	U	P	K	A	F	H	X	J	K	Q	C	J	M	V	N
	S	E	C	R	E	T	A	R	Y	_	O	F	_	S	T	A	T	E	_					_		
9.	O	L	X	M	A	Z	Y	O	M	B	R	E	H	R	D	P	P	D	Y	C	F	C	Y	H	B	G
	T	H	E	_	*P*	R	*E*	*S*	*I*	*D*	*E*	*N*	T	_	*D*	*I*	*R*	E	*C*	*T*	*S*	_				
10.	H	W	J	G	N	X	F	N	A	U	K	F	S	A	Y	I	K	D	Q	W	J	L	U	O	Q	Z
	R	E	F	E	R	R	I	N	G	_	T	O	_			_			*E*					*S*	_	
11.	Q	L	D	H	B	X	L	X	S	B	U	S	H	L	S	F	B	V	P	L	F	U	Z	G	U	O
	I	N	_	R	E	G	A	R	D	_	T	O	_			*E*				*T*	*T*	*E*		_		
12.	E	F	H	M	A	W	Y	O	H	B	U	S	H	F	U	G	E	F	L	W	V	I	T	H	T	C
	T	H	E	R	E	_	H	A	S	_	B	E	E	N	_	*N*	*O*	_	*C*	*H*	*A*	*N*	*G*	*E*	_	
13.	H	W	J	M	A	F	E	B	I	B	P	L	J	D	R	N	N	P	Q	Y	H	G	C	J	U	I
	L	A	T	E	S	T	_	R	E	P	O	R	T	S	_	*F*	*R*	*O*	*M*	_						
14.	C	R	S	H	E	Z	D	O	P	A	R	Z	S	R	R	Y	K	X	D	B	P	U	S	Z	D	N
	T	H	*I*	*S*	_	*A*	*F*	*T*	E	*R*	*N*	*O*	*O*	N	_	A	T	_	*T*	*H*	*R*	*E*	*E*	_		
15.	H	W	P	F	R	P	I	M	P	R	S	S	E	D	R	P	P	P	K	Y	E	I	K	H	D	V
	S	E	*V*	E	R	*A*	*L*	_					E	S	T							_				
16.	O	L	R	H	B	P	A	Z	U	N	N	P	J	R	D	D	E	L	U	O	N	L	D	Q	C	I
			E	R		_		E	*C*		*N*		_		*E*		*S*				*E*			*I*		
17.	I	U	J	M	S	F	K	Q	Q	N	S	G	H	D	A	U	T	W	L	A	B	Q	J	P	T	F
	D	E	C	*I*	S	*I*	*O*	N	_	*I*	*S*	_				*E*						*N*	*E*	*C*		
18.	F	L	X	Y	E	I	M	X	Y	G	H	O	N	N	K	G	Y	B	E	I	K	G	K	X	V	D
	P	R	E			R	A	*T*	*I*		*N*		_					_			*E*	*N*				
19.	S	Z	J	C	T	X	Y	M	A	O	S	A	H	V	T	T	R	P	R	N	B	G	J	K	Q	B

```
1. Typed.  Previous work.
2. Red – 12th assumption.
```

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
	F	O	R	–	T	E		T	–	P	U	R	P	O	S	E	S	–	T	H	E	–		E		
1.	R	S	C	G	D	G	P	M	Y	A	Z	Z	T	Q	E	G	T	P	K	Y	B	L	X	J	K	O
	P	L	E	A	S	E	–	R	E	P	O	R	T	–	E				T	–					*I*	*T*
2.	S	M	J	D	E	G	D	O	P	A	R	Z	S	A	A	S	C	S	K	B	C	U	S	Z	N	Z
	T	A	K	E	–	T	H	E	–	N	E	C	E	S	S	A	R	Y	–	S	T	E	P	S	–	*T*
3.	H	R	L	H	R	Z	E	Q	Y	V	K	B	J	R	E	P	K	C	Y	K	V	I	E	G	U	Z
	T	H	E	–	D	E	*P*	A	*R*	T	*M*	E	*N*	*T*	–	F	*E*	E	*L*	S	–					–
4.	H	W	J	G	Y	G	X	B	U	W	B	L	Q	F	R	Y	R	D	E	K	K	H	L	F	E	F
	B	Y	–	D	I	R	E	C	T	I	O	N	–	O	F	–	T	H	E	–	*P*	*R*	E	S	*I*	*D*
5.	T	V	H	N	M	X	F	R	K	G	R	F	H	Q	C	F	P	T	P	B	R	Q	K	G	N	B
	I	N	–	O	R	D	E	R	–	T	O	–	I	N	S	U	R	E	–	T	*H*	E	–	O		*D*
6.	E	F	H	T	B	B	F	O	Y	W	R	O	P	D	E	K	K	D	Y	W	I	I	J	E	Y	B
	R	E	*Q*	*U*	E	*S*	*T*	–	T	H	E	*M*	–	*T*	*O*	–					E		–			
7.	Q	L	B	B	A	D	N	Z	K	Y	K	I	H	F	Z	F	H	I	J	T	B	C	J	F	K	O
	D	I	R	E	C	T	–	T		*E*			I		E	–		O		S			–		*E*	*N*
8.	F	T	C	H	J	Z	D	M	C	N	J	U	P	K	A	F	H	X	J	K	Q	C	J	M	V	N
	S	E	C	R	E	T	A	R	Y	–	O	F	–	S	T	A	T	E	–					–		*E*
9.	O	L	X	M	A	Z	Y	O	M	B	R	E	H	R	D	P	P	D	Y	C	F	C	Y	H	B	G
	T	H	E	–	P	R	E	S	I	D	E	N	T	–	D	I	R	E	C	T	S	–	*T*	*H*	*A*	*T*
10.	H	W	J	G	N	X	F	N	A	U	K	F	S	A	Y	I	K	D	Q	W	J	L	U	O	Q	Z
	R	E	F	E	R	R	I	N	G	–	T	O	–			–			E					S	–	
11.	Q	L	D	H	B	X	L	X	S	B	U	S	H	L	S	F	B	V	P	L	F	U	Z	G	U	O
	I	N	–	R	E	G	A	R	D	–	T	O	–	*T*	*H*	E	–	*M*	*A*	T	T	E	*R*	–		
12.	E	F	H	M	A	W	Y	O	H	B	U	S	H	F	U	G	E	F	L	W	V	I	T	H	T	C
	T	H	E	R	E	–	H	A	S	–	B	E	E	N	–	N	O	–	C	H	A	N	G	E	–	*I*
13.	H	W	J	M	A	F	E	B	I	B	P	L	J	D	R	N	N	P	Q	Y	H	G	C	J	U	I
	L	A	T	E	S	T	–	R	E	P	O	R	T	S	–	F	R	O	M	–						*N*
14.	C	R	S	H	E	Z	D	O	P	A	R	Z	S	R	R	Y	K	X	D	B	P	U	S	Z	D	N
	T	H	I	S	–	A	F	T	E	R	N	O	O	N	–	A	T	–	T	H	R	E	E	–		
15.	H	W	P	F	R	P	I	M	P	R	S	S	E	D	R	P	P	P	K	Y	E	I	K	H	D	V
	S	E	V	E	R	A	L	–	*R*	*E*	*Q*	*U*	E	S	T	*S*	–	*F*	*R*	*O*	*M*	–				*I*
16.	O	L	R	H	B	P	A	Z	U	N	N	P	J	R	D	D	E	L	U	O	N	L	D	Q	C	I
			E	R		–		E	C	*E*	N		–	*N*	E		S		*A*		E	*R*	–	I		–
17.	I	U	J	M	S	F	K	Q	Q	N	S	G	H	D	A	U	T	W	L	A	B	Q	J	P	T	F
	D	E	C	I	S	I	O	N	–	I	S	–				E			*L*		–	N	E	C	*E*	*S*
18.	F	L	X	Y	E	I	M	X	Y	G	H	O	N	N	K	G	Y	B	E	I	K	G	K	X	V	D
	P	R	E	*P*	*A*	R	A	T	I	*O*	N	*S*	–	*H*	*A*	*V*	*E*	–	*B*	*E*	E	N	–	*M*	*A*	*D*
19.	S	Z	J	C	T	X	Y	M	A	O	S	A	H	V	T	T	R	P	R	N	B	G	J	K	Q	B

Order of Plain Text Letters (From Frequency Tables, Pages 2 and 3)



```
A to A Cipher      C   QEFSR  AHO                       T              Not given by
       Plain    MCLQURIDPFNOATSY-HEK                B,G,V,W,X,Z   above table
```

Combination of Plain Text and Cipher Alphabets
(From Frequency Tables, Pages 2 and 3)

```
Plain                M C L Q U R I D P F N O A T S Y – H E K            (B
1st Column Cipher        C       Q E F S R       A H O
```

```
                           B                         ↓?  ↓?
                           ↓                         _   _
Plain                M C L Q U R I D P F N O A T S Y – H E K
2nd Column Cipher    I B M   P Z T       E F S R   A V O
                                                     _
                                                     H
```

Cipher shifts 3 letters to right. $d_1 = 3$

```
                                                 ?V  ?   ↓?
                                                 _↓  _   ↓
Plain                M C L Q B U R I D P F N O A T S Y – H E K            (V
3rd Column Cipher    K X(I)B(M)   C P(Z)T D Q E(F)S G(A)H O J L             R
                                                   _     _
                                                   R     V
```

Cipher shifts 2 letters to right. $d_2 = 2$

```
                          ?                                   ?     ?     ?
                         ___                                  _     _     _
Plain                M C L Q B U R I D P F N O A T V S Y   – H   E K
4th Column Cipher     (J L K X I)B M Y N C(P)(Z)T D(Q)(E)F(SR) G(?A) H(V0)
                       _________                            __
                           ?                                V
```

Cipher shifts 3 letters to right. $d_3 = 3$

```
                          ?                                   ?     ?      ?
                         ___                                  _     _      _
Plain                M C L Q B U R I D P F N O A T V  S Y   – H   E  K
5th Column Cipher    (O)J (L K X)(I)B M Y N C(P)(Z)T D (Q) E(F)(S)(R)(G)(?) A (H)(V)
                          _____
                            ?
```

Cipher shifts 1 letters to right. $d_4 = 1$

```
                          G                                    ?       ?      ?
                          ↓                                    _       _      _
Plain                M C L Q B U R I D P F N O A T V S  Y   –  H   E  K    (
6th Column Cipher    (H)(V)(O) J   K X I B (M) Y N (C) P Z T D (Q)(E) F (S)(R) G (?)(A) (V
```

Cipher shifts 2 letters to right. $d_5 = 2$

(Editor's note: some information not completely visible on the original document is missing from the right hand side of this page)

We now have ample material to construct a sliding pair of alphabets.

```
Plain Text       MCLQGBURIDPFNOATVS(?Y)-(?H)E(?K)
       KXIBMYNCPZTDQEFSRG?AHVOJWLKXIBMYNCPZTDQEFSR
```

Cipher → moves to the right by increment d.

The unknown letters of the plain text are W, X, Z; the single letter in question in the cipher alphabet is the letter between G and A which must be U. This is verified when we reach the 9th Column of the cipher.

The increments d indicate the number of teeth in each of the unknown number of blocks in the variable gear wheel. We have already determined increments d_1 to d_5 and by the same process, (aided by the sliding alphabets) the others are quickly determined. The whole series is

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

making a total of 43 teeth in 17 blocks.

All variables are now determined and the series of messages under study can be quickly deciphered by the use of the sliding alphabets moved according to the increments d.

Parker Hitt
3 December, 1929

Message No. 1, Kryha Cipher.

```
 3 2 3 1 2 3 2 4 2 6 1 2 1 3 2 1 5
R S C G D G P M Y A Z Z T Q E G T
F O R * T E S T * P U R P O S E S

P K Y B L X J K O Q D J O N G J A
* T H E * W E L L * K N O W N * S

H N C Q K E N X N C P Z S D B P P
E N T E N C E * Q U O T E * T H E

K N C N W H Q V A J I S V D T R F
* Q U I C K * B R O W N * F O X *

J U T G J W F S U K C X H N K N G
J U M P S * O V E R * T H E * L A

R F E L I G X I Z R J H E W X R U
Z Y * D ) G S * B A C K * U N Q U

H A L A O M V A C R I W P U V Y S
O T E * W I L L * B E * U S E D *

V N Y O Z C O G D P B V W O W L
B Y * A L L * S T A T I O N S *
```

Decipherment by alphabets and increments determined as indicated.

Hitt

Transcription Notes

- *Original material was in the form of a monochrome photocopy (white letters on black background) and in places is very hard to read, so there is a distinct 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 care was taken to reproduce exactly the original layout – the emphasis was on readability.*
- *Page 1 (as numbered by Hitt; first two pages are not numbered). Last 6 messages are very hard to read, but all messages are repeated on pages 4 through 7 and the ciphertexts have been recovered from there.*
- *Pages 2 and 3. Vertical bars have been used to represent Hitt's tally marks.*
- *Pages 4 through 7. From Hitt's notes at the top of each page, it is clear that colored pencils were used to enter recovered plaintext letters on the original notes, but of course this information is lost on the monochrome copies. It is possible to guess the order in which Hitt proceeded with the recoveries, but there is plenty of room for error, especially on Pages 6 and 7.*
- *Page 8 is very hard to read in places, especially in one column where the original was folded (one column to the right of the aligned As). Hitt's original table was written onto squared graph paper with an inner grid size smaller than each handwritten letter. No attempt has been made to reproduce the inner grid; the outer grid corresponds to the squares in the transcription. In addition, on the original some checkmarks and dashes near the boundaries of the outer grid were not carefully placed and it is hard to be sure in which square they should be located.*
- *Page 9 presents challenges in aligning transcribed characters in a way that corresponds to the handwritten original; these have been addressed by using different size fonts.*
- *The original document contained slips of paper bound between pages 9 and 10 with typewritten versions of the recovered alphabets and displacements. These were obviously used as an aid to decryption of the sample messages, but do not add any information to the main body of the document and have not been included in the transcription.*
- *The recovered stepping patterns are puzzling in that they do not correspond to any version of the Kryha machine that has been described in the cryptographic literature. They do, however, correspond exactly to a common version of the control wheel found in early models of the Kryha machine. These models produce displacements that are equal to a constant factor plus the number of teeth in the active segment of the control wheel; at the time of transcription it was not clear whether the constant factor is 3 or 4, but evidence from historical documents strongly suggests that it is 4. So Hitt's ciphertexts were either produced from an earlier version of the machine or perhaps via an experimental, manual encipherment based on partial knowledge of the machine. Other documents from the same source indicate that the first actual demonstration of the machine to Hitt by Alexander von Kryha and G. A. Evalenko (holder of the North American rights to the machine) took place on January 7th, 1930, thus after Hitt's solution of the sample messages. This fact, together with the content of the sample texts, makes the latter hypothesis more likely (would Alexander von Kryha, for example, have been likely to use "the quick brown fox" as a sample plaintext?). A later document from February, 1930, shows much more realistic stepping patterns, though from an entirely different control wheel.*