Classical Polygraphic Ciphers: Hill and Vigenère

Dr. Mohammed Tawfik kmkhol01@gmail.com

November 2025

1 1. Alphabet Mapping and Setup

The Hill Cipher operates on the principle that each letter of the English alphabet is assigned a numerical value, and all calculations are performed **modulo 26**.

Table 1: **Standard Alphabet-to-Number Mapping (A-M)**

Letter	A	B	C	D	E	F	G	H	I	J	K	L	M
Value	0	1	2	3	4	5	6	7	8	9	10	11	12

Table 2: **Standard Alphabet-to-Number Mapping (N-Z)**

Letter	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Value	13	14	15	16	17	18	19	20	21	22	23	24	25

2 2. Hill Cipher Example 1: Encryption (`CASH`, 2x2)

Key Details (Example 1)

- **Plaintext (P):** `CASH` (Digraphs: `CA`, `SH`)
- **Key Matrix ($\mathbf{K_1}$):** $\mathbf{K_1} = \begin{pmatrix} 3 & 5 \\ 2 & 7 \end{pmatrix}$

Step 2.1 & 2.2: Encryption

The core operation is matrix multiplication, $\mathbf{C} \equiv \mathbf{K} \cdot \mathbf{P} \pmod{26}$.

Matrix Multiplication Visualization
Ciphertext is calculated by $\mathbf{C} = \mathbf{K} \cdot \mathbf{P}$.

Figure 1: Visualization of the Hill Cipher Encryption formula: $\mathbf{C} \equiv \mathbf{K} \cdot \mathbf{P} \pmod{26}$

$$\texttt{CA} = \begin{pmatrix} 2 \\ 0 \end{pmatrix} \implies \mathbf{C_1} \equiv \begin{pmatrix} 3 & 5 \\ 2 & 7 \end{pmatrix} \begin{pmatrix} 2 \\ 0 \end{pmatrix} \equiv \begin{pmatrix} (3 \cdot 2) + (5 \cdot 0) \\ (2 \cdot 2) + (7 \cdot 0) \end{pmatrix} \equiv \begin{pmatrix} 6 \\ 4 \end{pmatrix} \pmod{26} \implies \textbf{GE}$$

$$\texttt{SH} = \begin{pmatrix} 18 \\ 7 \end{pmatrix} \implies \mathbf{C_2} \equiv \begin{pmatrix} 3 & 5 \\ 2 & 7 \end{pmatrix} \begin{pmatrix} 18 \\ 7 \end{pmatrix} \equiv \begin{pmatrix} 54 + 35 \\ 36 + 49 \end{pmatrix} \equiv \begin{pmatrix} 89 \\ 85 \end{pmatrix} \pmod{26} \equiv \begin{pmatrix} 11 \\ 7 \end{pmatrix} \implies \textbf{LH}$$

Final Encrypted Message (Example 1): `GELH`

---

3 3. Hill Cipher Example 1: Decryption (`GELH`)

Step 3.1: Find Determinant D_1 and Modular Inverse D_1^{-1}

- **Determinant (D_1):** $D_1 = det(\mathbf{K_1}) = (3 \cdot 7) - (5 \cdot 2) = \mathbf{11}$.
- **Modular Inverse (D_1^{-1}):** Find D_1^{-1} such that $11 \cdot D_1^{-1} \equiv 1 \pmod{26}$.

$$11 \cdot \mathbf{19} = 209$$

$$209 \bmod 26 = 1. \quad \text{Thus, } D_1^{-1} = \mathbf{19}$$

Step 3.2: Calculate the Inverse Matrix $\mathbf{K_1}^{-1}$

The decryption key is $\mathbf{K_1}^{-1} \equiv D_1^{-1} \cdot \text{adj}(\mathbf{K_1}) \pmod{26}$.

1. **Find Adjugate:** $\text{adj}(\mathbf{K_1}) = \begin{pmatrix} 7 & -5 \\ -2 & 3 \end{pmatrix}$
2. **Multiply by Inverse Det (19):**

$$\mathbf{K_1}^{-1} \equiv 19 \cdot \begin{pmatrix} 7 & -5 \\ -2 & 3 \end{pmatrix} \equiv \begin{pmatrix} 133 & -95 \\ -38 & 57 \end{pmatrix} \pmod{26}$$

3. **Reduce Elements** $\pmod{26}$**:**

$$\begin{aligned} 133 \bmod 26 &= \mathbf{3} \quad (5 \times 26 + 3) \\ -95 \bmod 26 &= \mathbf{9} \quad (-4 \times 26 + 9) \\ -38 \bmod 26 &= \mathbf{14} \quad (-2 \times 26 + 14) \\ 57 \bmod 26 &= \mathbf{5} \quad (2 \times 26 + 5) \end{aligned}$$

4. **Final Inverse Matrix:**

$$\mathbf{K_1}^{-1} = \boxed{\begin{pmatrix} 3 & 9 \\ 14 & 5 \end{pmatrix}}$$

Step 3.3 & 3.4: Decryption

$$\texttt{GE} = \begin{pmatrix} 6 \\ 4 \end{pmatrix} \implies \mathbf{P_1} \equiv \mathbf{K_1}^{-1} \cdot \begin{pmatrix} 6 \\ 4 \end{pmatrix} \equiv \begin{pmatrix} 18 + 36 \\ 84 + 20 \end{pmatrix} \equiv \begin{pmatrix} 54 \\ 104 \end{pmatrix} \pmod{26} \equiv \begin{pmatrix} 2 \\ 0 \end{pmatrix} \implies \textbf{CA}$$

$$\texttt{LH} = \begin{pmatrix} 11 \\ 7 \end{pmatrix} \implies \mathbf{P_2} \equiv \mathbf{K_1}^{-1} \cdot \begin{pmatrix} 11 \\ 7 \end{pmatrix} \equiv \begin{pmatrix} 33 + 63 \\ 154 + 35 \end{pmatrix} \equiv \begin{pmatrix} 96 \\ 189 \end{pmatrix} \pmod{26} \equiv \begin{pmatrix} 18 \\ 7 \end{pmatrix} \implies \textbf{SH}$$

Final Decrypted Message (Example 1): `CASH`

---

4 4. Hill Cipher Example 2: Encryption (`AJLOUN UNIVIRSITY`, 2x2)

Key Details (Example 2)

- **Plaintext (P):** `AJLOUNUNIVIRSITY` (16 letters)
- **Digraphs:** `AJ, LO, UN, UN, IV, IR, SI, TY`
- **New Key Matrix (K_2):** $\mathbf{K_2} = \begin{pmatrix} 23 & 2 \\ 5 & 3 \end{pmatrix}$

Step 4.1: Encryption

The core operation is $\mathbf{C} \equiv \mathbf{K_2} \cdot \mathbf{P} \pmod{26}$.

$$\texttt{AJ} = \begin{pmatrix} 0 \\ 9 \end{pmatrix} \implies \mathbf{C_1} \equiv \mathbf{K_2} \cdot \begin{pmatrix} 0 \\ 9 \end{pmatrix} \equiv \begin{pmatrix} 0+18 \\ 0+27 \end{pmatrix} \equiv \begin{pmatrix} 18 \\ 27 \end{pmatrix} \pmod{26} \equiv \begin{pmatrix} 18 \\ 1 \end{pmatrix} \implies \textbf{SB}$$

$$\texttt{LO} = \begin{pmatrix} 11 \\ 14 \end{pmatrix} \implies \mathbf{C_2} \equiv \mathbf{K_2} \cdot \begin{pmatrix} 11 \\ 14 \end{pmatrix} \equiv \begin{pmatrix} 253+28 \\ 55+42 \end{pmatrix} \equiv \begin{pmatrix} 281 \\ 97 \end{pmatrix} \pmod{26} \equiv \begin{pmatrix} 21 \\ 19 \end{pmatrix} \implies \textbf{VT}$$

$$\texttt{UN} = \begin{pmatrix} 20 \\ 13 \end{pmatrix} \implies \mathbf{C_3} \equiv \mathbf{K_2} \cdot \begin{pmatrix} 20 \\ 13 \end{pmatrix} \equiv \begin{pmatrix} 460+26 \\ 100+39 \end{pmatrix} \equiv \begin{pmatrix} 486 \\ 139 \end{pmatrix} \pmod{26} \equiv \begin{pmatrix} 18 \\ 9 \end{pmatrix} \implies \textbf{SJ}$$

$$\texttt{UN} = \begin{pmatrix} 20 \\ 13 \end{pmatrix} \implies \mathbf{C_4} \equiv \mathbf{K_2} \cdot \begin{pmatrix} 20 \\ 13 \end{pmatrix} \equiv \begin{pmatrix} 460+26 \\ 100+39 \end{pmatrix} \equiv \begin{pmatrix} 486 \\ 139 \end{pmatrix} \pmod{26} \equiv \begin{pmatrix} 18 \\ 9 \end{pmatrix} \implies \textbf{SJ}$$

$$\texttt{IV} = \begin{pmatrix} 8 \\ 21 \end{pmatrix} \implies \mathbf{C_5} \equiv \mathbf{K_2} \cdot \begin{pmatrix} 8 \\ 21 \end{pmatrix} \equiv \begin{pmatrix} 184+42 \\ 40+63 \end{pmatrix} \equiv \begin{pmatrix} 226 \\ 103 \end{pmatrix} \pmod{26} \equiv \begin{pmatrix} 18 \\ 25 \end{pmatrix} \implies \textbf{SZ}$$

$$\texttt{IR} = \begin{pmatrix} 8 \\ 17 \end{pmatrix} \implies \mathbf{C_6} \equiv \mathbf{K_2} \cdot \begin{pmatrix} 8 \\ 17 \end{pmatrix} \equiv \begin{pmatrix} 184+34 \\ 40+51 \end{pmatrix} \equiv \begin{pmatrix} 218 \\ 91 \end{pmatrix} \pmod{26} \equiv \begin{pmatrix} 10 \\ 13 \end{pmatrix} \implies \textbf{KN}$$

$$\texttt{SI} = \begin{pmatrix} 18 \\ 8 \end{pmatrix} \implies \mathbf{C_7} \equiv \mathbf{K_2} \cdot \begin{pmatrix} 18 \\ 8 \end{pmatrix} \equiv \begin{pmatrix} 414+16 \\ 90+24 \end{pmatrix} \equiv \begin{pmatrix} 430 \\ 114 \end{pmatrix} \pmod{26} \equiv \begin{pmatrix} 14 \\ 10 \end{pmatrix} \implies \textbf{OK}$$

$$\texttt{TY} = \begin{pmatrix} 19 \\ 24 \end{pmatrix} \implies \mathbf{C_8} \equiv \mathbf{K_2} \cdot \begin{pmatrix} 19 \\ 24 \end{pmatrix} \equiv \begin{pmatrix} 437+48 \\ 95+72 \end{pmatrix} \equiv \begin{pmatrix} 485 \\ 167 \end{pmatrix} \pmod{26} \equiv \begin{pmatrix} 17 \\ 11 \end{pmatrix} \implies \textbf{RL}$$

Final Encrypted Message (Example 2): `SBVTSJSJSZKNORL`

---

5 5. Hill Cipher Example 2: Decryption (SBVTSJSJ...)

Step 5.1: Find Determinant D_2 and Modular Inverse D_2^{-1}

- **Determinant (D_2):** $D_2 = det(\mathbf{K_2}) = (23 \cdot 3) - (2 \cdot 5) = 69 - 10 = \mathbf{59}$.
- **Modular Determinant:** $D_2 \equiv 59 \text{ mod } 26 = \mathbf{7} \pmod{26}$.
- **Modular Inverse (D_2^{-1}):** Find D_2^{-1} such that $7 \cdot D_2^{-1} \equiv 1 \pmod{26}$.

$$7 \cdot \mathbf{15} = 105$$

$$105 \text{ mod } 26 = 1. \quad \text{Thus, } D_2^{-1} = \boxed{\mathbf{15}}$$

Step 5.2: Calculate the Inverse Matrix $\mathbf{K_2}^{-1}$

The decryption key is $\mathbf{K_2}^{-1} \equiv D_2^{-1} \cdot \text{adj}(\mathbf{K_2}) \pmod{26}$.

1. **Find Adjugate:** $\text{adj}(\mathbf{K_2}) = \begin{pmatrix} 3 & -2 \\ -5 & 23 \end{pmatrix}$
2. **Multiply by Inverse Det (15):**

$$\mathbf{K_2}^{-1} \equiv 15 \cdot \begin{pmatrix} 3 & -2 \\ -5 & 23 \end{pmatrix} \equiv \begin{pmatrix} 45 & -30 \\ -75 & 345 \end{pmatrix} \pmod{26}$$

3. **Reduce Elements** $\pmod{26}$**:**

$$\begin{aligned} 45 \text{ mod } 26 &= \mathbf{19} \quad (1 \times 26 + 19) \\ -30 \text{ mod } 26 &= \mathbf{22} \quad (-2 \times 26 + 22) \\ -75 \text{ mod } 26 &= \mathbf{3} \quad (-3 \times 26 + 3) \\ 345 \text{ mod } 26 &= \mathbf{7} \quad (13 \times 26 + 7) \end{aligned}$$

4. **Final Inverse Matrix:**

$$\mathbf{K_2}^{-1} = \boxed{\begin{pmatrix} 19 & 22 \\ 3 & 7 \end{pmatrix}}$$

Step 5.3: Decryption (Selected Blocks)

$$\text{SB} = \begin{pmatrix} 18 \\ 1 \end{pmatrix} \implies \mathbf{P_1} \equiv \mathbf{K_2}^{-1} \cdot \begin{pmatrix} 18 \\ 1 \end{pmatrix} \equiv \begin{pmatrix} 342 + 22 \\ 54 + 7 \end{pmatrix} \equiv \begin{pmatrix} 364 \\ 61 \end{pmatrix} \pmod{26} \equiv \begin{pmatrix} 0 \\ 9 \end{pmatrix} \implies \boxed{\textbf{AJ}}$$

$$\text{VT} = \begin{pmatrix} 21 \\ 19 \end{pmatrix} \implies \mathbf{P_2} \equiv \mathbf{K_2}^{-1} \cdot \begin{pmatrix} 21 \\ 19 \end{pmatrix} \equiv \begin{pmatrix} 399 + 418 \\ 63 + 133 \end{pmatrix} \equiv \begin{pmatrix} 817 \\ 196 \end{pmatrix} \pmod{26} \equiv \begin{pmatrix} 11 \\ 14 \end{pmatrix} \implies \boxed{\textbf{LO}}$$

$$\text{RL} = \begin{pmatrix} 17 \\ 11 \end{pmatrix} \implies \mathbf{P_8} \equiv \mathbf{K_2}^{-1} \cdot \begin{pmatrix} 17 \\ 11 \end{pmatrix} \equiv \begin{pmatrix} 323 + 242 \\ 51 + 77 \end{pmatrix} \equiv \begin{pmatrix} 565 \\ 128 \end{pmatrix} \pmod{26} \equiv \begin{pmatrix} 19 \\ 24 \end{pmatrix} \implies \boxed{\textbf{TY}}$$

Final Decrypted Message (Example 2): `AJLOUNUNIVIRSITY`

---

6 6. Hill Cipher Example 3: Encryption (`AJLOUN CASTEL`, 3x3)

Key Details (Example 3)

- **Plaintext (P):** `AJLOUNCASTEL` (12 letters)
- **Trigraphs:** `AJL`, `OUN`, `CAS`, `TEL`
- **Key Matrix ($\mathbf{K_3}$):** $\mathbf{K_3} = \begin{pmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{pmatrix}$

Step 6.1: Encryption

$$\texttt{AJL} = \begin{pmatrix} 0 \\ 9 \\ 11 \end{pmatrix} \implies \mathbf{C_1} \equiv \mathbf{K_3} \cdot \begin{pmatrix} 0 \\ 9 \\ 11 \end{pmatrix} \equiv \begin{pmatrix} 0+216+11 \\ 0+144+110 \\ 0+153+165 \end{pmatrix} \equiv \begin{pmatrix} 227 \\ 254 \\ 318 \end{pmatrix} \pmod{26} \equiv \begin{pmatrix} 19 \\ 20 \\ 6 \end{pmatrix} \implies \textbf{TUG}$$

$$\texttt{OUN} = \begin{pmatrix} 14 \\ 20 \\ 13 \end{pmatrix} \implies \mathbf{C_2} \equiv \mathbf{K_3} \cdot \begin{pmatrix} 14 \\ 20 \\ 13 \end{pmatrix} \equiv \begin{pmatrix} 84+480+13 \\ 182+320+130 \\ 280+340+195 \end{pmatrix} \equiv \begin{pmatrix} 577 \\ 642 \\ 725 \end{pmatrix} \pmod{26} \equiv \begin{pmatrix} 5 \\ 18 \\ 25 \end{pmatrix} \implies \textbf{FSZ}$$

$$\texttt{CAS} = \begin{pmatrix} 2 \\ 0 \\ 18 \end{pmatrix} \implies \mathbf{C_3} \equiv \mathbf{K_3} \cdot \begin{pmatrix} 2 \\ 0 \\ 18 \end{pmatrix} \equiv \begin{pmatrix} 12+0+18 \\ 26+0+180 \\ 40+0+270 \end{pmatrix} \equiv \begin{pmatrix} 48 \\ 206 \\ 310 \end{pmatrix} \pmod{26} \equiv \begin{pmatrix} 22 \\ 24 \\ 24 \end{pmatrix} \implies \textbf{WYY}$$

$$\texttt{TEL} = \begin{pmatrix} 19 \\ 4 \\ 11 \end{pmatrix} \implies \mathbf{C_4} \equiv \mathbf{K_3} \cdot \begin{pmatrix} 19 \\ 4 \\ 11 \end{pmatrix} \equiv \begin{pmatrix} 114+96+11 \\ 247+64+110 \\ 380+68+165 \end{pmatrix} \equiv \begin{pmatrix} 229 \\ 405 \\ 528 \end{pmatrix} \pmod{26} \equiv \begin{pmatrix} 21 \\ 15 \\ 8 \end{pmatrix} \implies \textbf{VPF}$$

Final Encrypted Message (Example 3): `TUGFSZWYYVPF`

---

7 7. Hill Cipher Example 3: Decryption (`TUGFSZ...`)

Step 7.1: Find Determinant (D_3) and Inverse (D_3^{-1})

The Most Complex Step: Finding the 3×3 Modular Inverse.

$$D_3 = det(\mathbf{K_3}) = 6(240-170) - 24(195-200) + 1(221-320) = \mathbf{441}$$

- **Modular Determinant:** $D_3 \equiv 441 \bmod 26 = \mathbf{19} \pmod{26}$.

- **Modular Inverse:** We seek D_3^{-1} such that $19 \cdot D_3^{-1} \equiv 1 \pmod{26}$.

$$19 \cdot \mathbf{11} = 209$$

$$209 \bmod 26 = 1. \quad D_3^{-1} = \boxed{\mathbf{11}}$$

Step 7.2: Calculate the Inverse Matrix ($\mathbf{K_3}^{-1}$)

- **Adjugate Matrix (reduced $\pmod{26}$):** This is obtained by finding the cofactor matrix, transposing it, and reducing $\pmod{26}$.

$$\text{adj}(\mathbf{K_3}) \equiv \begin{pmatrix} 18 & 21 & 16 \\ 5 & 18 & 5 \\ 5 & 14 & 18 \end{pmatrix} \pmod{26}$$

- **Final Inverse Matrix ($\mathbf{K_3}^{-1} \equiv 11 \cdot \textbf{adj}(\mathbf{K_3})$):**

$$\mathbf{K_3}^{-1} \equiv 11 \cdot \begin{pmatrix} 18 & 21 & 16 \\ 5 & 18 & 5 \\ 5 & 14 & 18 \end{pmatrix} \equiv \begin{pmatrix} 198 & 231 & 176 \\ 55 & 198 & 55 \\ 55 & 154 & 198 \end{pmatrix} \pmod{26}$$

$$\mathbf{K_3}^{-1} = \boxed{\begin{pmatrix} 16 & 23 & 20 \\ 3 & 16 & 3 \\ 3 & 24 & 16 \end{pmatrix}}$$

Step 7.3: Decryption

$$\texttt{TUG} = \begin{pmatrix} 19 \\ 20 \\ 6 \end{pmatrix} \implies \mathbf{P_1} \equiv \mathbf{K_3}^{-1} \cdot \begin{pmatrix} 19 \\ 20 \\ 6 \end{pmatrix} \equiv \begin{pmatrix} 304 + 460 + 120 \\ 57 + 320 + 18 \\ 57 + 480 + 96 \end{pmatrix} \equiv \begin{pmatrix} 884 \\ 395 \\ 633 \end{pmatrix} \pmod{26} \equiv \begin{pmatrix} 0 \\ 9 \\ 11 \end{pmatrix} \implies \boxed{\textbf{AJL}}$$

$$\texttt{FSZ} = \begin{pmatrix} 5 \\ 18 \\ 25 \end{pmatrix} \implies \mathbf{P_2} \equiv \mathbf{K_3}^{-1} \cdot \begin{pmatrix} 5 \\ 18 \\ 25 \end{pmatrix} \equiv \begin{pmatrix} 80 + 414 + 500 \\ 15 + 288 + 75 \\ 15 + 432 + 400 \end{pmatrix} \equiv \begin{pmatrix} 994 \\ 378 \\ 847 \end{pmatrix} \pmod{26} \equiv \begin{pmatrix} 14 \\ 20 \\ 13 \end{pmatrix} \implies \boxed{\textbf{OUN}}$$

Final Decrypted Message (Example 3): `AJLOUNCASTEL`

---

8 8. The Vigenère Cipher: Polyalphabetic Substitution

The Vigenère Cipher is a method of encrypting alphabetic text by using a simple series of Caesar ciphers based on the letters of a keyword. It's classified as a **polyalphabetic cipher** because a single plaintext letter can map to multiple ciphertext letters, making it much more robust against frequency analysis than simple monoalphabetic ciphers.

Vigenère Tableau (Vigenère Square)

The tableau consists of 26 different Caesar ciphers. The **row** index is determined by the plaintext letter, and the **column** index is determined by the key letter.

Table 3: **Vigenère Tableau**

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

Formulas

- **Encryption:** $C_i = (P_i + K_i) \pmod{26}$
- **Decryption:** $P_i = (C_i - K_i) \pmod{26}$

9 9. Vigenère Cipher Example 4: Encryption

Key Details (Example 4)

- **Plaintext (P):** ATTACKATDAWN
- **Key (K):** LEMON

Step 9.1: Set up Key Stream

Plaintext (P)	A	T	T	A	C	K	A	T	D	A	W	N
Key Stream (K)	L	E	M	O	N	L	E	M	O	N	L	E

Step 9.2: Encryption Calculation

Index (i)	1	2	3	4	5	6	7	8	9	10	11	12
P_i (Value)	0	19	19	0	2	10	0	19	3	0	22	13
K_i (Value)	11	4	12	14	13	11	4	12	14	13	11	4
$C_i = (P_i + K_i)$ mod 26	11	23	5	14	15	21	4	5	17	13	7	17
Ciphertext	L	X	F	O	P	V	E	F	R	N	H	R

Final Encrypted Message (Example 4): LXFOPVEFRNHR

10 10. Vigenère Cipher Example 5: Decryption

Key Details (Example 5)

- **Ciphertext (C):** LXFOPVEFRNHR
- **Key (K):** LEMON

Step 10.1: Decryption Calculation

The decryption formula is $P_i = (C_i - K_i) \pmod{26}$.

Index (i)	1	2	3	4	5	6	7	8	9	10	11	12
C_i (Value)	11	23	5	14	15	21	4	5	17	13	7	17
K_i (Value)	11	4	12	14	13	11	4	12	14	13	11	4
$P_i = (C_i - K_i)$ mod 26	0	19	-7	0	2	10	0	-7	3	0	-4	13
Final P_i (mod26)	0	19	19	0	2	10	0	19	3	0	22	13
Plaintext	A	T	T	A	C	K	A	T	D	A	W	N

Final Decrypted Message (Example 5): ATTACKATDAWN

---

11 11. Conclusion: Cipher Comparison

The Hill and Vigenère Ciphers are both polyalphabetic ciphers designed to defeat frequency analysis, but they achieve this through fundamentally different mathematical and structural approaches.

- **Hill Cipher (Block-based):** This cipher uses **linear algebra and matrix operations** to encrypt blocks of text (digraphs, trigraphs, etc.). The substitution for each letter in a block is dependent on every other letter in that block. This creates high **diffusion**, where changing one plaintext letter drastically changes the entire ciphertext block. However, it requires complex matrix inversion for decryption.
- **Vigenère Cipher (Stream-based):** This cipher uses **modular addition** to encrypt text one letter at a time, based on a repeating keyword. It creates a key stream that shifts the alphabet cyclically. It offers good security against simple frequency analysis but is vulnerable to the Kasiski attack if the keyword length is discovered.