Classic Ciphers (Continued)

CЯ4CK1NG-THΞ-C0D3

Today’s Roadmap

- Continuation of Substitution Ciphers (Playfair, Hill)
- Introduction to Transposition Ciphers (Rail Fence, Columnar)
- Hands-on with Ciphers, CTF and Assignment discussion

Recap on Substitution Ciphers

- Three types:
  - Monoalphabetic cipher
  - Polyalphabetic cipher
  - Polygraphic cipher
- Question:

  Now place the ciphers we learnt last class into the above types

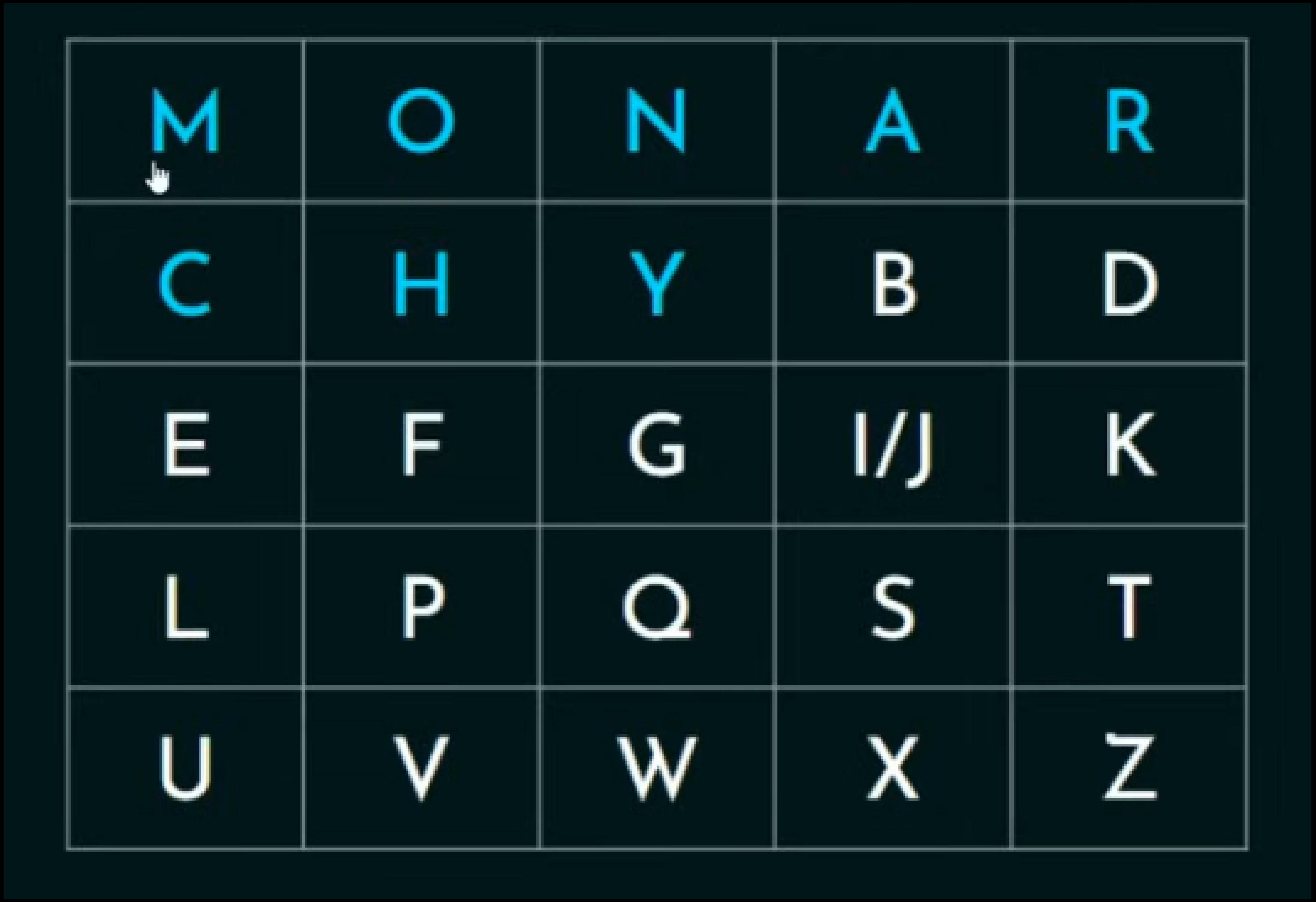
Introduction to a Polyalphabetic Substitution Cipher

The Playfair Cipher

- Origin: Developed in the mid-19th century and widely used during WW I and II.
- Inventor: Sir Charles Wheatstone designed it in 1854, but it was promoted by Lord Playfair - hence the name.
- Method: A digraph substitution cipher that encrypts pairs of letters using a 5×5 grid generated from a keyword. Each pair of letters is substituted according to the positions of letters in the grid.
- Purpose: By encrypting two letters at a time, it breaks the simple frequency patterns of single-letter substitution, making it significantly harder to crack with frequency analysis.

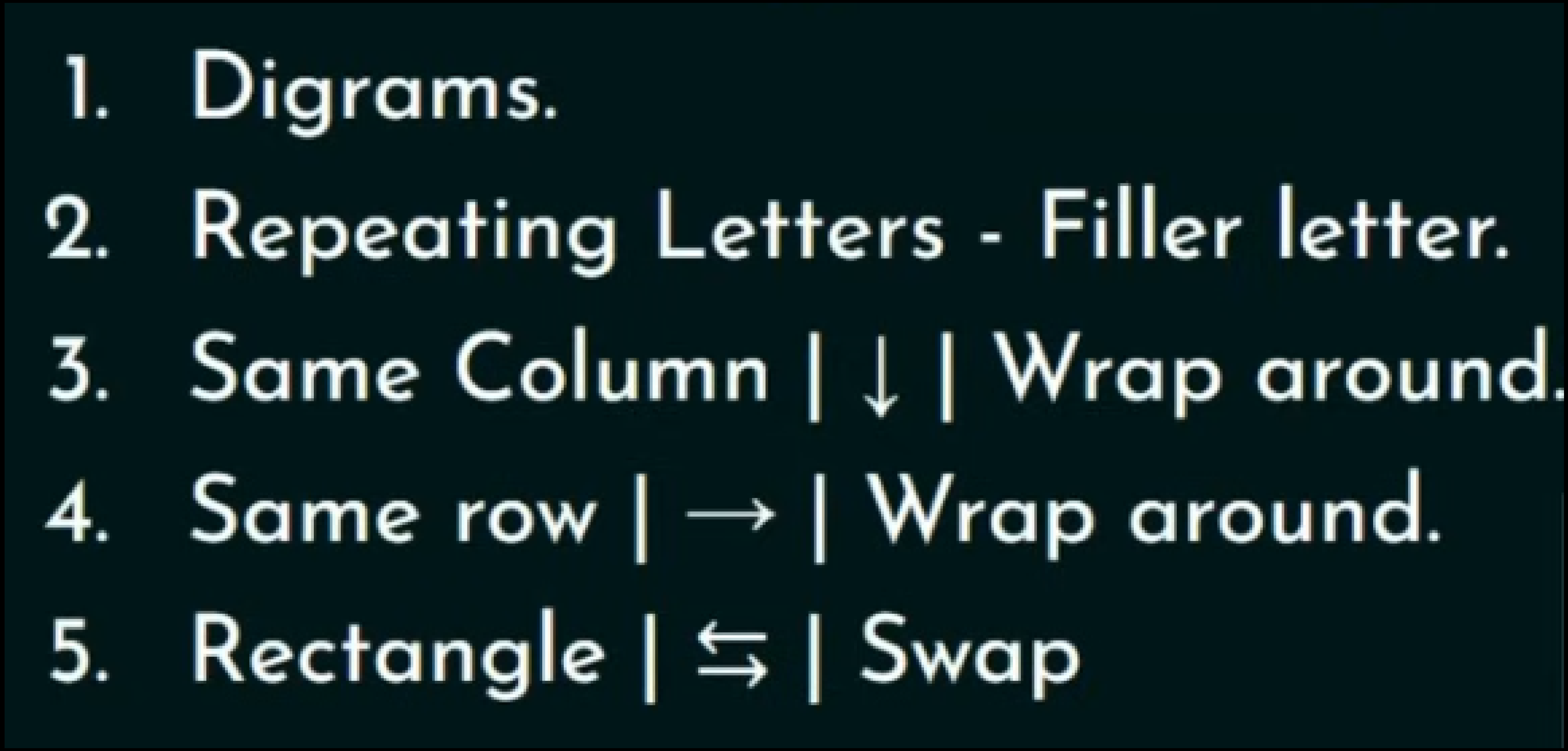
Step 1: Matrix Construction

Here, as an example, the Keyword is ‘MONARCHY’



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

Step 2: Rules of Encryption

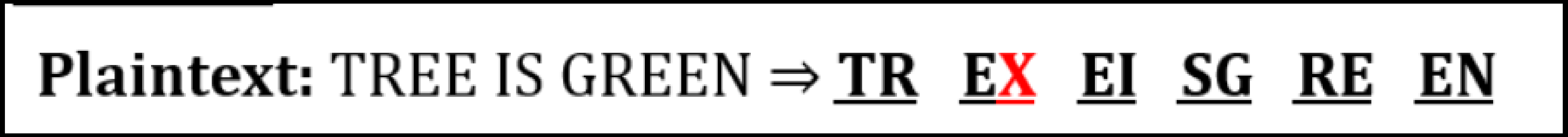


1. Digrams.
2. Repeating Letters - Filler letter.
3. Same Column | ↓ | Wrap around.
4. Same row | → | Wrap around.
5. Rectangle | ⇆ | Swap

Step 3: Creating Digraph and using Fillers

What is a Digraph?

- In cryptography, a digraph is simply a pair of letters treated as a single unit.
- In monoalphabetic ciphers (like Caesar), you encrypt one letter at a time.
- In the Playfair cipher, you encrypt two letters (a digraph) at a time.



Plaintext: TREE IS GREEN ⇒ **TR EX EI SG RE EN**

Questions

Write the digraphs for the following:

Plain text: attack

digraphs:

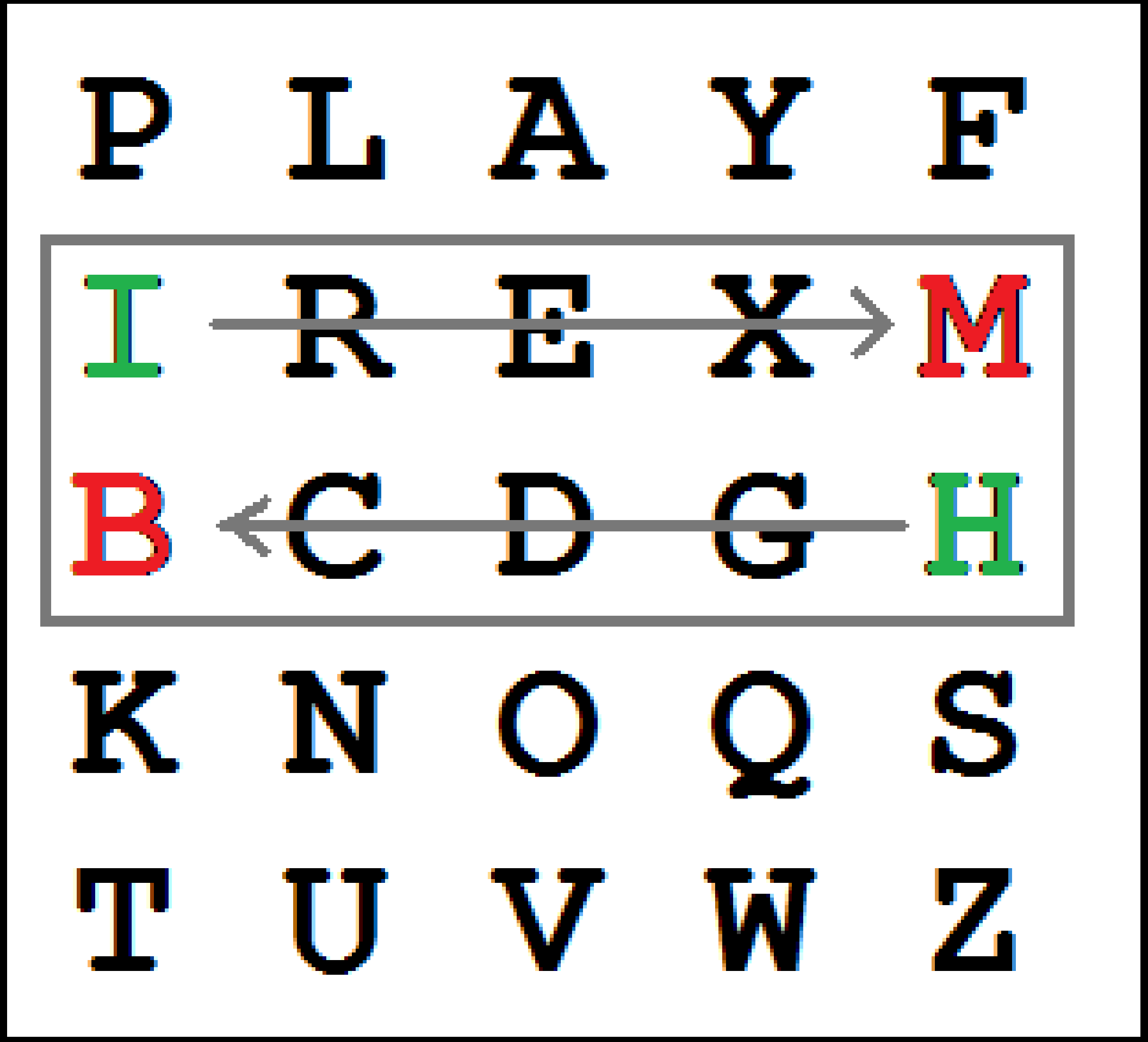
Plain text: instruments

digraphs:

Plain text: balloon

digraphs:

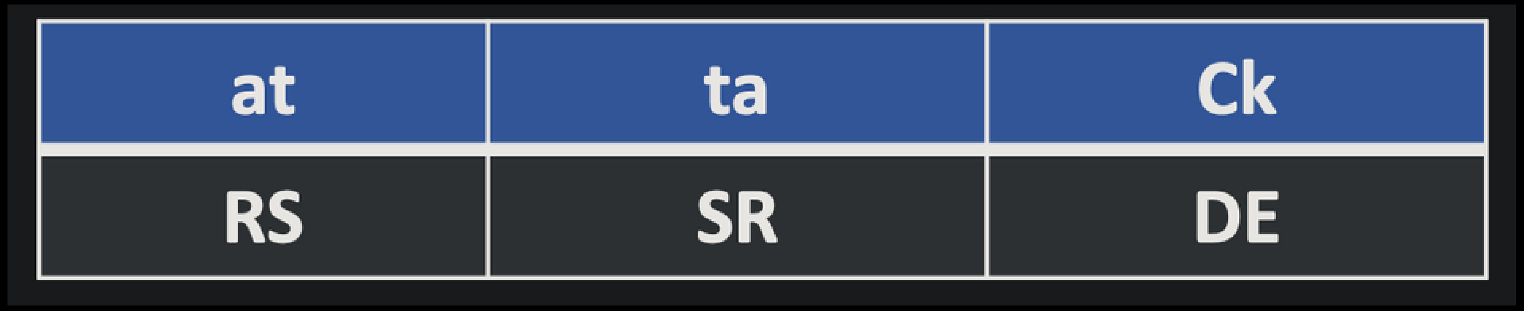
digraphs:



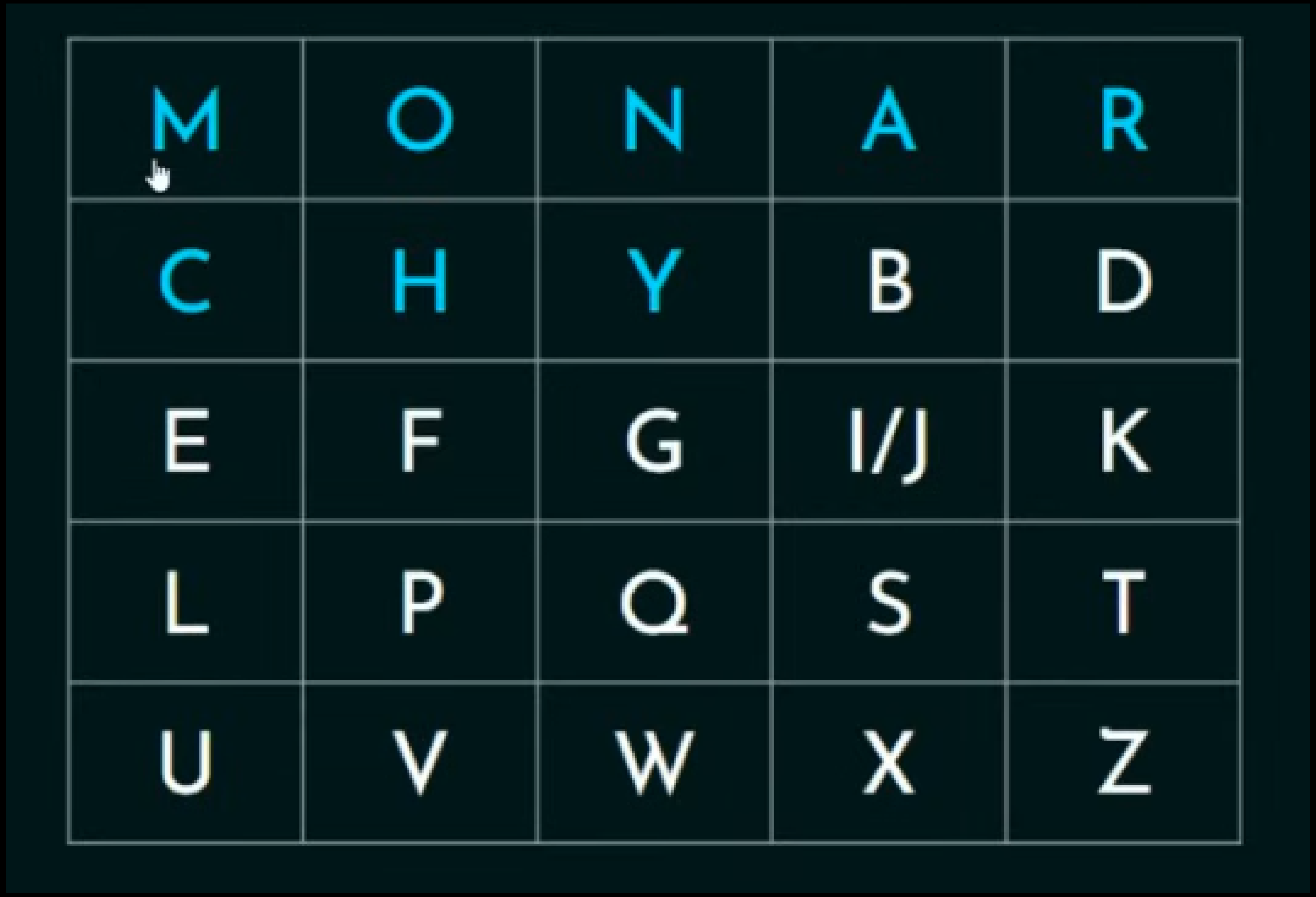
P	L	A	Y	F
I	R	E	X	M
B	C	D	G	H
K	N	O	Q	S
T	U	V	W	Z

Example question

- Plain text: attack
- Diagram: at ta ck
- Cipher text:



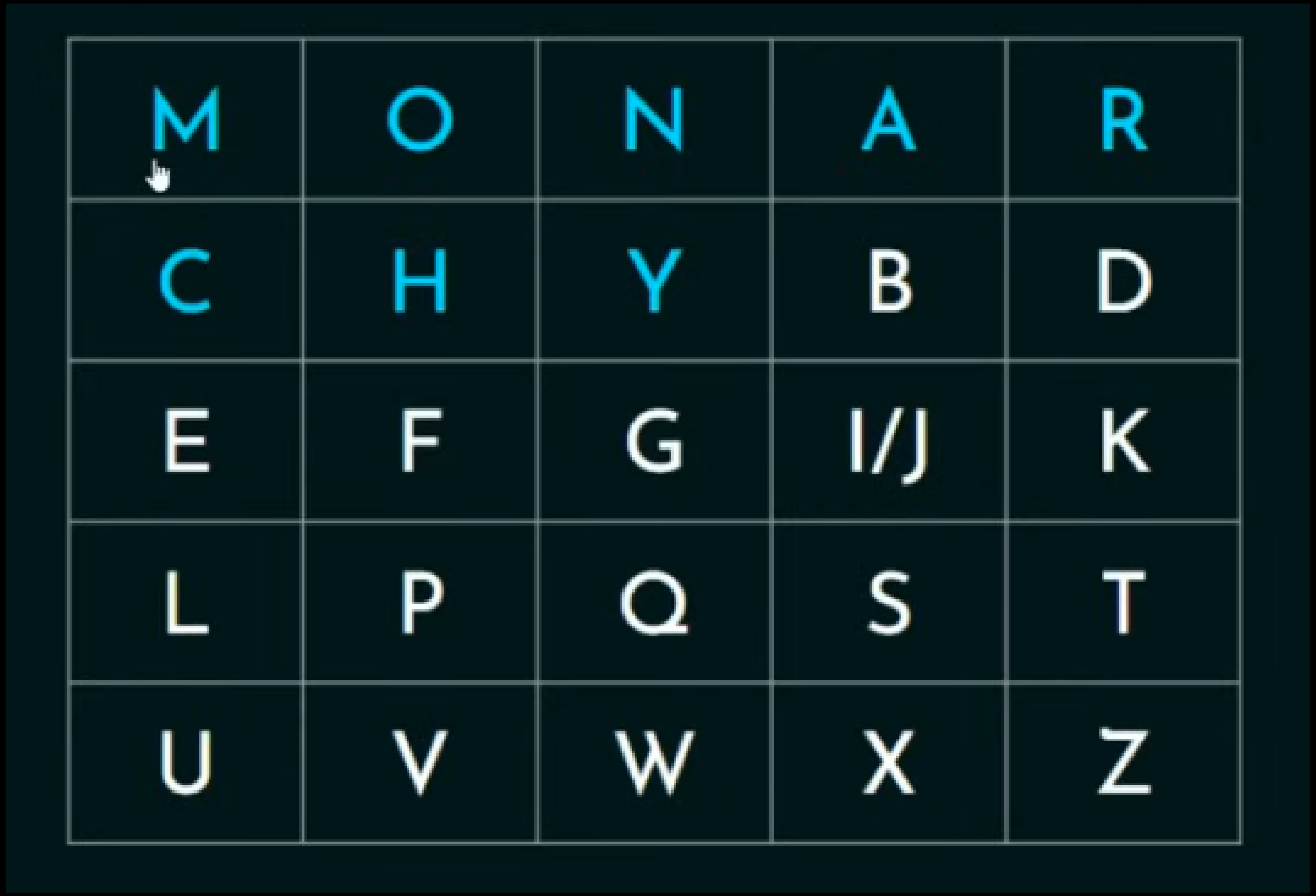
at	ta	Ck
RS	SR	DE



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

Question

- Plain text: instruments
- Key: Monarchy
- Cipher text: gatlmzclrqtx



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

Finally, The Polygraphic Substitution Cipher

The Hill Cipher

- Origin: Introduced in 1929 as one of the first ciphers based on linear algebra.
- Inventor: Lester S. Hill, an American mathematician.
- Method: A polygraphic cipher that encrypts blocks of letters by turning them into vectors and multiplying with an invertible key matrix (mod 26).
- Purpose: Conceals frequency patterns by encrypting multiple letters at once, making simple frequency analysis ineffective and showcasing the power of math in cryptography.

Hill Cipher Prerequisites

Concepts to be familiar with

- Matrix Multiplication
- Finding inverse and adjoint of matrix
- Calculating mod and inverse mod of a number

Hill Cipher Notations

- P = Plaintext Matrix
- C = Ciphertext Matrix
- K = Key Matrix

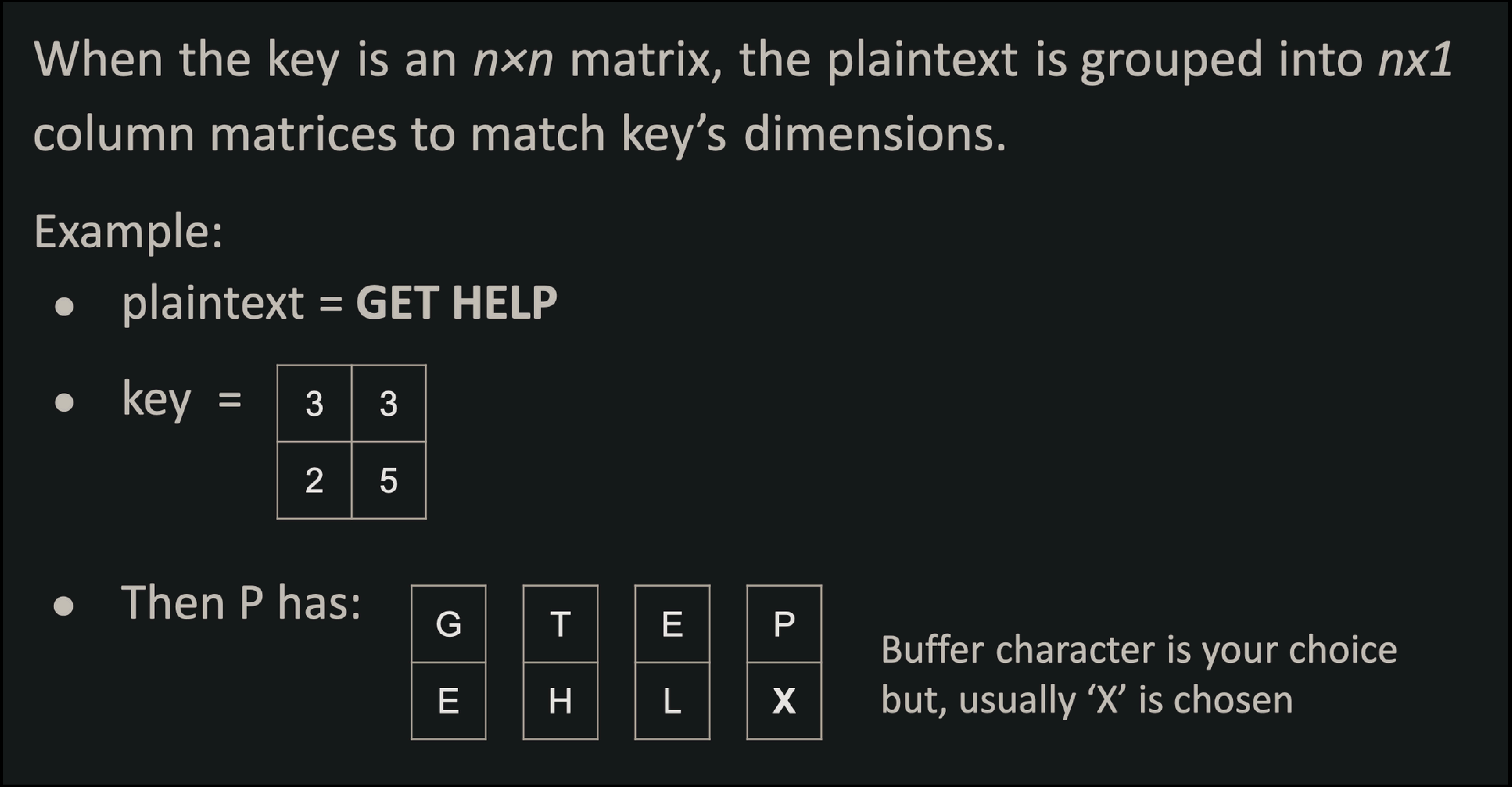
Formulae (when input is alphabetical)

- Encryption:
    - C = KP mod 26
- Decryption:
    - P = K^(-1)C mod 26

OK, but what does any of that mean?

Lets take an example

Step 1: Grouping Plaintext Characters



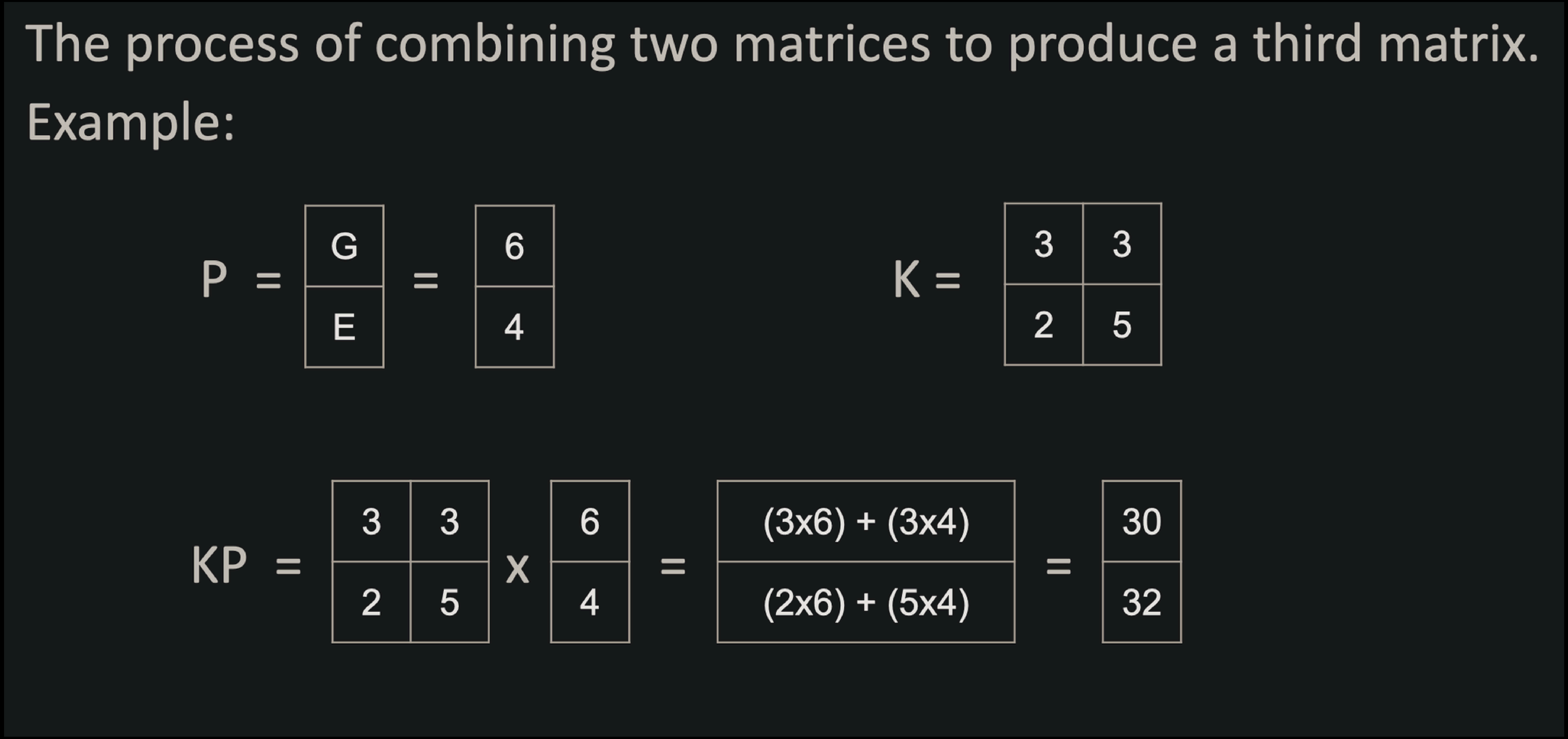
When the key is an *n×n* matrix, the plaintext is grouped into *nx1* column matrices to match key's dimensions.

Example:

- plaintext = **GET HELP**
- key = $\begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix}$
- Then P has: $\begin{bmatrix} G \\ E \end{bmatrix}$ $\begin{bmatrix} T \\ H \end{bmatrix}$ $\begin{bmatrix} E \\ L \end{bmatrix}$ $\begin{bmatrix} P \\ \mathbf{X} \end{bmatrix}$

Buffer character is your choice but, usually 'X' is chosen

Step 2: Matrix Multiplication



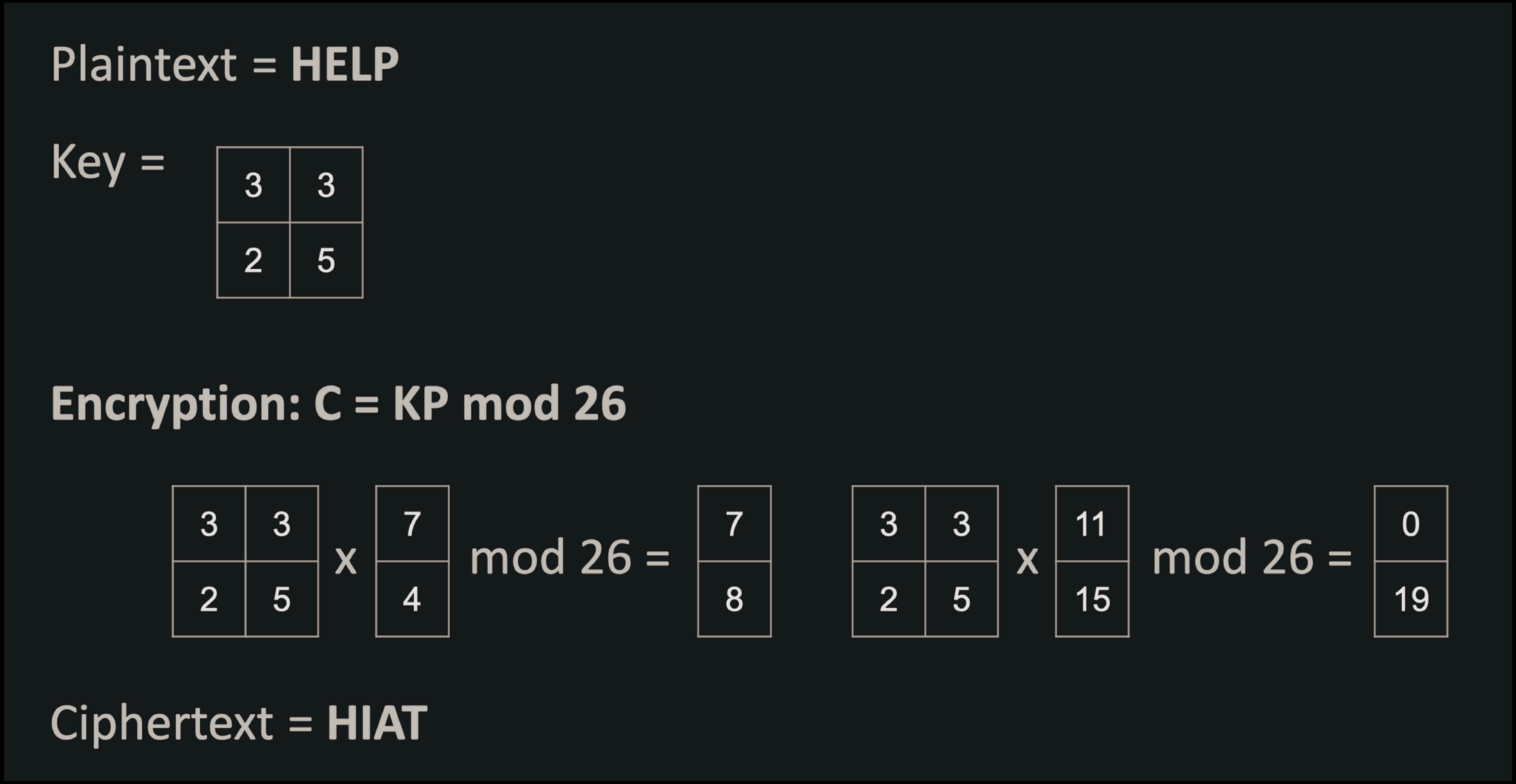
The process of combining two matrices to produce a third matrix.

Example:

$$P = \begin{bmatrix} G \\ E \end{bmatrix} = \begin{bmatrix} 6 \\ 4 \end{bmatrix} \qquad K = \begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix}$$

$$KP = \begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix} \text{x} \begin{bmatrix} 6 \\ 4 \end{bmatrix} = \begin{bmatrix} (3\text{x}6) + (3\text{x}4) \\ (2\text{x}6) + (5\text{x}4) \end{bmatrix} = \begin{bmatrix} 30 \\ 32 \end{bmatrix}$$

Step 3: Conversion to Alphabet



Plaintext = **HELP**

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

Encryption: C = KP mod 26

$$\begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix} \text{ x } \begin{bmatrix} 7 \\ 4 \end{bmatrix} \text{ mod } 26 = \begin{bmatrix} 7 \\ 8 \end{bmatrix} \qquad \begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix} \text{ x } \begin{bmatrix} 11 \\ 15 \end{bmatrix} \text{ mod } 26 = \begin{bmatrix} 0 \\ 19 \end{bmatrix}$$

Ciphertext = **HIAT**

Decryption Process

It might get a little tedious to bear with us

Steps:

1. Inverse of Matrix
2. Adjoint of Matrix
3. Modulo of the resultant

Lets do it with an example

Ciphertext = **HIAT**

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

Decryption: $P = K^{-1}C \bmod 26$

1. Calculate $K^{-1} \bmod 26$

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

Thats a lot..

lets take a break from all that solving

Cracking the Uncrackable Code 😌
Copy link
GREAT BIG STORY
Watch on YouTube

Lastly, Transposition Ciphers

Transposition Ciphers

- A transposition cipher (also known as a permutation cipher) is a method of encryption which scrambles the positions of characters (transposition) without changing the characters themselves.

- Transposition ciphers reorder units of plaintext (typically characters or groups of characters) according to a regular system to produce a ciphertext.

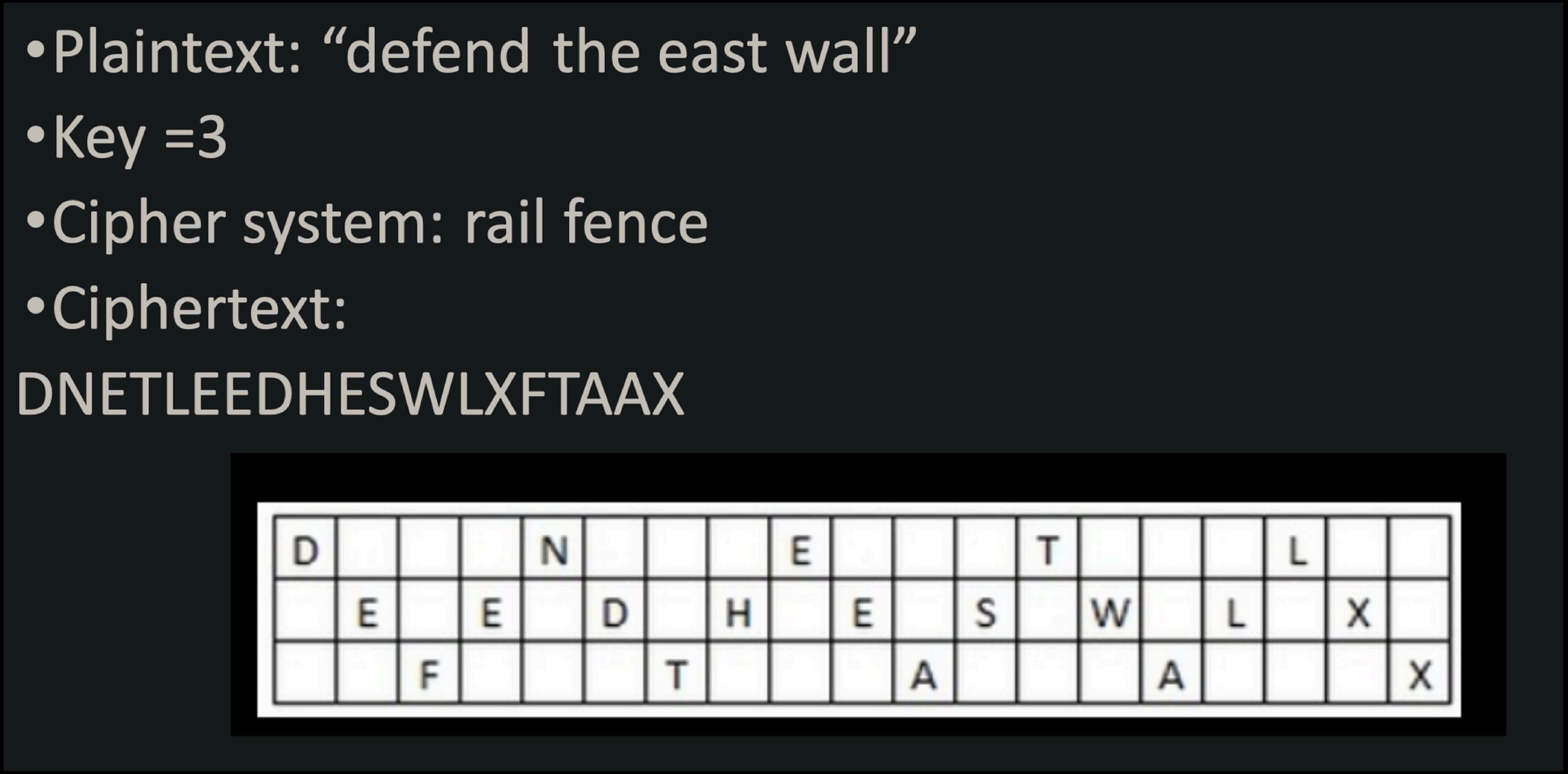
Types:

- Three types:
    - Rail Fence Transposition Cipher
    - Block (Single Columnar) Transposition Cipher
    - Double Columnar Transposition Cipher

The Rail Fence Cipher

- Origin: Dates back to ancient times; widely recognized as a simple form of transposition cipher.
- Inventor: Exact origin unknown, but commonly used as a basic teaching example of transposition.
- Method: A transposition cipher where letters of the plaintext are written diagonally in a zig-zag (rail fence) pattern across multiple “rails” and then read row by row to form ciphertext.
- Purpose: Rearranges letters instead of substituting them, making the message unreadable without knowing the number of rails (the key). It demonstrates how secrecy can be achieved purely by reordering, not altering characters.

Lets get into it with an example



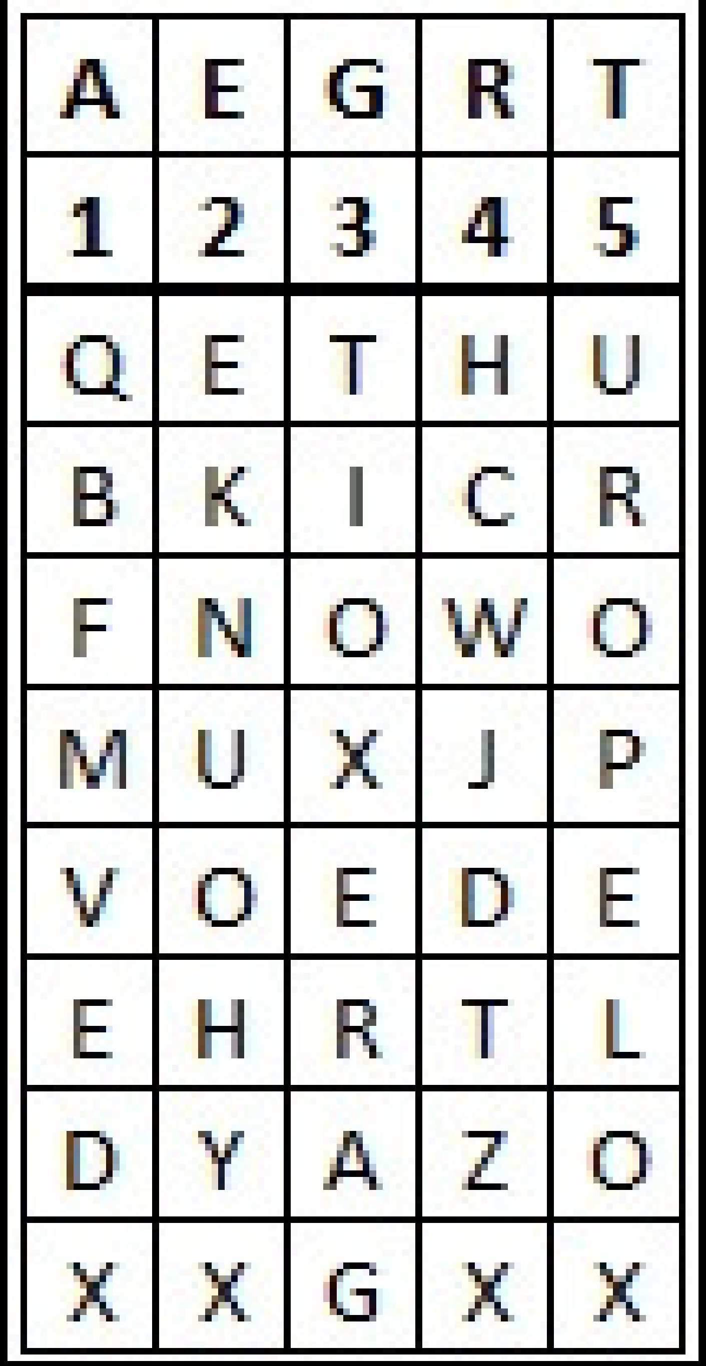
- Plaintext: “defend the east wall”
- Key =3
- Cipher system: rail fence
- Ciphertext:

DNETLEEDHESWLXFTAAX

D				N				E				T				L		
	E		E		D		H		E		S		W		L		X	
		F				T				A				A				X

Now how would you decrypt that?

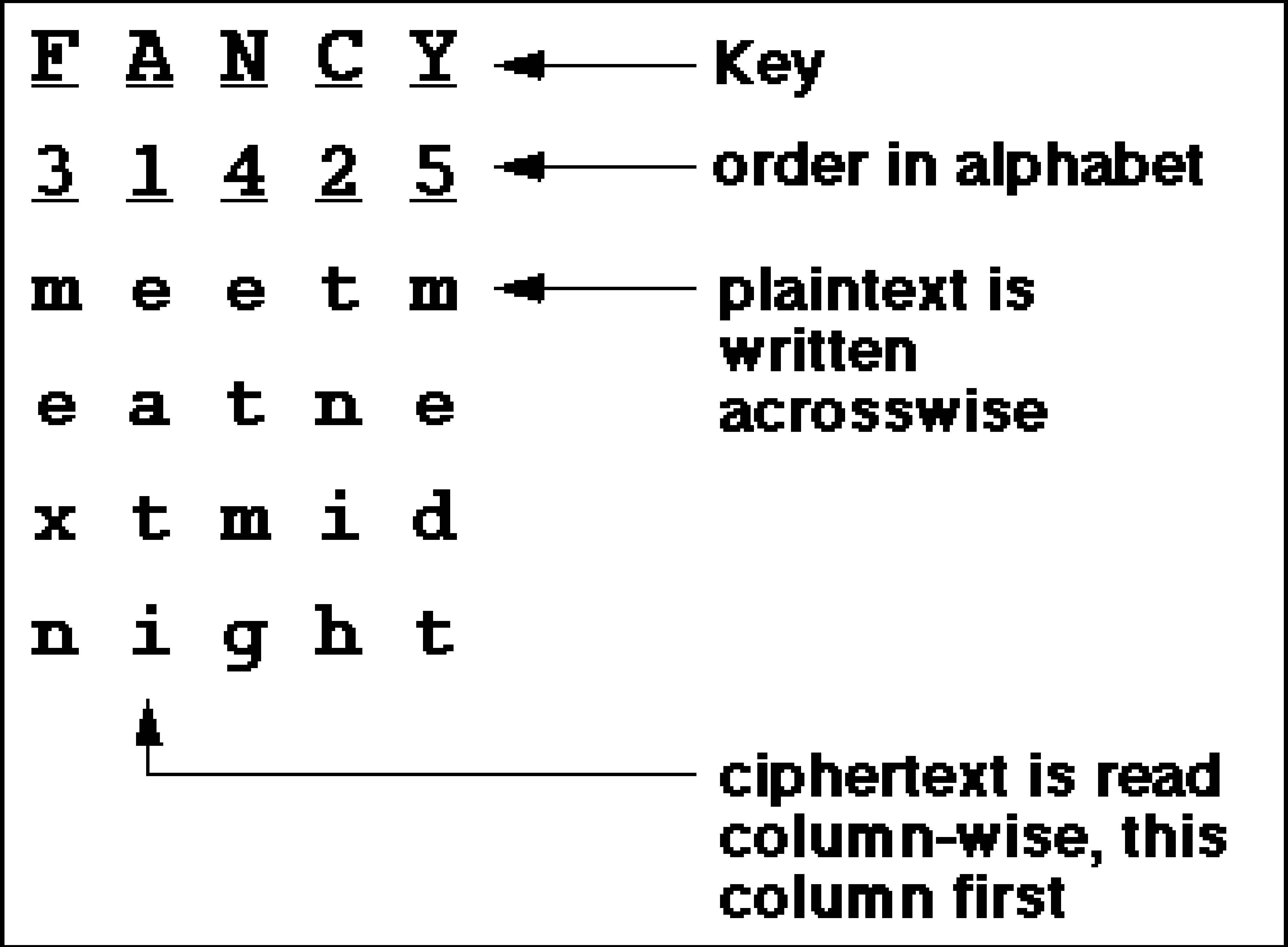
The Columnar Transposition cipher



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

- Origin: Traces back to early manual encryption techniques used in classical cryptography.
- Inventor: It evolved naturally from simpler transposition methods like the rail fence cipher.
- Method: A transposition cipher where the plaintext is written in rows under a keyword. The columns are then rearranged based on the alphabetical order of the keyword’s letters to generate the ciphertext.
- Purpose: Focuses on rearranging letter positions rather than substituting them, providing stronger scrambling than the rail fence cipher. It highlights how structured reordering and a secret key can effectively obscure the original message.

Here’s an example



F	A	N	C	Y
3	1	4	2	5
m	e	e	t	m
e	a	t	n	e
x	t	m	i	d
n	i	g	h	t

Key

order in alphabet

plaintext is written acrosswise

ciphertext is read column-wise, this column first

So now what would a “Double Columnar Transposition Cipher” be?

Hands on for implementing the same

Read carefully:

Among the endless symbols a secret lies,
digits of earth and sky disguise.
In the poster’s maze where @’s and &’s roam,
seek the numbers that point you home.
Two parts—north and west—form a pair;
enter them together and the flag waits there.

The poster you’ve been seeing all this while is not just art—it’s a cipher.
Find the numbers hidden inside, piece them into coordinates, and enter them on our website.