DAD'S CHALLENGE

La Guillotine

Mr. Bennett was a puzzle nut, and a lot of it had rubbed off on his son, George. Whenever one of them had something to fool the other, he was eager to show it off. George thought he had something when he brought the following table home from school:

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I	J
3	K	L	M	N	O
4	P	Q	R	S	T
5	U	V	W	X	Y

"Ever see anything like this before?" he asked.

"Hm—yes, it looks like something we used to call Checker-board. It was used to write a message using only five different symbols. The numbers for T would be 4 and 5, so you would use your fourth and fifth symbols together to represent T."

"No, this is something different. It is called La Guillotine, and it was used by the resistance movement during the Second World War. You remember that Germany defeated France, and for a while part of France was occupied and part wasn't?"

"I believe I heard my great-grandfather remark something about it," said Mr. Bennett dryly.

"Let me show you how it works. I want to write the message, 'Patrol is quiet,' so I'll copy down the message and put the proper number below each letter."

```
P    A    T    R    O    L    I    S    Q    U    I    E    T
41   11   45   43   35   32   24   44   42   51   24   15   45
```

"Is that all? That would be very easy."

"No, there is another step. Now you take each figure and substitute some letter of the alphabet that appears on that line. The first figure is 4, so I could choose P, Q, R, S, or T. The next figure is 1, so I could choose A, B, C, D, or E. I wrote the message like this."

PB CB RY TM OU NF FQ SR QI UD GQ AY SX

"That's better, but probably not too difficult, even so."

"No, but this was unoccupied France, and the Germans weren't there, and the French government was disorganized. It was good enough then. You could change the table, of course, and you wouldn't *show* that there were two letters in a group."

"Those letters you selected, suppose I—"

"Just play along, Dad. Do you think you would have much trouble reading it?"

"I shouldn't think so."

"Let me show you, anyway. You take each letter in the message, find it on the table, and substitute the figure at the top of the column. Like this."

PB CB RY TM OU NF FQ SR QI UD GQ AY SX
12 32 35 53 51 41 12 43 24 14 22 15 44

"Wow!"

"You get it now, Dad? You take each of these two figures, and find out what letter they give you from the table. The message now reads: 'Blow up bridges.' "

"That's great, George. It might not fool people too long, but it could have its purposes. If the French police intercepted the messenger, he could show them how to read it one way, but if it got through to the resistance movement, they would know enough to read it the other way. Let me see how you wrote the message."

On his paper George had it all written out:

```
P   A   T   R   O   L   I   S   Q   U   I   E   T
41  11  45  43  35  32  24  44  42  51  24  15  45
B   L   O   W   U   P   B   R   I   D   G   E   S
12  32  35  53  51  41  12  43  24  14  22  15  44
PB  CB  RY  TM  OU  NF  FQ  SR  QI  UD  GQ AY  SX
```

The bottom line was found by making substitutions from the two digits above. Thus, 41, reading down, gave P; 12, reading down, gave B; 13 gave C, and so on.

(Variation: One Checkerboard table could be used for changing letters into numbers, and a different Checkerboard for changing numbers back into letters.)

"It makes you wonder, doesn't it," said Mr. Bennett, after he had studied it out, "to whom your loyalty really belongs. Many French thought they ought to support their Vichy government, and others thought they should support the refugee government in London. Which ones were really traitors?"

"Gee, Dad, if they didn't know which government to support, maybe they should have written their messages so the same answer would come out no matter which way you read it."

His father gave him a strange look.

Playfair

"Your code reminds me of something the British army used during the First World War called Playfair. Simple to use and able to be varied quickly, it really isn't very safe—probably only an hour's security—but usually that was enough for a field cipher. The order would be given and carried out, and after that, who cared whether the Germans broke it or not?"

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