BLETCHLEY RIDDLE OF THE WEEK

Attacking Caesar's Shift

Welcome code-breakers. Try your hand at this one:

J LXVYDCNA FXDUM MNBNAEN CX KN LJUUNM RWCNUURPNWC RO RC LXDUM MNLNREN J QDVJW RWCX KNURNERWP CQJC RC RB QDVJW

-JUJW CDARWP

Need a tad more information? Very well. This is an example of a 2,000-year-old cipher known as the Caesar Shift. To encipher a message with the Caesar Shift, you simply shift each letter of your message down the alphabet some set number of places. For a Caesar Shift of one, A becomes B, B becomes C, and so on. For a shift of two, A becomes C, B becomes D.

Say we're using a Caesar Shift of 4. You might find it quite useful to create a table with both your plain and cipher alphabets:

A better idea: use clues in the message. Look at the first J in the cipher. How many one-letter words are there in English? How many places would you need to shift from each of those words to get to J? Which of these solutions turns other enciphered words into plain English? As you figure out the cipher alphabet, fill it in here:

C	Caesar Shift = Plain a										al	oha	bet	•											
a	b	c	٩	e	£	9	h	i	j	k	ı	m	٨	C	Р	9	r	S	t	>	٧	W	x	У	Z

CIPHER ALPHABET

And now you're ready to crack the cipher:

C	C91	ar S	2Y!	f+:	-4					Pl	ain	al	oha	bet	•										
a	Ь	c	٩	e	f	9	h	i	j	k	I	m	٨	٥	Р	9	Γ	s	t	C	٧	W	х	У	Z
E	F	G	н	I	J	K	L	Μ	N	0	P	Q	R	S	т	υ	V	W	X	У	Z	Α	В	С	D

CIPHER ALPHABET

Turn these words from cipher to plain text:

CIPHER TEXT	plain text
XLI	
PSRHSR	
WIGVIX	

Got it? Well done.

Now, to decipher a Caesar Shift message, you must figure out the number of places the letters have been shifted. One strategy is to check every possible solution. There are only twenty-five Caesar shifts, since a shift of twenty-six gets you back where you began.

ADVERTISERS' ANNOUNCEMENTS

