Playfair Cipher

Overview

The Playfair cipher is a **c**ipher in w**h**ich each pair of consecutive characters is replaced by another.

How this is done **i**s determined by a secret keyword that is agreed upon ahead of ti**m**e by the message's sender and rec**e**iver.

Encryption

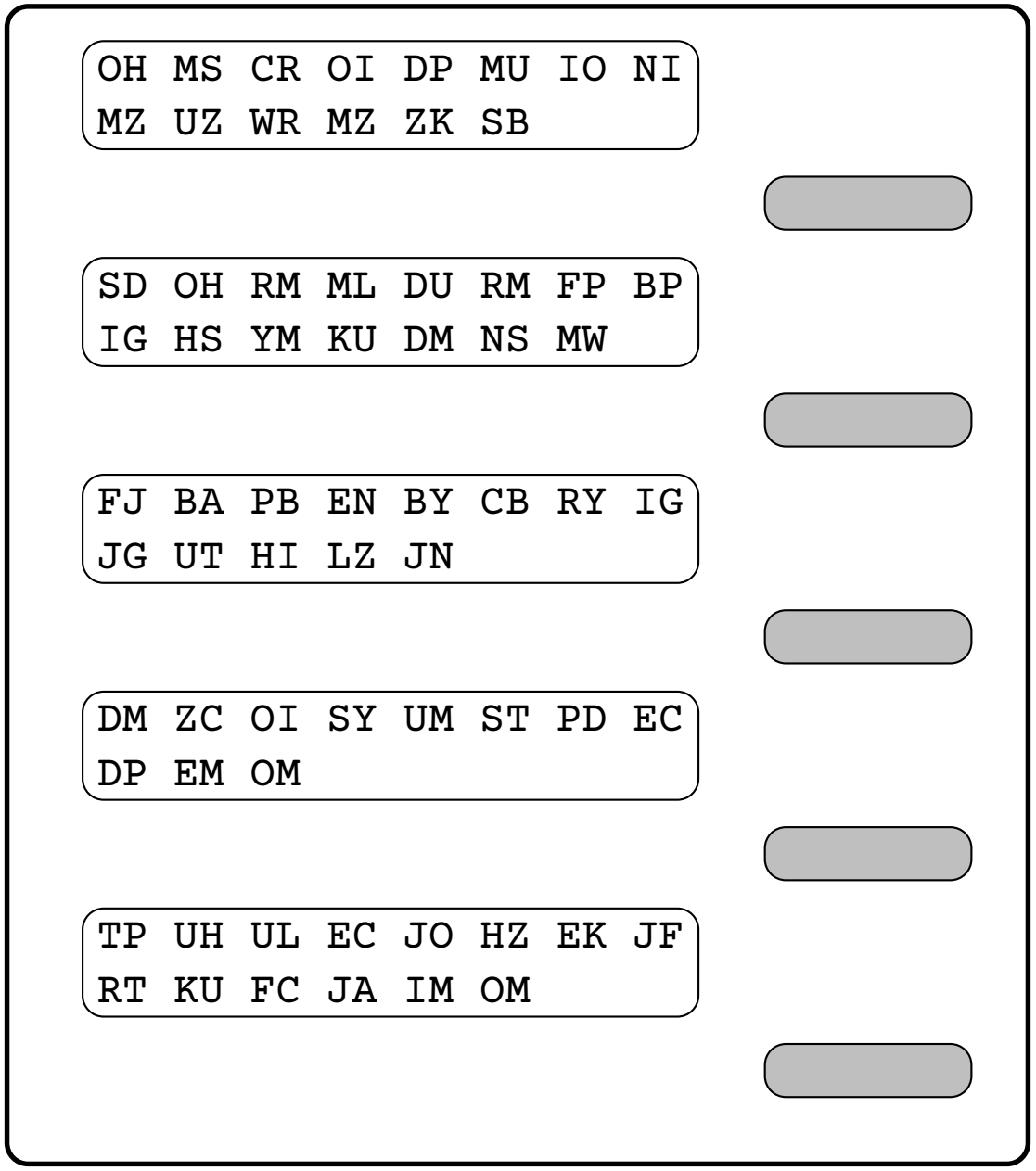
To encrypt a message with a keyword of length *n*:

1. Write out the keyword as the first *n* entries in a 5 × 5 table. Fill the rest of the table with the remaining letters (omit Q).
2. Insert an X between any repeated letters. Break the message into digraphs.
3. Replace each digraph via:

   If both letters appear in the same row, replace each one with the letter to its right.

   If both letters appear in the same column, replace each one with the letter below it.

   Otherwise, replace each letter with the one on the same row as it and the same column as the other letter in the digraph.



Example

Use the keyword GOBLIN to encrypt the message:

PASSIONATE

1. Use the keyword to construct the 5x5 substitution table.

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

2. Insert an X between any repeated letters. Break the message into digraphs.

   PA SX SI ON AT EX

3. Use the substitution table to replace each digraph.

   PA → RN (rectangle)
   SX → XB (same column)
   SI → UB (rectangle)
   ON → GA (rectangle)
   AT → DR (rectangle)
   EX → CZ (rectangle)

This yields the ciphertext:

RNXBUBGADRCZ