F-61

22 SEPT 93

Intricacies of a remarkable Soviet spy cipher.

NUMBER ONE FROM MOSCOW [1]

David Kahn

At the trial in 1957 of Colonel Rudolf Abel for espionage on behalf of the Soviet Union, one of the exhibits in evidence was a bit of microfilm carrying ten columns, 21 rows, of five-figure groups. This cipher message, found inside a hollow nickel in 1953 and turned over to the FBI, had proved impregnable to solution until its key was made available four years later by the defection of Reino Hayhanen, Abel's erstwhile assistant, to whom the message had been addressed.[2] The inability of government cryptanalysts to read it was no reflection upon their competence, for the cryptographic system used in the message was the finest and most advanced mnemonic cipher ever made public. Although not theoretically insoluble, it is effectually unbreakable without prior knowledge of the system and on the basis of a single message.

At the trial, although prosecuting attorney Kevin Maroney did a masterful job of leading Hayhanen, as state's witness, through the intricacies of the system, the cipher was so complicated that its description bored the jurors and the process could not be followed even by a cryptographer without the written program furnished the jury. A better look at it at leisure will be rewarding to anyone with an interest in cryptography.

The Message

If the cipher were to be given a technical name, it would be known as a "straddling bipartite monoalphabetic substitution superenciphered by modified double transposition." Four mnemonic keys—the Russian word for "snowfall," a snatch of popular song, the date of the Soviet V–J Day, and the agent's personal number—were used to derive the arrangement of the

---

[1] This article is based on the author's booklet *Two Soviet Spy Ciphers* (Great Neck, N. Y.: David Kahn. 1960. L/C Card No. 60–16799.)

[2] For the full dramatic story of the Hayhanen/Abel case see W. W. Rocafort's "Colonel Abel's Assistant," Intelligence Articles III 4, p. 1 ff.

alphabet for the substitution and the order for the two transpositions. The system can most easily be illustrated by following through the encipherment of the exhibited message, Moscow's first to Hayhanen after his arrival in New York, much as some Soviet cipher clerk did it in a well-guarded office of the KGB on a wintry third of December, 1952. Translated, the message read:

> 1. We congratulate you on [your] safe arrival. We confirm the receipt of your letter to the address "V" and the reading of [your] letter No. 1.
> 2. For organization of cover we have given instructions to transmit to you three thousand in local [currency]. Consult with us prior to investing it in any kind of business, advising the character of the business.
> 3. According to your request, we will transmit the formula for the preparation of soft film and the news separately, together with [your] mother's letter.
> 4. [It is too] early to send you the gammas.[3] Encipher short letters, but do the longer ones with insertions. All the data about yourself, place of work, address, etc., must not be transmitted in one cipher message. Transmit insertions separately.
> 5. The package was delivered to [your] wife personally. Everything is all right with [your] family. We wish [you] success. Greetings from the comrades.
> No. 1, 3 December.

The Russian text was as follows:

1. Поздравляем с благополучным прибытием. Подтверждаем получение вашего письма в адрес "В" и прочтение письма №1.

2. Для организации прикрытия мы дали указание передать вам три тысячи местных. Перед тем как их вложить в какое либо дело посоветуйтесь с нами, сообщив характеристику этого дела.

3. По вашей просьбе рецептуру изготовления мягкой пленки и новостей[4] передадим отдельно вместе с письмом матери.

4. Гаммы высылать вам рано. Короткие письма шифруйте, а побольше—делайте со вставками. Все данные о себе, место работы, адрес и т.д. в одной шифровке передавать нельзя. Вставки передавайте отдельно.

5. Посылку жене передали лично. С семьей все благополучно. Желаем успеха. Привет от товарищей.

№1/03 Декабря.

[3] Probably one-time pad cipher keys.
[4] The genitive case is apparently an error.

The Substitution

The first major step in the encipherment of this text is substitution of one- and two-digit numbers for the Russian plaintext letters. For this purpose a table or "checkerboard" of 40 cells—ten across and four down—is set up as illustrated below.

	5	0	7	3	8	9	4	6	1	2
	С	Н	Е	Г	О	П	А			
6	Б	Ж	.	К	№	Р	ф	Ч	Ы	Ю
1	В	З	,	Л	Н/Ц	Т	Х	Ш	Ь	Я
2	Д	И	П/Л	М	Н/Т	У	Ц	Щ	Э	ПВТ

The first seven letters, СНЕГОПА, of the Russian word for "snowfall" are inscribed in the first row, leaving the last three cells blank. The remaining 23 letters of the modern Russian alphabet, omitting diacritical marks, are inscribed in sequence vertically in the other three rows, skipping the third and fifth columns, which, with the last cell remaining in the last column, are then filled by seven symbols. These are a period, a comma, the symbol П/Л, whose meaning is undetermined, the abbreviation №, the letter-number switch sign Н/Ц, the "message starts" sign Н/Т, and the abbreviation ПВТ for "repeat." Along the top of the checkerboard are written the ten digits in a mixed sequence determined by a process to be described later. The last three digits in the sequence, which stand over the blank cells at the end of the first row, are repeated at the left of the second, third and fourth rows. These digits are known as coordinates.

Each plaintext letter in the first row of the checkerboard is enciphered by substituting the single coordinate above it. Each letter and symbol in the other rows is enciphered by substituting the coordinate at the end of its row followed by the coordinate at the top of its column. Numbers are enciphered by placing them within a pair of the letter-number switch signs and repeating them three times.

Before these substitutions are made, however, the plaintext is bisected—chopped at random into two parts—and the true start of the message is tacked onto the true end. This true start is indicated by the "message starts" sign Н/Т. In this encipherment, as illustrated below, the sign stands seventh in the fourth line from the bottom of page A19.

9	69	20	63	69	61	19	20	12	23	61	25	4	13
П	Р	И	К	Р	Ы	Т	И	Я	М	Ы	Д	А	Л
20	29	63	4	10	4	0	20	7	9	7	69	7	25
И	У	К	А	З	А	Н	И	Е	П	Е	Р	Е	Д
4	19	11	15	4	23	19	69	20	19	61	5	12	66
А	Т	Ь	В	А	М	Т	Р	И	Т	Ы	С	Я	Ч
20	23	7	5	19	0	61	14	67	9	7	69	7	25
И	М	Е	С	Т	Н	Ы	Х	.	П	Е	Р	Е	Д
19	7	23	63	4	63	20	14	15	13	8	60	20	19
Т	Е	М	К	А	К	И	Х	В	Л	О	Ж	И	Т
11	15	63	4	63	8	7	13	20	65	8	25	7	13
Ь	В	К	А	К	О	Е	Л	И	Б	О	Д	Е	Л
8	9	8	5	8	15	7	19	29	20	19	7	5	11
О	П	О	С	О	В	Е	Т	У	И	Т	Е	С	Ь
5	0	4	23	20	17	5	8	8	65	26	20	15	14
С	Н	А	М	И	,	С	О	О	Б	Щ	И	В	Х
4	69	4	63	19	7	69	20	5	19	20	63	29	21
А	Р	А	К	Т	Е	Р	И	С	Т	И	К	У	Э
19	8	3	8	25	7	13	4	67	18	333	18	67	9
Т	О	Г	О	Д	Е	Л	А	.	Н/Ц	333	Н/Ц	.	П
8	15	4	16	7	20	9	69	8	5	11	65	7	69
О	В	А	Ш	Е	И	П	Р	О	С	Ь	Б	Е	Р
7	24	7	9	19	29	69	29	20	10	3	8	19	8
Е	Ц	Е	П	Т	У	Р	У	И	З	Г	О	Т	О
15	13	7	0	20	12	23	12	3	63	8	20	9	13
В	Л	Е	Н	И	Я	М	Я	Г	К	О	И	П	Л
7	0	63	20	20	0	8	15	8	5	19	7	20	9
Е	Н	К	И	И	Н	О	В	О	С	Т	Е	И	П
7	69	7	25	4	25	20	23	8	19	25	7	13	11
Е	Р	Е	Д	А	Д	И	М	О	Т	Д	Е	Л	Ь
0	8	15	23	7	5	19	7	5	9	20	5	11	23
Н	О	В	М	Е	С	Т	Е	С	П	И	С	Ь	М
8	23	23	4	19	7	69	20	67	18	444	18	67	3
О	М	М	А	Т	Е	Р	И	.	Н/Ц	444	Н/Ц	.	Г
4	23	23	61	15	61	5	61	13	4	19	11	15	4
А	М	М	Ы	В	Ы	С	Ы	Л	А	Т	Ь	В	А
23	69	4	0	8	67	63	8	19	8	19	63	20	7
М	Р	А	Н	О	.	К	О	Р	О	Т	К	И	Е
9	20	5	11	23	4	16	20	64	69	29	20	19	7
П	И	С	Ь	М	А	Ш	И	Ф	Р	У	И	Т	Е

17	4	9	8	65	8	13	11	16	7	19	20	69	7
,	А	П	О	Б	О	Л	Ь	Ш	Е	Т	И	Р	Е
25	7	13	4	20	19	7	5	8	15	5	19	4	15
Д	Е	Л	А	И	Т	Е	С	О	В	С	Т	А	В
63	4	23	20	67	15	5	7	25	4	0	0	61	7
К	А	М	И	.	В	С	Е	Д	А	Н	Н	Ы	Е
8	5	7	65	7	17	23	7	5	19	8	69	4	65
О	С	Е	Б	Е	,	М	Е	С	Т	О	Р	А	Б
8	19	61	17	4	25	69	7	5	20	19	67	25	67
О	Т	Ы	.	А	Д	Р	Е	С	И	Т	.	Д	.
15	8	25	0	8	20	16	20	64	69	8	15	63	7
В	О	Д	Н	О	И	Ш	И	Ф	Р	О	В	К	Е
9	7	69	7	25	4	15	4	19	11	0	7	13	11
П	Е	Р	Е	Д	А	В	А	Т	Ь	Н	Е	Л	Ь
10	12	67	15	5	19	4	15	63	20	9	7	69	7
З	Я	.	В	С	Т	А	В	К	И	П	Е	Р	Е
25	4	15	4	20	19	7	8	19	25	7	13	11	0
Д	А	В	А	И	Т	Е	О	Т	Д	Е	Л	Ь	Н
8	67	18	555	18	67	9	8	5	61	13	63	29	60
О	.	Н/Ц	555	Н/Ц	.	П	О	С	Ы	Л	К	У	Ж
7	0	7	9	7	69	7	25	4	13	20	13	20	66
Е	Н	Е	П	Е	Р	Е	Д	А	Л	И	Л	И	Ч
0	8	67	5	5	7	23	11	7	20	15	5	7	65
Н	О	.	С	С	Е	М	Ь	Е	И	В	С	Е	Б
13	4	3	8	9	8	13	29	66	0	8	67	60	7
Л	А	Г	О	П	О	Л	У	Ч	Н	О	.	Ж	Е
13	4	7	23	29	5	9	7	14	4	67	9	69	20
Л	А	Е	М	У	С	П	Е	Х	А	.	П	Р	И
15	7	19	8	19	19	8	15	4	69	20	26	7	20
В	Е	Т	О	Т	Т	О	В	А	Р	И	Щ	Е	И
68	18	111	18	25	69	8	65	11	8	18	333	18	25
№	Н/Ц	111	Н/Ц	Д	Р	О	Б	Ь	0[1]	Н/Ц	333	Н/Ц	Д
7	63	4	65	69	12	28	18	111	18	67	9	8	10
Е	К	А	Б	Р	Я	Н/Т	Н/Ц	111	Н/Ц	.	П	О	З
25	69	4	15	13	12	7	23	5	65	13	4	3	8
Д	Р	А	В	Л	Я	Е	М	С	Б	Л	А	Г	О
9	8	13	29	66	0	61	23	9	69	20	65	61	19
П	О	Л	У	Ч	Н	Ы	М	П	Р	И	Б	Ы	Т
20	7	23	67	9	8	25	19	15	7	69	60	25	4
И	Е	М	.	П	О	Д	Т	В	Е	Р	Ж	Д	А

[1] Apparently enciphered as a letter by error.

7	23	9	8	13	29	66	7	0	20	7	15	4	16
Е	М	П	О	Л	У	Ч	Е	Н	И	Е	В	А	Ш
7	3	8	9	20	5	11	23	4	15	4	25	69	7
Е	Г	О	П	И	С	Ь	М	А	В	А	Д	Р	Е
5	17	17	15	22	15	17	17	20	9	69	8	66	19
С	,	,	В	ПВТ	В	,	,	И	П	Р	О	Ч	Т
7	0	20	7	9	20	5	11	23	4	68	18	111	18
Е	Н	И	Е	П	И	С	Ь	М	А	№	Н/Ц	111	Н/Ц
67	18	222	18	67	25	13	12	8	69	3	4	0	20
.	Н/Ц	222	Н/Ц	.	Д	Л	Я	О	Р	Г	А	Н	И
10	4	24	20	20	2	1	4						
3	А	Ц	И	И	N	U	L	L	S				

Transpositions

The sequence of coordinates resulting from the substitution—which by itself affords virtually no security—is then thoroughly jumbled by passing it through two transposition tableaux. The first tableau (Fig. 1) is a standard columnar transposition. The substituted coordinates are written in horizontally under a set of keynumbers (the second of the two rows heading Figure 1) whose derivation will be given presently. They are taken out vertically, the column under keynumber 1 first and the others following in key order.

This new sequence of digits is then inscribed into the second tableau (Fig. 2) which, however, has a complication. This consists of a series of step-like disruption (D) areas determined as follows. The first D area begins in the top row under keynumber 1 and runs to the right side of that row. In each of the following rows, it begins one column to the right. When the columns are exhausted, one row is skipped and another D area is started in the following row with the column under keynumber 2, and so forth for as many rows as are needed to accommodate all the cipher digits.

The cipher digits taken vertically from the first tableau are inscribed horizontally from left to right into the rows of the second tableau, but leaving the D areas blank. When the non-D portions of all rows have been filled, the remaining digits are written in from left to right in the D areas, starting with the top row. From the completed tableau the digits are then taken out vertically in the order indicated by the

9	6	0	3	3	1	8	3	6	6	4	6	9	0	4	7	5
14	8	16	2	3	1	13	4	9	10	5	11	15	17	6	12	7
9	6	9	2	0	6	3	6	9	6	1	1	9	2	0	1	2
2	3	6	1	2	5	4	1	3	2	0	2	9	6	3	4	1
0	4	0	2	0	7	9	7	6	9	7	2	5	4	1	9	1
1	1	5	4	2	3	1	9	6	9	2	0	1	9	6	1	5
1	2	6	6	2	0	2	3	7	5	1	9	0	6	1	1	4
6	7	9	7	6	9	7	2	5	1	9	7	2	3	6	3	4
6	3	2	0	1	4	1	5	1	3	8	6	0	2	0	1	9
1	1	1	5	6	3	4	6	3	8	7	1	3	2	0	6	5
8	2	5	7	1	3	8	9	8	5	8	1	5	7	1	9	2
9	2	0	1	9	7	5	1	1	5	0	4	2	3	2	0	1
7	5	8	8	6	5	2	6	2	0	1	5	1	4	4	6	9
4	6	3	1	9	7	6	9	2	0	5	1	9	2	0	6	3
2	9	2	1	1	9	8	3	8	2	5	7	1	3	4	6	7
1	8	3	3	3	1	8	6	7	9	8	1	5	4	1	6	7
2	0	9	6	9	8	5	1	1	6	5	7	6	9	7	2	4
7	9	1	9	2	9	6	9	2	9	2	0	1	0	3	8	1
9	8	1	5	1	3	7	0	2	0	1	2	2	3	1	2	3
6	3	8	2	0	9	1	3	7	0	6	3	2	0	2	0	0
8	1	5	8	5	1	9	7	2	0	9	7	6	9	7	2	5
4	2	5	2	0	2	3	8	1	9	2	5	7	1	3	1	1
0	8	1	5	2	3	7	5	1	9	7	5	9	2	0	5	1
1	2	3	8	2	3	2	3	4	1	9	7	6	9	2	0	6
7	1	8	4	4	4	1	8	6	7	3	4	2	3	2	3	6
1	1	5	6	1	5	6	1	1	3	4	1	9	1	1	1	5
4	2	3	6	9	4	0	8	6	7	6	3	8	6	9	8	1
9	6	3	2	0	7	9	2	0	5	1	1	2	3	4	1	6
2	0	6	4	6	9	2	9	2	0	1	9	7	1	7	4	9
8	6	5	8	1	3	1	1	1	6	7	1	9	2	0	6	9
7	2	5	7	1	3	4	2	0	1	9	7	5	8	1	5	5
1	9	4	1	5	6	3	4	2	3	2	0	6	7	1	5	5
7	2	5	4	0	0	6	1	7	8	5	7	6	5	7	1	7
2	3	7	5	1	9	8	6	9	4	6	5	8	1	9	6	1
1	7	4	2	5	6	9	7	5	2	0	1	9	6	7	2	5
6	7	1	5	8	2	5	0	8	2	0	1	6	2	0	6	4
6	9	8	1	5	6	3	7	9	7	6	9	7	2	5	4	1
5	4	1	9	1	1	0	7	1	3	1	1	1	0	1	2	6
7	1	5	5	1	9	4	1	5	6	3	2	0	9	7	6	9
7	2	5	4	1	5	4	2	0	1	9	7	8	1	9	2	5
7	1	3	1	1	0	8	6	7	1	8	5	5	5	1	8	6
7	9	8	5	6.	1	1	3	6	3	2	9	6	0	7	0	7
9	7	6	9	7	2	5	4	1	3	2	0	1	3	2	0	6
6	0	8	6	7	5	5	7	2	3	1	1	7	2	0	1	5
5	7	6	5	1	3	4	3	8	9	8	1	3	2	9	6	6
0	8	6	7	6	0	7	1	3	4	7	2	3	2	9	5	9
7	1	4	4	6	7	9	6	9	2	0	1	5	7	1	9	8
1	9	1	9	8	1	5	4	6	9	2	0	2	6	7	2	0
6	8	1	8	1	1	1	1	8	2	5	6	9	8	6	5	1
1	8	1	8	3	3	3	1	8	2	5	7	6	3	4	6	5
6	9	1	2	2	8	1	8	1	1	1	1	8	6	7	9	8
1	0	2	5	6	9	4	1	5	1	3	1	2	7	2	3	5
6	5	1	3	4	3	8	9	8	1	3	2	9	6	6	0	6
1	2	3	9	6	9	2	0	6	5	6	1	1	9	2	0	7
2	3	6	7	9	8	2	5	1	9	1	5	7	6	9	6	0
2	5	4	7	2	3	9	8	1	3	2	9	6	6	7	0	2
0	7	1	5	4	1	6	7	3	8	9	2	0	5	1	1	2
3	4	1	5	4	2	5	6	9	7	5	1	7	1	7	1	5
2	2	1	5	1	7	1	7	2	0	9	6	9	8	6	6	1
9	7	0	2	0	7	9	2	0	5	1	1	2	3	4	6	8
1	8	1	1	1	1	8	6	7	1	8	2	2	2	1	8	6
7	2	5	1	3	1	2	8	6	9	3	4	0	2	0	1	0
4	2	4	2	0	2	0	2	1	4							

FIGURE 1. FIRST TRANSPOSITION TABLEAU.

column keynumbers without any regard to D areas. This final sequence of digits, in the standard groups of five, comprises the cipher text. A keygroup is inserted at a predetermined point before the message is sent. The result is shown in Figure 3.

Key Derivation

We have seen that one of the four mnemonic keys—СНЕГОПА—develops the alphabetic arrangement in the checkerboard. The other three—a phrase from a popular song, the V–J date, and Hayhanen's personal number, 13—interact to generate a series of virtually random numbers that in turn yield the keynumbers across the top of the checkerboard and the two transposition tableaux.

In the derivation of these keys two devices are used repeatedly—chain addition and conversion to sequential numbers. Chain addition produces a series of numbers of any length from a few priming digits: the first two digits of the priming series are added together modulo 10 (without tens digits) and the result placed at the end of the series; then the second and third digits are added and the sum placed at the end; and so forth, using also the newly generated digits when the priming series is exhausted, until the desired length is obtained. To illustrate: with the priming series *3 9 6 4,* 3 and 9 are added to get 2 (the 1 of the 12 being dropped), 9 and 6 yield 5, 6 and 4 add to 0. The series so far is 3 9 6 4 2 5 0; extended, it would run 3 9 6 4 2 5 0 6 7 5 6 3 2 1 . . . .

Conversion to sequential numbers, or the generation of a sequential key, is an adaptation from the standard practice of deriving a numerical key from a literal one by assigning consecutive numbers to the letters of the key in their alphabetical order, numbering identical letters from left to right. The literal key BABY, for example, would generate the sequential numerical key 2 1 3 4. In the Hayhanen system a series of digits is used as the breeder key, and consecutive numbers are assigned to them in their numerical order (0 is last), numbering identical digits from left to right. For example, if the breeder key is 3 9 6 4 6, the sequential key would be 1 5 3 2 4.

The derivation of the checkerboard and transposition keys for this message begins with the date—September 3, 1945—

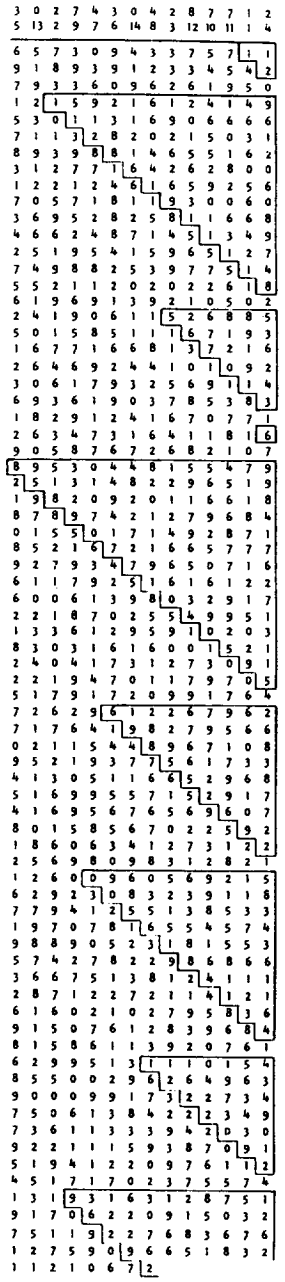
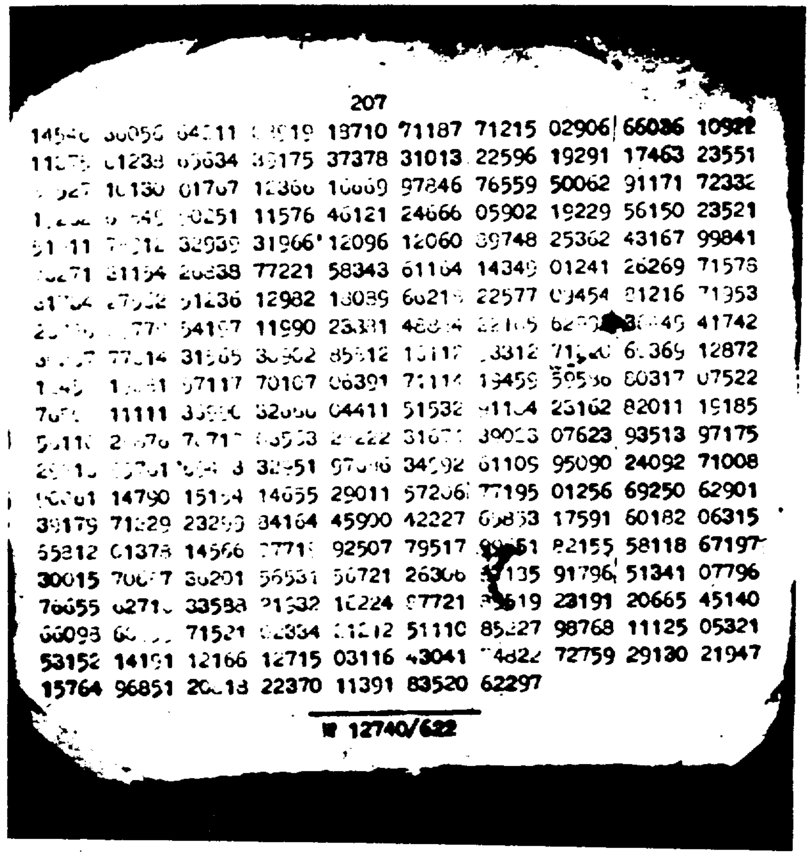


FIGURE 2. SECOND TRANSPOSITION TABLEAU, WITH DISRUPTIONS


207

[illegible]	[illegible]	[illegible]	[illegible]	13710	71187	71215	02906	66086	10922
[illegible]	[illegible]	[illegible]	[illegible]	37378	31013	22596	19291	17463	23551
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	97846	76559	50062	91171	72332
[illegible]	[illegible]	[illegible]	11576	46121	24666	05902	19229	56150	23521
[illegible]	[illegible]	[illegible]	31966	12096	12060	39748	25362	43167	99841
[illegible]	[illegible]	[illegible]	77221	58343	61164	[illegible]	01241	26269	71576
[illegible]	[illegible]	[illegible]	12982	[illegible]	[illegible]	22577	[illegible]	21216	71353
[illegible]	[illegible]	[illegible]	11990	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	41742
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	12872
[illegible]	[illegible]	97117	70107	06391	[illegible]	[illegible]	[illegible]	60317	07522
[illegible]	11111	[illegible]	[illegible]	04411	51532	[illegible]	25162	82011	19185
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	07623	93513	97175
[illegible]	[illegible]	[illegible]	32951	[illegible]	[illegible]	61109	95090	24092	71008
[illegible]	14790	[illegible]	14655	29011	57206	77195	01256	69250	62901
39179	71229	[illegible]	34164	45900	42227	[illegible]	17591	60182	06315
55812	01378	14566	[illegible]	92507	79517	[illegible]	82155	58118	67197
30015	[illegible]	36201	[illegible]	56721	[illegible]	[illegible]	91796	51341	07796
76655	[illegible]	33588	[illegible]	16224	57721	[illegible]	23191	20665	45140
66093	[illegible]	71521	[illegible]	[illegible]	51110	85227	98768	11125	05321
53152	14191	12166	12715	03116	43041	[illegible]	72759	29130	21947
15764	96851	[illegible]	22370	11391	83520	62297			

12740/622

FIGURE 3. THE CIPHER TEXT AS FOUND IN THE NICKEL.

that Russia achieved victory over Japan in World War II. It is written numerically in the Continental style: 3/9/1945. Its last digit, 5, indicates the position from the end of the message of an inserted arbitrary keygroup, presumably a different one for each message. In this message it is 2 0 8 1 8. The first five digits of the date, in Line B following, are subtracted from this keygroup (Line A) by modular arithmetic (without borrowing the tens digit). The result is Line C.

Line A	2 0 8 1 8
Line B	3 9 1 9 4
Line C	9 1 7 2 4

Then the first 20 letters of a line from the Russian popular song "The Lone Accordion" [6] are divided, in Line D, into two sections of ten letters, and sequential keys are derived for each part in Line E. Under the key for the first part is written, in Line F, the subtraction result of Line C, chain-added out to ten digits. Under the key for the second part is written a standard numerical sequence, 1, 2, 3, . . . 0. The first parts of Lines E and F are added modulo 10 to yield Line G.

Line D	Т	О	Л	Ь	К	О	С	Л	Ы	Ш	Н	О	Н	А	У	Л	И	Ц	Е	Г
Line E	7	4	2	0	1	5	6	3	9	8	6	8	7	1	9	5	4	0	3	2
Line F	9	1	7	2	4	0	8	9	6	4	1	2	3	4	5	6	7	8	9	0
Line G	6	5	9	2	5	5	4	2	5	2										

Then each digit of line G is located in the standard sequence of Line F and replaced by the number in Line E directly over it. The result of this substitution is Line H, which becomes the priming series for a chain addition that begins in Line K and proceeds—in rows of ten digits each—through lines L, M, N, and P.

Line H	5	9	3	8	9	9	1	8	9	8
Line J	3	7	2	4	8	9	1	5	0	6
Line K	4	2	1	7	8	0	9	7	7	2
Line L	6	3	8	5	8	9	6	4	9	8
Line M	9	1	3	3	7	5	0	3	7	7
Line N	0	4	6	0	2	5	3	0	4	7
Line P	4	0	6	2	7	8	3	*4*	*1*	1

13+4=17 (tableau 1)
13+1=14 (tableau 2)

The widths of the two transposition tableaux are found by adding respectively the eighth and ninth numbers—or perhaps the last two dissimilar numbers—in Line P to the agent's personal number, in this case 13. The first tableau will therefore have 17 columns and the second 14.

---

[6] The full phrase is the following:

Только слышно на улице где-то
Одинокая бродит гармонь.

The sequential key derived in Line J from Line H indicates the column sequence for a vertical transcription from the block formed by Lines K through P. The digits that result from this transcription, in Lines Q and R, become the breeder keys for the two transposition tableaux. They are repeated at the top of Figures 1 and 2 respectively, followed by the sequential keynumbers derived from them.

Line Q	9 6 0 3 3 1 8 3 6 6 4 6 9 0 4 7 5
Line R	3 0 2 7 4 3 0 4 2 8 7 7 1 2

Finally, a sequential key is derived in Line S from Line P.

Line P	4 0 6 2 7 8 3 4 1 1
Line S	5 0 7 3 8 9 4 6 1 2

This becomes the sequence of digits used as the coordinates for the checkerboard.

In 1956 Hayhanen's personal number was changed from 13 to 20, so that the width of the transposition tableaux was increased and their reconstruction thereby made slightly more difficult. In addition, the chain-added block was deepened by one row to increase the randomness of the digits that become the breeder keys for the transposition tableaux.

Evaluation

What can be said of the cryptographic merits of this cipher? That it is eminently secure was demonstrated by the FBI's inability to solve the nickel message. The system derives its great strength from complications introduced into a combination of two basically simple methods, monoalphabetic substitution and columnar transposition.

The complication in the substitution is the straddling device in the checkerboard. Ordinary checkerboards, having no unkeyed rows, produce two-digit equivalents for all plaintext letters. Here the irregular alternation of single and double coordinates makes it hard for a cryptanalyst to divide the running list of numbers into the proper pairs and singletons, a division which is of course prerequisite to the reduction to plaintext. A division entirely into pairs would straddle the correct equivalents (whence the term "straddling" in the cipher's technical description). Furthermore, this irregu-

larity undoubtedly increases the difficulty of reconstructing the transposition tableaux.

The complication in the transposition is the disruptions in the inscription of the second tableau. Their purpose is to block any attempt at reconstructing the first tableau. In the solution of ordinary double transposition, once the difficult job of reconstructing the second tableau is completed, the cryptanalyst can immediately proceed to the first with the premise that its columns will be found in the rows of the second. But the D areas forestall this direct attack here by mixing a part of one such column with a part of another. The cryptanalyst must sort out the columns before he can reconstruct the first tableau, and this sorting is a formidable task.

The keying method of this cipher adds to its cryptanalytic resistance. The long series of calculations performed in the key derivation results in a series of virtually random numbers whose lack of pattern makes it difficult for the cryptanalyst to reconstruct the original keys and thus get clues for the solution of subsequent messages. Even more important is the arbitrary five-digit group introduced at the start of the key derivation. It affects the derivation so strongly that keys with different groups would bear no apparent relation to one another. Since this group was apparently different for each message, and since each agent presumably had a different set of mnemonic keys, no two messages of all those sent out from Moscow by this system to secret agents all over the world would ever be keyed the same. Cryptanalysts, whose work becomes harder as they have less traffic in a single key, would have to attack each message separately.

Finally, the bisection of the message makes it harder for the cryptanalyst to find and exploit stereotyped beginnings and endings.

The system also has a number of operational advantages. First, the individual operations are easy and rapid, minimizing the chance of garbled messages. Second, the cipher text runs only about half again as long as the plain, not twice as long, as it often does in high-security pencil-and-paper systems. This reduction from the usual doubling is effected by the use of single coordinates in the checkerboard for high-frequency letters, for which the keyword is specially chosen.

The keyword СНЕГОПА includes the most frequent letter in Russian (O, with 11 percent), four other high-frequency letters (C, H, E, A) and two low-frequency letters. The seven account for 40 percent of normal Russian text, so that the cipher text should average 60 percent longer than the plain. (The nickel message is 62 percent longer.) The relative reduction means briefer communications, with consequent lowered risk of detection.

Third, the most important and unusual operational advantage of the cipher is the way an entire encipherment can be developed from four easily memorized items. The agent must also know, of course, the procedure for deriving from these the final keys, but this does not appear very hard to remember. Each step seems to lead to the next in much the same way that one portion of a piano piece leads to another. No spy cipher of comparable security that achieves this feat of mnemonics is known. To a spy, who lives in fear of sudden raids and searches, a cipher system that requires no betraying memoranda is a boon. Ironically, however, Hayhanen—or his superiors—did not trust his memory: when he arrived in the United States he carried microfilm notes on his cipher in case he forgot what was so easy to remember!

For all the impressive security of this cipher, it is not theoretically impossible to reconstruct the second transposition tableau in correct form for deriving a first tableau whose rows would yield the required monoalphabetic frequency distribution, and when this were done the monoalphabetic substitution could be solved with relative ease. Once the system were known and with a large volume of traffic in it, an electronic computer might be able to run through the billions of trials needed for a solution. But that a single message could have been solved while the system itself remained unknown is highly unlikely. The weakening of frequency characteristics caused by the way it uses the numbers and the obliteration of repetitions by the thorough transpositions leave virtually no clues for the cryptanalyst.