PROBLEM SIX: THE TIME POLICE AND PLAYFAIR'S CIPHER

Cryptography is the study and application of complex ciphers, used to pass messages through foreign and hostile settings. During World War I, the British used a cipher algorithm called Playfair's Cipher because it was reasonably fast to use and required no special equipment. It was later adopt by the Germans during World War II. Playfair's Cipher is no longer used in any real-world application because modern computer could easily break the cipher within seconds.

You are computer programmer from the early 1990's who has been selected by the Time Police to be sent back in time to fight the Nazis during World War II. Your are equipped with nothing but your IBM ThinkPad and a unending battery to provide the ThinkPad with power. You must write an algorithm to quickly translate intercept cryptographic message encoded using Playfair's Cipher.

Playfair's Cipher uses a 5x5 table containing a keyword or phrase. To generate the key table, fill in the spaces in the table with the letters of the keyword (dropping any duplicate letters), then fill the remaining spaces with the rest of the letters of the alphabet in order. The letter 'J' is combined into the letter 'I' onto one square. They key can be written in the top rows of the table, from left to right. The keyword together with the conventions for filling in the 5x5 table constitute the cipher key.

To encrypt a message, one would break the message into diagraphs (groups of 2 letters) such that, for example, "HelloWorld" becomes "HE LL OW OR LD", and map them out on the key table. The two letters of the digraph are considered as the opposite corners of a rectangle in the key table. Note the relative position of the corners of this rectangle. Then apply the following 4 rules, in order, to each pair of letters in the plaintext:

1. If both letters are the same (or only one letter is left), add an "X" after the first letter. Encrypt the new pair and continue. Some variants of Playfair use "Q" instead of "X", but any uncommon monograph will do.
2. If the letters appear on the same row of your table, replace them with the letters to their immediate right respectively (wrapping around to the left side of the row if a letter in the original pair was on the right side of the row).
3. If the letters appear on the same column of your table, replace them with the letters immediately below respectively (wrapping around to the top side of the column if a letter in the original pair was on the bottom side of the column).
4. If the letters are not on the same row or column, replace them with the letters on the same row respectively but at the other pair of corners of the rectangle defined by the original pair. The order is important – the first letter of the encrypted pair is the one that lies on the same **row** as the first letter of the plaintext pair.

To decrypt, use the INVERSE (opposite) of the first 3 rules, and the 4th as-is (dropping any extra "X"s (or "Q"s) that don't make sense in the final message when finished).

Write a program that uses the Playfair's Cipher algorithm to decode the following message using the keyword "**DASBOAT**":

KT XF XT YB OD BV XC BP FT AM
UT GD HP WD ST UA IB VT VS DU
EV CF KY IB RV OD BV

You may hard-code the message and keyword into your program, but it must be translated by your program using the algorithm above.

REQUIRED INPUT: None
REQUIRED OUTPUT: The deciphered message; decoded using Playfair's Cipher algorithm.