DISGUISING THE KGB SENORITA

PETER NEWBY
Chesterfield, Derbyshire, England

A simple cipher which merely shuffles the alphabet such that (say) A is represented by Q and B by G is child's play for a codebreaker. The plethora of Q in a message immediately suggests itself as a SENORITA letter and, for example, what else could ZQPQTQPQWQXQZQ be other than TARAMARASALATA? Notwithstanding such as KRAAL and AARDVARK, a double Q denies the prospect of Q being A, but it could be virtually any of the other popular letters of the AEINORST alphome, and all one does is consider its occurrences elsewhere in the message. Foolish adherence to formal style in letter-writing was one of the great 'giveaways' to the wartime codebreakers and once one has a toehold, no matter how tenuous, it is surprising how easy it becomes to decipher the whole of the message. How should one deal with the problem?

One of the simplest and most ingenious systems employs numerals, especially as these can be modified by a mathematical operation known, in theory, only to the sender and intended recipient. This mathematical operation is the 'value' of a keyword. Basically, the sender adds a keyword (which can be changed as often as deemed practicable) which the recipient subtracts prior to decoding. Ignoring the obvious ploy of standard alphanumerics (A=1, B=2, etc.), the operators use such as the Polybius Square to generate 'values'. Named after the ancient Greek who devised it for use with hand-held torches for cross-country communication, it typically has I and J sharing the same unambiguous 'value':

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

SENORITA is now perceived as
43.15.33.34.42.24.44.11

But, let us consider the value of a continuously-added keyword, (say) ZYMURGY:

S	E	N	O	R	I	T	A
Z	Y	M	U	R	G	Y	Z
78	69	65	79	84	46	98	66

Now, unlike the simple alphabetical shuffle, a solitary letter can be represented by a host of symbols--the gamut of its potential values--and such as the 'double Q' is no longer available to betray the word. Even more disconcerting is the fact that the same value can represent a var-

iety of different letters. For example, S+A = G+M = Q+C = B+R, any of which equates to Y without a keyword. Not only can the keyword be changed but, within reason, so can the grid itself. However, that is taking us beyond the scope of this basic discussion.

To add a further refinement, the numbers are usually transmitted bunched together in groups of five. Thus, a message despatched as 67886 45774 56669 is seen as the following pairs: 67.88.64.57.74.56.66 with the ultimate 9 ignored as a null (or, meaningless addition) intended to confuse the enemy. Subtract ZYMURGY to discover a phrase of symmetry utterly unlike the numerical 'shape'--BOMB MOB. Obviously, one can introduce natural break symbols to avoid ambiguity with such as THE Q PEN Q IS Q MIGHTIER Q THAN Q etc., or refine it in any other fashion deemed sensible. But, I'll conclude with an unrefined problem. Like all codebreaking, a background knowledge of the circumstances leading to its interception is an essential first clue but, unlike simple ciphers, the resolution of the problem depends upon ascertaining the keyword.

It is early 1945 and the new president, Harry S Truman, is keen to attend his first Big Three conference with Stalin and Britain's new prime minister, Attlee. Germany is on her knees. A suspected Red agent, the Apache dancer Rita Nose, has been arrested. All she was carrying was a copy of the Salvation Army journal, War Cry, with the following numerical sequence scribbled on the title page:

54265 67777 58676 95659 85484 45699

Can you decipher it? The Answer is given in Answers and Solutions.