# Four-Square Cipher

## Overview

The Four-Square cipher is a cipher in which each pair of consecutive characters is replaced by another.

How this is done is determined by four tables which are derived from a pair of secret keywords agreed upon ahead of time by the message's sender and receiver.

## Encryption

To encrypt a message with the keywords $k_1$ and $k_2$:

1. Write out $k_1$ as the first entries in the bottom-left table. Fill the rest of the table with the remaining letters (omit Q).
2. Write out $k_2$ as the first entries in the top-right table. Fill the rest of the table with the remaining letters (omit Q).
3. Replace each digraph $x_1x_2$ via:

   Locate $x_1$ in the top-left table and $x_2$ in the bottom-right table.

   Locate the letters $y_1$ in the top-right table and $y_2$ in the bottom-left table that complete the rectangle defined by $x_1x_2$.

   Replace $x_1x_2$ with $y_1y_2$.

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

| | | | | |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

| | | | | |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

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

## Example

Use the keywords $k_1$ = DRAGONS and $k_2$ = HOARD to encrypt:

TREASURE

1. Use $k_1$ to construct the bottom-left table.

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

2. Use $k_2$ to construct the top-right table.

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

3. Use all four tables to replace each digraph with another.

TR → PT  EA → HO
SU → UP  RE → UR

This yields the ciphertext:

PTHOUPUR