The Islamic University
College of Technical Engineering
Department of Computer Technical Engineering

Fourth Stage

Security

Lecture 9

Asst. Lec. Yousif Samer Mudhafar

Email: yousif.samir19@gmail.com

Lecture objective

The student will recognize the following objective :

- **Encryption and Decryption using Mono Alphabetic Cipher.**

Mono Alphabetic Or Substitution Cipher

- A monoalphabetic substitution cipher, also known as a simple substitution cipher, relies on a fixed replacement structure. That is, the substitution is fixed for each letter of the alphabet. Thus, if "a" is encrypted to "R", then every time we see the letter "a" in the plaintext, we replace it with the letter "R" in the Ciphertext.
- With only 25 possible keys, the Caesar Cipher is far from secure. A dramatic increase in the key space can be achieved by allowing by allowing an arbitrary substitution. Before proceeding, we define the term permutation. A permutation of a finite set of elements is an ordered sequence of all the elements of, with each element appearing exactly once.

Mono Alphabetic

Alice

Sender

Bob

Receiver

Depends on Alice in Message Encryption Mode or Cipher text Mode

Encryption

Depends on the sender for setting it to encrypt messages

Decryption

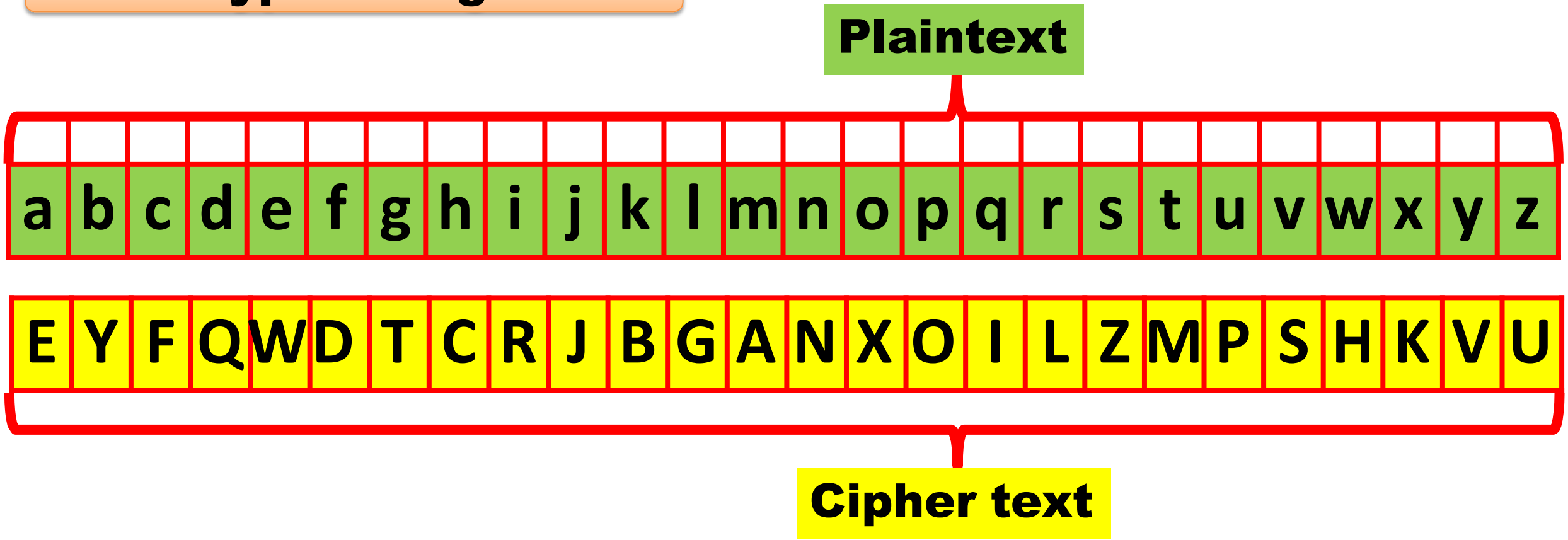
Cipher text

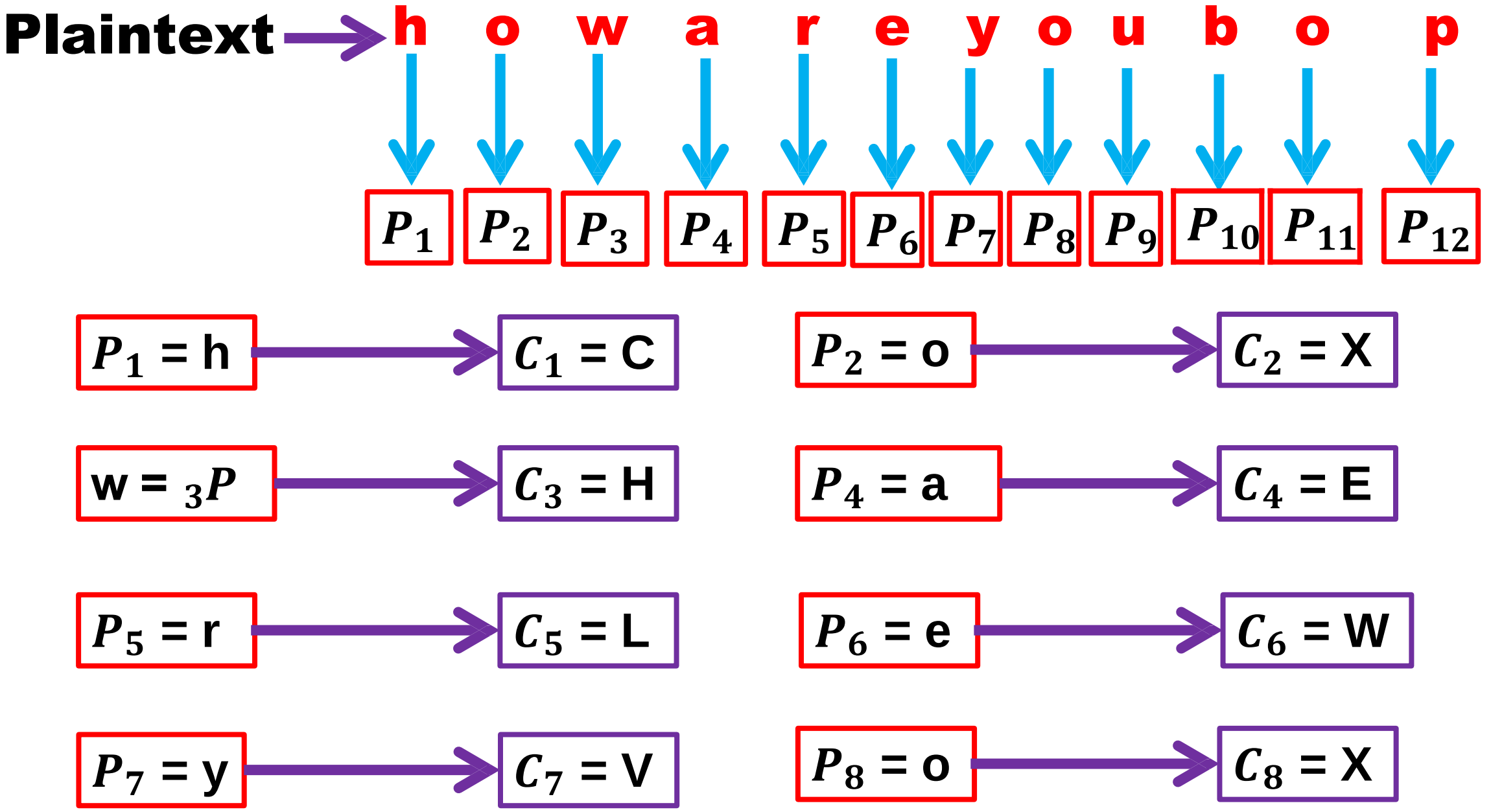
Example 1

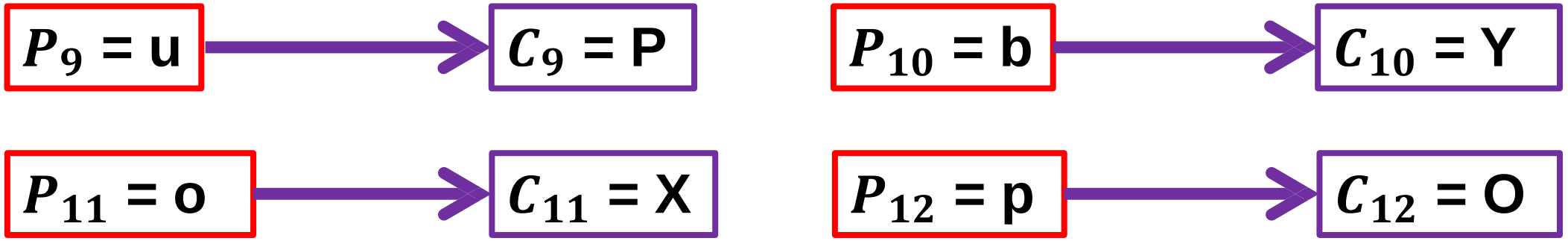
Encrypt and decrypt the message “**how are you bop**” by using **Mono Alphabetic**.

Ans:-

1. Encryption Algorithm




Plaintext
h o w a r e y o u b o p
P_1 P_2 P_3 P_4 P_5 P_6 P_7 P_8 P_9 P_{10} P_{11} P_{12}
P_1 = h
C_1 = C
P_2 = o
C_2 = X
w = $_3P$
C_3 = H
P_4 = a
C_4 = E
P_5 = r
C_5 = L
P_6 = e
C_6 = W
P_7 = y
C_7 = V
P_8 = o
C_8 = X



The **Cipher text** is "**CXHELWVXPYXO**"

2. Decryption Algorithm

Cipher text

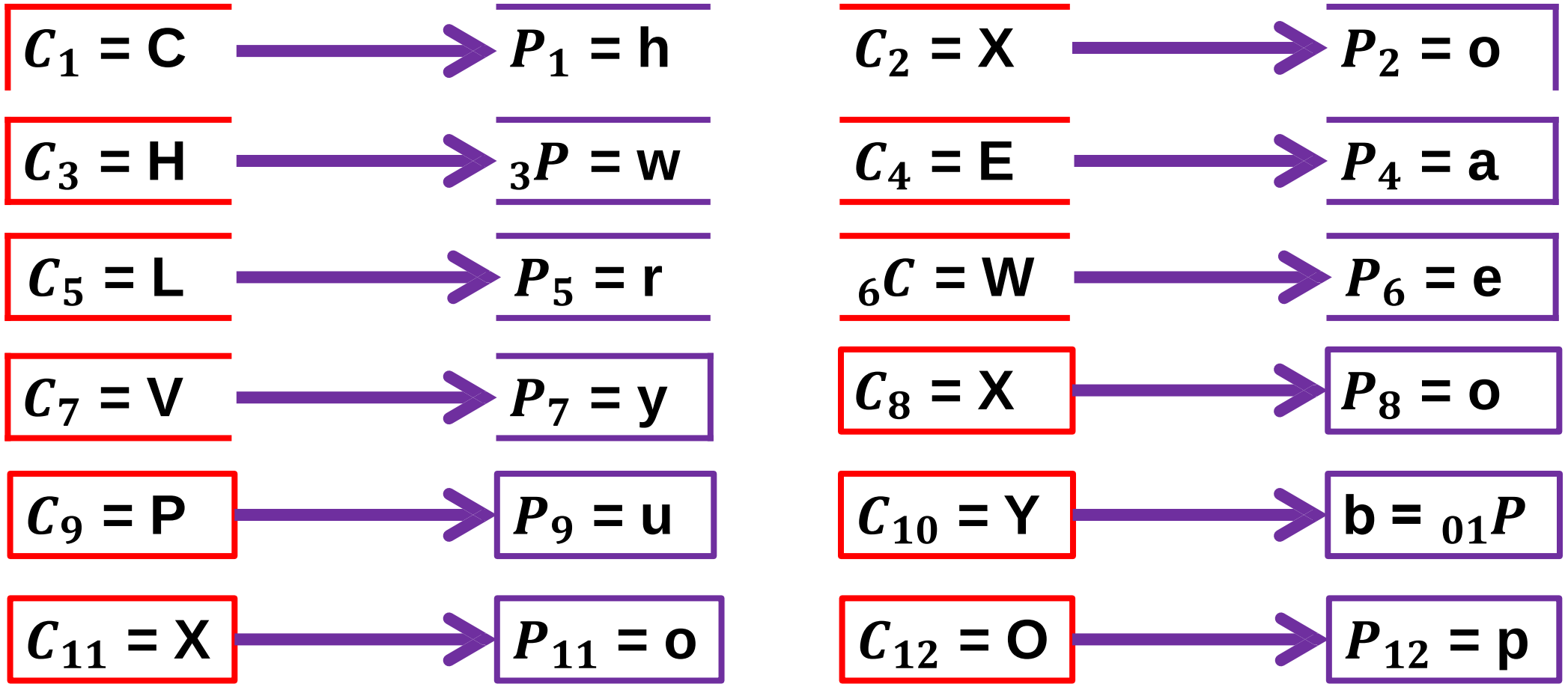
E Y F Q W D T C R J B G A N X O I L Z M P S H K V U

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

Plaintext

Ciphertext → C X H E L W V X P Y X O

C_1 C_2 C_3 C_4 C_5 C_6 C_7 C_8 C_9 C_{10} C_{11} C_{12}



The **Plaintext** is "**how are you bop**"

Depends on Sender in Message Encryption Mode

Depends on the sender for setting it to Encrypt messages

how are you bop

(Sender)

Encryption algorithm By using Mono Alphabetic Cipher

CXHELWVXPYXO

Decryption algorithm By using Mono Alphabetic Cipher

how are you bop

(receiver)

Homework

Encrypt and decrypt the message “**meet me after the toga party**” by using **Mono Alphabetic**.