(DEEMED TO BE UNIVERSITY)

NETWORK PROTOCOLS & SECURITY 23EC2210 R/A/E

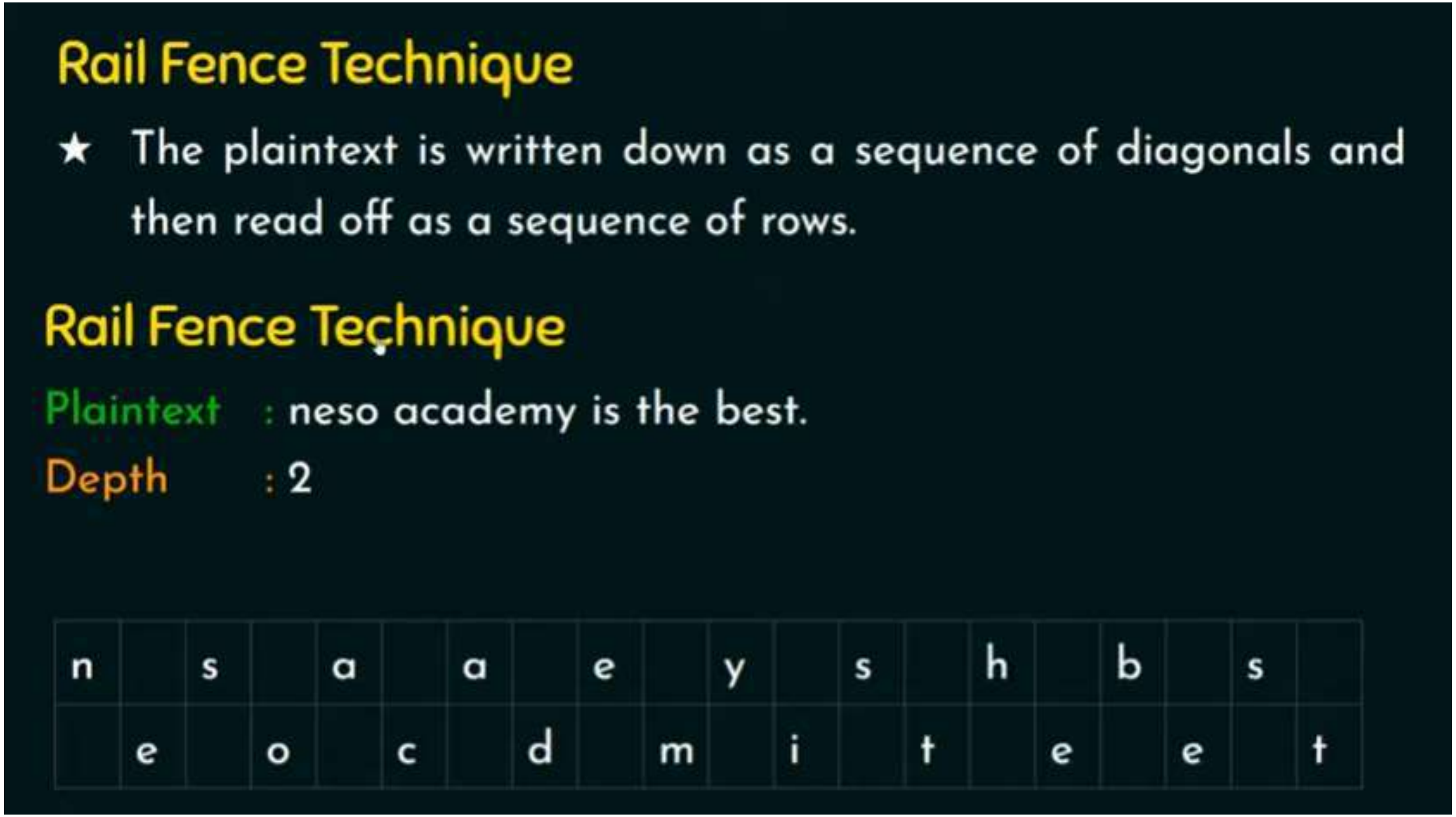
Topic:

Transposition Techniques

Session – 36

Transposition Ciphers

Rail Fence Technique



Rail Fence Technique

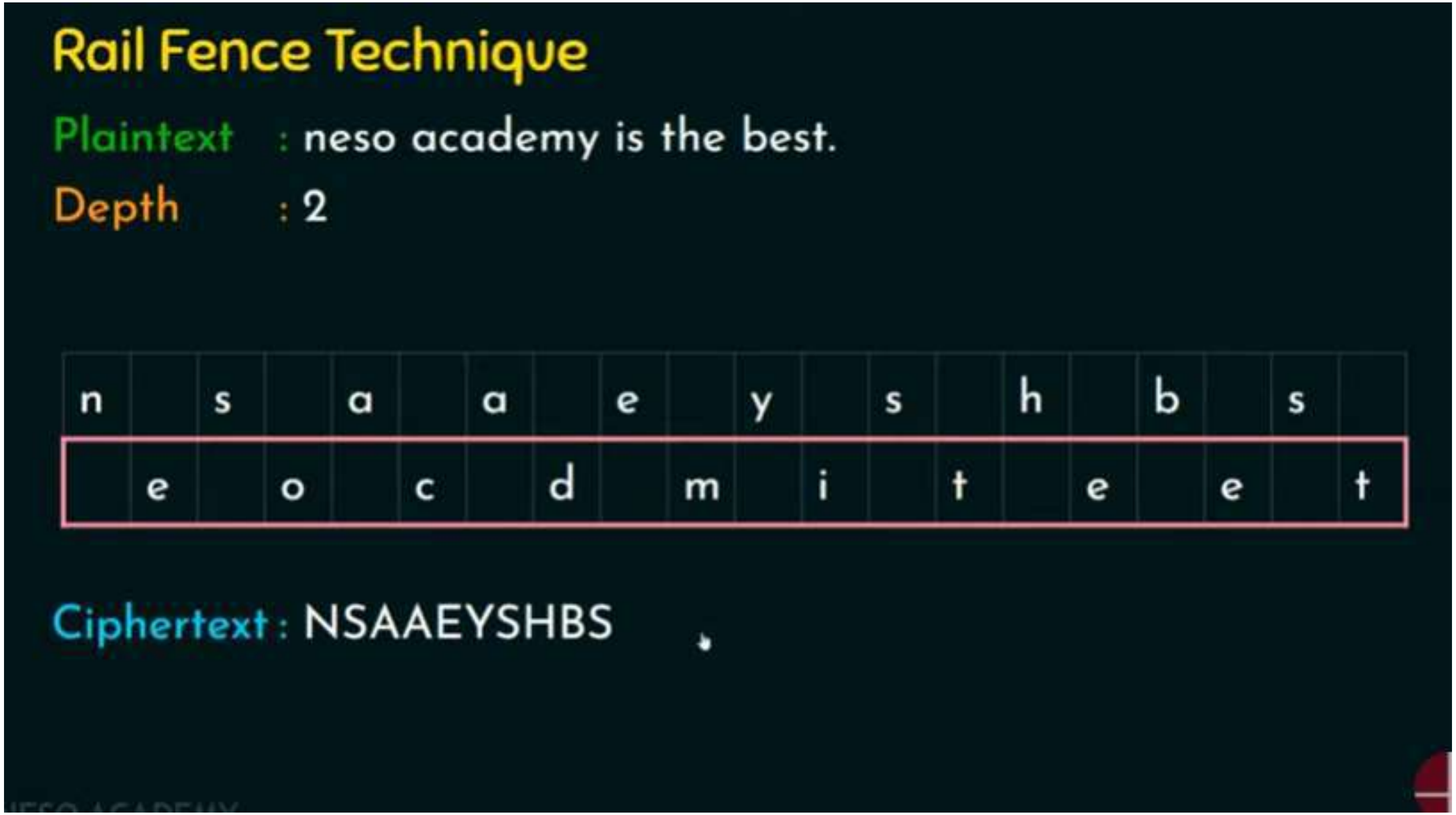
- ★ The plaintext is written down as a sequence of diagonals and then read off as a sequence of rows.

Rail Fence Technique

Plaintext : neso academy is the best.

Depth : 2

n		s		a		a		e		y		s		h		b		s	
	e		o		c		d		m		i		t		e		e		t



Rail Fence Technique

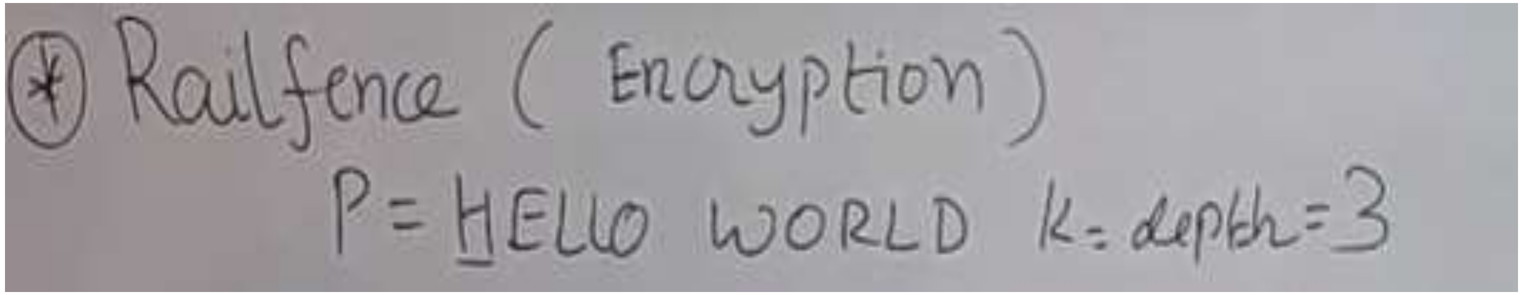
Plaintext : neso academy is the best.

Depth : 2

n		s		a		a		e		y		s		h		b		s	
	e		o		c		d		m		i		t		e		e		t

Ciphertext : NSAAEYSHBS

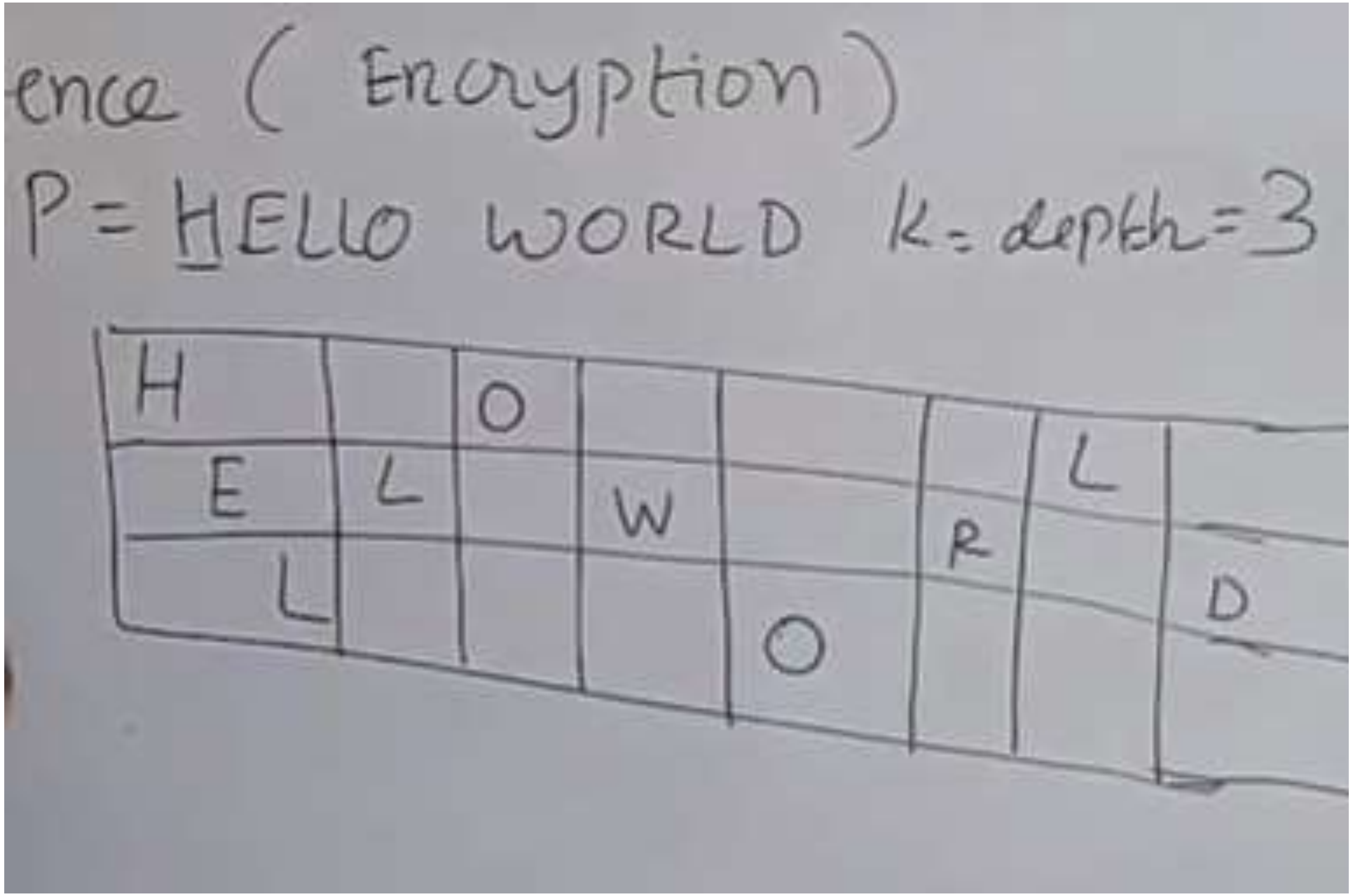
Rail Fence Technique



⊛ Railfence (Encryption)

P = HELLO WORLD k = depth = 3

Rail Fence Technique

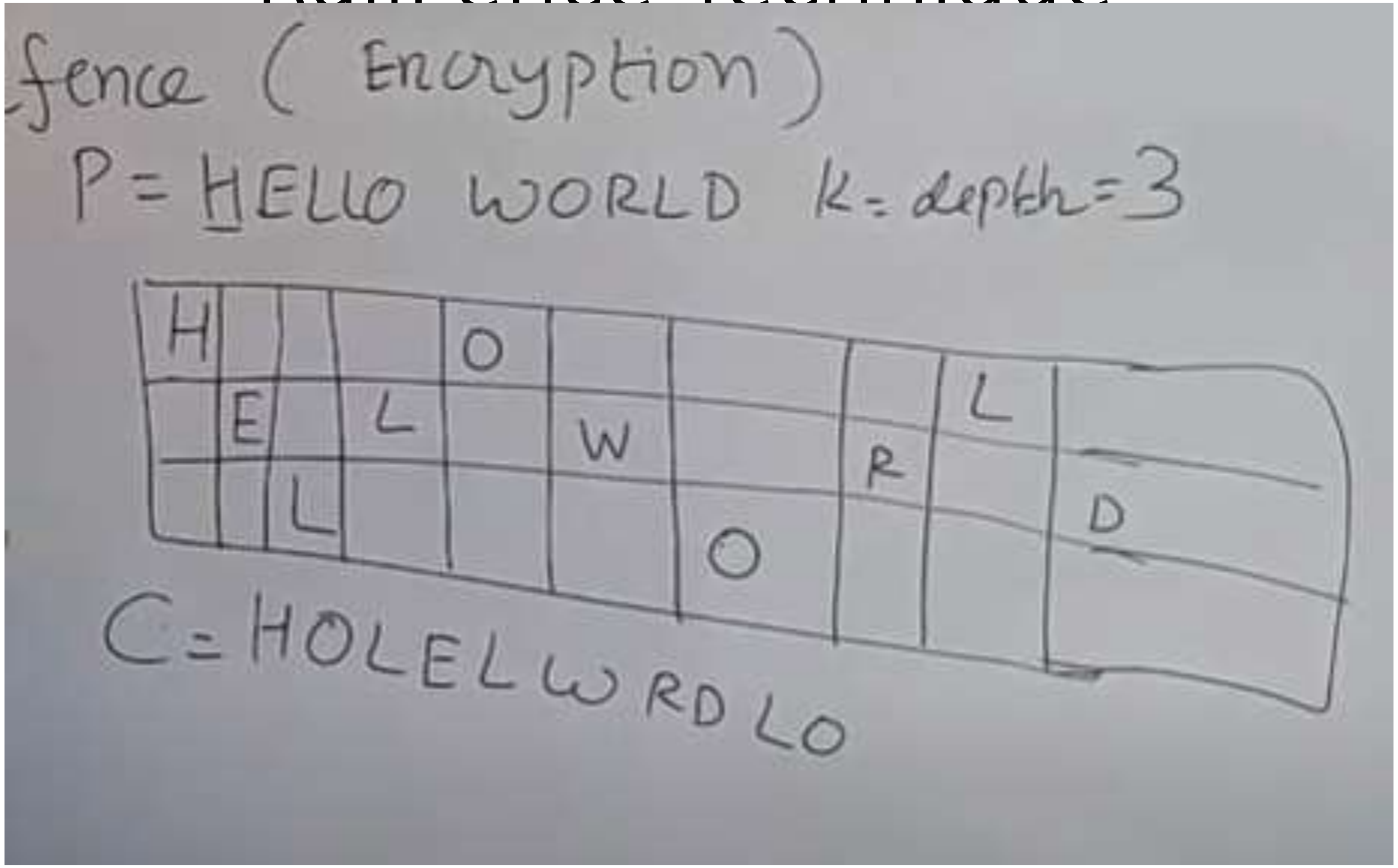


ence (Encryption)

P = HELLO WORLD k = depth = 3

H		O				L	
E	L		W		R		
L				O			D

RailFence Technique



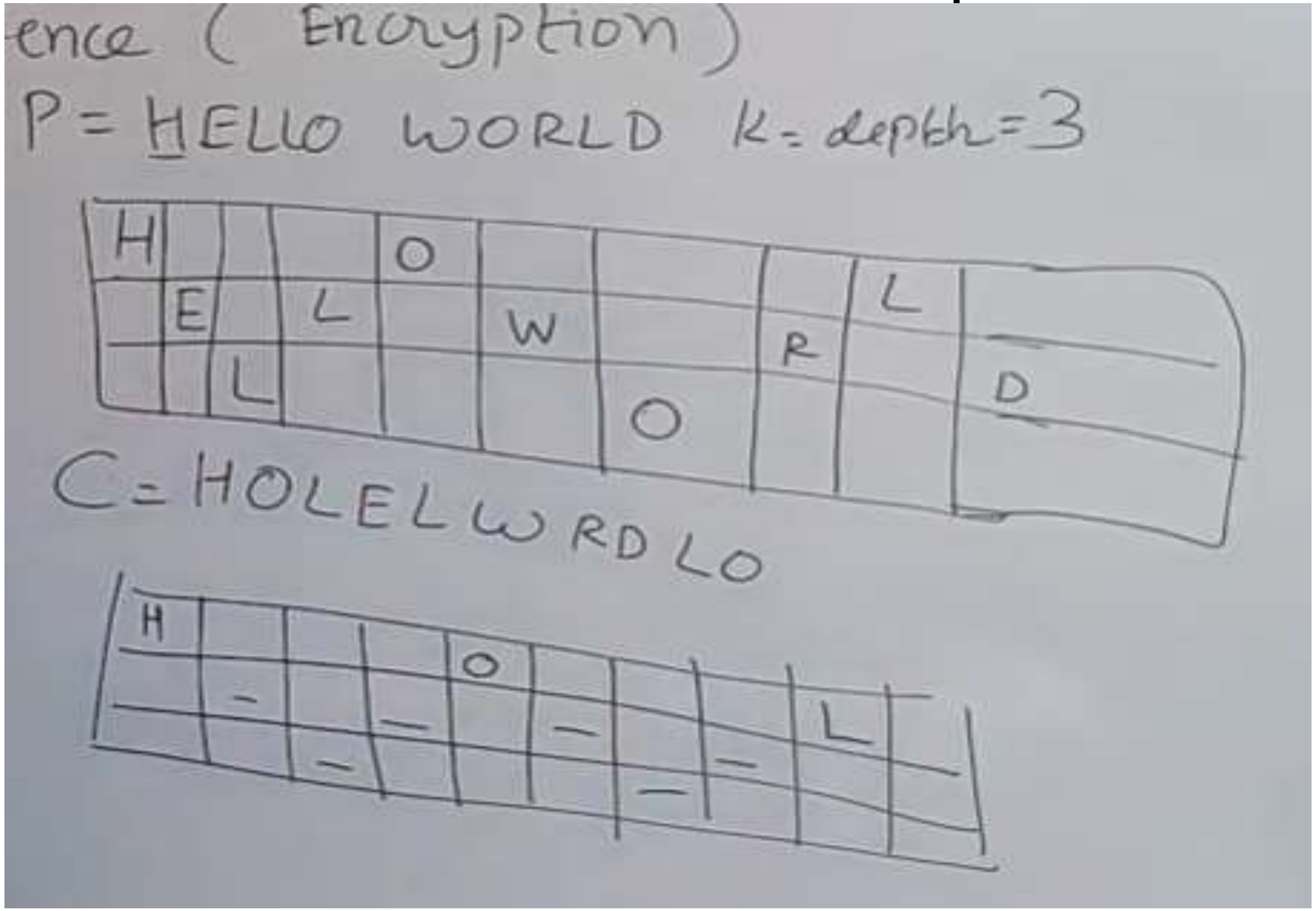
fence (Encryption)

P = HELLO WORLD k = depth = 3

H				O				L	
	E		L		W		R		
		L				O			D

C = HOLELWRDLO

RailFence Technique



ence (Encryption)

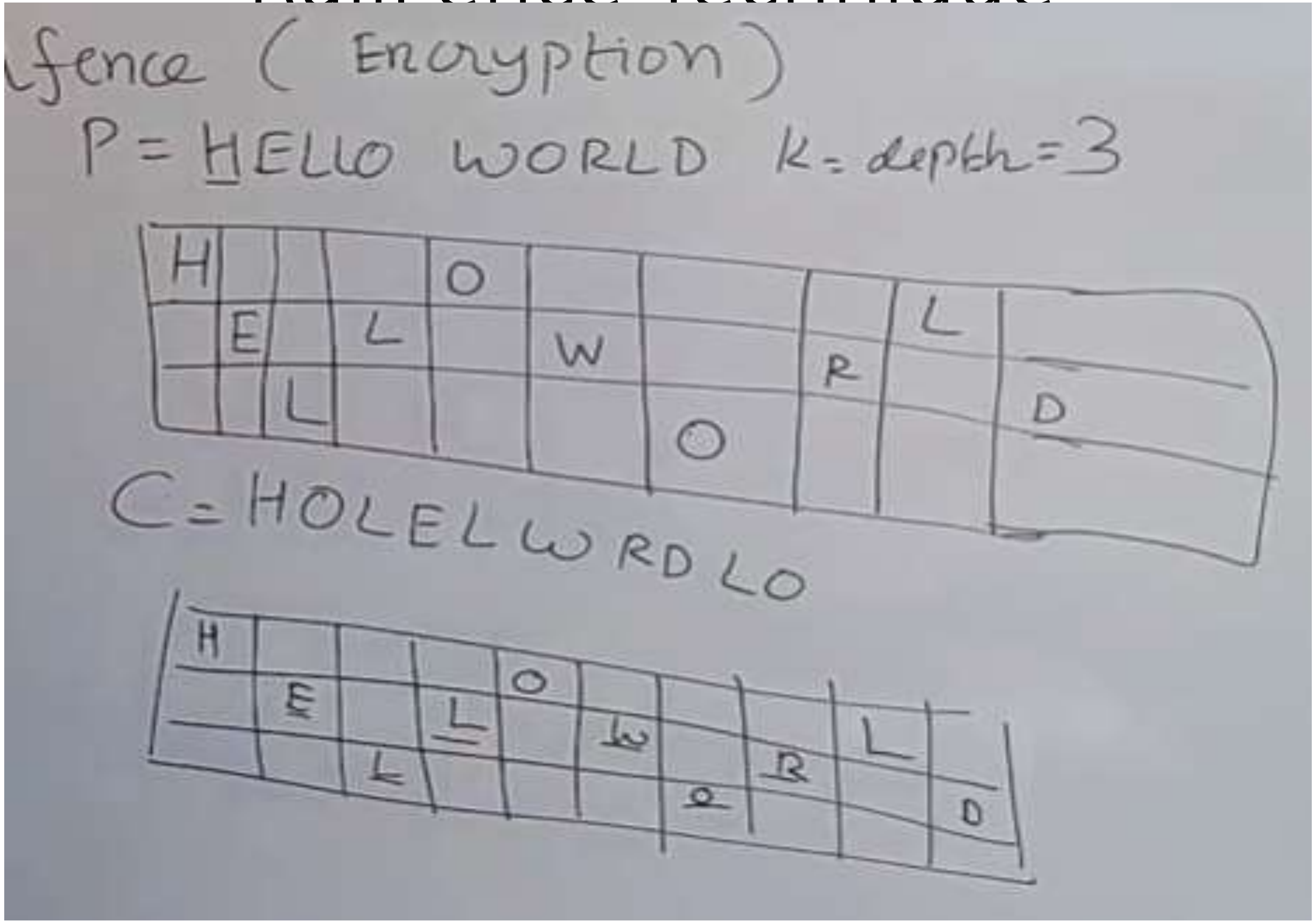
P = HELLO WORLD k = depth = 3

H				O				L	
	E		L		W		R		D
		L				O			

C = HOLELWRDLO

H				O					
	_		_		_		_	L	
		_				_			

RailFence Technique



fence (Encryption)

P = HELLO WORLD k = depth = 3

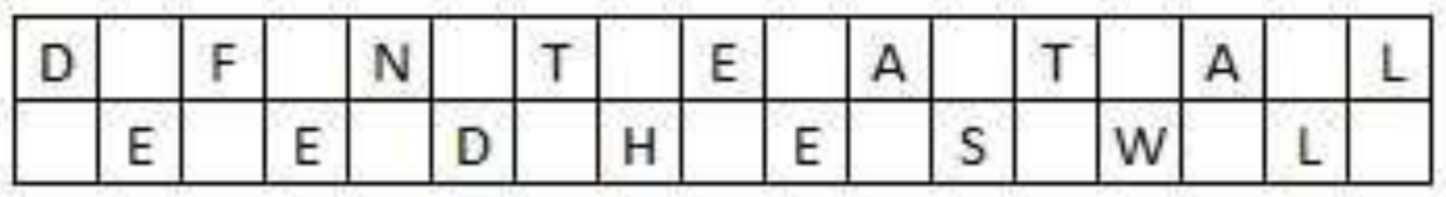
H				O				L	
	E		L		W		R		D
		L				O			

C = HOLELWRDLO

H				O				L	
	E		L		W		R		
		L				O			D

Rail fence Cipher

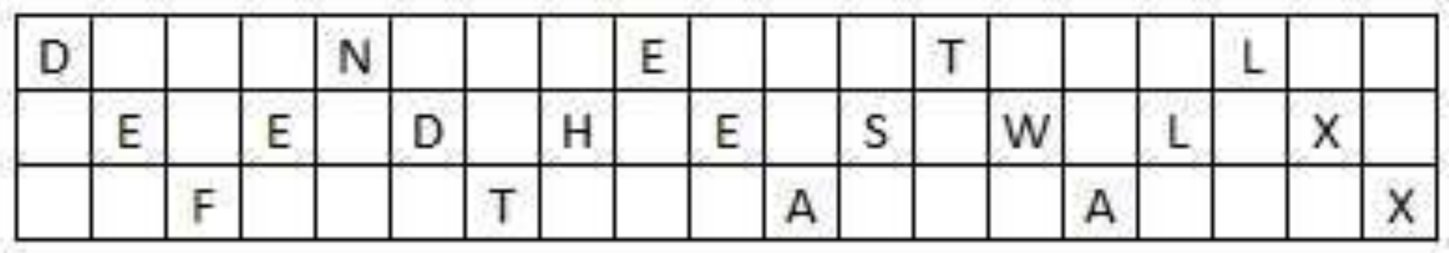
- Plaintext: "defendtheeastwall“
- Rails / Key: 2



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

- Ciphertext: DFNTEATALEEDHESWL

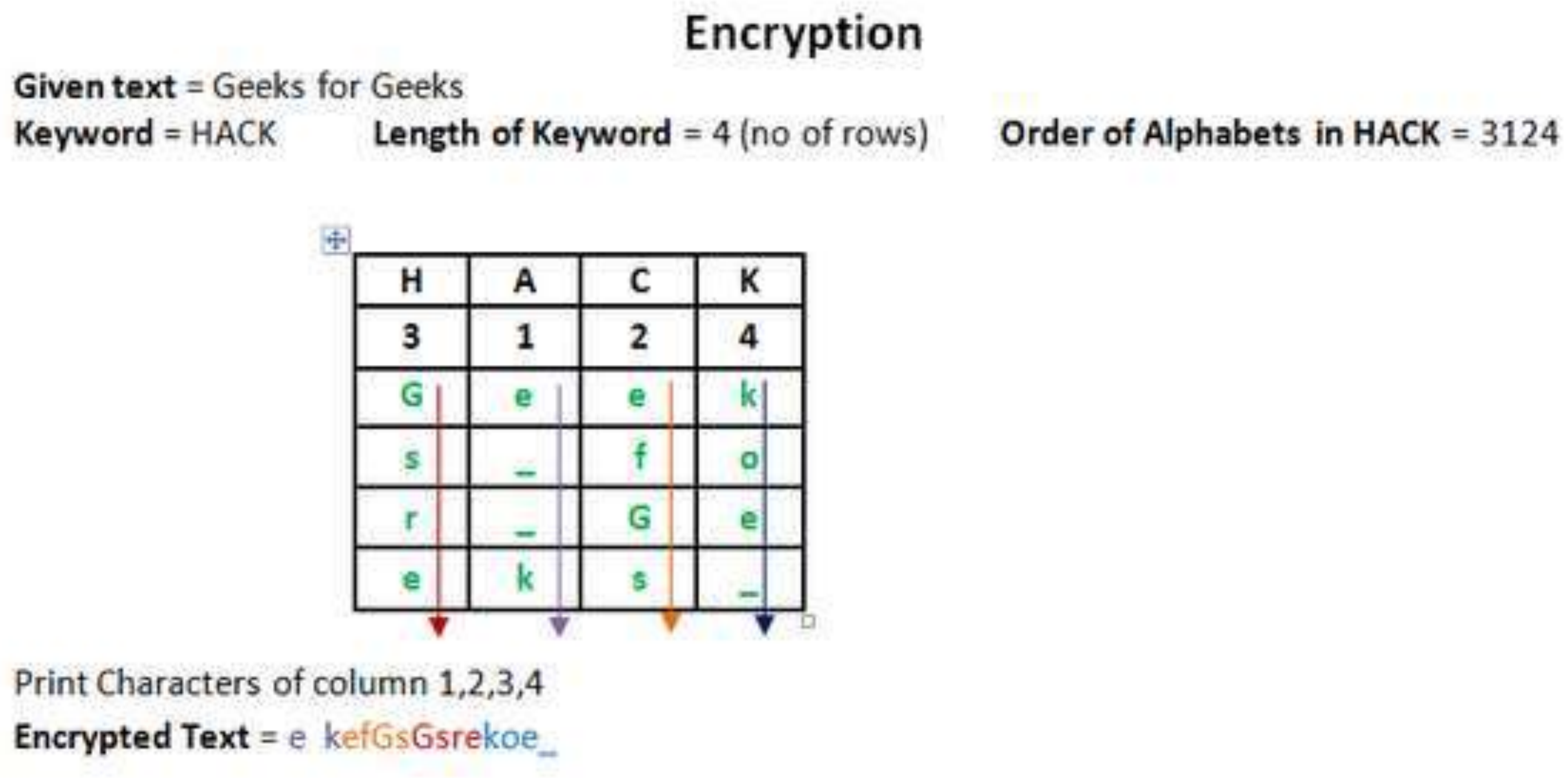
- Key: 3



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

- Ciphertext: DNETLEEDHESWLXFTAAX

Columnar Encryption Technique



Encryption

Given text = Geeks for Geeks

Keyword = HACK **Length of Keyword** = 4 (no of rows) **Order of Alphabets in HACK** = 3124

H	A	C	K
3	1	2	4
G	e	e	k
s	_	f	o
r	_	G	e
e	k	s	_

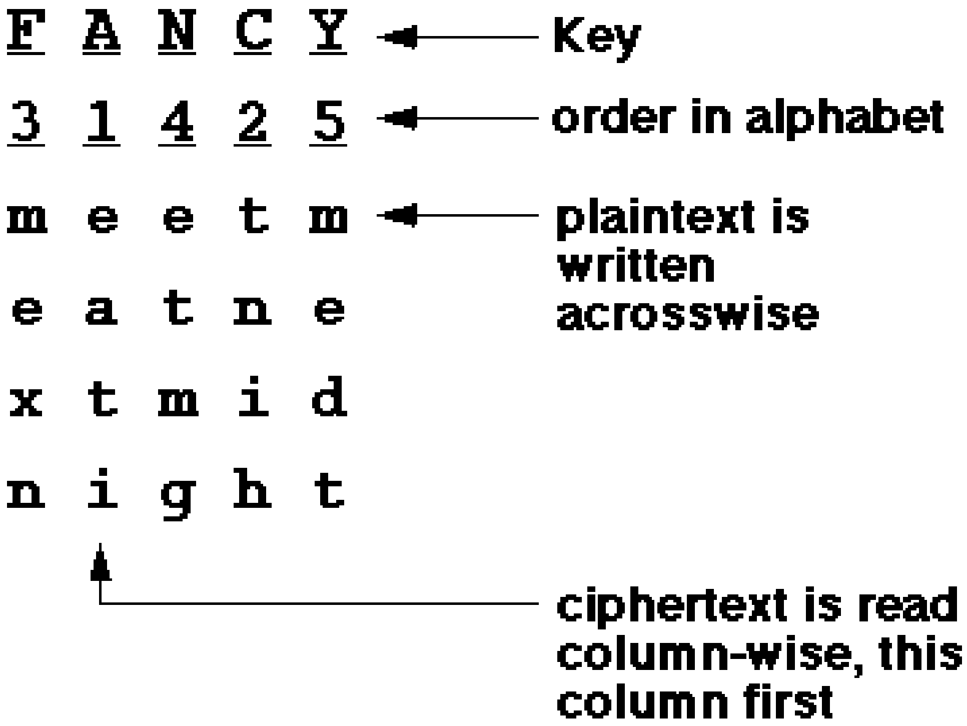
Print Characters of column 1,2,3,4

Encrypted Text = e kefGsGsrekoe_

Columnar Cipher

- Message: meetmeatnextmidnight
- Key: FANCY

- Ciphertext: eatitnihmexnetmgmedt



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

- Ciphertext: DNETLEEDHESWLXFTAAX
- Key : 3