Playfair Cipher

Overview

The Playfair cipher i<u>s</u> a cipher in w<u>h</u>ich each pair of consecutive characters is replaced by <u>a</u>nother.

How this is done is determined by a secret keyword that is ag<u>r</u>eed upon ahead of time by the message's send<u>e</u>r and receiver.
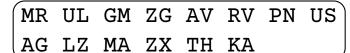
Encryption

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.

```
MR UL GM ZG AV RV PN US
AG LZ MA ZX TH KA
```

```
OR RU SJ UB WT NE SK MJ
VB PR FY HV LN RW
```

```
WT ZM PU LN NV AZ AG WT
TE MA ZX TH FP PW PW
```

```
PJ HN UG OR NV FM JL HG
XR OP HF SE TM SR PV
```

```
LN SJ PI NV AZ AG RP AS
HR TE NE
```

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