A World War II German Army Field Cipher and How We Broke It

CHARLES DAVID

In 1942 the U.S. Army Signal Corps was looking for college graduates to train in radar work, which was then new and promising. I enlisted, and after six months of pre-radar courses in calculus, physics, chemistry, and radio theory at Rutgers University, I found myself in Camp Crowder, Missouri, the Signal Corps basic training center.

Once I was there, a classification sergeant informed me that Camp Murphy, the radar facility in Florida, was overcrowded and that I'd be assigned to some other training. Checking my academic record and Army Classification Test score, he suddenly asked me if I had ever heard of "cryptography."

As he thumbed through his manual, my memory reverted to a cryptanalysis course that my fiancée had taken at Brooklyn College, given by Professor Jack Wolfe of the math department. She and I would sit in a sunny meadow in Prospect Park, and I helped with the frequency counts. My reverie was broken by the information that I was to be sent to Vint Hill Farms Station, near Warrenton, Virginia – close enough to my New York home and my wife-to-be to please me no end.

Vint Hill was an unusual army camp – in a bucolic setting, with evergreen trees surrounding the barracks and woods all around. It was a hush-hush place, and we were constantly warned to keep it so. One of its two parts was devoted to cryptanalysis studies, and the other was a working radio facility.

The students were men of strong academic backgrounds and achievements. Of course, there was a large supporting cast of administrative cadre who tormented us with the usual army routine – drills, hikes, KP, inspections, and the like. However, there was communion among the "crypt" people as a result of the learning atmosphere and the intellectual interest engendered by these new and uncommon studies.

Our classes were taught by sergeants. Once in a while an officer would appear from Arlington Hall, but Vint Hill was an enlisted men's camp and school. We religiously followed the texts of William Friedman and considered him our mentor. Men left after unpredictable time periods to join active units in both main theaters of the war. Most seemed to end up in our own signal centers and were involved with security matters.

After seven months I was called in for an interview, and I was asked if I knew any German. I had studied the language for two years in high school and was able to read and translate a newspaper handed to me by an officer. He said that would do just fine, and I was assigned to a special class being formed.

The new class of about thirty men was taught by a very bright Sergeant Dineen. He had just returned from Arlington Hall where he had been briefed on two German systems – one a lower-grade code and the other a medium-grade field cipher which the British had started to break. We learned about the cryptographic nature of the systems and then something of the analysis procedures. I knew then that working on them would be intriguing beyond compare. I found out I was right when I got a chance to work on the cipher as a member of Signal Security Detachment D, an element of General Omar Bradley's Twelfth Army Group.

In April 1944, I and other embryonic codebreakers debarked from a large troop ship in the bombed-out port of Liverpool, England. Our group was brought to London and billeted near Marble Arch. The next day we were brought to an apartment building on Weymouth Street that had been given to the Signal Corps for its intelligence work. A number of comrades and I were assigned to a breaking section working on the German army medium-grade cipher. We had been familiarized with it during our last month at Vint Hill and were told that the British had made good progress with the breaking. The system was used by all levels of the German army, from army groups on down, seemingly where the highest-level means (Enigma) were not necessary or available. The encryption method was a clever variation of the Playfair that rendered breaking very difficult. We called it NI, short for Non-Indicator, as the early intercepts showed no indicator. To the enemy it was Doppelkastenschlüssel (Two-Box Cipher).

At Weymouth Street it became apparent that all the operational work was performed by us enlisted men. This contrasted with the British army, where our equivalents were officers. Our men and officers were mostly professional people and scholars. On the whole they were older than the average G.I.

Our first weeks were spent on practice problems and perfecting our skills. We also took a class in military German. Although all of the men had had some past school contact with the language, this taught us likely army vocabulary. Oddly, however, many of the people who succeeded best in codebreaking had limited facility with German. The language experts, both trained and German-born, tended to see more than really was present in cipher text, and they neglected the more important principles as frequency and combination, which led to gradual but surer results.

Soon we were thrown in with the earlier arrivals, and we began to work on current intercepts. Before the 1944 invasion, the enemy signal units on the Atlantic Wall practiced their cryptography and radio transmission constantly. Often they sent personal messages, newspaper articles, nursery rhymes, and the like. As they practiced, so could we, and thus our skills were improved.

When the Normandy invasion began, the breaking proceeded apace. We gleaned both tactical and strategic information that was coordinated with other forms of signal intelligence, such as direction finding and traffic analysis. As our armies pressed inland, it was decided to form a mobile unit to accompany the advancing allied armies. This was necessary for two reasons. Firstly, our radio-intercept companies had to be near the front

in order to read enemy traffic more accurately. Secondly, they could send intercepts to us quickly by messenger.

I was chosen for this unit along with a mixture of the newer and the more experienced men. The unit was called Signal Security Detachment D, afterwards always S.S.D.D., and it was commanded by Lieutenant Colonel Charles Allen. We were attached to General Omar Bradley's Twelfth Army Group, but we always stayed by ourselves in the field.

S.S.D.D. consisted of various sections representing all phases of signal intelligence:

1. Cipher-breaking Team. This was my group. It was headed by Sergeant Howard Arnold, a fine cryptanalyst from Providence, Rhode Island, who later became president of a large department store in his home city. Besides continuing his own breaking activity, Howard supervised the group in a laid-back and thoughtful manner.

2. Codebreaking Section, headed by Sergeant James Wallace of North Dakota, a skilled and assiduous codebreaker. After the war Jim became a newspaper columnist in Brainerd, Minnesota. The enemy used code for lower-grade messages and for smaller units. He and his men were very successful.

3. Traffic Analysis Group was the largest. It studied message headings, radio frequencies, code signs of sending and receiving units, volumes of traffic, and more to derive indications of enemy placements and intentions. Led by Sergeant George Bauer, it was consistently productive.

4. Direction-finding Team, headed by my tentmate Sergeant Leonard Netzorg, successful Yale Law School graduate. It located and identified enemy units by triangulating bearings. Len later became an eminent attorney in Portland, Oregon; his career and views were the subject of a recent magazine article.

5. Emending Section. These German language experts removed mistakes from interpreted deciphered messages. Much of what was broken was so garbled that it required people very conversant in the language to make it coherent. Sergeant Hyman Sobel, a Harvard instructor, was in charge. The group's members were amazed at how we cryptanalysts broke traffic that was so full of errors, and we were surprised at their ability to make it understandable.

6. Intelligence Coordination Section. This group collated the information, evaluated it, and passed reports based on it to the Twelfth Army Group headquarters. It was headed by a very bright Master Sergeant Samuel Lieberman, whose ability was respected by all of us.

There was also a small photographic unit, a signal center, and the usual administrative personnel, motor transport, mess people, etc.

S.S.D.D. landed in Normandy. We started by living in the field and working under tents. We bivouacked in the countryside near such towns as Coutances, Laval, Chartres, and Meaux, and in the tiny Lorraine village of Mangiennes. Then came three months in the city of Luxembourg, where we were quartered in a school not far from the

headquarters of Generals Bradley and Dwight Eisenhower in the Hotel Alfa. After the Battle of the Bulge in December 1944, we went through parts of Belgium, entered Germany at Aachen, and after four months of movement, ended the war in Forchheim, north of Nuremberg.

As noted previously, all the operational work was performed by enlisted men. Many of the officers were sent by the Signal Corps to supervise subsidiary functions, such as transport and billeting, and had little knowledge of our work. Occasionally, men from the intercept units drifted in and out of the central groups, seemingly to absorb some notion of what was being done. Of course we had our own intelligence officers, and two in particular deserve special note for their hands-on attitude and productive work.

The officer supervising my cipher-breaking section was the very erudite Captain Benjamin Schwartz. He was a family man, over forty-five, who had volunteered to contribute his expertise to the war effort. Schwartz was skilled in Sanskrit, other ancient Indic languages, and several modern tongues, and he had headed departments for those exotic languages in the New York Public Library and the Library of Congress. He instructed us in cryptanalysis, watched over our daily efforts, and assumed a rather paternal role toward his men. He was a person who cared, and that meant a great deal.

Captain Howard Mendel supervised the traffic analysis team. He worked at it incessantly, and he was an intelligent and effective participant throughout. He was wounded in Luxembourg when a stray airplane bullet went through his side, but much to the relief of his men, their Howie soon recovered and came back.

Soon after we landed, an unexpected development struck our cipher-breaking section. Many of the approximately sixteen cryptanalysts – no matter how adept they had been in training classes – seemed unable to cope with a real-life situation in which a solution might not exist. A substantial portion of the enemy traffic could not be solved, and this uncertainty created a psychological barrier that stopped men before they started. As a consequence, many faltered and produced few results.

Four of our men did most of our breaking. They were George Hussey of Bronxville, New York, and Eric Porter of El Segundo, California, who worked marvelously together, Howard Arnold, and this writer.

Though we were the signal intelligence arm of the Twelfth Army Group, S.S.D.D. traveled by itself in the field. We were an isolated outfit, known only to the intelligence people. Our security and secrecy were superb, even within the outfit. People in one section knew very little about the doings in other sections. On a few occasions, senior officers from headquarters stopped by to express appreciation for our results, and they would mention a specific case or two that were outstanding.

Our daily intelligence production was notable from the start, but it reached a crescendo during the three months in Luxembourg. Our deciphered intercepts, traffic analysis, and direction finding indicated unusual enemy activity before the Battle of the Bulge began on 16 December 1944. I judge that people at army group headquarters simply

did not evaluate these data properly. It probably seemed impossible to them for the Germans to stage a major armored offensive over unfavorable terrain, especially when most of their forces were tied up on the Russian front. After the Ardennes offensive was stopped a month later, the cipher section broke the radio traffic to the German units retreating from the Bulge. It revealed the detailed instructions to each unit as to exactly where it should be virtually every minute of the day. With the skies now clear, the Allied air forces made very effective use of this information.

In January, S.S.D.D. moved again through different parts of Belgium and entered Germany, remaining there until the end of the war. We stayed near Cologne, crossed the Rhine at Remagen, camped at Bad Wildungen, and were in Forchheim, Bavaria, on VE Day. We then moved to the town of Russelsheim, where everyone wondered what our destination would be in the war with Japan. But that soon ended, and gradually we worked our separate ways home.

Many of us had a strong affection for S.S.D.D. Our fellow soldiers were often quite accomplished and thoughtful. There were professors, attorneys, classical musicians, writers, and businessmen – all on their way to join the hopeful postwar world.

A short, personal epilogue: Several years later, I visited Captain Schwartz in Washington, D.C. He had stayed in the army and had become a colonel in Army Signal Intelligence. We were happy to see each other and had much to discuss. He thanked me for my wartime efforts and then offered me an immediate commission to reenlist and come to work with him. I'm afraid that my destiny was as a civilian, but it was gratifying to have the praise and appreciation of the boss.

NI DESCRIPTION AND BREAKING

The medium-grade field cipher was called "Doppelkastenschlüssel" – Two-Box Cipher – by the Germans. Because the first messages when intercepted by the British bore no indicator, the Allies called it the Non-Indicator or NI system.

The NI was used from army groups to all lower units down to company level and carried both tactical and strategic information. It ranked just below the Enigma, the high-grade electromechanical machine cipher. The Enigma could not be distributed to the multitude of lower field units, and thus the NI served as a more practical hand system.

During the North African campaign, the British overran a German signal center and discovered the nature of the system.

System Rules

The NI cipher combines a transposition, or more precisely, a seriation of the plain text, and then two Playfair-like encipherments. The apparatus of the system consists of two 5x5 random-alphabet squares (which omit J) such as those in figure 1.

Box 1					Box 2				
K	X	N	Z	Y	G	S	A	O	R
E	M	O	B	P	V	F	H	Z	W
L	Q	F	V	I	B	N	Y	C	Q
R	A	W	G	U	U	I	E	M	X
H	S	C	D	T	K	L	D	P	T

Fig. 1. Enciphering boxes

A plaintext bigram, say EU, is enciphered by finding the first letter in Box 1 and the second letter in Box 2. In this case E is on row 2 of Box 1, and U is on row 4 of Box 2. The two letters are considered as diagonal corners of a rectangle, and the intermediate cipher bigram is those two letters which complete the rectangle, namely VR.

Box 1					Box 2				
K	X	N	Z	Y	G	S	A	O	R
E	M	O	B	P	V	F	H	Z	W
L	Q	F	V	I	B	N	Y	C	Q
R	A	W	G	U	U	I	E	M	X
H	S	C	D	T	K	L	D	P	T

Fig. 2. First encipherment

The bigram VR is now itself enciphered just as the original plaintext bigram was and the resultant diagonals form the final cipher letters – QZ.

Box 1					Box 2				
K	X	N	Z	Y	G	S	A	O	R
E	M	O	B	P	V	F	H	Z	W
L	Q	F	V	I	B	N	Y	C	Q
R	A	W	G	U	U	I	E	M	X
H	S	C	D	T	K	L	D	P	T

Fig. 3. Second encipherment

In this way EU becomes QZ in cipher.

If the two letters of a bigram to be encrypted lie along the same line in both boxes, we take the letters immediately to the left as cipher values. These we called liners. For example, DL = KC. The rectangular cases we called diagonals.

Box 1					Box 2				
K	X	N	Z	Y	G	S	A	O	R
E	M	O	B	P	V	F	H	Z	W
L	Q	F	V	I	B	N	Y	C	Q
R	A	W	G	U	U	I	E	M	X
H	S	C	D	T	K	L	D	P	T

Fig. 4. Linear encipherment

For cryptanalytic purposes it is important to see that four combinations of diagonals (D) and liners (L) exist:

	D-D	D-L	L-D	L-L
Plain text	en	ea	gi	yr
Intermediate	FL	HK	UW	OZ
Cipher text	NC	TT	XP	HM

The seriation of the plain text consists of writing in blocks of two lines of twenty-one letters each. For example, using the first line of Heine's poem "Die Lorelei":

Ich weiss nicht was soll es bedeuten
dass ich so traurig bin

and replacing the common *ch* combination with *q*:

```
i q w e i s s n i q t w a s s o l l e s b
e d e u t e n d a s s i q s o t r a u r i

g b

i n
```

The *vertical* bigrams (I-E, Q-D, W-E, etc.) are the pairs actually enciphered:

```
G G Y Q Q D C M A R N E R Q W M B G Q T B
i q w e i s s n i q t w a s s o l l e s b
e d e u t e n d a s s i q s o t r a u r i
U Z Y Z S Z I Q I Q I Y A R U F S T Z U N

X B
g b
i n
P O
```

The cipher text is then read off horizontally in groups of five letters for transmission.

```
GGYQQ   DCMAR   NERQW   MBGQT   BUZYZ   SZIQI   WIYAR
UFSTZ   UNXBP   O
```

German Communication Protocols

Each German division had its own set of cipher boxes. It was assigned six different boxes for each day. These were paired in different combinations for each day's eight three-hour periods. In effect, there were eight keys per day.

The German encipherers followed certain conventions, though they grew lax as the war progressed. They placed an X before and after all numbers, proper names, place names, sentences, within abbreviations, and at the end of plain texts having an odd number of letters. As a result, plaintext X had an abnormally high frequency and tended to mask the identification of the usual high-frequency German letters.

The word *zwei* ("two") was changed to *zwo*, and *ch* plain text was changed to *q*, distorting the frequency of *q* also. The use of occasional "quatsch" (German for nonsense) sequences was encouraged to distort combinations and frequencies.

All in all, the Germans seemed to feel that the NI system was impervious to timely cryptanalysis. They had readied a different system on general security grounds but kept the NI right to the end.

Some Cipher Security Considerations

The seriation (vertical reading of the plaintext bigrams) ensured that the enciphered bigrams were not same letter combinations of normal German text. The most frequent ciphertext bigrams certainly did not reflect the most frequent German combinations (*en, er, ei, ie, in*, etc.). What the ciphertext bigrams did reflect was the individual frequencies of disconnected German letters taken two at a time. The most frequent NI cipher bigram had a good possibility of representing plaintext *ee*, for example, but this was by no means always the case.

Even knowing the mechanics of the system, we found that the reconstruction of the cipher boxes was extremely difficult because of the double encipherment feature. No doubt the German signal experts counted heavily on this.

By using different boxes for each division and by changing the boxes every three hours of every day, the Germans made the cipher uncomfortably close to a one-time pad system – unbreakable in theory and practice. Nevertheless we broke it and, generally, in useful time.

AIDS TO CRYPTANALYSIS: THE INITIAL BREAKS

Each message was preceded by three-letter callsigns of the sending and receiving units and the time of day. Our traffic analysis teams were quite adept at identifying them. This plus the assigned radio frequency used aided in sorting the messages by unit – and therefore by key.

In cryptanalyzing the NI system, we used very large sheets of paper, colored pencils, and good erasers. These sheets and colors cannot be fairly reproduced in a journal. I will describe our analytic tools, show how we used them, and then leave it to the initiative of the reader to complete the analysis to reach the final plain text.

```
1205
MXY    A-V D L V V K X R K C X V R B X A B A S K D
URT      D F X E G K M N Z I W B T A W P F Y O K E

       B-G K S Q A V I S K S N U T E K O C K C G F
         V U A Z N R I M Z R W I F G K K K L T T D

       C-W P N M Y Y K G C C D Y M W O K F I S M Q
         T D Q Y C X K D Y P O P I S Z F L S O A E

       D-U Q D O U N K I N D H G O Y P H M K N Y B
         I Q M Q Y D K B F A G Q D M D A A I O Y F

       E-D O E R F B P V P U
         L K D I O R E M Q O

1215
REX    F-M U M V I B V O
IXY      P Q K O I W D U

1240
ZBT    G-K L O A Z W S E Z U C K S P K O T X C Y U
QLS      K S L F Q M F D X D P Z Q X N M O V K D S

       H-C X S Z O K W
         K C A C M K P

1305
RLS    I-K N D C V M K S A N I L Y S M C A P W B Q
BNQ      K S U P O K Z K A Q I K C L S K W S X C G

       J-Y K C S I U T O S G M D O G K K C K O O H
         W L D M Z Z P K A S Y A R Z K Q M K V Z B

       K-N C F Y K F
         L U T T Z A
```

```
1340
DEF     L-K U G Y X K W S K R M K A U O V H K K N C
GHI       K K B W W Z H M M Z U K E B K B G K F I P

        M-V C G D S O L C K O K I W A S V K F S U A
          B Q Q O V S R P L K Q I B F R M K S X I N

        N-S N O O V A
          A Z M K R P


1350
POR     O-T C K U
CLV       N U K O

1415
QZB     P-V D L V V K B U O U S H W V D Y E B Q O G
LTS       D F X E G K Z W Z K A Z X D F P D O A Z Q

        Q-K F U K Y L K U G O K I X W Z L O X F K C
          K P D K E W I D V K T M M X C S N R X B P

        R-X P B T M K F O T L S C D A N I M P S P Z
          N Q F B D K S Z Q P A A B R I I P Q A X T
```

Fig. 5. Transcribed messages for a single period

Usually we needed a sufficient number of letters in the same key to make inroads into the cipher. We were delighted if many more letters arrived for a three-hour period, but often not enough traffic was intercepted to afford us an entry.

To illustrate the solution of the cipher, I have composed a sample problem of eighteen lines of cipher text supposedly intercepted from units of one division during a three-hour period. Also listed are the times of transmission and the callsigns of the sending and receiving radio stations. Each pair of lines is given a line identification letter (see Fig. 5).

The messages have been manipulated to allow showing a number of techniques in a relatively short space. This sample is much less difficult than the messages we encountered, although the language is typical of the German radio traffic of the time.

Knowing how the system worked, we were able immediately to rewrite the intercepted messages in two lines of twenty-one letters each. Once the messages were in this form, we made a bigram frequency – one of our most useful tools. The count was made in a 25x25 matrix on graph paper.

Each line of the problem was given an identifying letter at the left, as can be seen in figure 6. When a bigram was entered on the frequency count, that line-identification letter was entered in the appropriate square instead of a tally mark allowing us to locate the occurrences rapidly (see Fig. 6).

With the frequency count as a guide, we attacked the messages using a technique we called anagramming. This started with an assumption – an educated guess – followed by a good deal of trial and error. The intent was to substitute these plaintext assumptions throughout the problem, check surrounding values, and search for clues to expand our guesses.

We could not immediately start reconstructing the boxes even when our assumptions were corroborated because of the double-encipherment feature. The middle bigram is unknown, and a workable number of plaintext values must be ascertained before a start can be made in forming the boxes.

In the frequency count, we find that KK cipher text stands out with the highest count by far. We can start by assuming that it represents *ee*. We replace KK with *ee* throughout the text and see where it leads us.

The Germans often sent very short messages that reflected basic military necessities and which were therefore constantly repeated. The most common six-, eight-, ten-, and twelve-letter messages were known to us. Curiously, we were almost never given information about the military situation that might yield more specific probable words for our attacks. I don't know why. Perhaps it was security, perhaps ignorance, perhaps lack of time.

Note Line O in our sample problem:

Line O – T C K U
N U K O

To the experienced eye, this is a dead giveaway. The Germans were constantly asking, "What is your position?" or *wie lage*. The phrase might be preceded by a "please" or "request" or an addressee, but time was critical, and the eight-letter message was common.

We thus have assurance that our KK = *ee* assumption is probably correct, and we have:

w i e l
Line O – T C K U
N U K O
a g e x

Our initial assumption has grown: We now have plaintext pairs *wa*, *wg*, and *lx*.

The Germans used many stereotyped openings. With experience, we cryptanalysts could recognize them. For instance, messages frequently began with *an* ("to") followed by the person or unit receiving the signal.

We are fortunate in having three of our practice messages begin with KK cipher text. In German military text, about 95 percent of the time a message starts with *e*, the opening

	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	I				L	GM							BM		AN		R					I		A	
B	A		I			ADR								P								F			P
C	R				J				A	BGH		J	M		CGL LMQ	M			B	KO				C	
D	DJ	R		A		APP					E	D		C						I					
E				EGP			B																		
F	K			B							C			E	Q				MR	K			Q		
G		L		C												DM P		J	B		BQ				J
H	D	J					DL																		P
I		D							BEI MR			Q						C							J
K		Q				CL			D Q	RAA BOC DM	BJ M	L	G			JM			Q	B					ABC KL
L										PGHI QJJL QLL M				R			M	GQ				Q	AP		
M	CD		R						C	FI					FR			I		L				CJ	
N				D		D			LR		K			D		CI		I				O			N
O				D						EJL MO	BJ	GH N	Q			D	J	M		F	J				CJP PR
P				CD	E											ERR		I					GR		
Q					C		I									D									B
R									E				A						A						L
S	BHJ NPR R					G				I	I	BJ L		AC		G	BM				M		M		
T		R				B							O	G	J	R									
U		L	L	GQQ					BDM	LO			EO			F		G				P		D	J
V		LM		AFP P	AP							BM		FI			BM								
W		M				L				G			H			C	C						IPQ		
X			H							AQ			R				Q				G	AL			
Y			CI	G	Q					D					CP			K				JL	C	D	
Z			HQ													G			R				G		

Fig. 6.

words will be one of four: *erbitte* ("request"), *eigene* ("our, our own"), *ein* ("a"), and *eins* ("one"). Let us see how this works in our text.

If we try *erbitte* in Line I, the final *e* falls on ciphertext KZ, which has a high frequency. (Frequencies are always our strong ally.)

```
                e r b i t t e
Line I -        K N D C V M K S A . . .
                K S U P O K Z K A . . . .
                e
```

KZ also occurs in line L in position 6. This is a perfect opening for *eigene*:

```
                e i g e n e           e
Line L-         K U G Y X K W S K R M K A . . .
                K K B W W Z H M M Z U K E . . .
                e                     e
```

Although these are only the upper values of bigrams, when they are substituted throughout the text, we gain opportunities for assumptions for additional anagramming. For example, bigram CP in Line I has a rather high frequency, and it is a good assumption that the bottom plaintext letter is *e*.

We now examine other lines, with our assumed plain text entered, and see what can be done:

```
                      e  e n   n    e
Line A -        VDLVVKXRKCXVRBXABASKD
                DFXEGKMNZIWBTANPFYOKE
                     e
```

Units in the field constantly sent reports to various headquarters. German operations officers in a unit's staff (G-3 in American nomenclature) had the designator 1a. Messages to higher headquarters often began "*an roem eins Anton*" ("to roman numeral one Anton" – "Anton" being the German phonetic equivalent of our "Able"). Line A has several values that fit this possibility:

```
                anxroemxeinsxanton e
Line A -        VDLVVKXRKCXVRBXABASKD
                DFXEGKMNZIWBTANPFYOKE
                                   e
```

Often this opening was followed by "enemy something or other" as "enemy tanks, or planes, or troops." ("Enemy" is "Feind" [noun] or "Feindliche" [adjective] in German.) That seems a likely entry here because of the KK (*ee*) second from the end on top and around the bottom where "Feindliqe" connects with it. Now we have six more probable equivalents to substitute throughout.

```
                anxroemxeinsxantonfei
Line A -        VDLVVKXRKCXVRBXABASKD
                DFXEGKMNZIWBTANPFYOKE
               ndliqe                e
```

Let us examine one more short message to see if anything can be made of it:

```
                    t t e   a
Line F -        M U M V I B V O
                P Q K O I W D U
```

That first word just has to be *bitte* ("please"). But please what? A common request was for a situation report, and a frequent sixteen-letter message was therefore *bitte lage meldung* ("situation report, please"). Checking the frequency chart also shows higher counts for a few of the cipher bigrams that accord well with their plaintext equivalents (e.g., II = *e d* has a count of 5 and VD = *an* a count of 3). We always looked for frequency indications that tended to confirm what were still only assumptions. Thus we have eight more probable bigrams:

```
                b i t t e l a g
Line F -        M U M V I B V O
                P Q K O I W D U
                e m e l d u n g
```

It was a good break if we found two messages with the same beginning. It was especially helpful if the beginning was longer than twenty-one letters and thus continued on the second line. Such a case may be seen in Lines A and P. We have already anagrammed some of Line A, and it seems as though it may share the first twenty-seven letters with Line P. Note the six-bigram repeated block at the beginning of Lines A and P and the repetition of vertical bigrams at positions 1 and 14 of Line P.

```
                anxroemxeinsxantonfei
Line A -        VDLVVKXRKCXVRBXABASKD
                DFXEGKMNZIWBTANPFYOKE
                ndliqe                e

                anxroemxeinsxantonfei
Line P -        VDLVVKBUOUSHWVDYEBQOG
                DFXEGKZWZKAZXDFPDOAZQ
                ndliqe          nd
```

Thus it seems we have another fifteen upper letters to substitute in the problem.

One of the greatest helps to the cryptanalyst is to know what the enemy is likely to talk about. There were plenty of the German equivalents of "enemy," "aircraft," "troops," "armor," and so on. But by far the most common words were the cardinal numbers: *eins*,

zwo, *drei*, etc. Supply reports, casualty figures, radio frequencies, times of day, location grids, and much more all required numbers.

Often when no other openings were visible, numbers could be spotted in the middle of messages – after some judicious assumptions based on frequency and combinations. The ten digits were frequently used in groups (e.g., four digits for the time of day plus *uhre*, "hours") and were separated one from another by *X*.

Security violations and operator mistakes greatly helped us. Of course, we were always looking for that rare happening – the same message sent in plain and cipher text – but that was rare.

Let us examine Line G of the problem:

```
            e       e  ie
Line G -    KLOAZWSEZUCKSPKOTXCYU
            KSLFQMFDXDPZQXNMOVKDS
            e          e
```

We already have some letters of Line G, one of them being an initial *e*. Now look in figure 5 at the header of the message:

```
ZBT
QLS
1240
```

The alert cryptanalyst now rubs his hands in glee because he realizes that the careless German code clerk has included the time of day at the beginning of the message. (This occurred once in a long while.) We now have the following:

```
            einsxzwoxvierxnulluhr
Line G -    KLOAZWSEZUCKSPKOTXCYU
            KSLFQMFDXDPZQXNMOVKDS
            e          e
```

There is a slight problem here because the code clerk accidentally omitted the *X* after *null*, but that is seen when *uhre* fits into the bottom *e* of cipher KK.

The above examples should give a good idea of how the initial plaintext wedges were made. Again, I caution that the sample problem is contrived – it was never this easy. Very few of these entry points, if any, appeared within the same three-hour period. It took a very patient cryptanalyst to find correct plain text in the average set of messages.

This involved daring assumptions and detailed tracking of surrounding bigrams to find promising combinations. Trial and error, persistence, and some sixth sense could lead to progress. We stuck with a three-hour period as long as it seemed to show promise – a large volume, a good frequency count, likely plain texts. Conversely, we abandoned a period for a new one – usually on the basis of instinct and experience – when we were getting nowhere.

Once a sufficient number of bigrams was recovered – one cannot quantify it exactly – we set about trying to reconstruct the cipher squares, a process we called "boxing." This could be the most daunting task of all. As the squares were completely random, we did not get help from any pattern or keyword.

The first step was to make "encipher" and "decipher" charts. These were large sheets with 25x25 matrices, each cell with four quadrants (see Fig. 7).

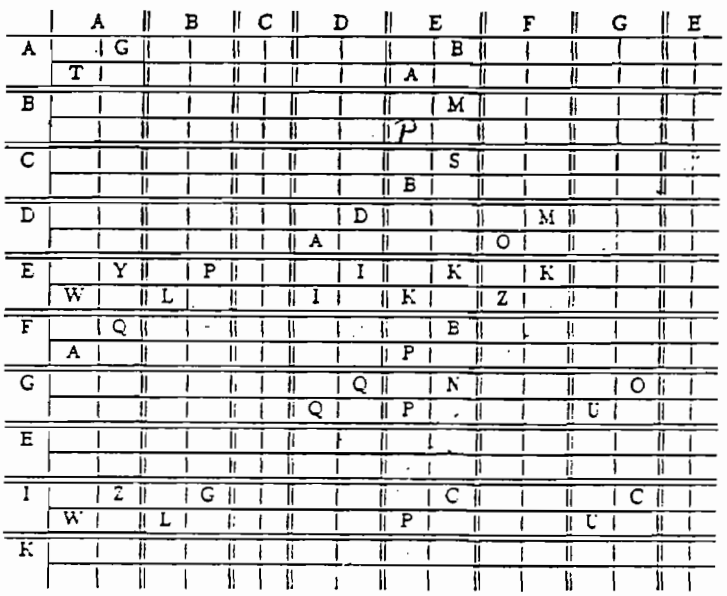

Fig. 7. Portion of encipher chart

The charts were over a foot square and were preprinted for us in horizontal sets of two, which made it easier for us to fill in and work from both at the same time.

In the encipher chart, the bigram coordinates of the matrix represented the plain text, with the cipher equivalents written in the appropriate square. The first letter of the cipher bigram was written in the upper right quadrant of the square, and the second letter in the lower left quadrant, thus serving as a reminder of which letter belonged in which box.

The decipher chart was the reverse. The coordinates were the cipher bigrams, with the plaintext bigrams written in the upper right and lower left quadrants of the inner squares. The upper left and lower right quadrants were reserved for the unknown intermediate bigrams of the cipher which might be discovered as we progressed with pencil and paper. These charts now served as the the software for the computer in the cryptanalysts' minds.

With graph paper and pencils, the problem then was to somehow string these letters together so as to recover the original cipher boxes. For a start we used numbers to represent the middle letters, and then by using other related values we tried to "hook"

some of the letters together. Except in the unlikely event of a very great amount of anagrammed plain text, this became an eye-twisting exercise in frustration for several reasons.

First, we had no idea of the middle bigram. Second, as I explained earlier, the final cipher bigram can be the result of four possible enciphering combinations: diagonal-diagonal, liner-diagonal, diagonal-liner, and liner-liner. Third, we had no idea of which letters in each box were on the same line, or in the same column, or opposite which line in the other box.

Fortunately, the inherent properties of the boxes and the enciphering method offered ways to help reconstruct the boxes. I will use the cipher boxes of figure 1 to illustrate the three most useful phenomena.

1. Reversibles – If the middle bigram of the encipherment is a repeated letter, the result of the second must be the reverse of the original plaintext bigram:

ed = HH = DE

This can result only from a double diagonal, which is a clue we really need in our boxing effort.

2. Reciprocal – Assume a plaintext bigram enciphered via two diagonals. If the reverse of its cipher bigram happens to be a plaintext bigram, its own cipher equivalent is the reverse of the original plaintext bigram:

(1) ne = AW = XM

(2) mx = WA = EN

Thus if we find two of our anagrammed bigrams in this forward-reverse relationship, we know that they can result only from a diagonal-diagonal encipherment. We encircle these in red on the encipherment and decipherment charts. Eliminating the possibility of liners is invaluable in rebuilding the boxes.

3. Appendixing – "Appendixing" aided the analyst in determining which letters were on the same line in a box. If any letters are on the same line (e.g., K, X, N, Z, or Y in Box 1 of figure 1) and are combined with one particular letter in Box 2 – say the letter E in the fourth row – then the first letter of the middle bigram must be the same for all the bigrams:

ke = AR = XX

xe = AA = EX

ne = AW = XM

ze = AG = UX

ye = AU = XR

When the middle bigram is reenciphered, since the first letter (in this case A) is always the same, the final bigram can consist of only one of five values in each box, instead of the usual twenty-five: (in this case U, I, E, M, or X in Box 2, and X, M, Q, A, or S in Box 1 or letters to the left when a liner is involved).

So if we find a pattern of repeats going down a column of our charts, there is a greater than normal chance that the corresponding outside letters on the left are on the same line in their box. This can be fortified if another column shows a similar pattern. None of this is certain, but it bolsters the odds.

From this point, the cryptanalyst resorts to trial-and-error boxing. If the reader has experience with a particularly difficult Playfair cipher, where it appears that some letters must be all at once on the same row, in the same column, and on the diagonal with others, he will have some appreciation of what we faced.

Common Boxes

As mentioned earlier, each German unit was supplied with a group of six boxes for the day. Since two boxes were necessary for each of eight three-hour periods, some of the boxes were used more than once. For instance, Boxes 1 through 6 might be used as follows:

Time of Day	Box Combination
0001–0300	1 & 2
0301–0600	3 & 4
0601–0900	4 & 1
0901–1200	5 & 6
1201–1500	3 & 5
1501–1800	2 & 6
1801–2100	5 & 2
2101–2400	6 & 3

The difficult and crucial breaking was of the first workable period that appeared during the day. This was not necessarily the 0001–0300 slot but the first period with enough text to attack. We called that the original period. Which it would be was not predictable; no period was regularly the busiest. After that a search was made for other periods that used one of the two boxes now known. If one was discovered, its period was a rather easy one to solve.

Locating a common box in the double encipherment was not simple. A period had to be anagrammed and boxing started before there was a basis for comparison. However, once a common box was spotted, an experienced analyst could quickly reconstruct the second one.

I would like to discuss the major reasons for the NI cipher-breaking being so difficult and daunting.

1. Volume: The enemy changed its boxes every three hours of every day. The quantity of cipher text available in a three-hour period was often insufficient to work with, or just marginally sufficient, and might not bear fruit.

2. Peculiarities: Even with adequate volume, a particular text might have a makeup that frustrated continuity, even after sensible beginnings. Worst of all was an aberrant frequency count, which would result in interminable false starts. Though this is common with limited message volume, many longer texts displayed abnormal frequency indications. Despite this, we had the feeling that, given time, we could break into most problems, which brings up the next obstacle.

3. Time strictures: Messages enciphered in NI dealt with both tactical and strategic matters. However, after a day or two, the intelligence became stale, and we had to go on to new and fresh material. Working under this kind of pressure proved impossible for some of the men.

4. Garbles: This was the greatest obstacle. The German cryptographers made mistakes, their radiomen transmitted wrongly, and our interceptors made errors in picking up what was often a weak signal. At times we had the same messages from three or four intercept companies, and the variation could be most marked. If breaking assumptions are based on wrong cipher values, the analyst is dead in the water from the start. Sometimes we displayed an almost sixth sense about incorrect letters, but garbles greatly hindered us.

A Simplification – Single Encipherment

With the invasion of Normandy in June 1944, much of the enemy traffic began to be enciphered only singly, the second, double encipherment being omitted. The German communication experts perhaps realized that the double encipherment took too long and was too prone to error at both ends to use in combat situations.

To illustrate its use, here are the opening words of "Die Lorelei" singly enciphered in the boxes of figure 1:

```
Y Y I V Q D L A Y N L U X L P W Q Y V T F
i q w e i s s n i q t w a s s o l l e s b
e d e u t e n d a s s i q s o t r a u r i
U S A R T A Q C Y X Y A Q X X C K K R X G
```

Ct: YYIVQ DLAYN LULXP WQYVT FUSAR TAQCY XYAQX XCKKR XG

It will be seen that our task was much simplified. The diabolical middle bigram no longer exists, and the analyst can use a reciprocal process of simultaneous anagramming and boxing. Some salient helping points are as follows:

1. When enciphered, a plaintext letter must result in a different cipher letter in the same box. Thus, for example, bigram *ab* cannot possibly show a cipher B on top or a cipher A on bottom. This helps prevent wrong anagramming.

2. Single plaintext values allow a start to be made in boxing. If we know that plaintext *u-* is cipher XY, then we also know that X in Box 2 is on the same line as *u* in Box

1, and that Y in Box 1 is in the same column as *u* in Box 1, or in the same line adjacent to *u*. Single values are far less useful in double encipherment.

3. Plaintext assumptions lead more quickly to boxing contradictions than they do in double encipherment, letting us discover anagramming errors much earlier.

Unfortunately, while these aids are valid, they were rather moot in practice. Often the reason was the lack of sufficient traffic in any three-hour period. Add to this the numerous garbles, and breaking the cipher was still difficult – especially in a usable time frame. Nevertheless a large volume of the single encipherment was broken in time to be of use. Because of security necessities and our isolation, we were largely in the dark as to the use of our information, but we were assured by officers from General Bradley's headquarters that it was of constant and great value.

To sum up, I found that breaking the NI cipher system was a complex and often mind-bending process. It would be interesting to learn if it were the last of the "pencil-and-paper" systems used by a major army in a major conflict. It was tempting to think of it as "interesting" or "intriguing," but in wartime that seems incongruous. Perhaps now, many years later, we can study it with a greater degree of academic equanimity.

(U) Mr. David was born in Brooklyn, New York, and graduated from Brooklyn College in 1941. After taking graduate courses at Columbia University, he enlisted in the U.S. Army Signal Corps in 1942 and served as a cryptanalyst until his discharge in 1946. Mr. David then went to work as a sales representative, from which he retired in 1988. He presented a talk on the subject of this article at the 1994 Cryptologic History Symposium.