Playfair cipher

The Playfair cipher is a digraph substitution cipher that encrypts pairs of letters using a 5×5 key matrix built from a keyword. Here's how you create the key matrix:

1. **Choose a keyword or key phrase.**
   Example: `MONARCHY`
2. **Remove duplicate letters.**
   From `MONARCHY`, we get `MONARCHY`. (No duplicates here.)
3. Fill the matrix row by row with the keyword letters.
   (Combine I and J into one cell to fit 25 letters.)
4. Fill the remaining spaces with unused letters of the alphabet.

So, for `MONARCHY`, the matrix becomes:

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

Example 1

Let's build the **Playfair cipher key matrix** step by step using the keyword **"SIX"**.

Step 1: Write the keyword (remove duplicates)

Keyword: **SIX**
No duplicates → we keep it as `SIX`.

Step 2: Prepare the alphabet

Playfair uses **25 letters**, combining **I** and **J** into a single cell.
Alphabet (I/J counted as one):
`A B C D E F G H I/J K L M N O P Q R S T U V W X Y Z`

Step 3: Fill the matrix

Start with `SIX`, then add remaining letters (excluding duplicates and skipping `J` since I/J share one cell):

- Start: `S I X`
- Remaining letters: `A B C D E F G H K L M N O P Q R T U V W Y Z`

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

let's encrypt **HELLO** step by step using the Playfair matrix we just built for **SIX**:

Step 1: Write the Key Matrix Again

Step 2: Prepare the Plaintext

Plaintext: **HELLO**

- Break into **pairs of letters**: HE | LL | O
- If a pair has the same letter (LL), insert an **X** between them:
  - HE | LX | LO
- If there's a single letter left at the end, add an **X** (not needed here because we now have three pairs).

So our digraphs are: **HE**, **LX**, **LO**.

Step 3: Encrypt Each Pair

Pair 1: H – E

- H = row 3, column 1
- E = row 2, column 3
- **Rectangle rule**: Take letters in the same row as the other letter → form the corners.

H (row 3, col 1) → same row as E’s column → **L**
E (row 2, col 3) → same row as H’s column → **C**

HE → LC

Pair 2: L – X

- L = row 3, column 3
- X = row 1, column 3
- **Same column rule**: Replace each with the letter **below** it (wrap to top if needed).

L → M (one row down)
X → Q (one row down from row 1 to row 4)

LX → MQ

Pair 3: L – O

- L = row 3, column 3
- O = row 4, column 1
- **Rectangle rule** again.

L (row 3, col 3) → take O’s column (col 1) → **H**
O (row 4, col 1) → take L’s column (col 3) → **Q**

LO → HQ

Step 4: Combine Results

Encrypted text = **LCMQHQ**

Example 2:

Step 1: Keyword

Keyword: **BALLOON**
Remove duplicates → `BALON`
(We keep first occurrences only: B, A, L, O, N)

Step 2: Prepare Alphabet (I/J combined)

Alphabet (25 letters total):
`A B C D E F G H I/J K L M N O P Q R S T U V W X Y Z`

Step 3: Build the 5×5 Matrix

Start with **BALON**, then fill remaining letters (excluding duplicates and skipping J):

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

Resulting matrix:

	1	**2**	**3**	**4**	**5**
1	B	A	L	O	N
2	C	D	E	F	G
3	H	I/J	K	M	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

Using the Playfair matrix for **BALLOON** (rows: `B A L O N`/`C D E F G`/`H I/J K M P`/`Q R S T U`/`V W X Y Z`), I split **HELLO** into digraphs **HE | LX | LO** (inserting X between the double Ls). Encrypting: **HE** → **KC** (rectangle rule), **LX** → **EL** (same column, move down), **LO** → **ON** (same row, move right). So the final ciphertext is **KCELON**.

Ciphertext to decrypt: **K C E L O N** → split into digraphs **KC | EL | ON**

Decryption rules (short):

- **Same row:** shift each letter one cell **left** (wrap around).
- **Same column:** shift each letter one cell **up** (wrap around).
- **Rectangle (different row & column):** each letter takes the column of the other letter while staying in its own row.

Step-by-step:

1. **KC**
    - K at (3,3); C at (2,1). They form a rectangle.
    - Take letter in row of K and col of C → (3,1) = **H**.
    - Take letter in row of C and col of K → (2,3) = **E**.
    - **KC → HE**
2. **EL**
    - E at (2,3); L at (1,3). Same **column** (col 3).
    - Shift each letter **up** one row: E → (1,3) = **L**; L → (5,3) = **X** (wrap from row1 to row5).
    - **EL → LX**
3. **ON**
    - O at (1,4); N at (1,5). Same **row** (row 1).
    - Shift each letter **left** one column: O → (1,3) = **L**; N → (1,4) = **O**.
    - **ON → LO**

Combine decrypted digraphs: **HE | LX | LO = HELXLO**. Remove the filler X that was inserted between the double Ls during encryption → **HELLO**.

Example 3:

Example Word: TAXI

Step 1: Break into digraphs

TAXI → TA | XI
(Remember: I/J share a cell, so I is valid.)

Step 2: Encrypt Each Pair

Pair 1: TA

- T = (4,4), A = (1,2) → rectangle rule.
- T → take column of A (col 2) → (4,2) = **R**
- A → take column of T (col 4) → (1,4) = **O**
  TA → RO

Pair 2: XI

- X = (5,3), I = (3,2) → rectangle rule.
- X → take column of I (col 2) → (5,2) = **W**
- I → take column of X (col 3) → (3,3) = **K**
  XI → WK

Final Ciphertext

Combine results: **RO | WK = ROWK**

Step 3: Decryption (to show X handling works)

Now decrypt **ROWK** back to plaintext:

1. **RO** → R(4,2), O(1,4) → rectangle rule → (4,4)=T, (1,2)=A → **TA**
2. **WK** → W(5,2), K(3,3) → rectangle rule → (5,3)=X, (3,2)=I → **XI**

Result: **TAXI**

Hill Cipher

The Hill Cipher is a **polygraphic substitution cipher** that works on blocks of letters (usually 2 or 3 at a time). It converts letters into numbers, uses a **key matrix** to transform them, and converts the result back to letters.

Steps for Encryption

Let’s say we use a **2×2 Hill Cipher** with key matrix

K=[abcd]K=[acbd]

and plaintext **"HI"**.

Step 1: Convert letters to numbers

Use A=0, B=1, …, Z=25.

- H → 7
- I → 8

Plaintext vector:

P=[78]P=[78]

Step 2: Multiply by key matrix (mod 26)
C=K×Pmod 26C=K×Pmod26

This gives the ciphertext vector CC.

Step 3: Convert back to letters

Each number becomes a letter (0→A, …, 25→Z).

Example 1

Suppose our key matrix is

$$K = \begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix}$$

Encrypting "HI" (P = [7, 8]):

$$C = \begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix} \begin{bmatrix} 7 \\ 8 \end{bmatrix} = \begin{bmatrix} 3 \times 7 + 3 \times 8 \\ 2 \times 7 + 5 \times 8 \end{bmatrix} = \begin{bmatrix} 45 \\ 54 \end{bmatrix} \mod 26 = \begin{bmatrix} 19 \\ 2 \end{bmatrix}$$

19 → T, 2 → C → Ciphertext = **TC**

Decryption

Decryption uses the inverse matrix of K (mod 26).
You compute inverse K mod 26, multiply by ciphertext vector, then convert back to letters.

Calculating the **inverse key matrix**

Example 1 — 2×2 Hill Cipher

Key matrix:

$$K = \begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix}$$

Step 1 — Compute the determinant

$$\det(K) = (3 * 5 - 3 * 2) = 15 - 6 = 9$$

Check gcd(9,26)=1 → ✅ invertible.

Step 2 — Find modular inverse of determinant

Find x such that:

$$9 \cdot x \equiv 1 \pmod{26}$$

- $9 * 3 = 27 \equiv 1 \pmod{26}$ → $det^{-1} = 3$

Step 3 — Compute adjugate matrix

For 2×2:

$$\text{adj}(K) = \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} = \begin{bmatrix} 5 & -3 \\ -2 & 3 \end{bmatrix}$$

Convert negative numbers modulo 26:

- -3 ≡ 23, -2 ≡ 24

$$\text{adj}(K) \mod 26 = \begin{bmatrix} 5 & 23 \\ 24 & 3 \end{bmatrix}$$

Step 4 — Multiply adjugate by det inverse

$$K^{-1} = det^{-1} \cdot adj(K) \mod 26 = 3 \cdot \begin{bmatrix} 5 & 23 \\ 24 & 3 \end{bmatrix} \mod 26$$

Multiply each entry by 3:

$$\begin{bmatrix} 15 & 69 \\ 72 & 9 \end{bmatrix} \mod 26 = \begin{bmatrix} 15 & 17 \\ 20 & 9 \end{bmatrix}$$

✅ **2×2 inverse matrix:**

$$K^{-1} = \begin{bmatrix} 15 & 17 \\ 20 & 9 \end{bmatrix}$$

3×3 Hill Cipher Inverse

Key matrix:

$$K = \begin{bmatrix} 2 & 4 & 5 \\ 9 & 2 & 1 \\ 3 & 17 & 7 \end{bmatrix}$$

Step 1 — Compute determinant

$$\det(K) = 2(2*7 - 1*17) - 4(9*7 - 1*3) + 5(9*17 - 2*3)$$

Step by step:

1. $2*7 - 1*17 = 14 - 17 = -3$ → 2*(-3) = -6
2. $9*7 - 1*3 = 63 - 3 = 60$ → -4*60 = -240
3. $9*17 - 2*3 = 153 - 6 = 147$ → 5*147 = 735

Sum: -6 - 240 + 735 = 489

Modulo 26: 489 mod 26 = 21 → $\det(K) = 21$

Check gcd(21,26)=1 → ✅ invertible.

Step 2 — Modular inverse of determinant

Find x: 21 * x ≡ 1 mod 26

- Try x=5 → 21*5=105 ≡ 1 mod 26 ✅
- So det^{-1} = 5

Step 3 — Compute adjugate (cofactor matrix transposed)

- Compute each cofactor $C_{ij} = (-1)^{i+j} \times \det(\text{minor})$
- I'll show a few:

1. C11: det of minor $\begin{bmatrix} 2 & 1 \\ 17 & 7 \end{bmatrix} = 2 * 7 - 1 * 17 = -3$ → multiply by (+1) = -3
2. C12: det of minor $\begin{bmatrix} 9 & 1 \\ 3 & 7 \end{bmatrix} = 9 * 7 - 1 * 3 = 63 - 3 = 60$ → multiply by (-1) = -60
3. C13: det of minor $\begin{bmatrix} 9 & 2 \\ 3 & 17 \end{bmatrix} = 9 * 17 - 2 * 3 = 153 - 6 = 147$ → (+1)*147=147

... Continue for all 9 entries, then **transpose** to get adjugate matrix.

Step 4 — Multiply adjugate by det^{-1} modulo 26

$$K^{-1} = 5 * adj(K) \mod 26$$

- Multiply each entry by 5, then reduce mod26 (convert negatives to positive by adding 26).
- This gives the final **3×3 inverse matrix**, which can then be used for decryption.

Example 2:

encryption **and** decryption **HELP** using the 2×2 Hill cipher with key matrix

$$K = \begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix}.$$

Step 1 — Convert letters to numbers (A=0 ... Z=25)

H=7, E=4, L=11, P=15. I split the plaintext into 2-letter blocks: **HE | LP** → vectors $P_1 = \begin{bmatrix} 7 \\ 4 \end{bmatrix}$, $P_2 = \begin{bmatrix} 11 \\ 15 \end{bmatrix}$.

Step 2 — Encrypt each block: compute $C = K \cdot P \bmod 26$.

For **HE**:

- Multiply: $\begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix} \begin{bmatrix} 7 \\ 4 \end{bmatrix} = \begin{bmatrix} 3 \times 7 + 3 \times 4 \\ 2 \times 7 + 5 \times 4 \end{bmatrix} = \begin{bmatrix} 21 + 12 \\ 14 + 20 \end{bmatrix} = \begin{bmatrix} 33 \\ 34 \end{bmatrix}$.
- Reduce mod 26: $33 \bmod 26 = 7,\ 34 \bmod 26 = 8$. So $C_1 = \begin{bmatrix} 7 \\ 8 \end{bmatrix}$ → numbers 7,8 map to letters **H I**.

For **LP**:

- Multiply: $\begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix} \begin{bmatrix} 11 \\ 15 \end{bmatrix} = \begin{bmatrix} 3 \times 11 + 3 \times 15 \\ 2 \times 11 + 5 \times 15 \end{bmatrix} = \begin{bmatrix} 33 + 45 \\ 22 + 75 \end{bmatrix} = \begin{bmatrix} 78 \\ 97 \end{bmatrix}$.
- Reduce mod 26: $78 \bmod 26 = 0,\ 97 \bmod 26 = 19$. So $C_2 = \begin{bmatrix} 0 \\ 19 \end{bmatrix}$ → numbers 0,19 map to letters **A T**.

Ciphertext: combine blocks → **HIAT**.

Step 3 — Decryption (recover plaintext from HIAT).

I need K^{-1} modulo 26. First compute $\det(K) = 3 \times 5 - 3 \times 2 = 15 - 6 = 9$. The modular inverse of 9 modulo 26 is the number d^{-1} with $9 \cdot d^{-1} \equiv 1 \pmod{26}$. Since $9 \cdot 3 = 27 \equiv 1 \pmod{26}$, we have $9^{-1} = 3$.

Compute the adjugate of K: $\mathrm{adj}(K) = \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} = \begin{bmatrix} 5 & -3 \\ -2 & 3 \end{bmatrix}$. Multiply adjugate by $9^{-1} = 3$ and reduce mod26:

$$K^{-1} = 3 \cdot \begin{bmatrix} 5 & -3 \\ -2 & 3 \end{bmatrix} \bmod 26 = \begin{bmatrix} 15 & -9 \\ -6 & 9 \end{bmatrix} \bmod 26 = \begin{bmatrix} 15 & 17 \\ 20 & 9 \end{bmatrix},$$

because $-9 \equiv 17$ and $-6 \equiv 20$ (mod 26). So $K^{-1} = \begin{bmatrix} 15 & 17 \\ 20 & 9 \end{bmatrix}$.

Now decrypt each ciphertext block C with $P = K^{-1} \cdot C \bmod 26$.

For first block $C_1 = \begin{bmatrix} 7 \\ 8 \end{bmatrix}$ (HI):

- Multiply: $\begin{bmatrix} 15 & 17 \\ 20 & 9 \end{bmatrix} \begin{bmatrix} 7 \\ 8 \end{bmatrix} = \begin{bmatrix} 15 \times 7 + 17 \times 8 \\ 20 \times 7 + 9 \times 8 \end{bmatrix} = \begin{bmatrix} 105 + 136 \\ 140 + 72 \end{bmatrix} = \begin{bmatrix} 241 \\ 212 \end{bmatrix}$.
- Reduce mod26: $241 \bmod 26 = 7,\ 212 \bmod 26 = 4$. That recovers $\begin{bmatrix} 7 \\ 4 \end{bmatrix}$ → **H E**.

For second block $C_2 = \begin{bmatrix} 0 \\ 19 \end{bmatrix}$ (AT):

- Multiply: $\begin{bmatrix} 15 & 17 \\ 20 & 9 \end{bmatrix} \begin{bmatrix} 0 \\ 19 \end{bmatrix} = \begin{bmatrix} 15 \times 0 + 17 \times 19 \\ 20 \times 0 + 9 \times 19 \end{bmatrix} = \begin{bmatrix} 323 \\ 171 \end{bmatrix}$.
- Reduce mod26: $323 \bmod 26 = 11,\ 171 \bmod 26 = 15$. That recovers $\begin{bmatrix} 11 \\ 15 \end{bmatrix}$ → **L P**.

Combine recovered blocks → **H E | L P** → **HELP**. Decryption successful.

Example 3:

I split and number the plaintext: HELLO → pad → **HELLOX** → blocks **HE | LL | OX**. Numerical vectors: HE = [7,4], LL = [11,11], OX = [14,23]. Encryption: $C = K \cdot P \bmod 26$.

1. For **HE**: $K \begin{bmatrix} 7 \\ 4 \end{bmatrix} = \begin{bmatrix} 3 \times 7 + 3 \times 4 \\ 2 \times 7 + 5 \times 4 \end{bmatrix} = \begin{bmatrix} 21 + 12 \\ 14 + 20 \end{bmatrix} = \begin{bmatrix} 33 \\ 34 \end{bmatrix} \bmod 26 = \begin{bmatrix} 7 \\ 8 \end{bmatrix}$ → letters **H I**.
2. For **LL**: $K \begin{bmatrix} 11 \\ 11 \end{bmatrix} = \begin{bmatrix} 3 \times 11 + 3 \times 11 \\ 2 \times 11 + 5 \times 11 \end{bmatrix} = \begin{bmatrix} 33 + 33 \\ 22 + 55 \end{bmatrix} = \begin{bmatrix} 66 \\ 77 \end{bmatrix} \bmod 26 = \begin{bmatrix} 14 \\ 25 \end{bmatrix}$ → letters **O Z**.
3. For **OX**: $K \begin{bmatrix} 14 \\ 23 \end{bmatrix} = \begin{bmatrix} 3 \times 14 + 3 \times 23 \\ 2 \times 14 + 5 \times 23 \end{bmatrix} = \begin{bmatrix} 42 + 69 \\ 28 + 115 \end{bmatrix} = \begin{bmatrix} 111 \\ 143 \end{bmatrix} \bmod 26 = \begin{bmatrix} 7 \\ 13 \end{bmatrix}$ → letters **H N**.

Combine blocks → ciphertext **H I O Z H N** → **HIOZHN**.

Now decryption to verify: det(K)=$3 \cdot 5 - 3 \cdot 2 = 9$, inverse of 9 mod 26 is 3, adjugate = $\begin{bmatrix} 5 & -3 \\ -2 & 3 \end{bmatrix}$, so $K^{-1} = 3 \cdot \text{adj} \bmod 26 = \begin{bmatrix} 15 & 17 \\ 20 & 9 \end{bmatrix}$. Apply $P = K^{-1} \cdot C \bmod 26$ to each ciphertext block: HI → [7,8] → $K^{-1}[7, 8] = [7, 4]$ → HE; OZ → [14,25] → $K^{-1}[14, 25] = [11, 11]$ → LL; HN → [7,13] → $K^{-1}[7, 13] = [14, 23]$ → OX. Recovered plaintext vector sequence → HELLOX; remove the padding **X** → **HELLO**.

Example 4: 3 x 3 Hill Cipher

Step 1 — Prepare plaintext

- Plaintext: **HELLO** (length 5)
- 3×3 Hill cipher requires blocks of 3 → pad with **X** to make it 6 letters: **HELLOX**
- Blocks: **HEL | LOX**

Step 2 — Convert letters to numbers (A=0 ... Z=25)

- H=7, E=4, L=11, L=11, O=14, X=23
- Block vectors:
  - HEL → $[7, 4, 11]$
  - LOX → $[11, 14, 23]$

Step 3 — Choose a 3×3 key matrix

Example key:

$$K = \begin{bmatrix} 2 & 4 & 5 \\ 9 & 2 & 1 \\ 3 & 17 & 7 \end{bmatrix}$$

Key must be **invertible modulo 26** for decryption.

Step 4 — Encrypt each block

Ciphertext vector: $C = K \cdot P \bmod 26$

1. **HEL → [7,4,11]**

$$C = \begin{bmatrix} 2 & 4 & 5 \\ 9 & 2 & 1 \\ 3 & 17 & 7 \end{bmatrix} \begin{bmatrix} 7 \\ 4 \\ 11 \end{bmatrix} = \begin{bmatrix} 2*7+4*4+5*11 \\ 9*7+2*4+1*11 \\ 3*7+17*4+7*11 \end{bmatrix} = \begin{bmatrix} 14+16+55 \\ 63+8+11 \\ 21+68+77 \end{bmatrix} = \begin{bmatrix} 85 \\ 82 \\ 166 \end{bmatrix} \quad \bmod 26 = \begin{bmatrix} 7 \\ 4 \\ 10 \end{bmatrix}$$

Numbers → letters: 7=H, 4=E, 10=K → **HEK**

2. **LOX → [11,14,23]**

$$C = K \cdot P \bmod 26 = \begin{bmatrix} 2*11+4*14+5*23 \\ 9*11+2*14+1*23 \\ 3*11+17*14+7*23 \end{bmatrix} = \begin{bmatrix} 22+56+115 \\ 99+28+23 \\ 33+238+161 \end{bmatrix} = \begin{bmatrix} 193 \\ 150 \\ 432 \end{bmatrix} \quad \bmod 26 = \begin{bmatrix} 11 \\ 20 \\ 16 \end{bmatrix}$$

Numbers → letters: 11=L, 20=U, 16=Q → **LUQ**