1D	1U	1M	1K
Vinod	111803111 Atharva Kailas	111803104 Akanksha Kish	111803078 Prathamesh U	111803058 Omkar Anand

01:17 / 57:24

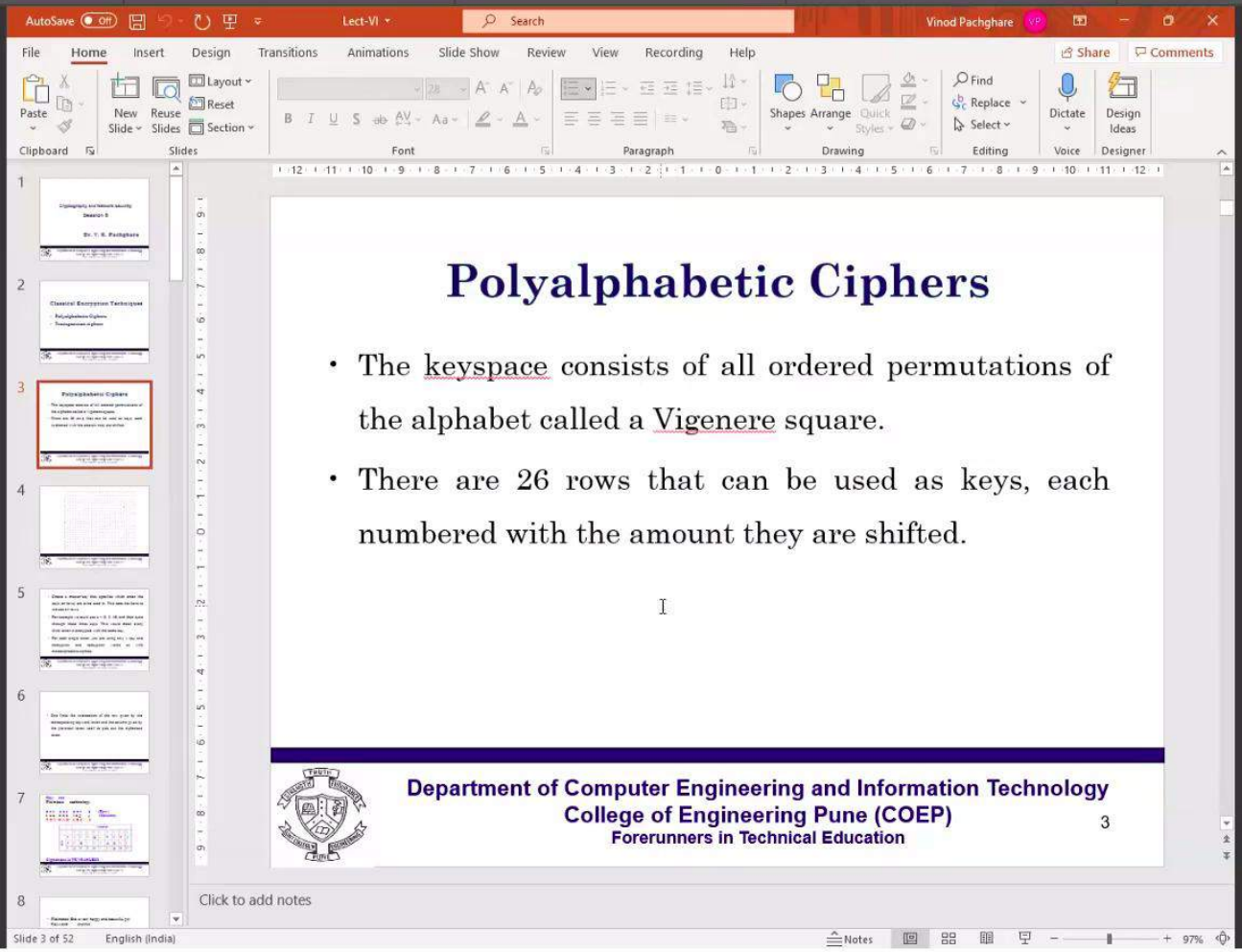
1D

1U

1M

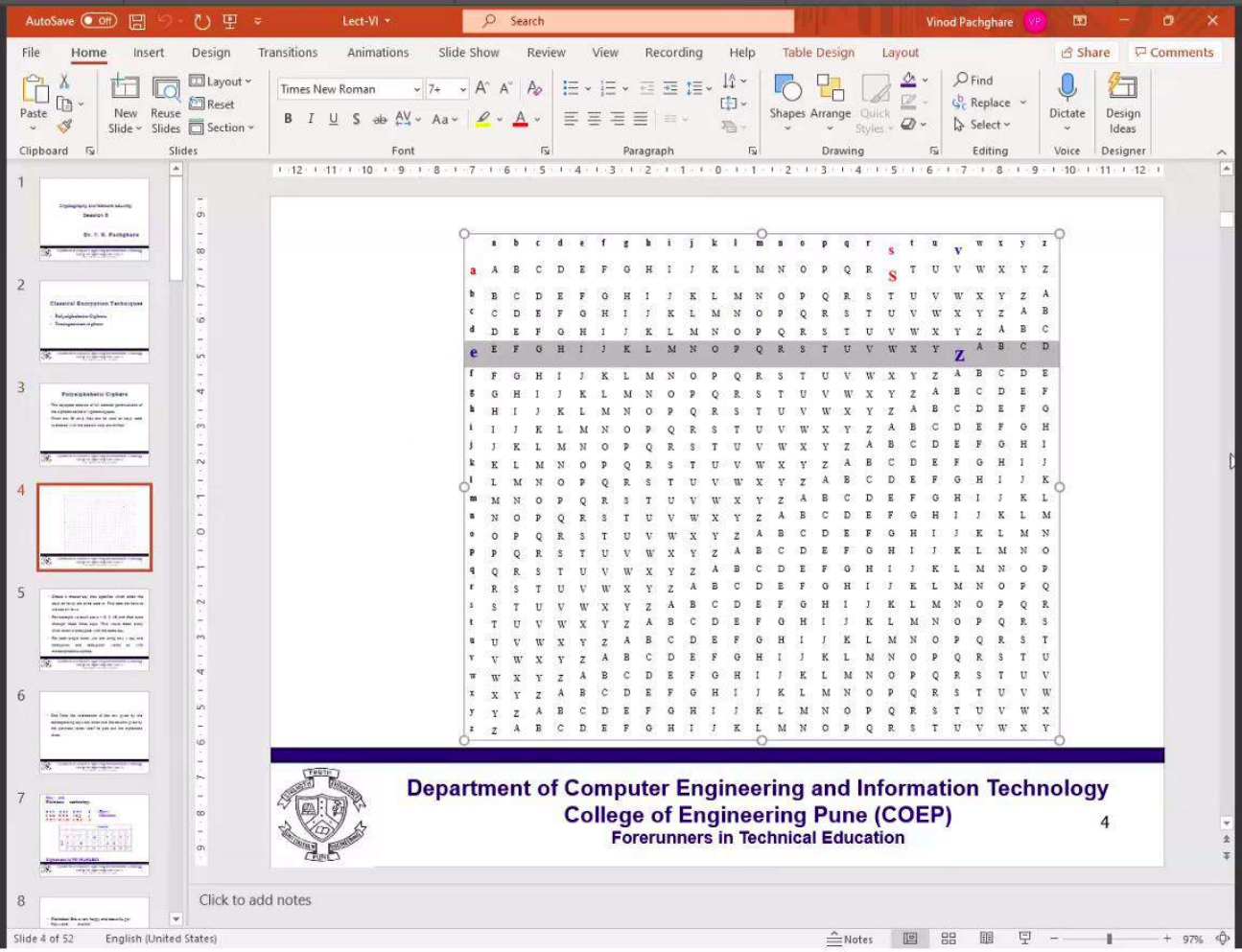
1K

Vinod | 111803111 Atharva Kailas | 111803104 Akanksha Kish | 111803078 Prathamesh U | 111803058 Omkar Anand



03:13 / 57:24

Vinod	111803111 Atharva Kailas	111803104 Akanksha Kish	111803078 Prathamesh U	111803058 Omkar Anand



04:59 / 57:24

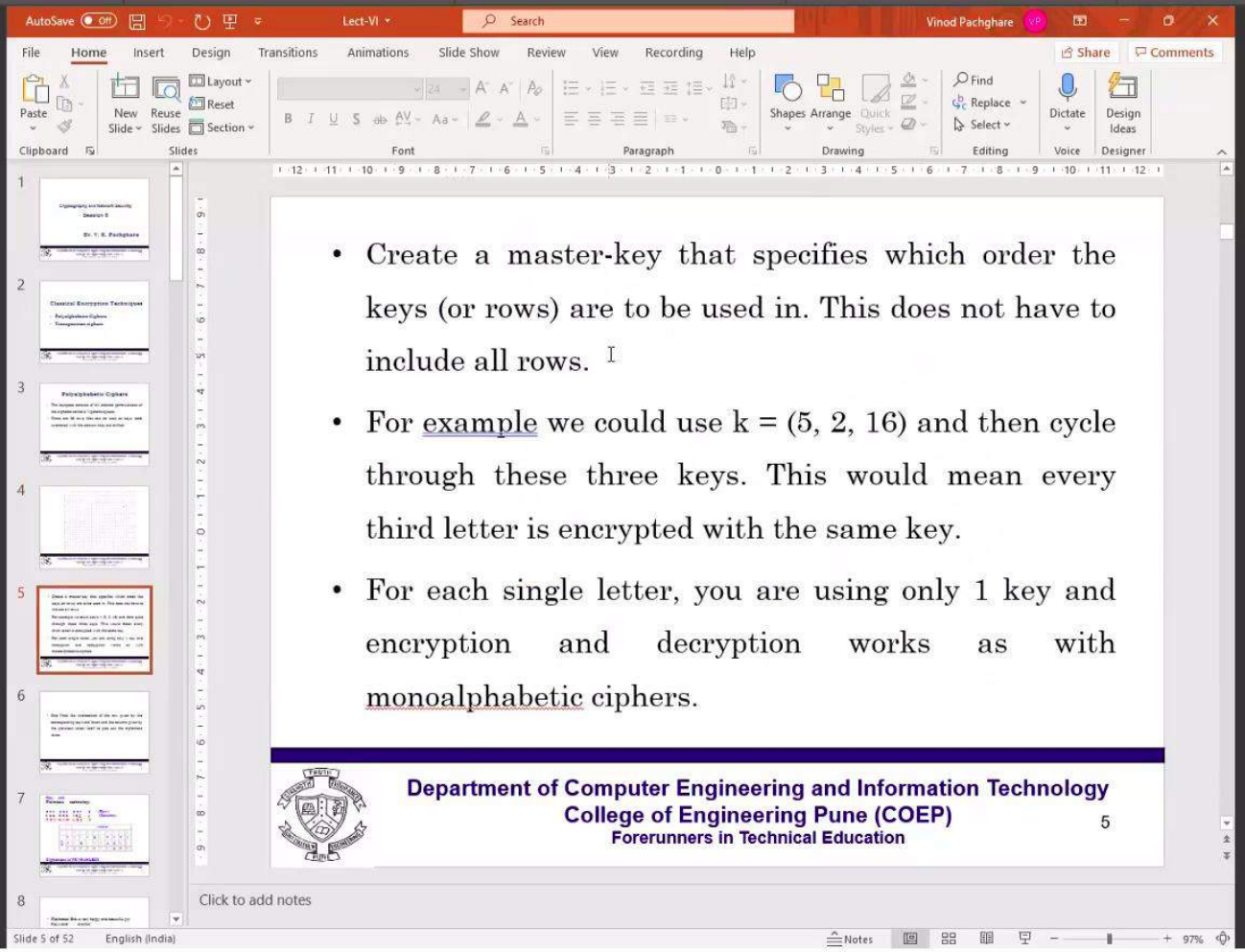
1D

1U

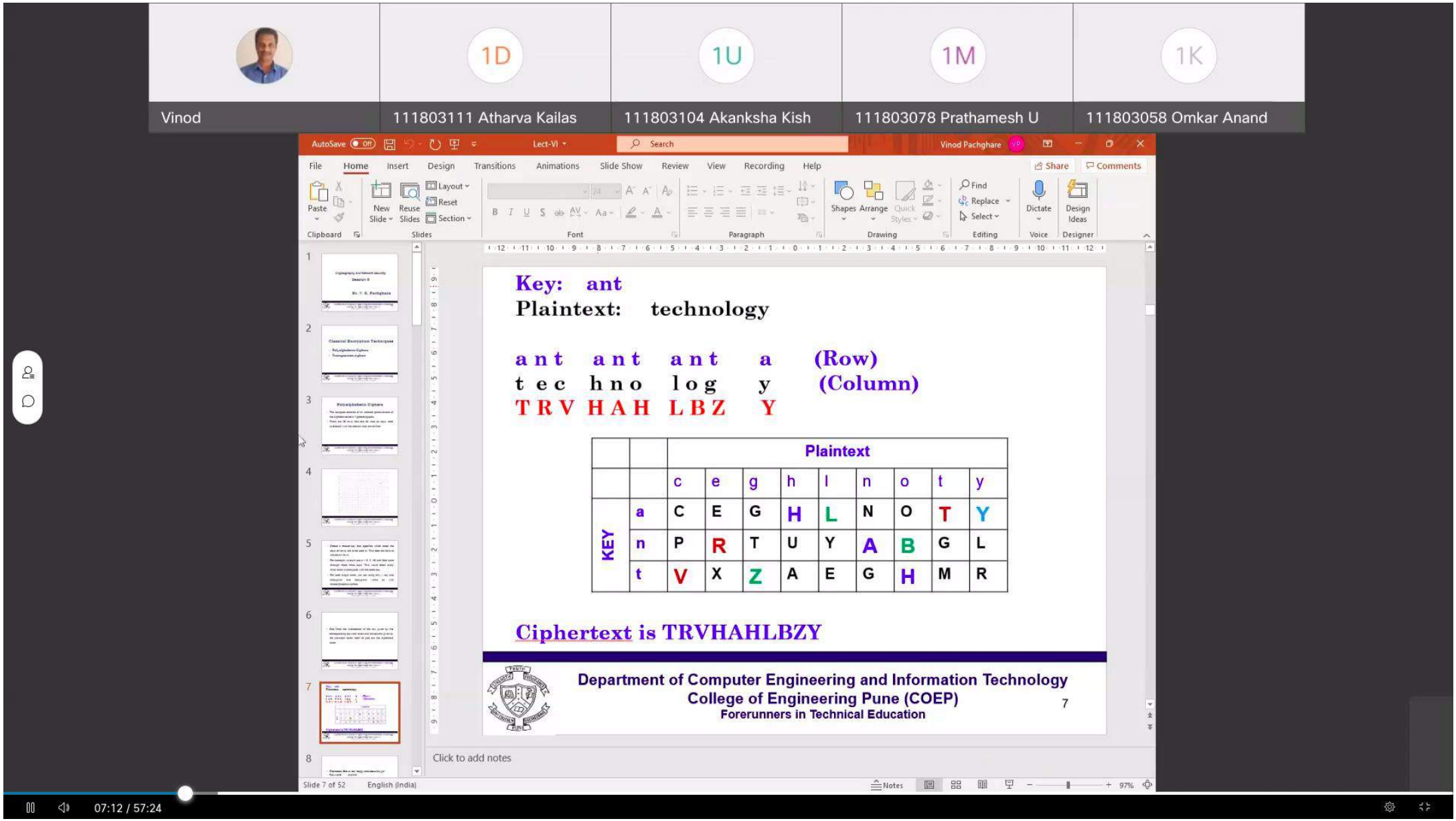
1M

1K

Vinod | 111803111 Atharva Kailas | 111803104 Akanksha Kish | 111803078 Prathamesh U | 111803058 Omkar Anand



05:54 / 57:24


Vinod
1D
111803111 Atharva Kailas
1U
111803104 Akanksha Kish
1M
111803078 Prathamesh U
1K
111803058 Omkar Anand
Key: ant
Plaintext: technology
a n t a n t a n t a (Row)
t e c h n o l o g y (Column)
T R V H A H L B Z Y
Plaintext
c e g h l n o t y
KEY
a C E G H L N O T Y
n P R T U Y A B G L
t V X Z A E G H M R
Ciphertext is TRVHAHLBZY
Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education
7
Click to add notes
07:12 / 57:24

1S	1U	1M	1K
Vinod	111803109 Akanksha Sha	111803104 Akanksha Kish	111803078 Prathamesh U	111803058 Omkar Anand

AutoSave Off | Lect-VI | Search | Vinod Pachghare

File Home Insert Design Transitions Animations Slide Show Review View Recording Help | Share | Comments

Paste | New Slide | Reuse Slides | Layout | Reset | Section | Clipboard | Slides | Font | Paragraph | Shapes | Arrange | Quick Styles | Drawing | Find | Replace | Select | Editing | Dictate | Voice | Design Ideas | Designer

3 4 5 6 7 8 9 10

Click to add title

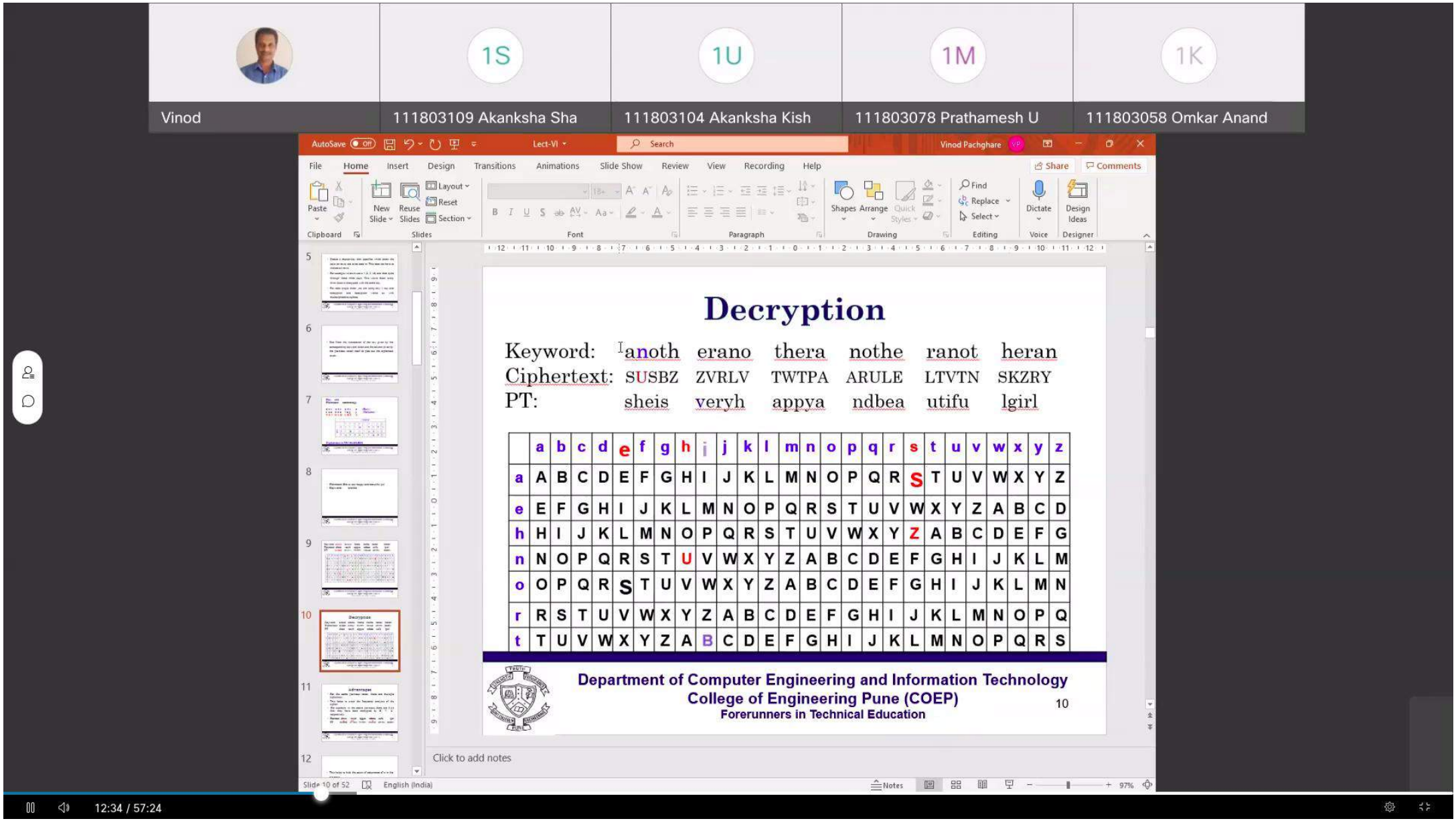
- **Plaintext:** She is very happy and beautiful girl
- **Keyword:** 'another'

Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education
8

Click to add notes

Slide 8 of 52 | English (India) | Notes | 97%

+96


Vinod
111803109 Akanksha Sha
111803104 Akanksha Kish
111803078 Prathamesh U
111803058 Omkar Anand
Lect-VI
Search
Vinod Pachghare
Decryption
Keyword: anoth erano thera nothe ranot heran
Ciphertext: SUSBZ ZVRLV TWTPA ARULE LTVTN SKZRY
PT: sheis veryh appya ndbea utifu lgirl
Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education
10
Click to add notes
Slide 10 of 52
English (India)
12:34 / 57:24

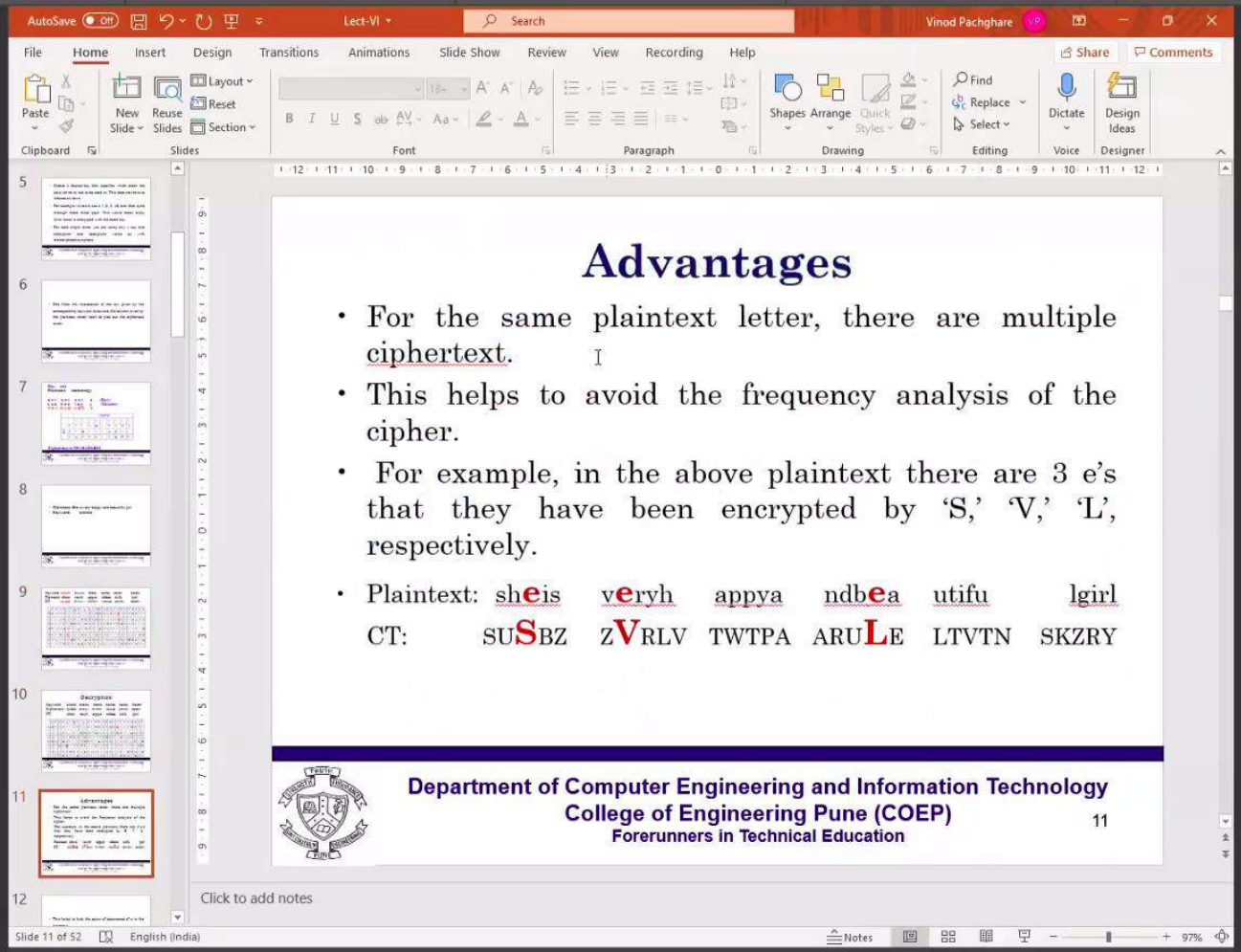
1S

1U

1M

1K

Vinod | 111803109 Akanksha Sha | 111803104 Akanksha Kish | 111803078 Prathamesh U | 111803058 Omkar Anand



+108

1S

1U

1M

1K

Vinod | 111803109 Akanksha Sha | 111803104 Akanksha Kish | 111803078 Prathamesh U | 111803058 Omkar Anand

AutoSave Off | Lect-VI | Search | Vinod Pachghare

File Home Insert Design Transitions Animations Slide Show Review View Recording Help | Share | Comments

Paste | New Slide | Reuse Slides | Layout | Reset | Section | Clipboard | Slides | Font | Paragraph | Shapes | Arrange | Quick Styles | Drawing | Find | Replace | Select | Editing | Dictate | Voice | Design Ideas | Designer

7 8 9 10 11 12 13 14

Click to add title

- This helps to hide the count of occurrence of e in the plaintext.
- So, it makes frequency analysis of the letters in the plaintext difficult.
- The implementation of this cipher is easy.

Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education
12

Click to add notes

Slide 12 of 52 | English (India) | Notes | 97%

+107

1S	1U	1M	1K
Vinod	111803109 Akanksha Sha	111803104 Akanksha Kish	111803078 Prathamesh U	111803058 Omkar Anand

AutoSave Off | Lect-VI | Search | Vinod Pachghare

File Home Insert Design Transitions Animations Slide Show Review View Recording Help | Share | Comments

Paste | New Slide | Reuse Slides | Layout | Reset | Section | Clipboard | Slides | Font | Paragraph | Shapes | Arrange | Quick Styles | Drawing | Find | Replace | Select | Editing | Dictate | Voice | Design Ideas | Designer

7 8 9 10 11 12 13 14

Disadvantages

- If the attacker is able to find out the **length of the key**, then frequency analysis is possible.
- The chosen-plaintext attack is possible against this cipher.

Click to add notes

Slide 13 of 52 | English (India) | Notes | 97%

18:24 / 57:24

1S	1U	1M	1K
Vinod	111803109 Akanksha Sha	111803104 Akanksha Kish	111803078 Prathamesh U	111803058 Omkar Anand

AutoSave Off | Lect-VI | Search | Vinod Pachghare

File Home Insert Design Transitions Animations Slide Show Review View Recording Help | Share | Comments

Paste | New Slide | Reuse Slides | Layout | Reset | Section | Clipboard | Slides | Font | Paragraph | Shapes | Arrange | Quick Styles | Find | Replace | Select | Drawing | Editing | Dictate | Voice | Design Ideas | Designer

9 10 11 12 13 14 15 16

Transposition ciphers

Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education

14

Click to add notes

Slide 14 of 52 | English (India) | Notes | 97%

+108

1S	1U	1M	1K
Vinod	111803109 Akanksha Sha	111803104 Akanksha Kish	111803078 Prathamesh U	111803058 Omkar Anand

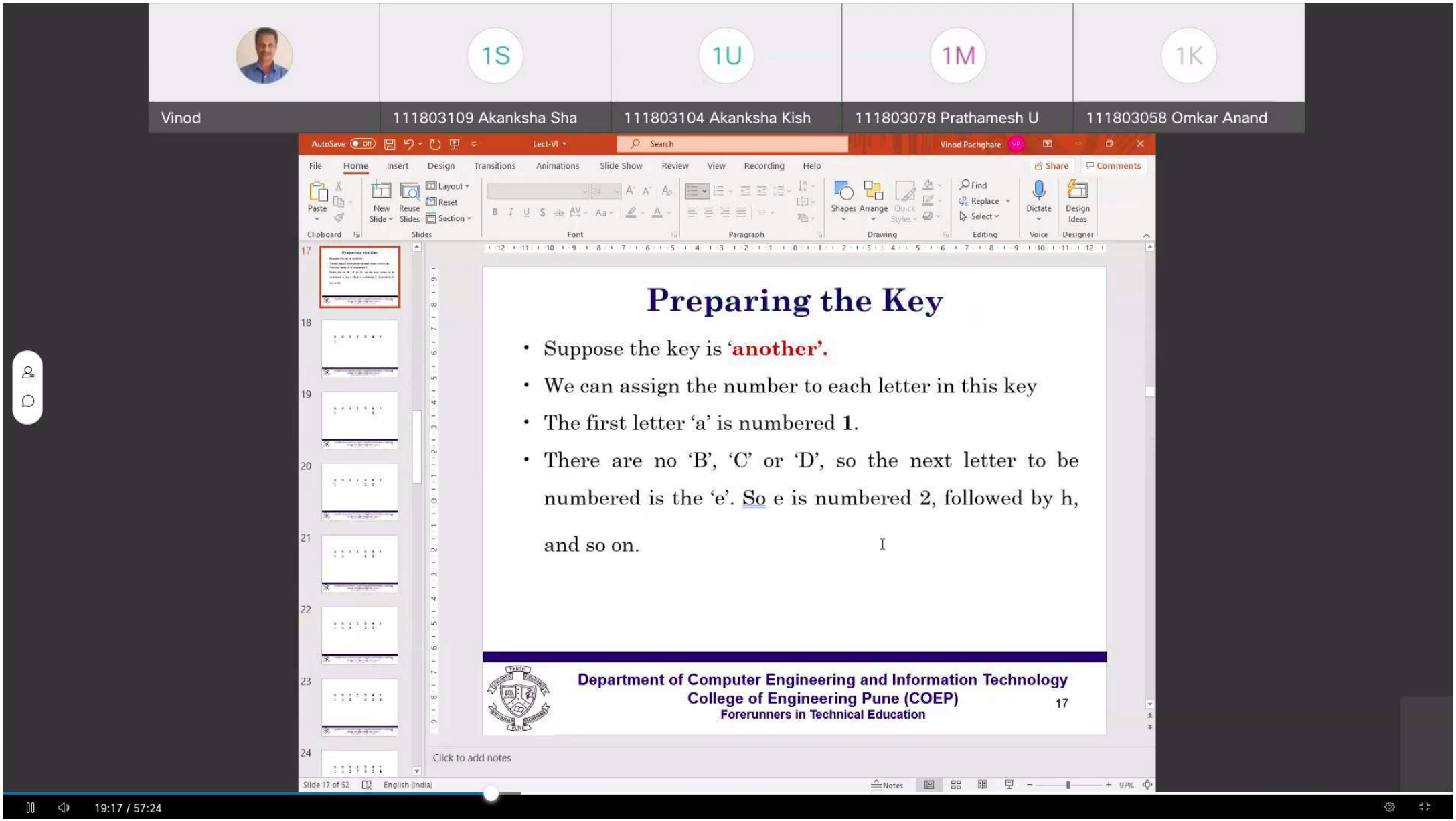
Transposition ciphers

- Letters are written in a row under the key
- Arrange the column as per alphabetical order.
- Transposition ciphers encrypt plaintext by moving small pieces of the message around
- There are two types of transposition ciphers:
  - single columnar and
  - double columnar transposition ciphers

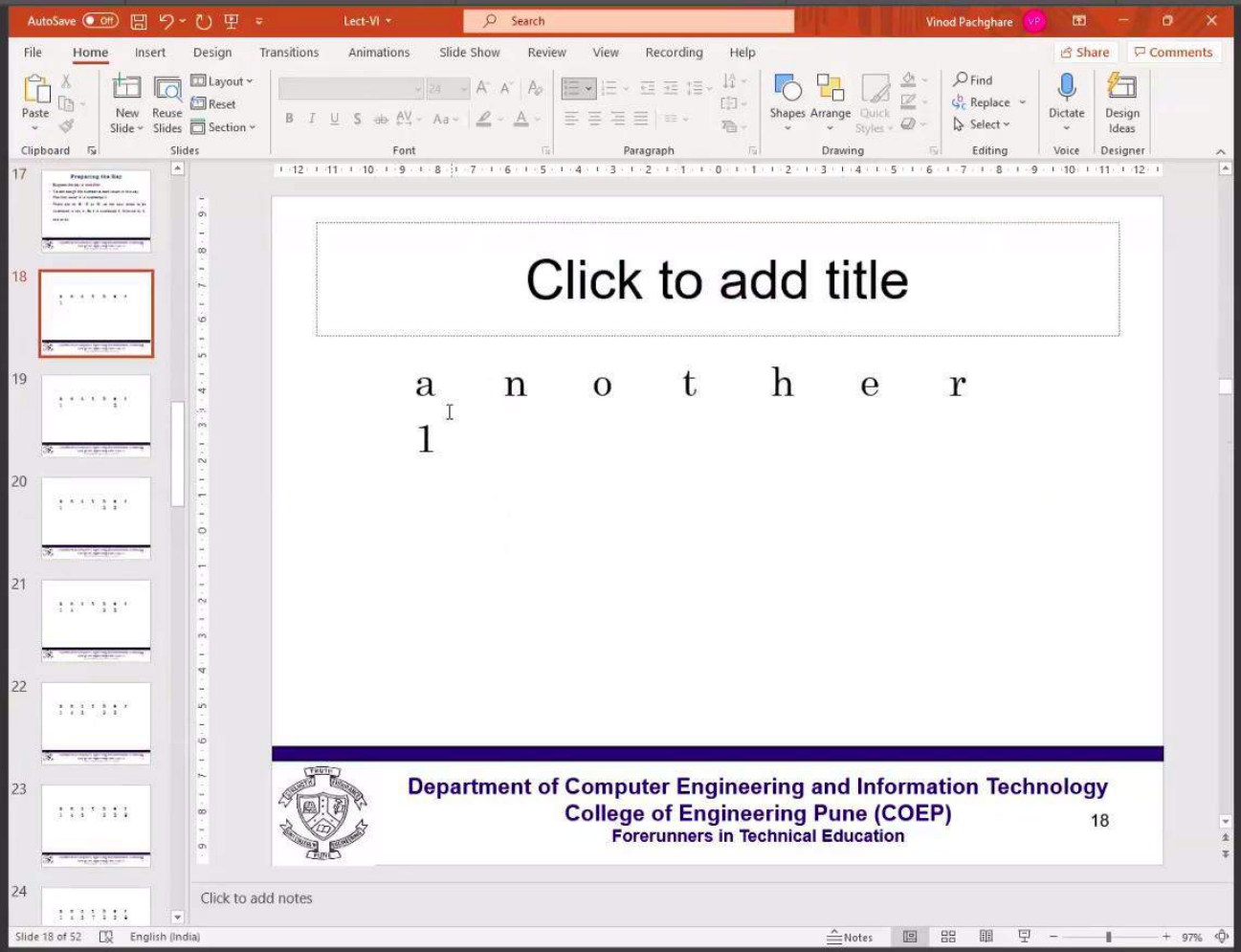
Click to add notes

Slide 15 of 52 English (India) Notes 97%

+108

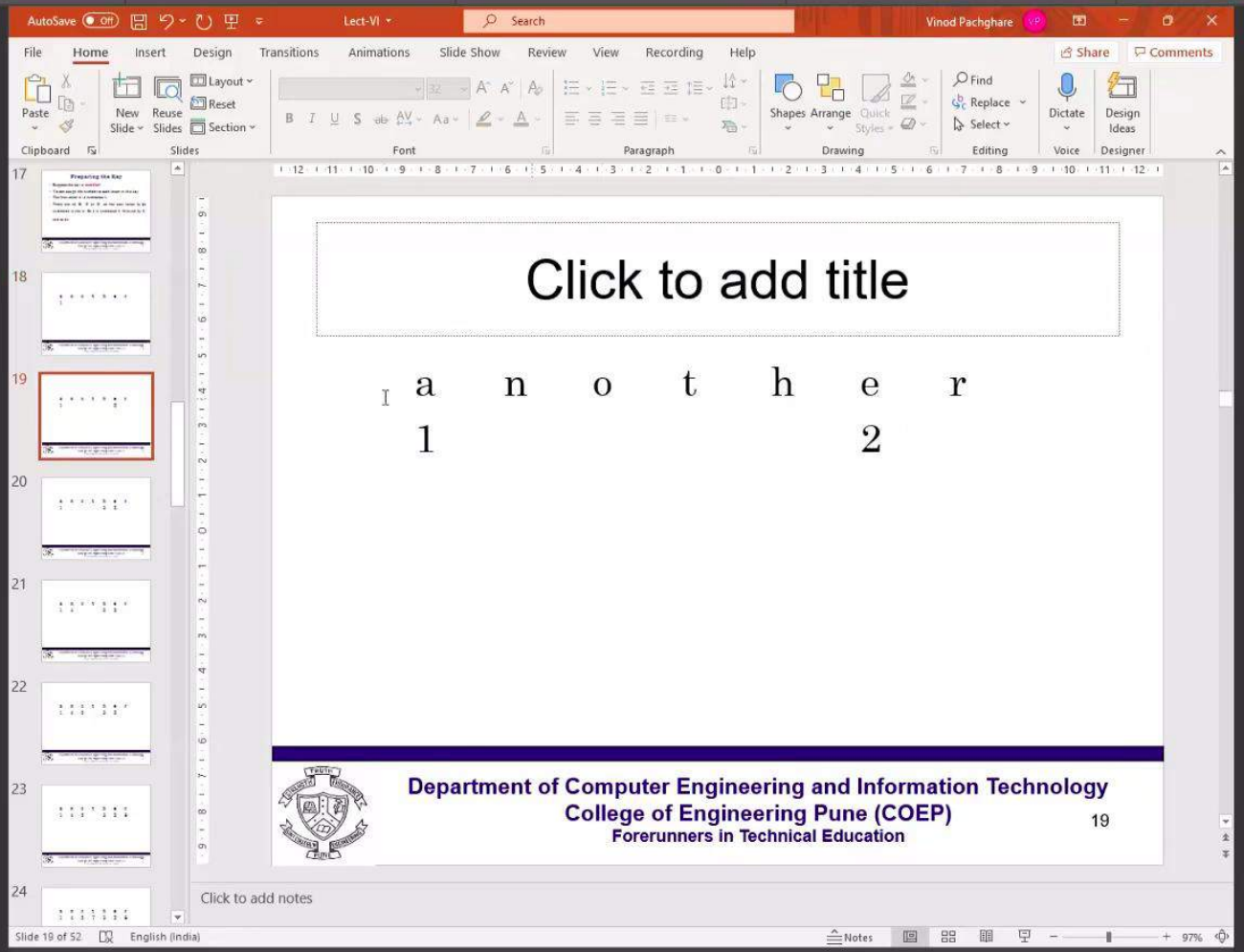

Vinod
111803109 Akanksha Sha
111803104 Akanksha Kish
111803078 Prathamesh U
111803058 Omkar Anand
Lect-VI
Search
Vinod Pachghare
Preparing the Key
Suppose the key is 'another'.
We can assign the number to each letter in this key
The first letter 'a' is numbered 1.
There are no 'B', 'C' or 'D', so the next letter to be numbered is the 'e'. So e is numbered 2, followed by h, and so on.
Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education
17
Click to add notes
Slide 17 of 52
English (India)
19:17 / 57:24

1S	1U	1M	1K
Vinod	111803109 Akanksha Sha	111803104 Akanksha Kish	111803078 Prathamesh U	111803058 Omkar Anand

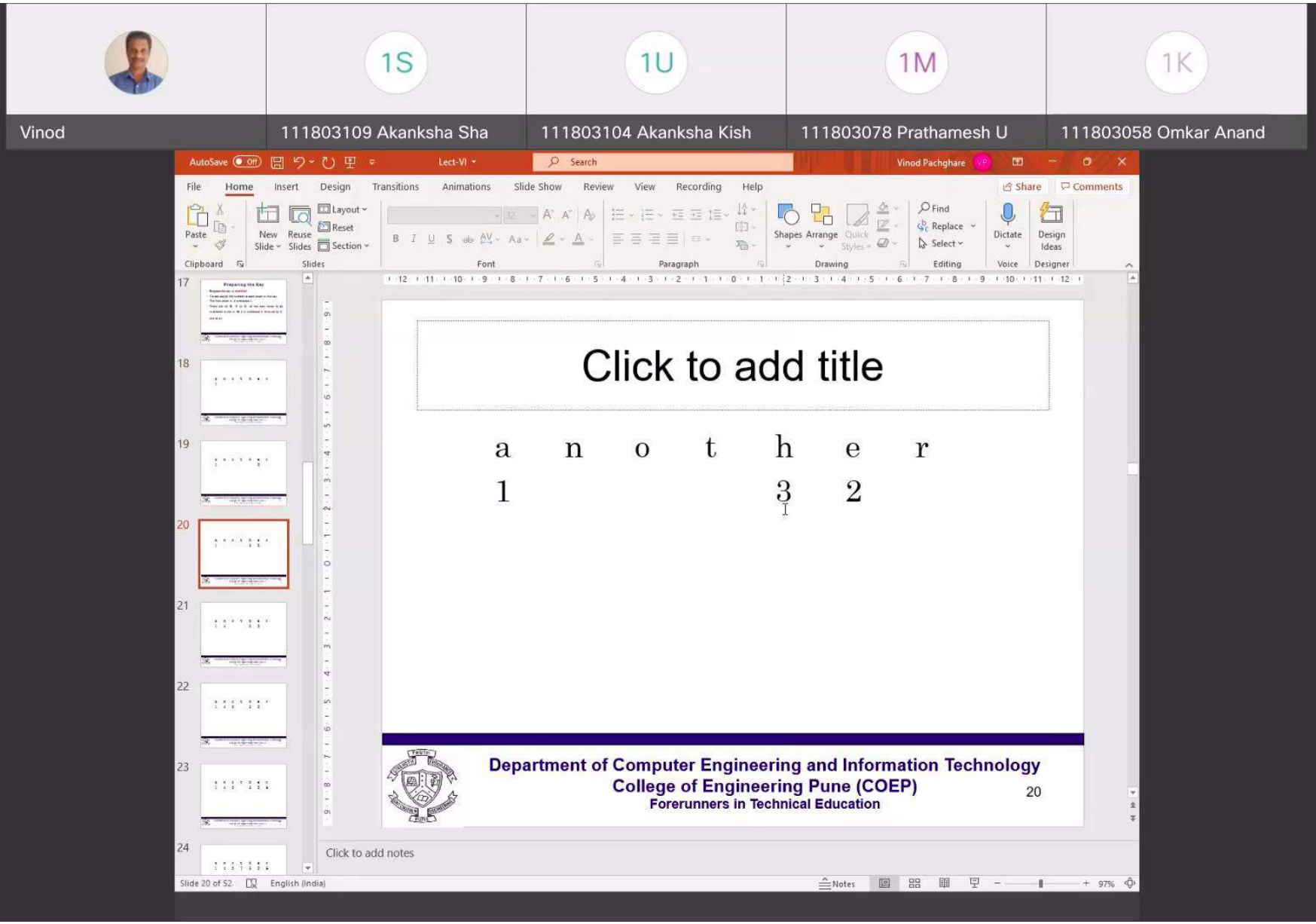


+112

	1S	1U	1M	1K
Vinod	111803109 Akanksha Sha	111803104 Akanksha Kish	111803078 Prathamesh U	111803058 Omkar Anand



+114


Vinod
111803109 Akanksha Sha
111803104 Akanksha Kish
111803078 Prathamesh U
111803058 Omkar Anand
Click to add title
a n o t h e r
1 3 2
Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education
20
Click to add notes
+114

1S	1U	1M	1K
Vinod	111803109 Akanksha Sha	111803104 Akanksha Kish	111803078 Prathamesh U	111803058 Omkar Anand

AutoSave Off | Lect-VI | Search | Vinod Pachghare

File Home Insert Design Transitions Animations Slide Show Review View Recording Help | Share | Comments

Paste | New Slide | Reuse Slides | Layout | Reset | Section | Clipboard | Slides | Font | Paragraph | Shapes | Arrange | Quick Styles | Drawing | Find | Replace | Select | Editing | Dictate | Voice | Design Ideas | Designer

17 18 19 20 21 22 23 24

Click to add title

a n o t h e r

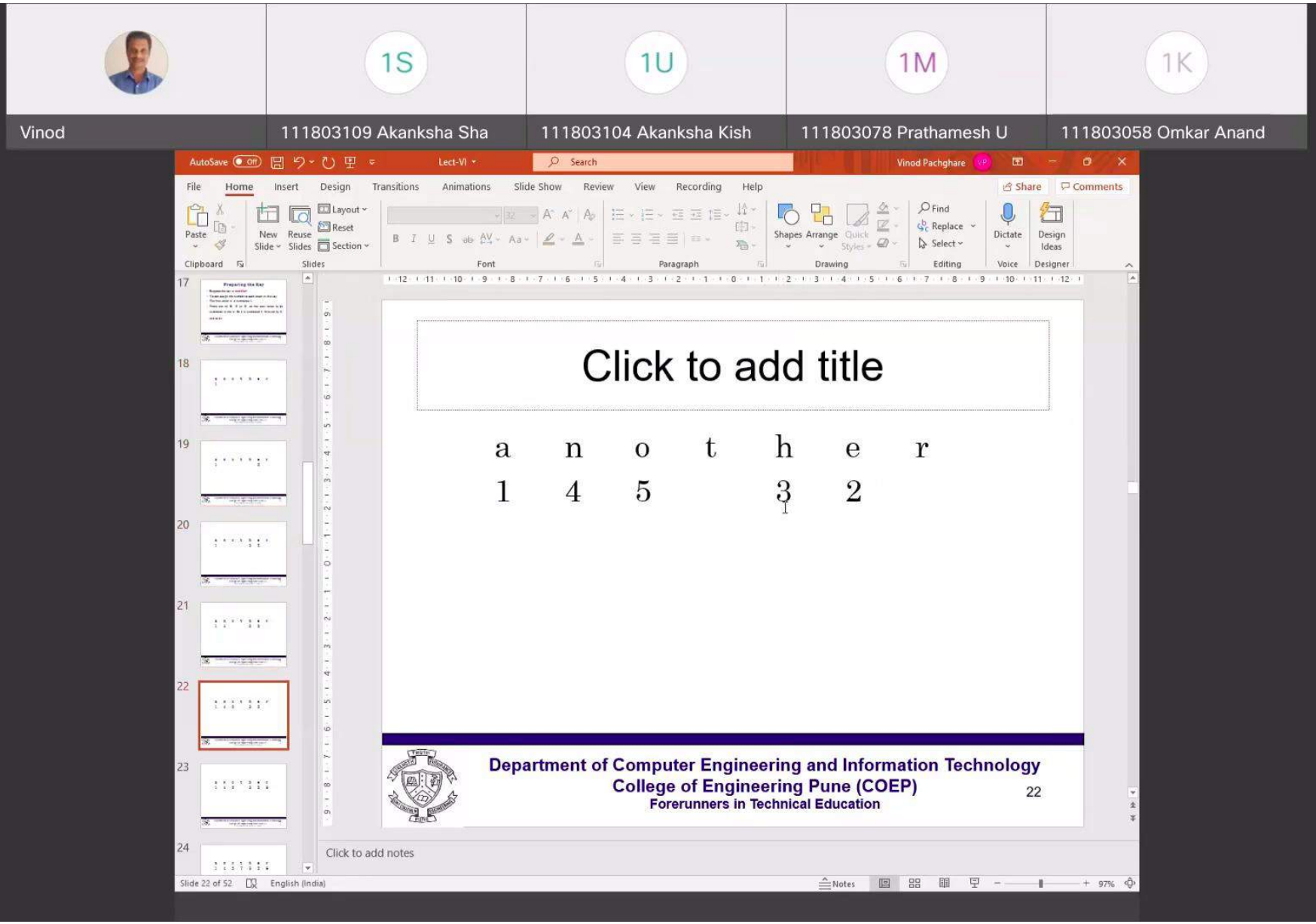
1 4 3 2

Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education
21

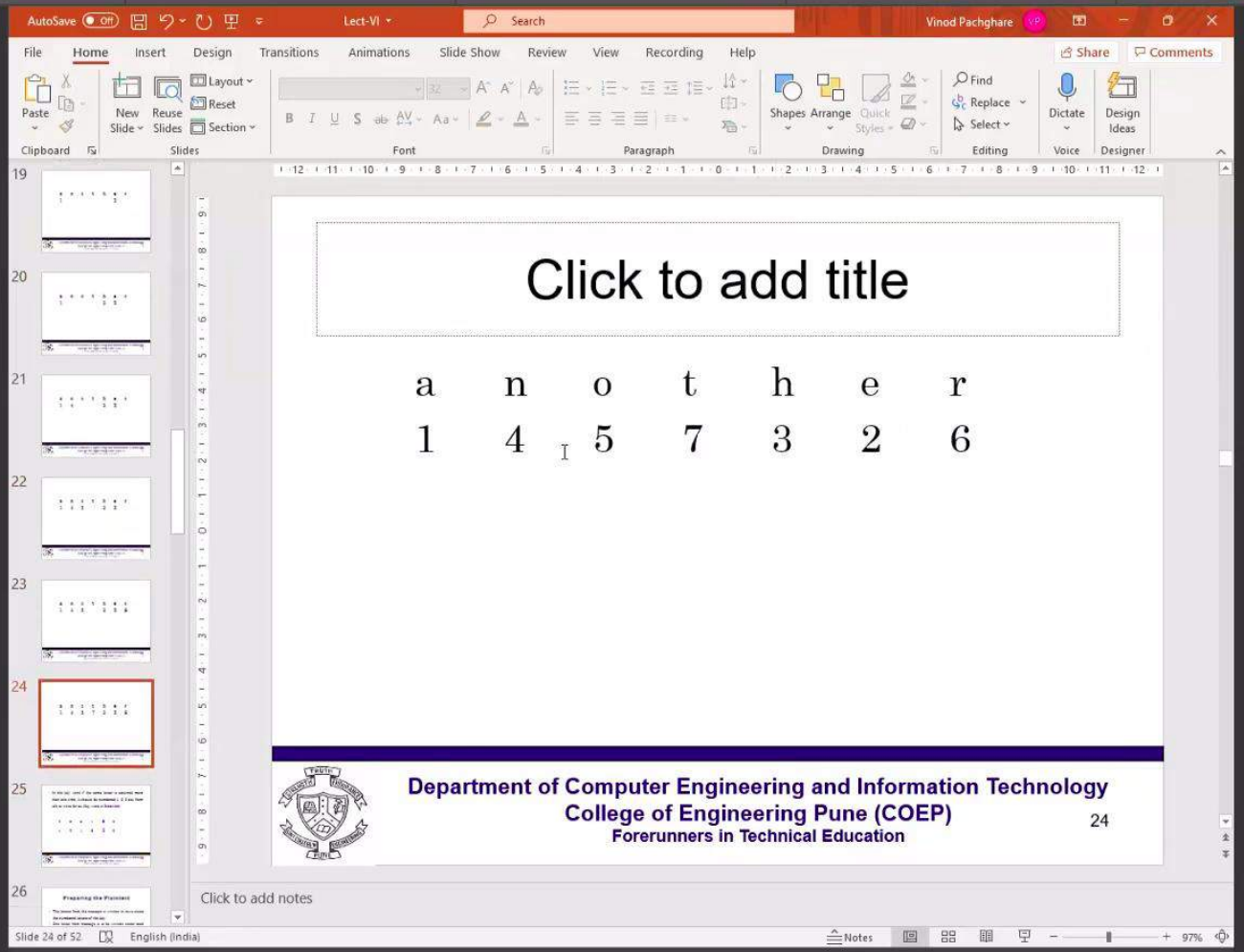
Click to add notes

Slide 21 of 52 | English (India) | Notes | 97%

+114

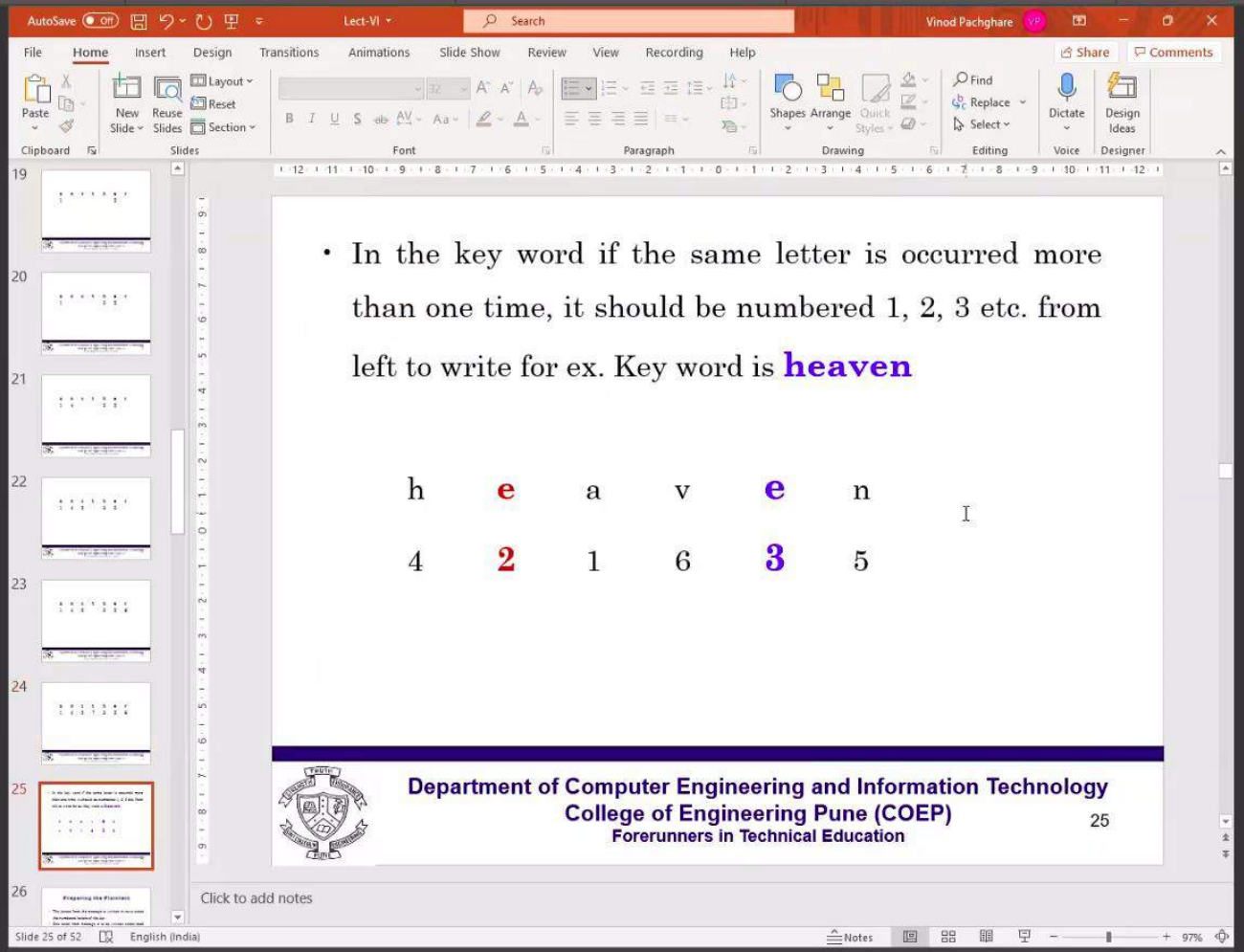

Vinod
111803109 Akanksha Sha
111803104 Akanksha Kish
111803078 Prathamesh U
111803058 Omkar Anand
Click to add title
a n o t h e r
1 4 5 3 2
Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education
22
Click to add notes
+114

1S	1U	1M	1K
Vinod	111803109 Akanksha Sha	111803104 Akanksha Kish	111803078 Prathamesh U	111803058 Omkar Anand



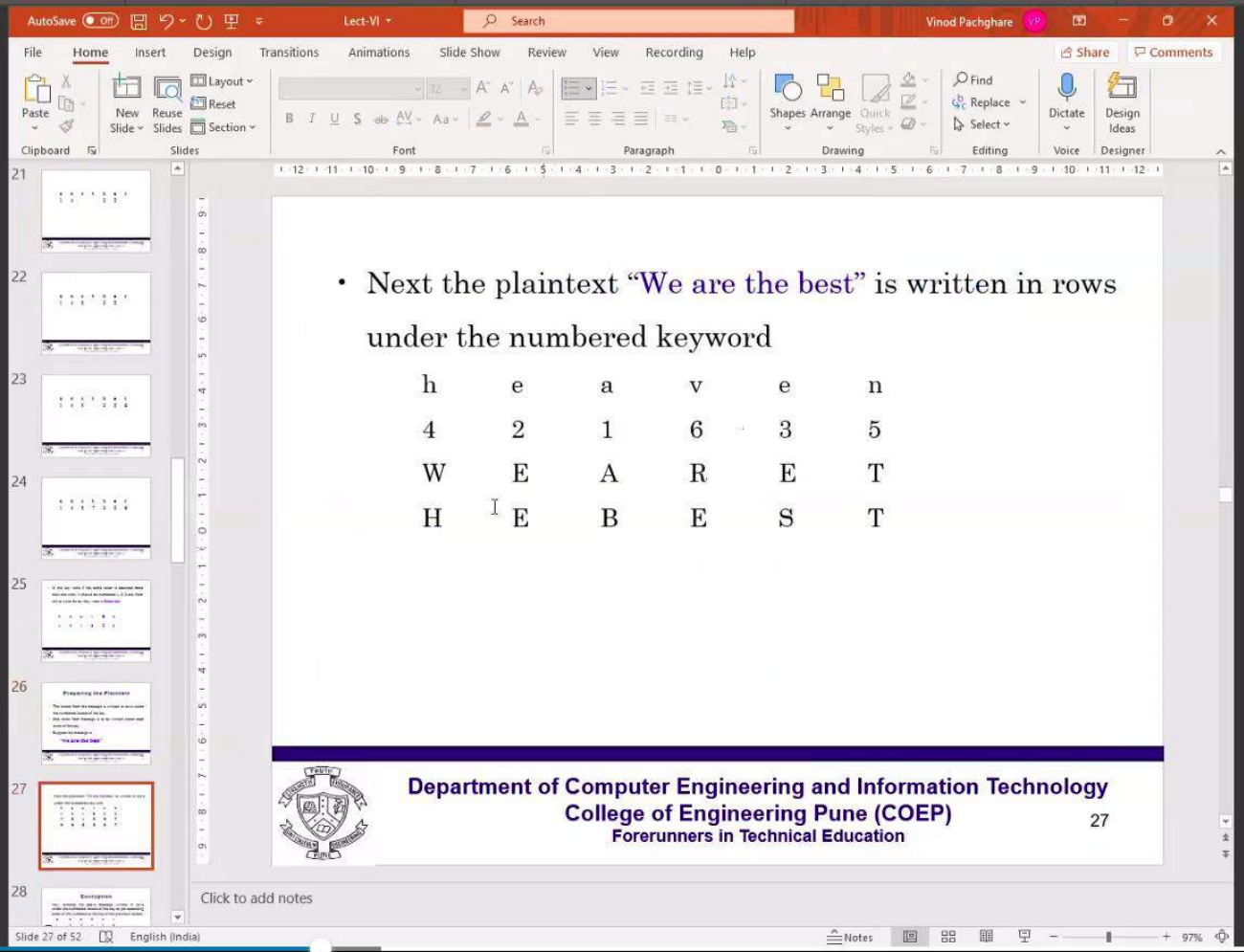
+114

1S	1U	1M	1K
Vinod	111803109 Akanksha Sha	111803104 Akanksha Kish	111803078 Prathamesh U	111803058 Omkar Anand

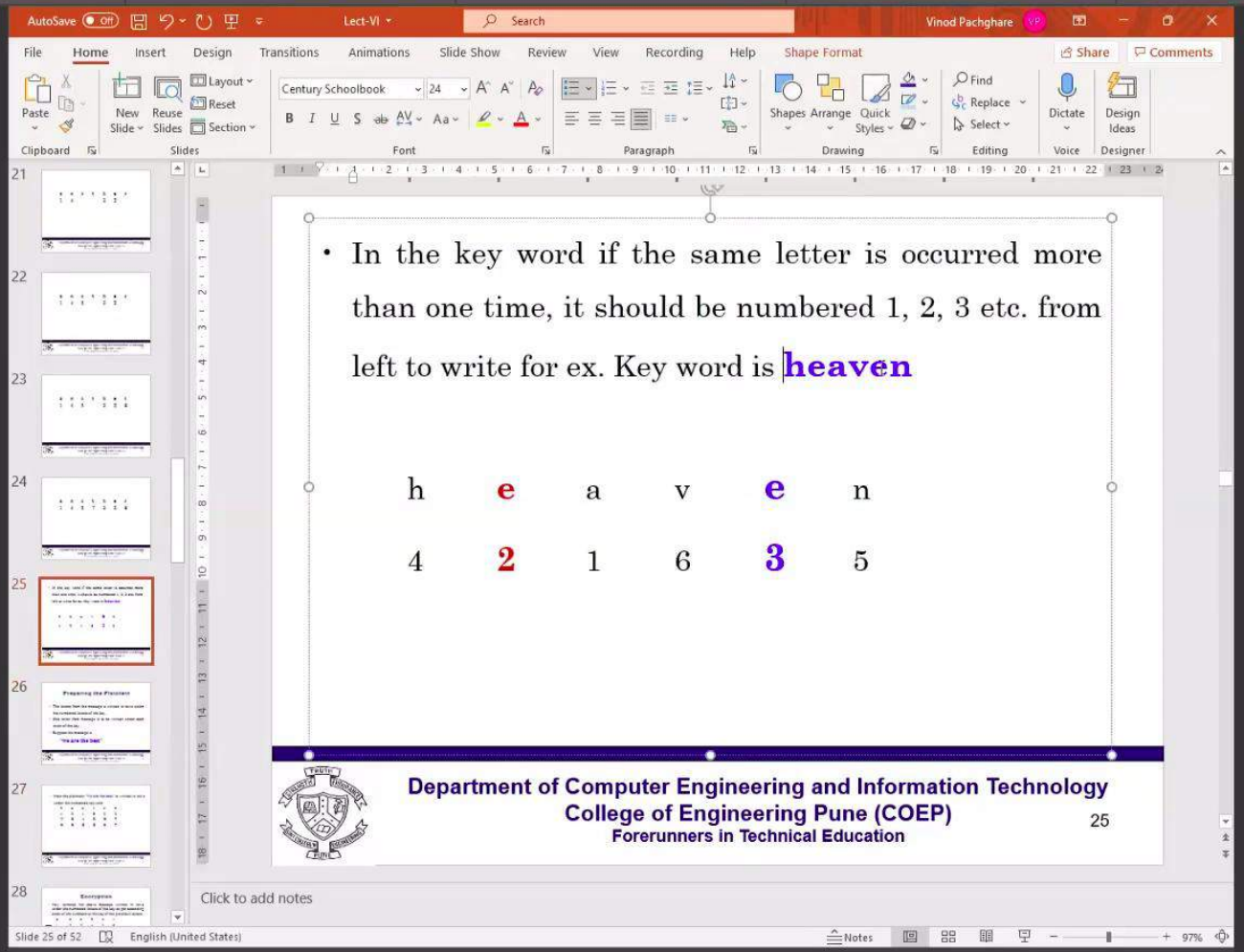


+114

Vinod	111803109 Akanksha Sha	111803104 Akanksha Kish	111803078 Prathamesh U	111803058 Omkar Anand

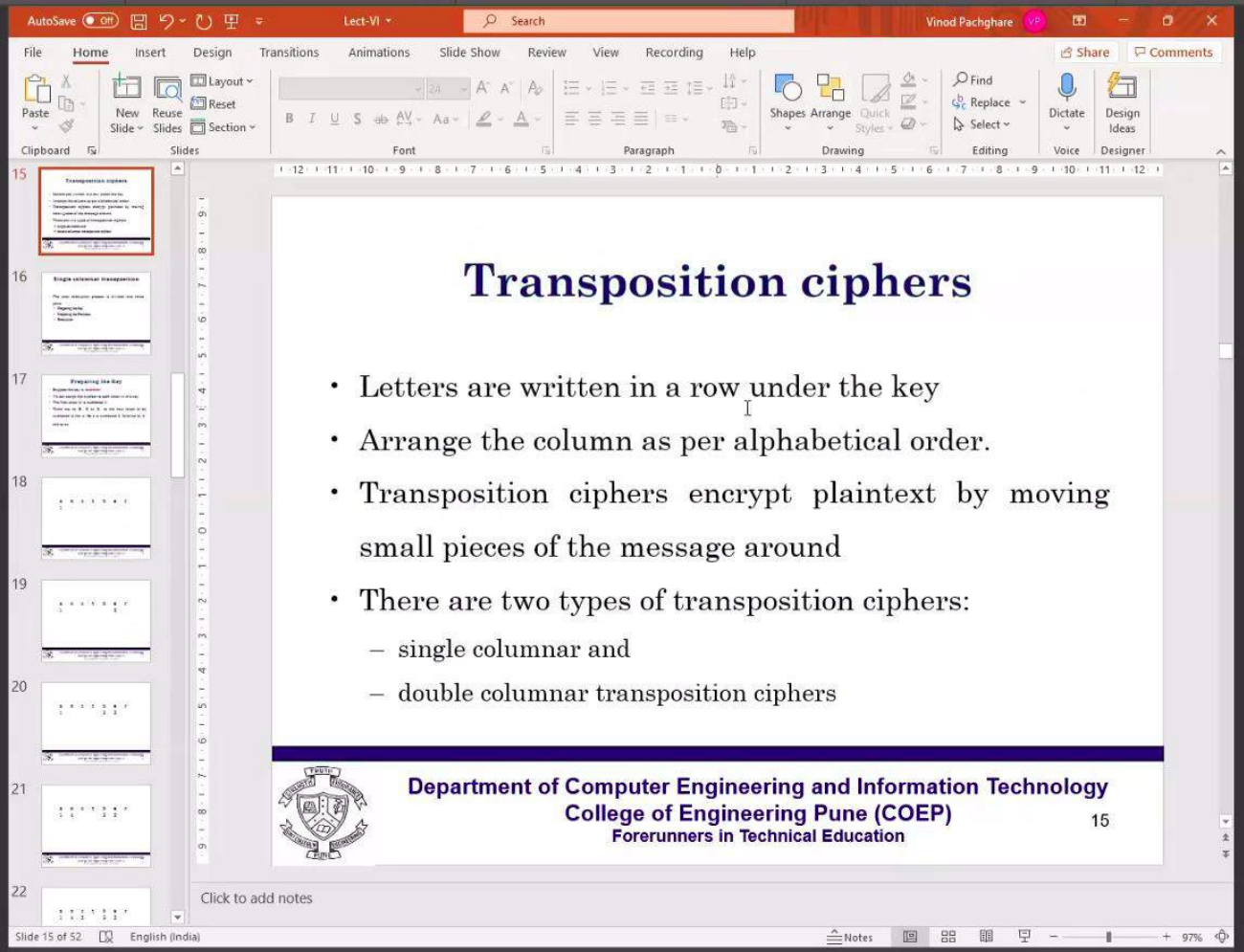


1S	1U	1M	1K
Vinod	111803109 Akanksha Sha	111803104 Akanksha Kish	111803078 Prathamesh U	111803058 Omkar Anand



+114

Vinod | 111803109 Akanksha Sha | 111803104 Akanksha Kish | 111803078 Prathamesh U | 111803058 Omkar Anand



+115

1S	1U	1M	1K
Vinod	111803109 Akanksha Sha	111803104 Akanksha Kish	111803078 Prathamesh U	111803058 Omkar Anand

AutoSave Off | Lect-VI | Search | Vinod Pachghare

File Home Insert Design Transitions Animations Slide Show Review View Recording Help | Share | Comments

Paste | New Slide | Reuse Slides | Layout | Reset | Section | Clipboard | Slides | Font | Paragraph | Shapes | Arrange | Quick Styles | Drawing | Find | Replace | Select | Editing | Dictate | Voice | Design Ideas | Designer

15 16 17 18 19 20 21 22

Single columnar transposition

- The total encryption process is divided into three parts:
  - Preparing the Key
  - Preparing the Plaintext
  - Encryption

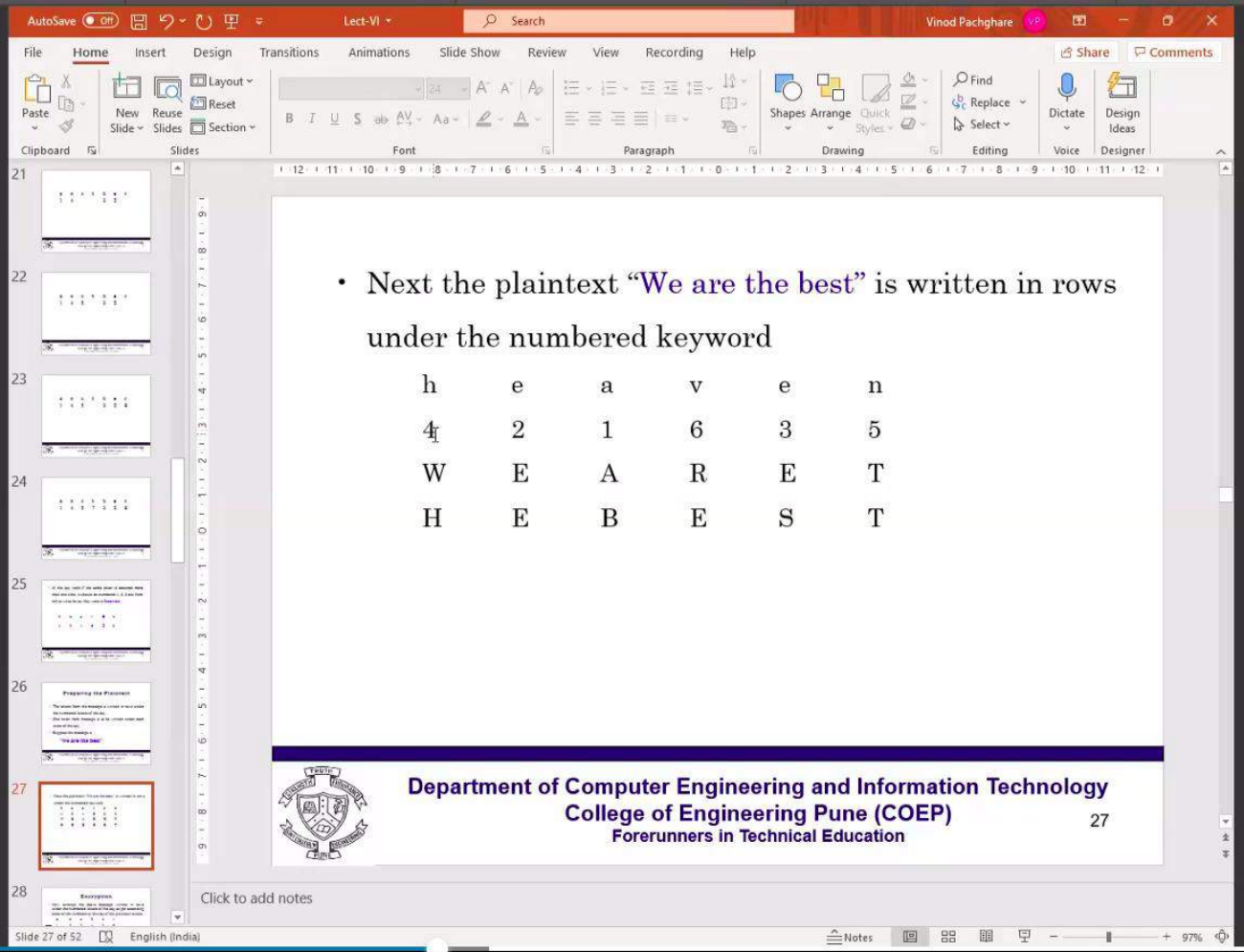
Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education
16

Click to add notes

Slide 16 of 52 | English (India) | Notes | 97%

+118

1S	1U	1M	1K
Vinod	111803109 Akanksha Sha	111803104 Akanksha Kish	111803078 Prathamesh U	111803058 Omkar Anand



23:34 / 57:24

1S	1U	1M	1K
Vinod	111803109 Akanksha Sha	111803104 Akanksha Kish	111803078 Prathamesh U	111803058 Omkar Anand

- Next the plaintext "We are the best" is written in rows under the numbered keyword

h	e	a	v	e	n
4	2	1	6	3	5
W	E	A	R	E	T
H	E	B	E	S	T

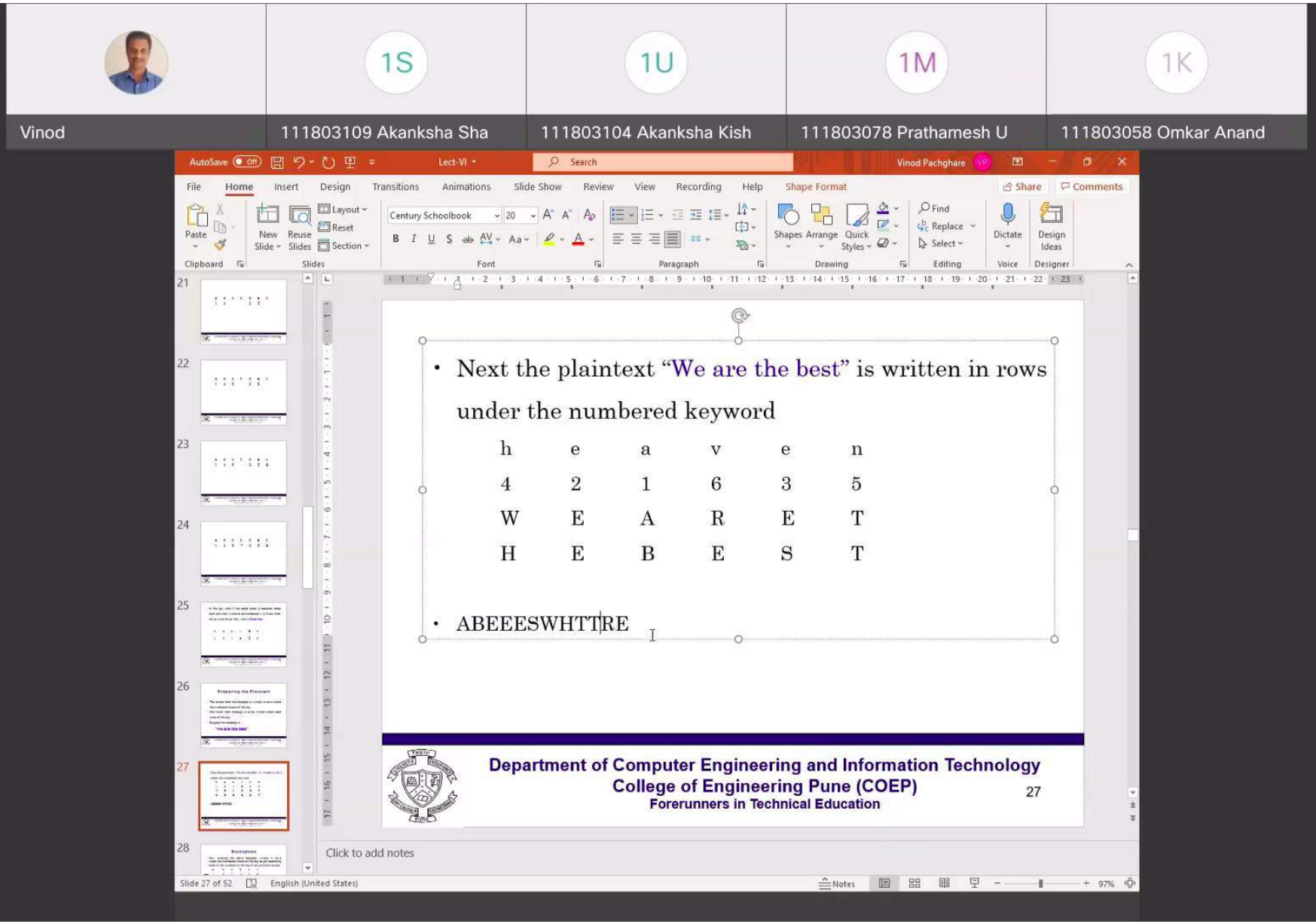
- AB EE ES WH TT RE

Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education
27

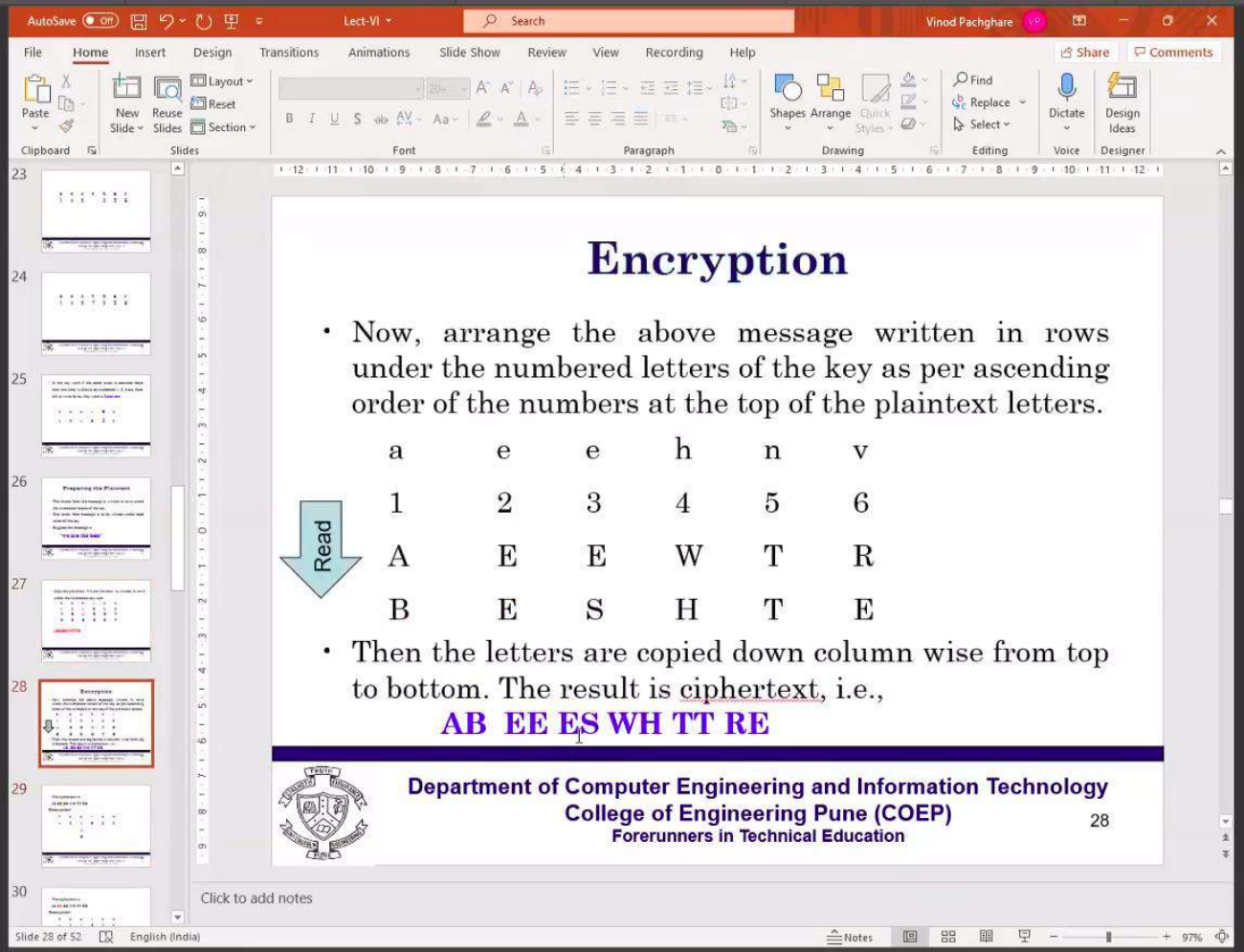
Click to add notes

Slide 27 of 52 English (United States)

+117

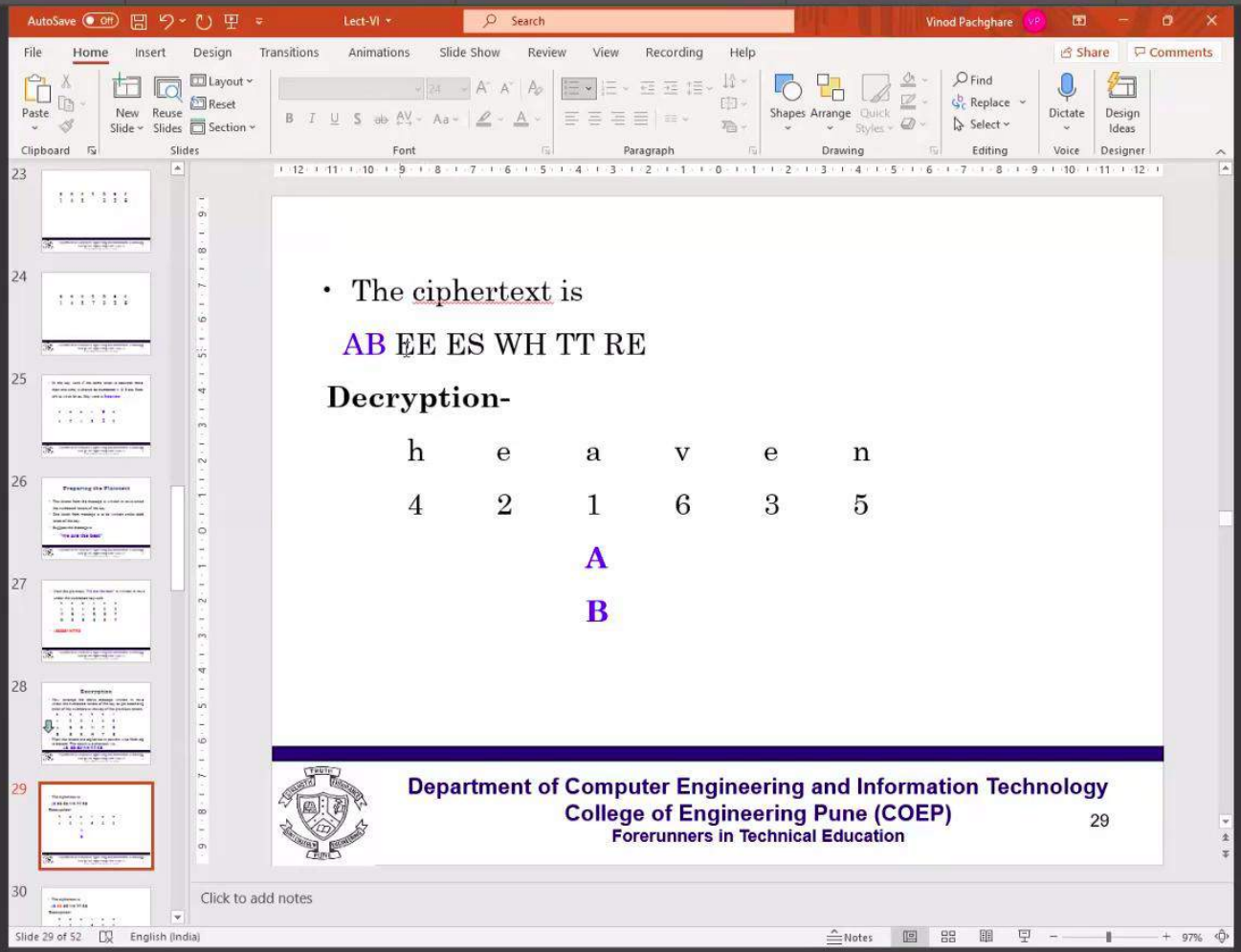

1S
1U
1M
1K
Vinod
111803109 Akanksha Sha
111803104 Akanksha Kish
111803078 Prathamesh U
111803058 Omkar Anand
AutoSave
Lect-VI
Search
Vinod Pachghare
File Home Insert Design Transitions Animations Slide Show Review View Recording Help Shape Format
Share
Comments
Century Schoolbook
20
Paste
New Slide
Reuse Slides
Layout
Reset
Section
Clipboard
Slides
Font
Paragraph
Shapes
Arrange
Quick Styles
Drawing
Find
Replace
Select
Editing
Dictate
Voice
Design Ideas
Designer
Next the plaintext "We are the best" is written in rows under the numbered keyword
h e a v e n
4 2 1 6 3 5
W E A R E T
H E B E S T
ABEEESWHTTRE
Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education
27
Click to add notes
Slide 27 of 52
English (United States)
Notes
97%
+118

1S	1U	1M	1K
Vinod	111803109 Akanksha Sha	111803104 Akanksha Kish	111803078 Prathamesh U	111803058 Omkar Anand

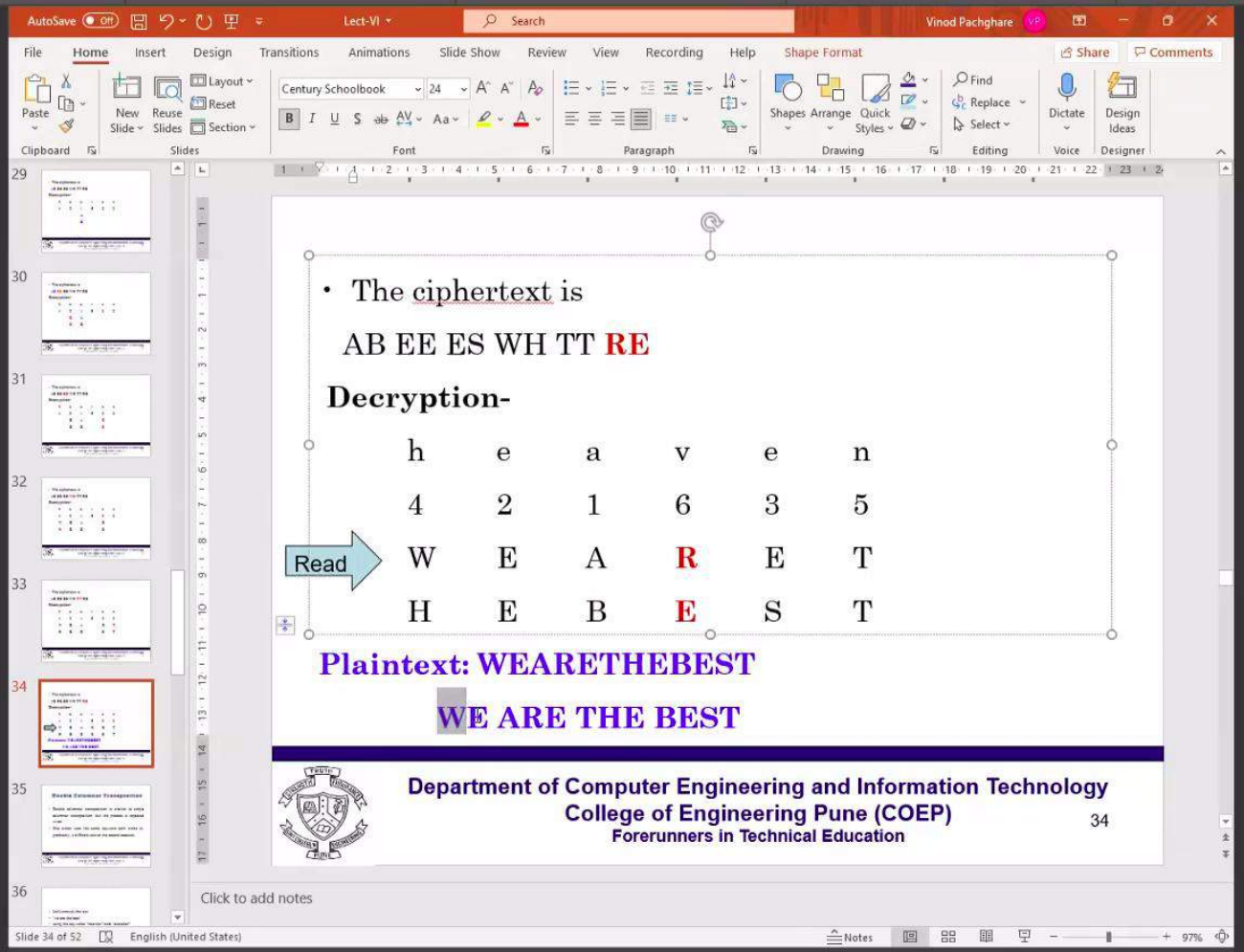


+118

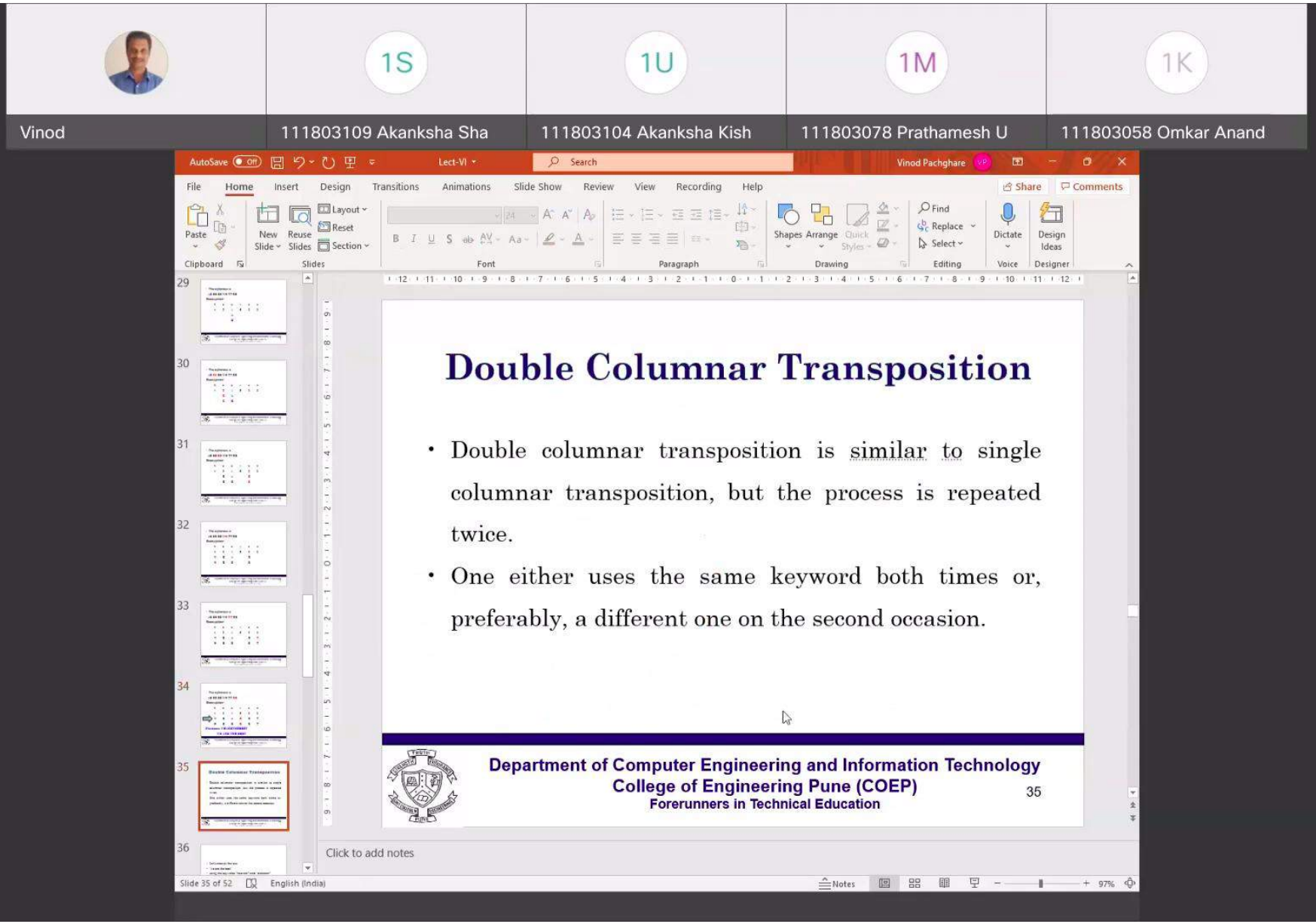
1S	1U	1M	1K
Vinod	111803109 Akanksha Sha	111803104 Akanksha Kish	111803078 Prathamesh U	111803058 Omkar Anand



1S	1U	1M	1K
Vinod	111803109 Akanksha Sha	111803104 Akanksha Kish	111803078 Prathamesh U	111803058 Omkar Anand



+118


Vinod
111803109 Akanksha Sha
111803104 Akanksha Kish
111803078 Prathamesh U
111803058 Omkar Anand
Lect-VI
Search
Vinod Pachghare
Double Columnar Transposition
Double columnar transposition is similar to single columnar transposition, but the process is repeated twice.
One either uses the same keyword both times or, preferably, a different one on the second occasion.
Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education
35
Click to add notes
Slide 35 of 52
English (India)
+118

1S	1U	1M	1K
Vinod	111803109 Akanksha Sha	111803104 Akanksha Kish	111803078 Prathamesh U	111803058 Omkar Anand

- Next the plaintext "We are the best ONE" is written in rows under the numbered keyword

h	e	a	v	e	n
4	2	1	6	3	5
W	E	A	R	E	T
H	E	B	E	S	T
O	N	E			

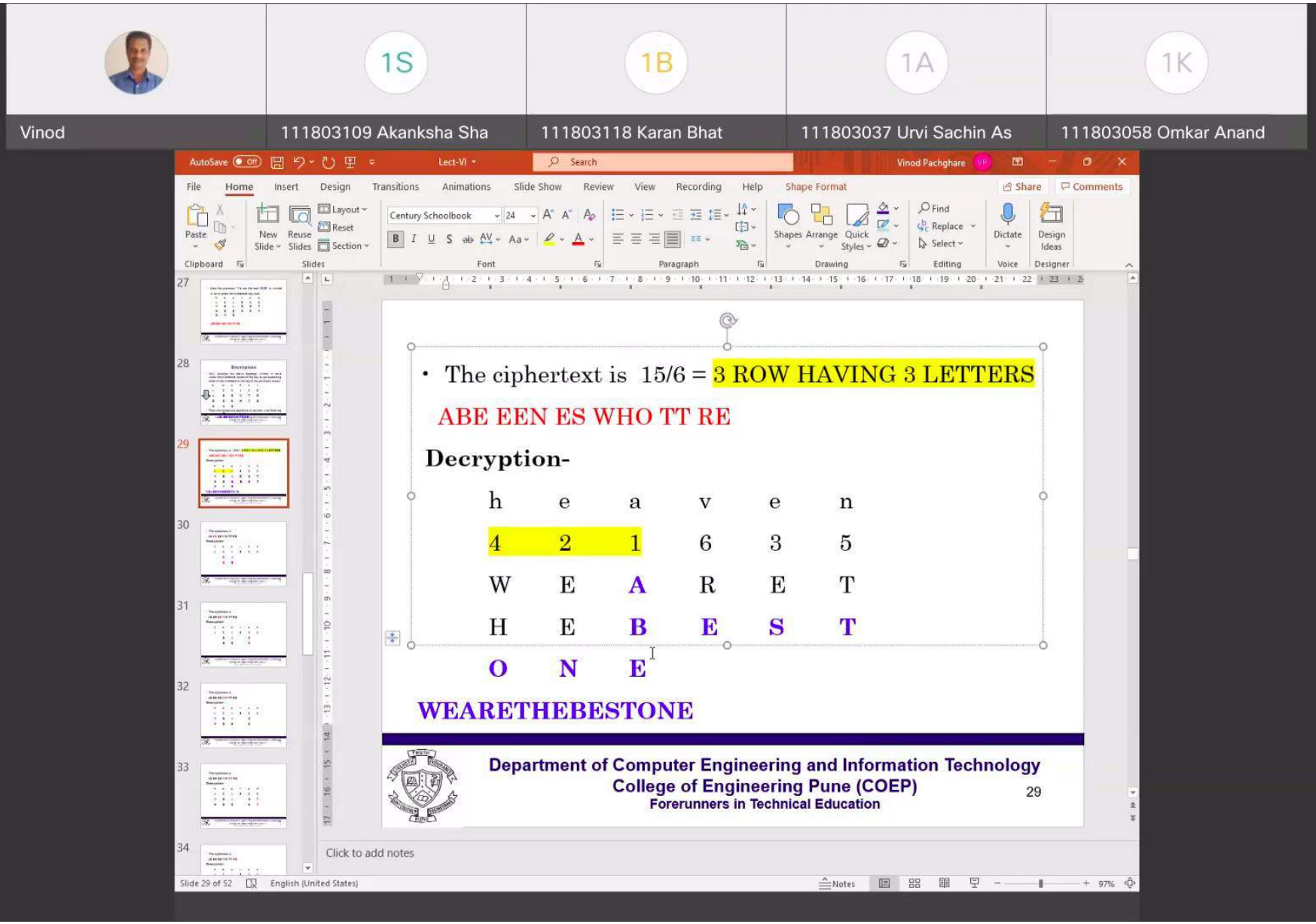
- ABE EEN ES WHO TT RE

Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education
27

Click to add notes

Slide 27 of 52 English (United States)

+121


Vinod
111803109 Akanksha Sha
111803118 Karan Bhat
111803037 Urvi Sachin As
111803058 Omkar Anand
1S
1B
1A
1K
AutoSave
Lect-VI
Search
Vinod Pachghare
File Home Insert Design Transitions Animations Slide Show Review View Recording Help Shape Format
Share
Comments
Century Schoolbook
24
Paste
New Slide
Reuse Slides
Layout
Reset
Section
Shapes
Arrange
Quick Styles
Find
Replace
Select
Dictate
Design Ideas
Clipboard
Slides
Font
Paragraph
Drawing
Editing
Voice
Designer
• The ciphertext is 15/6 = 3 ROW HAVING 3 LETTERS
ABE EEN ES WHO TT RE
Decryption-
h e a v e n
4 2 1 6 3 5
W E A R E T
H E B E S T
O N E
WEARETHEBESTONE
Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education
29
Click to add notes
Slide 29 of 52
English (United States)
Notes
97%
+120

Vinod | 1S | 111803109 Akanksha Sha | 1B | 111803118 Karan Bhat | 1A | 111803037 Urvi Sachin As | 1K | 111803058 Omkar Anand

AutoSave Off | Lect-VI | Search | Vinod Pachghare

File Home Insert Design Transitions Animations Slide Show Review View Recording Help | Share | Comments

Paste | New Slide | Reuse Slides | Layout | Reset | Section | Clipboard | Slides | Font | Paragraph | Shapes | Arrange | Quick Styles | Find | Replace | Select | Editing | Dictate | Voice | Design Ideas | Designer

29 30 31 32 33 34 35 36

Double Columnar Transposition

- Double columnar transposition is similar to single columnar transposition, but the process is repeated twice.
- One either uses the same keyword both times or, preferably, a different one on the second occasion.

Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education

35

Click to add notes

Slide 35 of 52 | English (India) | Notes | 97%

javascript:void(0); 8:08 / 57:24

Vinod | 111803109 Akanksha Sha | 111803118 Karan Bhat | 111803037 Urvi Sachin As | 111803058 Omkar Anand

AutoSave Off | Lect-VI | Search | Vinod Pachghare

File Home Insert Design Transitions Animations Slide Show Review View Recording Help Table Design Layout | Share | Comments

Paste | New Slide | Reuse Slides | Layout | Reset | Section | Clipboard | Slides | Times New Roman | 12+ | Font | Paragraph | Shapes | Arrange | Quick Styles | Drawing | Find | Replace | Select | Editing | Dictate | Voice | Design Ideas | Designer

33 34 35 36 37 38 39 40

a n o t h e r

1 4 5 7 3 2 6

A B E E E S W

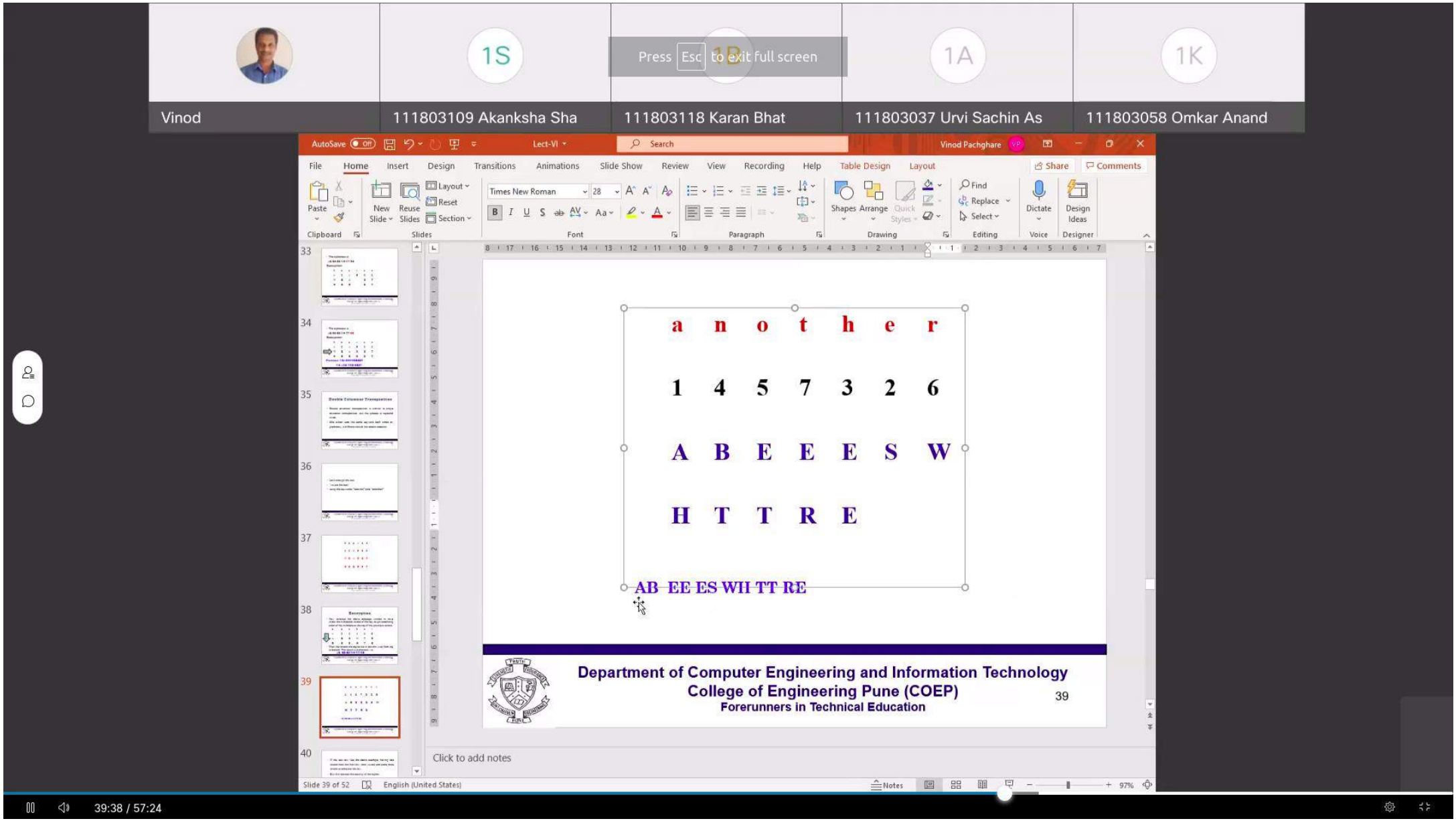
H T T R E

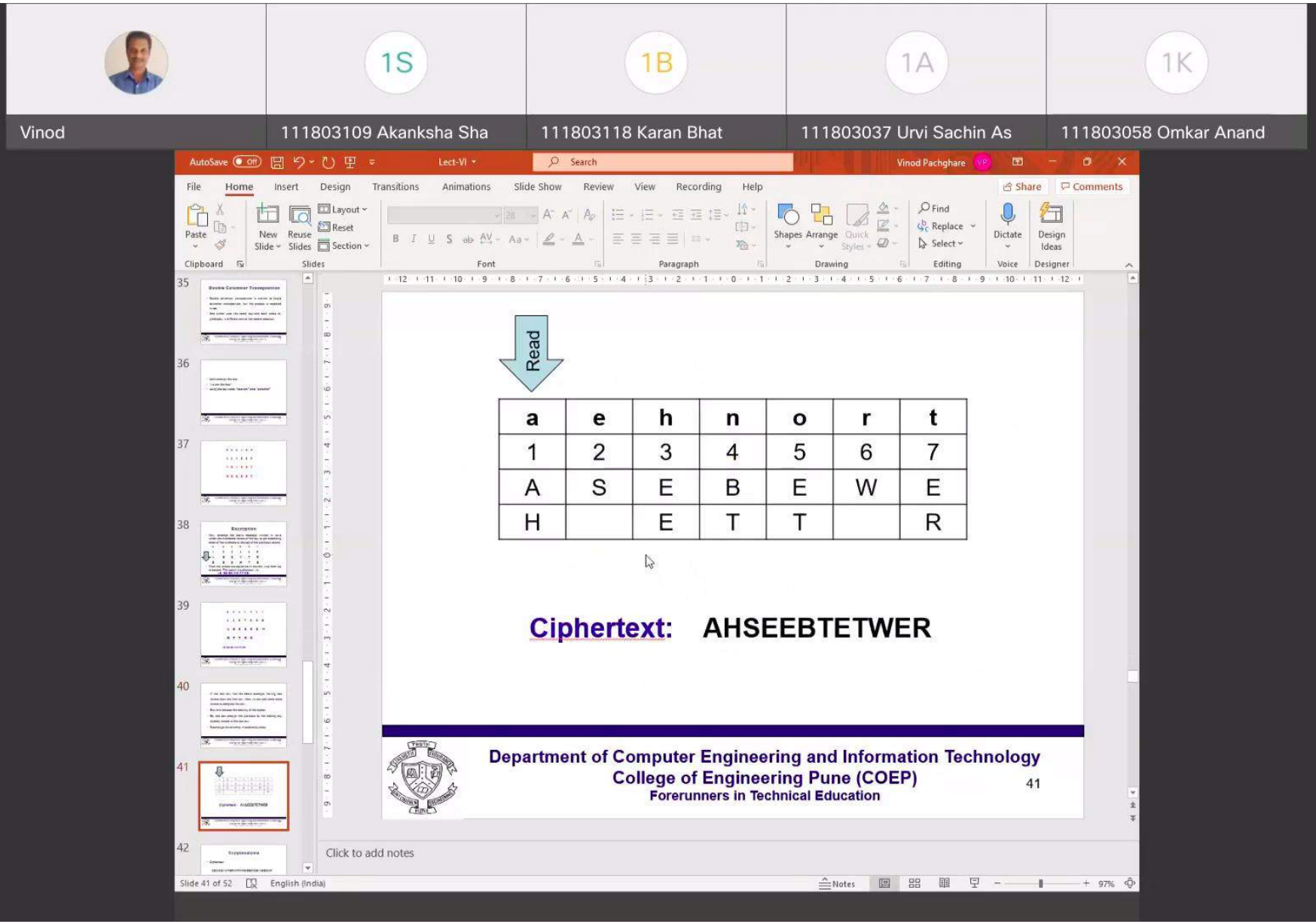
Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education
39

Click to add notes

Slide 39 of 52 | English (United States) | Notes | 97%

+118


Vinod
111803109 Akanksha Sha
111803118 Karan Bhat
111803037 Urvi Sachin As
111803058 Omkar Anand
Press Esc to exit full screen
another
1 4 5 7 3 2 6
A B E E E S W
H T T R E
AB EE ES WH TT RE
Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education
39
Click to add notes
Slide 39 of 52
English (United States)
39:38 / 57:24


Vinod
1S
111803109 Akanksha Sha
1B
111803118 Karan Bhat
1A
111803037 Urvi Sachin As
1K
111803058 Omkar Anand
Read
a e h n o r t
1 2 3 4 5 6 7
A S E B E W E
H E T T R
Ciphertext: AHSEEBTETWER
Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education
41
Click to add notes
Slide 41 of 52
English (India)
+117

1S	1B	1A	1K
Vinod	111803109 Akanksha Sha	111803118 Karan Bhat	111803037 Urvi Sachin As	111803058 Omkar Anand

Steganography

Steganography is the art and science of writing hidden messages in such a way that no one apart from the intended recipient knows of the existence of the message.

This can be achieve by concealing the existence of **information** within seemingly harmless **carriers or cover**

Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education
48

Click to add notes

+116

Vinod | 111803109 Akanksha Sha | 111803118 Karan Bhat | 111803037 Urvi Sachin As | 111803058 Omkar Anand

AutoSave Off | Lect-VI | Search | Vinod Pachghare

File Home Insert Design Transitions Animations Slide Show Review View Recording Help | Share | Comments

Paste | New Slide | Reuse Slides | Layout | Reset | Section | Clipboard | Slides | Font | Paragraph | Shapes | Arrange | Quick Styles | Drawing | Find | Replace | Select | Editing | Dictate | Voice | Design Ideas | Designer

43 44 45 46 47 48 49 50

Click to add title

- **Carrier:** text, image, video, audio, etc

Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education
49

Click to add notes

Slide 49 of 52 | English (India) | Notes | 97%

+115

Vinod | 1S | 111803109 Akanksha Sha | 1B | 111803118 Karan Bhat | 1A | 111803037 Urvi Sachin As | 1K | 111803058 Omkar Anand

AutoSave Off | Lect-VI | Search | Vinod Pachghare

File Home Insert Design Transitions Animations Slide Show Review View Recording Help | Share | Comments

Paste | New Slide | Reuse Slides | Layout | Reset | Section | Clipboard | Slides | Font | Paragraph | Shapes | Arrange | Quick Styles | Drawing | Find | Replace | Select | Editing | Dictate | Voice | Design Ideas | Designer

45 46 47 48 49 50 51 52

Question

Salutations, Mr. Robertson of CIS 5371. The Florida Society of Math and Cryptography is proud to present you with an small exam for qualification into our society. The key for passing is studying. Cryptography is rigorous and only those with patience in themselves pass. We have an exam PO Box in Tallahassee. But please submit by 12/12.

Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education
50

Click to add notes

Slide 50 of 52 | English (India) | Notes | 97%

+115

Vinod | 1S | 111803109 Akanksha Sha | 1B | 111803118 Karan Bhat | 1A | 111803037 Urvi Sachin As | 1K | 111803058 Omkar Anand

AutoSave Off | Lect-VI | Search | Vinod Pachghare

File Home Insert Design Transitions Animations Slide Show Review View Recording Help | Share | Comments

Paste | New Slide | Reuse Slides | Layout | Reset | Section | Clipboard | Slides | Font | Paragraph | Shapes | Arrange | Quick Styles | Drawing | Find | Replace | Select | Editing | Dictate | Voice | Design Ideas | Designer

45 46 47 48 49 50 51 52

Answer

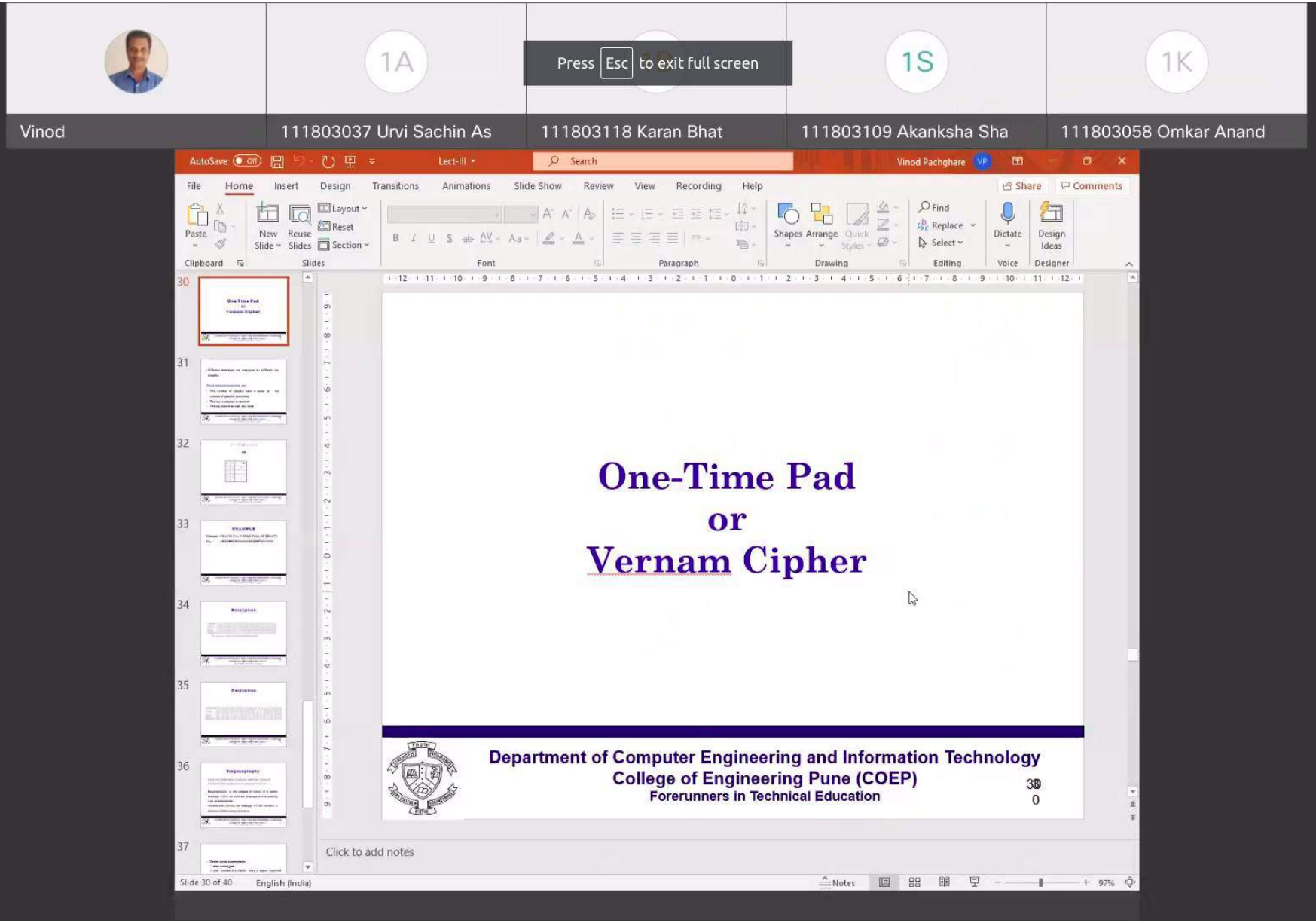
Salutations, Mr. Robertson of CIS 5371. **The** Florida Society of Math and **Cryptography** is proud to present you with an small **exam** for qualification into our society. The **key** for passing is studying. Cryptography **is** rigorous and only those with patience **in** themselves pass. We have an exam **PO Box** in Tallahassee. But please submit by **12/12**.

The Cryptography exam key is in PO Box 1212.

Click to add notes

Slide 51 of 52 | English (India) | Notes | 97%

+115


Press Esc to exit full screen
Vinod
111803037 Urvi Sachin As
111803118 Karan Bhat
111803109 Akanksha Sha
111803058 Omkar Anand
AutoSave
Lect-III
Search
Vinod Pachghare
File Home Insert Design Transitions Animations Slide Show Review View Recording Help
Share Comments
Paste New Slide Reuse Slides Layout Reset Section
Clipboard Slides Font Paragraph Drawing Editing Voice Designer
Shapes Arrange Quick Styles Find Replace Select Dictate Design Ideas
One-Time Pad or Vernam Cipher
Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education
Click to add notes
Slide 30 of 40
English (India)
Notes
97%

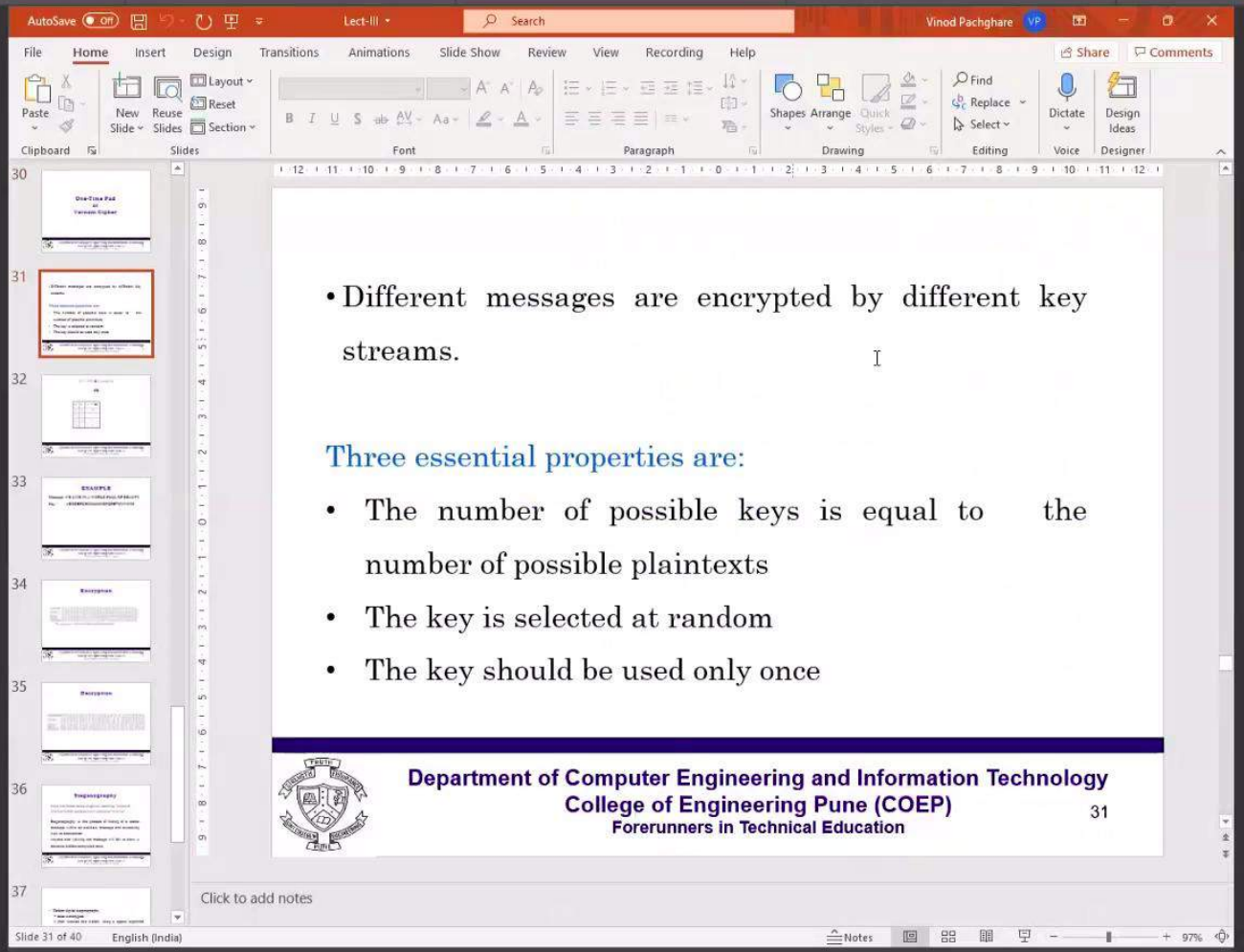
1A

Press Esc to exit full screen

1S

1K

Vinod | 111803037 Urvi Sachin As | 111803118 Karan Bhat | 111803109 Akanksha Sha | 111803058 Omkar Anand



+107

1A	1B	1S	1K
Vinod	111803037 Urvi Sachin As	111803118 Karan Bhat	111803109 Akanksha Sha	111803058 Omkar Anand

$$CT = (PT \oplus K) \bmod 26$$

OR

- Click icon to add table

PT	K	CT = PT ⊕ K
0	0	0
0	1	1
1	0	1
1	1	0

Click to add notes

Vinod	111803037 Urvi Sachin As	111803118 Karan Bhat	111803109 Akanksha Sha	111803058 Omkar Anand

53:21 / 57:24

Vinod	111803037 Urvi Sachin As	111803118 Karan Bhat	111803109 Akanksha Sha	111803058 Omkar Anand
	1A	1B	1S	1K

AutoSave Off | Lect-III | Search | Vinod Pachghare

File Home Insert Design Transitions Animations Slide Show Review View Recording Help | Share | Comments

Paste | New Slide | Reuse Slides | Layout | Reset | Section | Clipboard | Slides | Font | Paragraph | Shapes | Arrange | Quick Styles | Find | Replace | Select | Editing | Dictate | Voice | Design Ideas | Designer

30 31 32 33 34 35 36 37

Encryption

- Click icon to add table

PLAINTEXT	W	E	L	I	V	E	I	N	A	W	O	R	L	D	F	U	L	L	O	F	B	E	A	U	T	Y
	22	04	11	8	21	4	8	13	0	22	14	17	11	3	5	20	11	11	14	5	1	4	0	20	19	24
OTP KEY	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
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
RESULT	22	5	13	11	25	9	14	20	8	31	24	28	23	16	19	35	27	28	32	24	21	25	22	43	43	49
MOD 26	22	5	13	11	25	9	14	20	8	5	24	2	23	16	19	9	1	2	6	24	21	25	22	17	17	23
CIPHERTEXT	W	F	N	L	Z	J	O	U	I	F	Y	C	X	Q	T	J	B	C	G	Y	V	Z	W	R	R	X

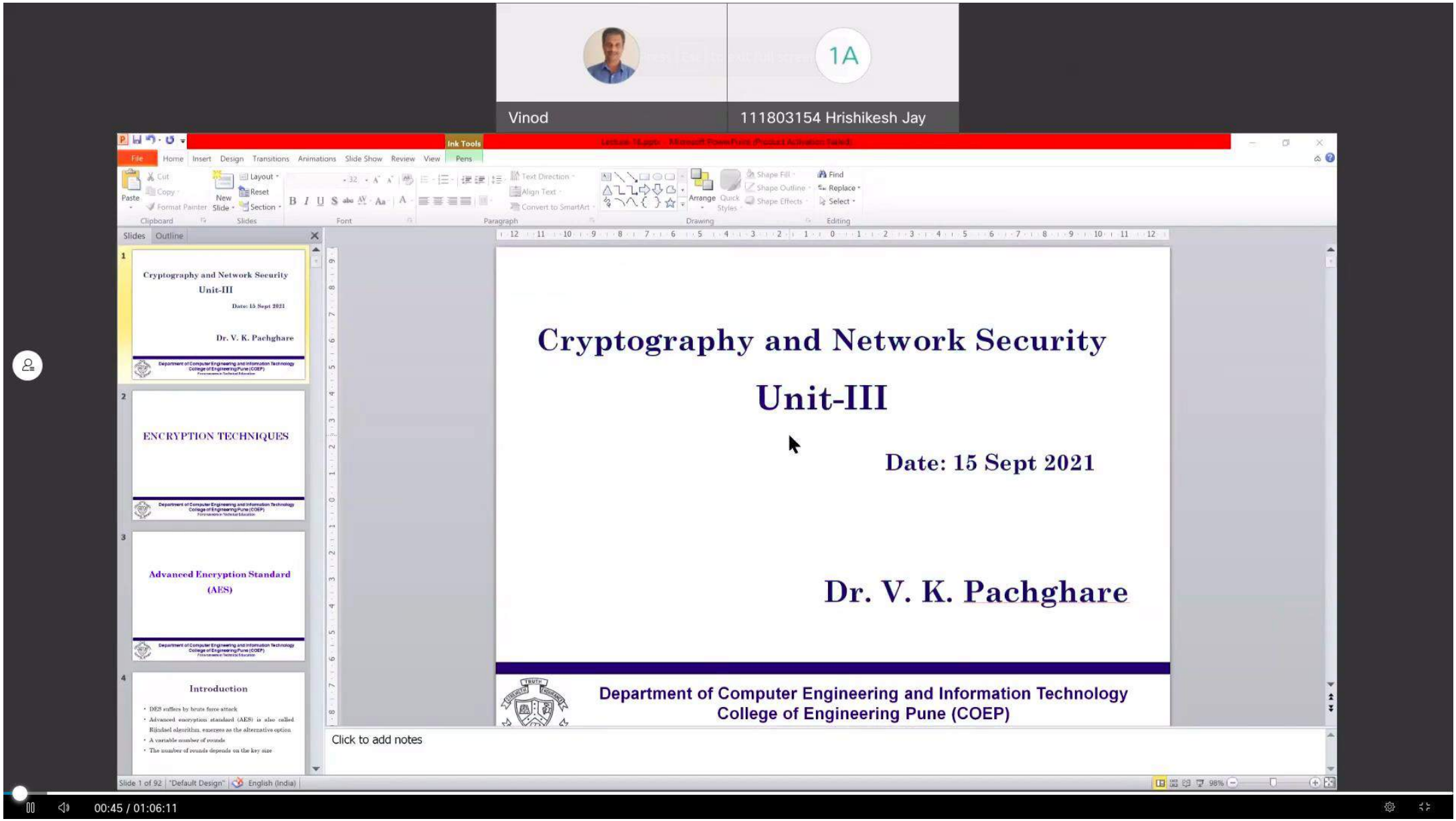
The ciphertext is "WFNLZJOUIFYCXQTJBCGYVZWRRX"

Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education
34

Click to add notes

Slide 34 of 40 | English (India) | Notes | 97%

54:14 / 57:24


Vinod
1A
111803154 Hrishikesh Jay
Cryptography and Network Security
Unit-III
Date: 15 Sept 2021
Dr. V. K. Pachghare
Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
ENCRYPTION TECHNIQUES
Advanced Encryption Standard (AES)
Introduction
DES suffers by brute force attack
Advanced encryption standard (AES) is also called Rijndael algorithm, emerges as the alternative option
A variable number of rounds
The number of rounds depends on the key size
Click to add notes
00:45 / 01:06:11

1A	1S	1N	1P
Vinod	111803154 Hrishikesh Jay	141903015 Vaishnavi Raje	111803158 Ruhee Rajesh	111803116 Aryan Prasad

Introduction

- DES suffers by brute force attack
- Advanced encryption standard (AES) is also called Rijndael algorithm, emerges as the alternative option
- A variable number of rounds
- The number of rounds depends on the key size

Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education

+27

1A	1S	1N	1P
Vinod	111803154 Hrishikesh Jay	141903015 Vaishnavi Raje	111803158 Ruhee Rajesh	111803116 Aryan Prasad

- Design of AES algorithm does not based on Feistel structure.

Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education

+74

1A	1S	1N	1P
Vinod	111803154 Hrishikesh Jay	141903015 Vaishnavi Raje	111803158 Ruhee Rajesh	111803116 Aryan Prasad

- Design of AES algorithm does not based on Feistel structure.
- It is based on linear transformation.
- AES uses different transformations such as
  - substitution,
  - permutation,
  - the mix column and
  - round key addition

1A	1S	1N	1P
Vinod	111803154 Hrishikesh Jay	141903015 Vaishnavi Raje	111803158 Ruhee Rajesh	111803116 Aryan Prasad

- This transformation forms a state.
- A state defines the current condition of the block during encryption.
- A state is nothing but the block of 4 x 4 matrix of bytes which is currently being processed on.

Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education

Slide 8 of 92 | "Default Design" | English (India)

11:31 / 01:06:11

1A	1S	1N	1P
Vinod	111803154 Hrishikesh Jay	141903015 Vaishnavi Raje	111803158 Ruhee Rajesh	111803116 Aryan Prasad

Terminology

State: Defines the current condition (state) of the block. That is the block of bytes that are currently being worked on. The state starts off being equal to the block, however it changes as each round of the algorithms executes. This is the block in progress.

Block: AES can currently encrypt blocks of 128 bits at a time; no other block sizes are presently a part of the AES standard.

Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education

1A	1S	1N	1P
Vinod	111803154 Hrishikesh Jay	141903015 Vaishnavi Raje	111803158 Ruhee Rajesh	111803116 Aryan Prasad

AES

- Plaintext block size: 128 bits
- Key size: 128 bits/192 bits/256 bits
- Number of Rounds: 10/12/14

Key Size [bits]	Number of Rounds
128	10
192	12
256	14

	1A	1S	1N	1P
Vinod	111803154 Hrishikesh Jay	141903015 Vaishnavi Raje	111803158 Ruhee Rajesh	111803116 Aryan Prasad

+96

	1A	1S	1N	1P
Vinod	111803154 Hrishikesh Jay	141903015 Vaishnavi Raje	111803158 Ruhee Rajesh	111803116 Aryan Prasad

Structure of AES

Key expansion	Subkeys are generated from original key for each round
Initial round	XOR operation between the state and the round key
Rounds 1 to 9	Each round has four steps: byte substitution shift rows, mix columns, add subkey
Final round	This round has three steps: byte substitution, shift rows, add subkey

Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education

+96

	1A	1S	1N	1P
Vinod	111803154 Hrishikesh Jay	141903015 Vaishnavi Raje	111803158 Ruhee Rajesh	111803116 Aryan Prasad

Structure of AES

Key expansion	Subkeys are generated from original key for each round
Initial round	XOR operation between the state and the round key
Rounds 1 to 9	Each round has four steps: byte substitution shift rows, mix columns, add subkey
Final round	This round has three steps: byte substitution, shift rows, add subkey

1A	1S	1N	1P
Vinod	111803154 Hrishikesh Jay	141903015 Vaishnavi Raje	111803158 Ruhee Rajesh	111803116 Aryan Prasad

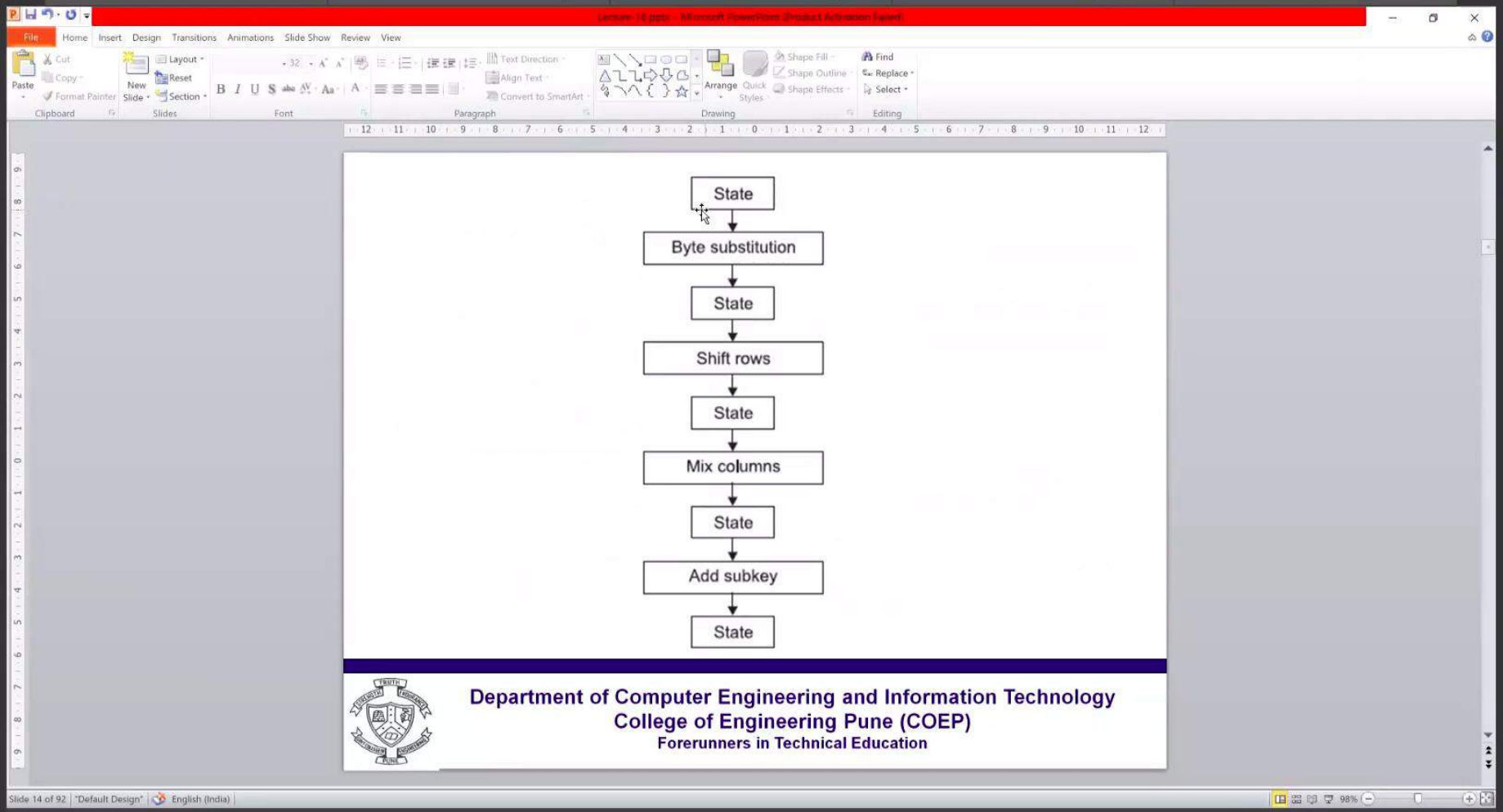
Each round consists of four stages

- Byte substitution (SubBytes)
- Shift Rows
- Mix Columns
- Add Subkey (AddRoundKey)

Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education

+106

	1A	1S	1N	1P
Vinod	111803154 Hrishikesh Jay	141903015 Vaishnavi Raje	111803158 Ruhee Rajesh	111803116 Aryan Prasad



+108

1A	1S	1N	1P
Vinod	111803154 Hrishikesh Jay	141903015 Vaishnavi Raje	111803158 Ruhee Rajesh	111803116 Aryan Prasad

1. Byte substitution (SubBytes)

- It is also called SubBytes step.
- Uses an S-box to perform a byte-by-byte substitution of the block
- This is a non-linear operation.
- It uses S-box structure similar to DES

Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education

1A	1S	1N	1P
Vinod	111803037 Urvi Sachin As	141903015 Vaishnavi Raje	111803158 Ruhee Rajesh	111803116 Aryan Prasad

S-box

x \ y	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education

+109

	1A	1S	1N	1P
Vinod	111803037 Urvi Sachin As	141903015 Vaishnavi Raje	111803158 Ruhee Rajesh	111803116 Aryan Prasad

Inv. S-box (Decryption)

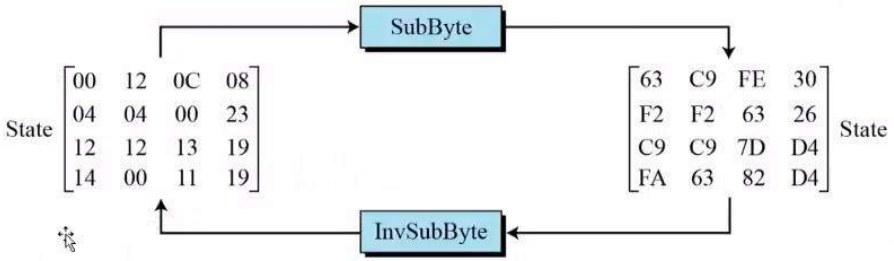
x \ y	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	52	09	6A	D5	30	36	A5	38	BF	40	A3	9E	81	F3	D7	FB
1	7C	E3	39	82	9B	2F	FF	87	34	8E	43	44	C4	DE	E9	CB
2	54	7B	94	32	A6	C2	23	3D	EE	4C	95	0B	42	FA	C3	4E
3	08	2E	A1	66	28	D9	24	B2	76	5B	A2	49	6D	8B	D1	25
4	72	F8	F6	64	86	68	98	16	D4	A4	5C	CC	5D	65	B6	92
5	6C	70	48	50	FD	ED	B9	DA	5E	15	46	57	A7	8D	9D	84
6	90	D8	AB	00	8C	BC	D3	0A	F7	E4	58	05	B8	B3	45	06
7	D0	2C	1E	8F	CA	3F	0F	02	C1	AF	BD	03	01	13	8A	6B
8	3A	91	11	41	4F	67	DC	EA	97	F2	CF	CE	F0	B4	E6	73
9	96	AC	74	22	E7	AD	35	85	E2	F9	37	E8	1C	75	DF	6E
A	47	F1	1A	71	1D	29	C5	89	6F	B7	62	0E	AA	18	BE	1B
B	FC	56	3E	4B	C6	D2	79	20	9A	DB	C0	FE	78	CD	5A	F4
C	1F	DD	A8	33	88	07	C7	31	B1	12	10	59	27	80	EC	5F
D	60	51	7F	A9	19	B5	4A	0D	2D	E5	7A	9F	93	C9	9C	EF
E	A0	E0	3B	4D	AE	2A	F5	B0	C8	EB	BB	3C	83	53	99	61
F	17	2B	04	7E	BA	77	D6	26	E1	69	14	63	55	21	0C	7D

Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education

+109

Byte substitution (SubBytes)

The SubBytes and Inv SubBytes transformations are inverses of each other



Vinod	111803037 Urvi Sachin As	141903015 Vaishnavi Raje	111803158 Ruhee Rajesh	111803116 Aryan Prasad

2. Shift Rows

- A simple permutation
- Provide diffusion to the cipher
- The first row of State is not altered.
- For the second row, a 1-byte circular left shift is performed.
- For the third row, a 2-byte circular left shift is performed.
- For the fourth row, a 3-byte circular left shift is performed.

	1A	1S	1N	1P
Vinod	111803037 Urvi Sachin As	141903015 Vaishnavi Raje	111803158 Ruhee Rajesh	111803116 Aryan Prasad

Shift Row

$$\begin{bmatrix} 87 & F2 & 4D & 97 \\ EC & 6E & 4C & 90 \\ 4A & C3 & 46 & E7 \\ 8C & D8 & 95 & A6 \end{bmatrix}$$

Before Shift

Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education

+115

1A	1S	1N	1P
Vinod	111803037 Urvi Sachin As	141903015 Vaishnavi Raje	111803158 Ruhee Rajesh	111803116 Aryan Prasad

Shift Row

$$\begin{bmatrix} 87 & F2 & 4D & 97 \\ EC & 6E & 4C & 90 \\ 4A & C3 & 46 & E7 \\ 8C & D8 & 95 & A6 \end{bmatrix} \qquad \begin{bmatrix} 87 & F2 & 4D & 97 \\ 6E & 4C & 90 & EC \\ & & & \\ & & & \end{bmatrix}$$

Before Shift *After Shift*

Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education

+115

1A	1S	1N	1P
Vinod	111803037 Urvi Sachin As	141903015 Vaishnavi Raje	111803158 Ruhee Rajesh	111803116 Aryan Prasad

Shift Row

$$\begin{bmatrix} 87 & F2 & 4D & 97 \\ EC & 6E & 4C & 90 \\ 4A & C3 & 46 & E7 \\ 8C & D8 & 95 & A6 \end{bmatrix} \qquad \begin{bmatrix} 87 & F2 & 4D & 97 \\ 6E & 4C & 90 & EC \\ 46 & E7 & 4A & C3 \\ A6 & 8C & D8 & 95 \end{bmatrix}$$

Before Shift *After Shift*

Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education

Speed 2x

javascript:void(0); :18 / 01:06:11

1A

1S

1N

1P

Vinod | 111803037 Urvi Sachin As | 141903015 Vaishnavi Raje | 111803158 Ruhee Rajesh | 111803116 Aryan Prasad

3. Mix Columns

- Mix Columns step provides diffusion to the cipher
- Each column is processed separately
- Each byte is replaced by a value dependent on all 4 bytes in the column

Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education

+116

1A	1S	1N	1P
Vinod	111803037 Urvi Sachin As	141903015 Vaishnavi Raje	111803158 Ruhee Rajesh	111803116 Aryan Prasad

3. Mix Columns

- Mix Columns step provides diffusion to the cipher
- Each column is processed separately
- Each byte is replaced by a value dependent on all 4 bytes in the column

Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education

33:03 / 01:06:11

1A	1S	1N	1P
Vinod	111803037 Urvi Sachin As	141903015 Vaishnavi Raje	111803158 Ruhee Rajesh	111803116 Aryan Prasad

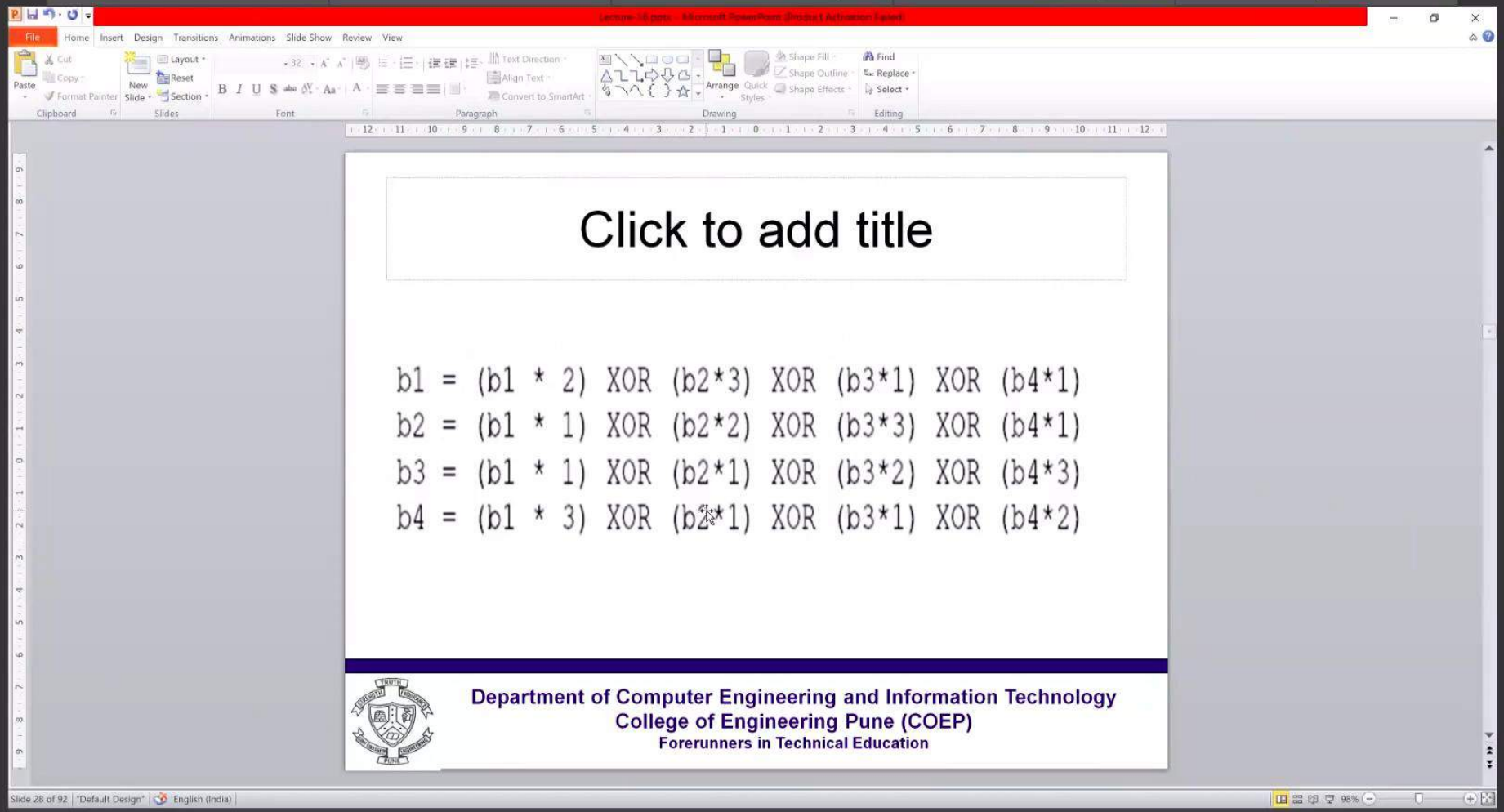
$$\begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix} \qquad \begin{bmatrix} b_1 & b_5 & b_9 & b_{13} \\ b_2 & b_6 & b_{10} & b_{14} \\ b_3 & b_7 & b_{11} & b_{15} \\ b_4 & b_8 & b_{12} & b_{16} \end{bmatrix}$$

Multiplication Matrix *State Matrix*

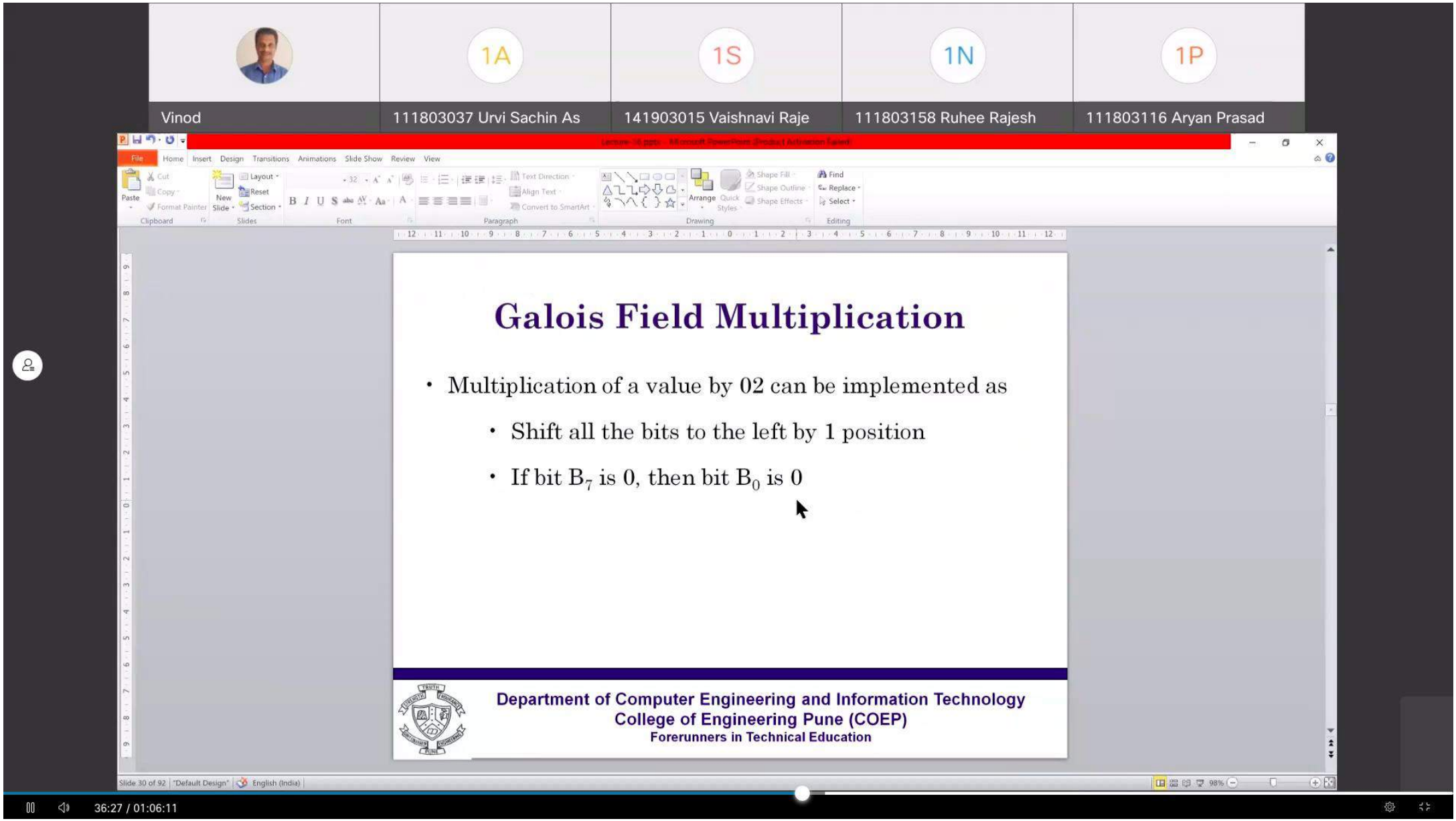
Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education

+116

	1A	1S	1N	1P
Vinod	111803037 Urvi Sachin As	141903015 Vaishnavi Raje	111803158 Ruhee Rajesh	111803116 Aryan Prasad



+116


1A
1S
1N
1P
Vinod
111803037 Urvi Sachin As
141903015 Vaishnavi Raje
111803158 Ruhee Rajesh
111803116 Aryan Prasad
Galois Field Multiplication
Multiplication of a value by 02 can be implemented as
Shift all the bits to the left by 1 position
If bit B_7 is 0, then bit B_0 is 0
Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education
36:27 / 01:06:11

Vinod | 111803037 Urvi Sachin As | 141903015 Vaishnavi Raje | 111803158 Ruhee Rajesh | 111803116 Aryan Prasad

Galois Field Multiplication

- Multiplication of a value by 02 can be implemented as
  a) Shift all the bits to the left by 1 position and make bit B_0 is 0
     - If bit B_7 is 0 (in the original number), then the output is step (a)
     - If bit B_7 is 1 (in the original number), then XOR the output of step (a) with 1B.

Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education

1A	1S	1N	1P
Vinod	111803037 Urvi Sachin As	141903015 Vaishnavi Raje	111803158 Ruhee Rajesh	111803116 Aryan Prasad

38:28 / 01:06:11

	1A	1S	1N	1P
Vinod	111803037 Urvi Sachin As	141903015 Vaishnavi Raje	111803158 Ruhee Rajesh	111803116 Aryan Prasad

For Ex: 02 * 87

Shift left by 1 bit position and $B_0 = 0$

0000 1110

40:07 / 01:06:11

1A	1S	1N	1P
Vinod	111803037 Urvi Sachin As	141903015 Vaishnavi Raje	111803158 Ruhee Rajesh	111803116 Aryan Prasad

03 . 6E can be written as

$6E \oplus \{02 * 6E\}$

Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education

+112

1A	1S	1N	1P
Vinod	111803037 Urvi Sachin As	141903015 Vaishnavi Raje	111803158 Ruhee Rajesh	111803116 Aryan Prasad

03 . 6E can be written as

$6E \oplus \{02 * 6E\}$

6E = 0110 1110

{02 * 6E} = 0110 1110

Shift left by 1 bit position and $B_0 = 0$

1101 1100

Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education

1A	1S	1N	1P
Vinod	111803037 Urvi Sachin As	141903015 Vaishnavi Raje	111803158 Ruhee Rajesh	111803116 Aryan Prasad

03 . 6E can be written as

6E ⊕ {02 * 6E} I

0110 1110 ⊕ 11011100

	0110	1110	(6E)
⊕	1101	1100	(02 * 6E)
	1011	0010	

03 . 6E = 1011 0010 [B2]

Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education

+113

1A	1S	1N	1P
Vinod	111803037 Urvi Sachin As	141903015 Vaishnavi Raje	111803158 Ruhee Rajesh	111803116 Aryan Prasad

4. Add Subkey (AddRoundKey)

- A portion of a key unique to this round is XOR with the round result.
- This operation provides confusion and incorporates the key

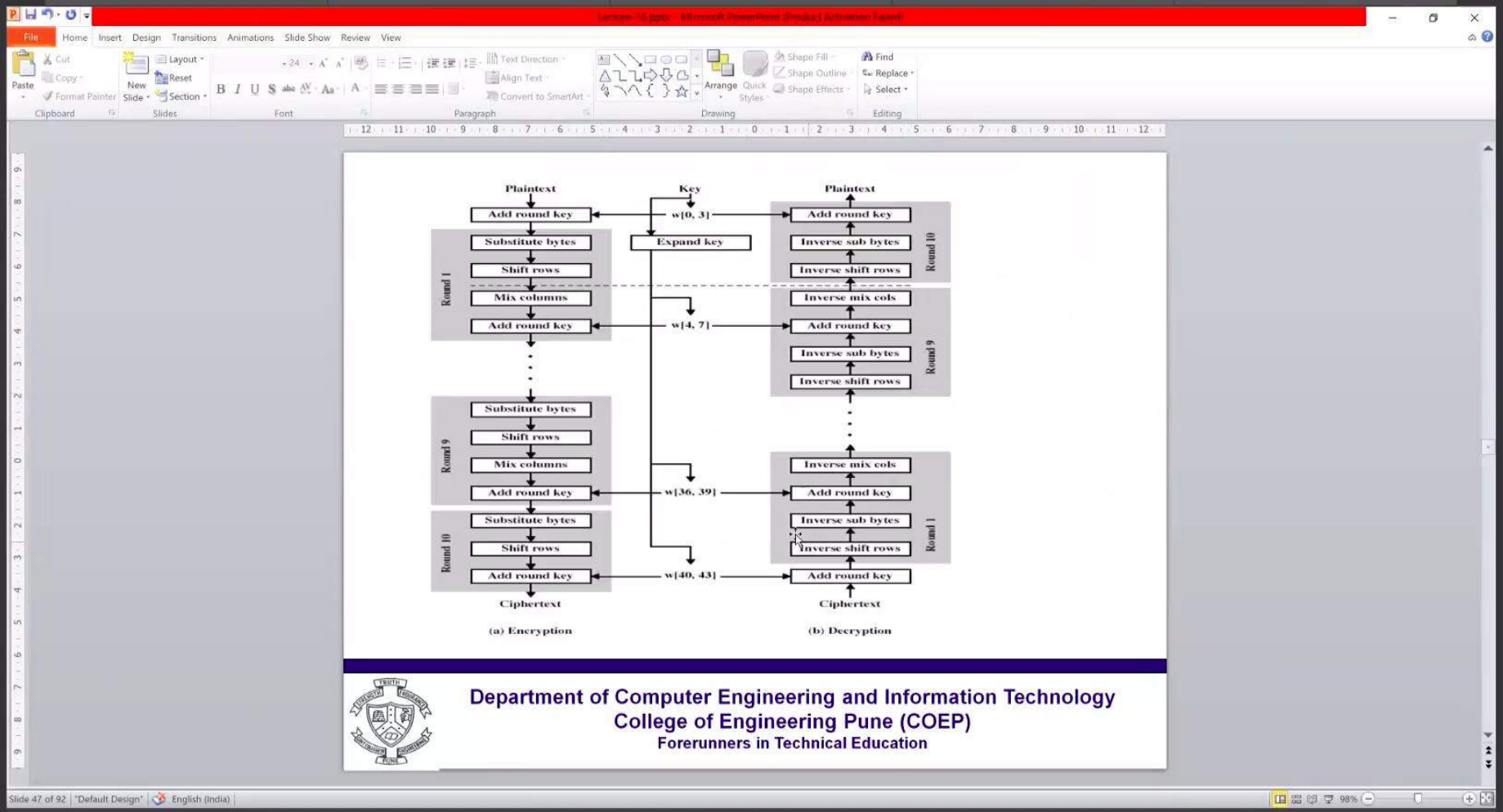
Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education

+113

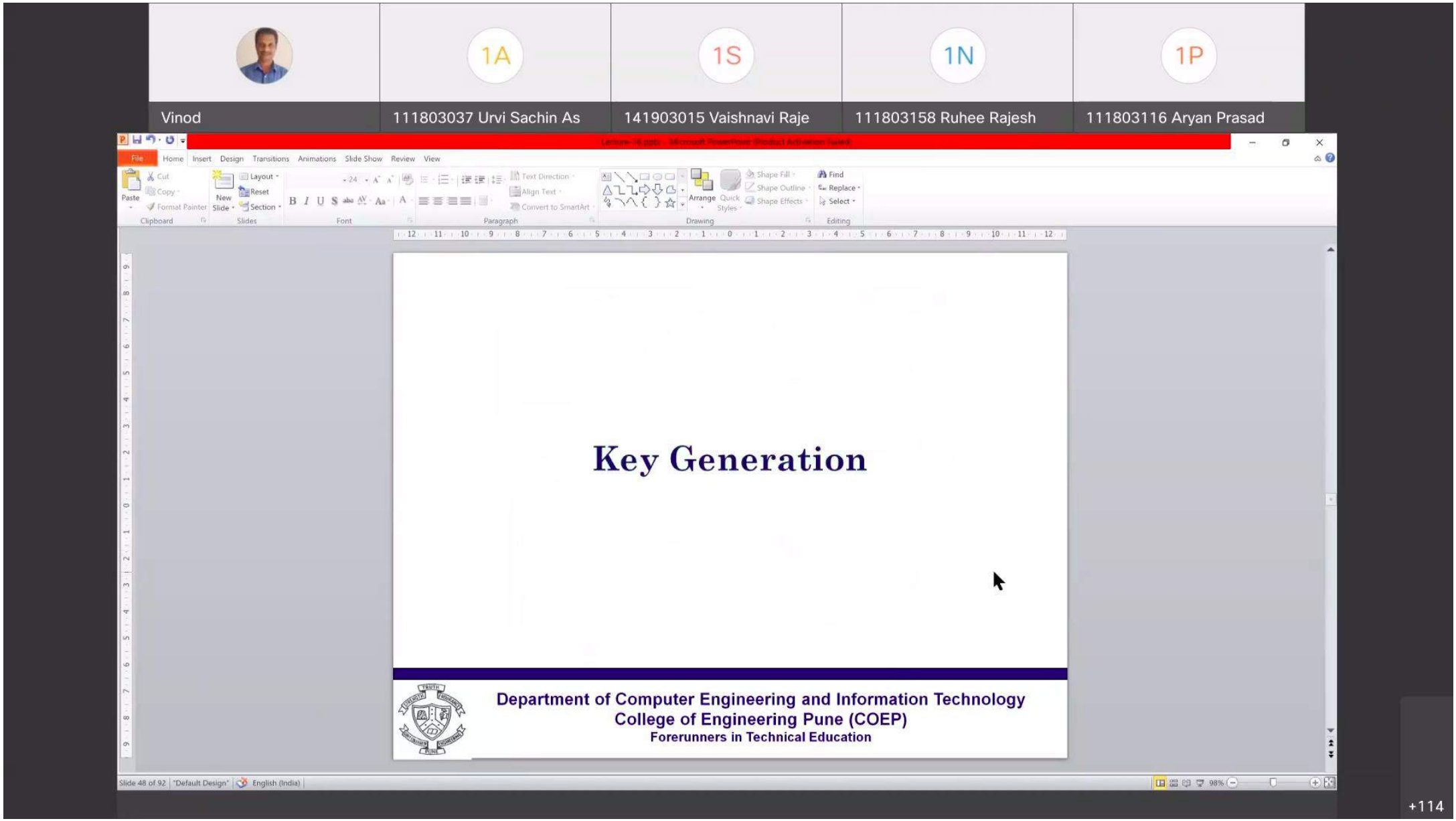
1A	1S	1N	1P
Vinod	111803037 Urvi Sachin As	141903015 Vaishnavi Raje	111803158 Ruhee Rajesh	111803116 Aryan Prasad

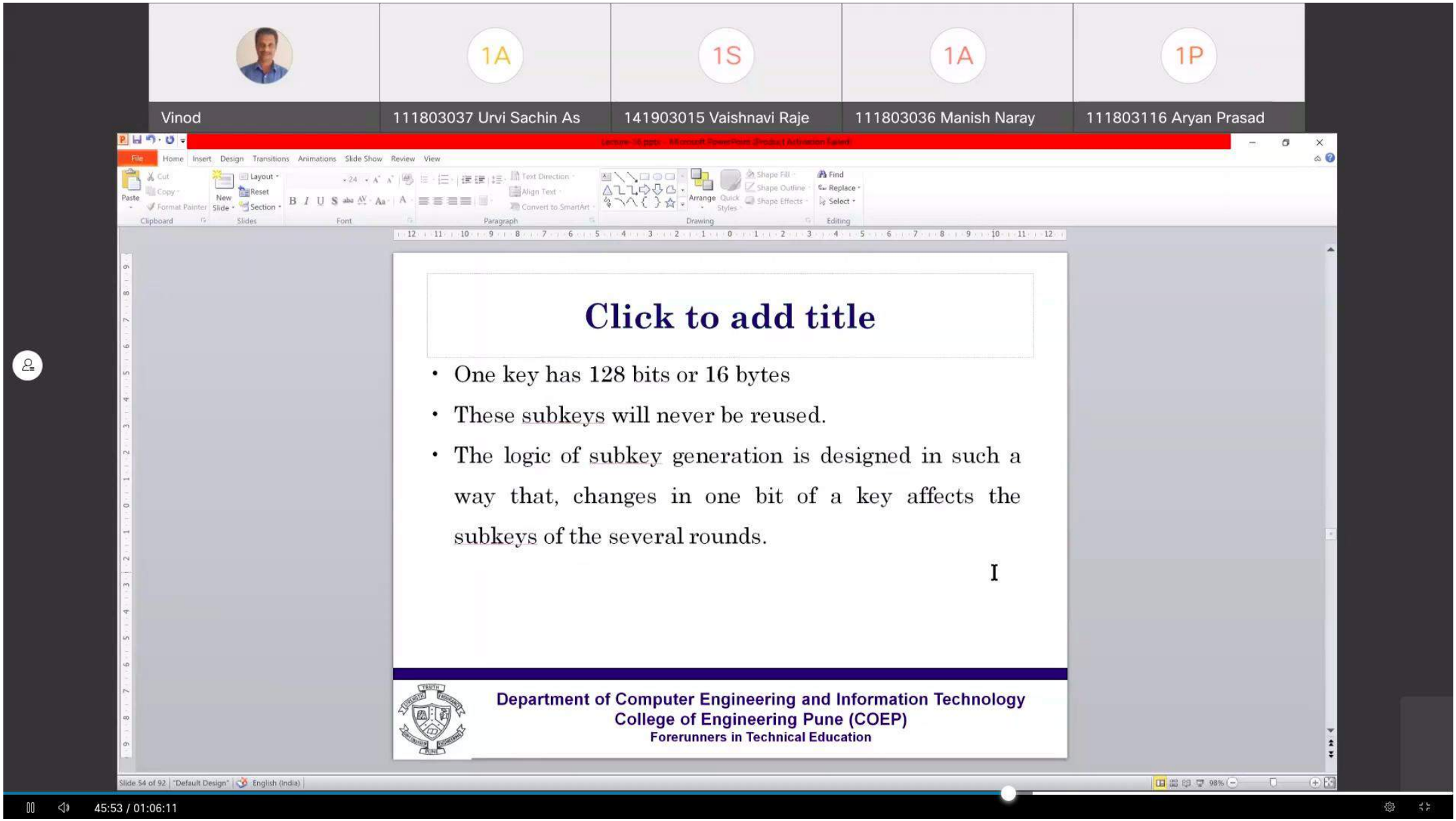
- An iteration of the above steps 1 to 4 is called a round.
- The amount of rounds of the algorithm depends on the key size.
- The only exception being that in the last round the Mix Column step is not performed, to make the algorithm reversible during decryption

	1A	1S	1N	1P
Vinod	111803037 Urvi Sachin As	141903015 Vaishnavi Raje	111803158 Ruhee Rajesh	111803116 Aryan Prasad



+113


Vinod
111803037 Urvi Sachin As
141903015 Vaishnavi Raje
111803158 Ruhee Rajesh
111803116 Aryan Prasad
1A
1S
1N
1P
File
Home
Insert
Design
Transitions
Animations
Slide Show
Review
View
Key Generation
Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education
Slide 48 of 92
"Default Design"
English (India)
+114


1A
1S
1A
1P
Vinod
111803037 Urvi Sachin As
141903015 Vaishnavi Raje
111803036 Manish Naray
111803116 Aryan Prasad
Click to add title
• One key has 128 bits or 16 bytes
• These subkeys will never be reused.
• The logic of subkey generation is designed in such a way that, changes in one bit of a key affects the subkeys of the several rounds.
Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education
45:53 / 01:06:11

1A	1S	1A	1P
Vinod	111803037 Urvi Sachin As	141903015 Vaishnavi Raje	111803036 Manish Naray	111803116 Aryan Prasad

Steps for subkeys generation

Step 1

- The key for AES is 128 bits or 16 bytes
- This 16 bytes are arranged in the form of 4 x 4 matrix.
- So, the first column of a matrix is filled by first 4 bytes
- The second column is filled by second 4 bytes
- The third column filled by third 4 bytes and
- The last column is filled by last 4 bytes of a key.

Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education

+115

1A	1S	1A	1P
Vinod	111803037 Urvi Sachin As	141903015 Vaishnavi Raje	111803036 Manish Naray	111803116 Aryan Prasad

$$\begin{bmatrix} b_0 & b_4 & b_8 & b_{12} \\ b_1 & b_5 & b_9 & b_{13} \\ b_2 & b_6 & b_{10} & b_{14} \\ b_3 & b_7 & b_{11} & b_{15} \end{bmatrix}$$

$$\begin{bmatrix} w_0 & w_1 & w_2 & w_3 \end{bmatrix}$$

Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education

+115

1A	1S	1A	1P
Vinod	111803037 Urvi Sachin As	141903015 Vaishnavi Raje	111803036 Manish Naray	111803116 Aryan Prasad

Each column stands as one word of key "w". Such as:

$w_0 = (b_0; b_1; b_2; b_3)$
$w_1 = (b_4; b_5; b_6; b_7)$
$w_2 = (b_8; b_9; b_{10}; b_{11})$
$w_3 = (b_{12}; b_{13}; b_{14}; b_{15})$

This is the key used for initial round.
Subkey for the next round is generated from this key.

Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education

+113

1A	1S	1A	1P
Vinod	111803037 Urvi Sachin As	141903015 Vaishnavi Raje	111803036 Manish Naray	111803116 Aryan Prasad

Step 2:

Calculate $g[w_3]$ using following steps.

a) Perform circular left shift of the bytes of w_3 (fourth word of a key).

b) Perform substitution of the bytes using S-box.

c) Add round constant

Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education

+114

1A	1S	1A	1P
Vinod	111803037 Urvi Sachin As	141903015 Vaishnavi Raje	111803036 Manish Naray	111803116 Aryan Prasad

Step 2:

Calculate $g[w_3]$ using following steps.

a) Perform circular left shift of the bytes of w_3 (fourth word of a key).

b) Perform substitution of the bytes using S-box.

c) Add round constant

Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education

+113

1A	1S	1A	1P
Vinod	111803037 Urvi Sachin As	141903015 Vaishnavi Raje	111803036 Manish Naray	111803116 Aryan Prasad

S-Box for Key Generation

	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
1	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
3	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
4	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
5	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
6	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
8	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
A	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
B	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
C	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
D	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
E	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
F	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education

+115

	1A	1S	1A	1P
Vinod	111803037 Urvi Sachin As	141903015 Vaishnavi Raje	111803036 Manish Naray	111803116 Aryan Prasad

Round Constant (RCon)

- RCon is a word in which the three rightmost bytes are zero
- It is different for each round and defined as:

  RCon[j] = (RCon[j],0,0,0)

  where RCon[1] =1 , RCon[j] = 2 * RCon[j-1]
- Multiplication is defined over GF(2^8) but can be implement in Lookup Table

Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education

confusion

+115

1A	1S	1A	1P
Vinod	111803037 Urvi Sachin As	141903015 Vaishnavi Raje	111803036 Manish Naray	111803116 Aryan Prasad

Round	Constant (RCon)	Round	Constant (RCon)
1	$(\underline{\mathbf{01}}\ 00\ 00\ 00)_{16}$	6	$(\underline{\mathbf{20}}\ 00\ 00\ 00)_{16}$
2	$(\underline{\mathbf{02}}\ 00\ 00\ 00)_{16}$	7	$(\underline{\mathbf{40}}\ 00\ 00\ 00)_{16}$
3	$(\underline{\mathbf{04}}\ 00\ 00\ 00)_{16}$	8	$(\underline{\mathbf{80}}\ 00\ 00\ 00)_{16}$
4	$(\underline{\mathbf{08}}\ 00\ 00\ 00)_{16}$	9	$(\underline{\mathbf{1B}}\ 00\ 00\ 00)_{16}$
5	$(\underline{\mathbf{10}}\ 00\ 00\ 00)_{16}$	10	$(\underline{\mathbf{36}}\ 00\ 00\ 00)_{16}$

Click to add title

Step 3

Generation of round key for first round.

$w_4 = w_0$ XOR $g(w_3)$

Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education

1A	1S	1A	1P
Vinod	111803037 Urvi Sachin As	141903015 Vaishnavi Raje	111803036 Manish Naray	111803116 Aryan Prasad

$w_4 = w_0$ XOR $g(w_3)$

$w_5 = w_1$ XOR w_4

$w_6 = w_2$ XOR w_5

$w_7 = w_3$ XOR w_6

Therefore, the round key for first round is $[w_4, w_5, w_6, w_7]$.

Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education

+114

1A	1S	1A	1P
Vinod	111803037 Urvi Sachin As	141903015 Vaishnavi Raje	111803036 Manish Naray	111803116 Aryan Prasad

Subkey 2

$w_0 = w_4$

$w_1 = w_5$

$w_2 = w_6$

$w_3 = w_7$

Repeat steps 1 to 3 above to generate the key for all the keys

Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education

1A	1S	1A	1P
Vinod	111803037 Urvi Sachin As	141903015 Vaishnavi Raje	111803036 Manish Naray	111803116 Aryan Prasad

AES Example

Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education

+113

1A	1S	1A	1P
Vinod	111803037 Urvi Sachin As	141903015 Vaishnavi Raje	111803036 Manish Naray	111803116 Aryan Prasad

Key in Hex (128 bits):

54 68 61 74 73 20 6D 79 20 4B 75 6E 67 20 46 75

Plaintext in Hex (128 bits):

54 77 6F 20 4F 6E 65 20 4E 69 6E 65 20 54 77 6F

Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education

+111

1A	1S	1A	1P
Vinod	111803037 Urvi Sachin As	141903015 Vaishnavi Raje	111803036 Manish Naray	111803116 Aryan Prasad

Key in Hex (128 bits):
0101 0100 0110 1000
54 68 61 74 73 20 6D 79 20 4B 75 6E 67 20 46 75

Plaintext in Hex (128 bits):

54 77 6F 20 4F 6E 65 20 4E 69 6E 65 20 54 77 6F

Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education

+109

1A	1S	1A	1P
Vinod	111803037 Urvi Sachin As	141903015 Vaishnavi Raje	111803036 Manish Naray	111803116 Aryan Prasad

Click to add title

$$\begin{bmatrix} 54 & 73 & 20 & 67 \\ 68 & 20 & 4B & 20 \\ 61 & 6D & 75 & 46 \\ 74 & 79 & 6E & 75 \end{bmatrix}$$

$$\begin{bmatrix} w_0 & w_1 & w_2 & w_3 \end{bmatrix}$$

Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education

Slide 74 of 92 | "Default Design" | English (India)

56:15 / 01:06:11

	1A	1S	1A	1P
Vinod	111803037 Urvi Sachin As	141903015 Vaishnavi Raje	111803036 Manish Naray	111803116 Aryan Prasad

Roundkey Generation

Key in Hex (128 bits):

54 68 61 74 73 20 6D 79 20 4B 75 6E 67 20 46 75

$w_0 = (54; 68; 61; 74);$

$w_1 = (73; 20; 6D; 79);$

$w_2 = (20; 4B; 75; 6E);$

$w_3 = (67; 20; 46; 75)$

Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education

+109

Vinod	111803037 Urvi Sachin As	141903015 Vaishnavi Raje	111803036 Manish Naray	111803116 Aryan Prasad
	1A		1A	1P

w[3] = (67; 20; 46; 75)

$g(w_3)$:

circular byte left shift of w_3:

(20; 46; 75; 67)

Byte Substitution (S-Box):

(B7; 5A; 9D; 85)

Adding round constant

(01; 00; 00; 00) gives:

$g(w_3)$ = (B6; 5A; 9D; 85)

0111

0001 0110

0110

	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
1	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
3	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
4	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
5	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
6	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
8	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
A	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
B	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
C	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
D	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
E	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
F	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education

S-Box

w_0

$\oplus$ $g(w_3)$

w_4

0101 0100	0110 1000	0110 0001	0111 0100
1011 0110	0101 1010	1001 1101	1000 0101
1110 0010	0011 0010	1111 1100	1111 0001
E2	32	FC	F1

$w_4 = w_0 \oplus g(w_3) = (E2; 32; FC; F1)$

$w_5 = w_1 \oplus w_4 = (91; 12; 91; 88)$

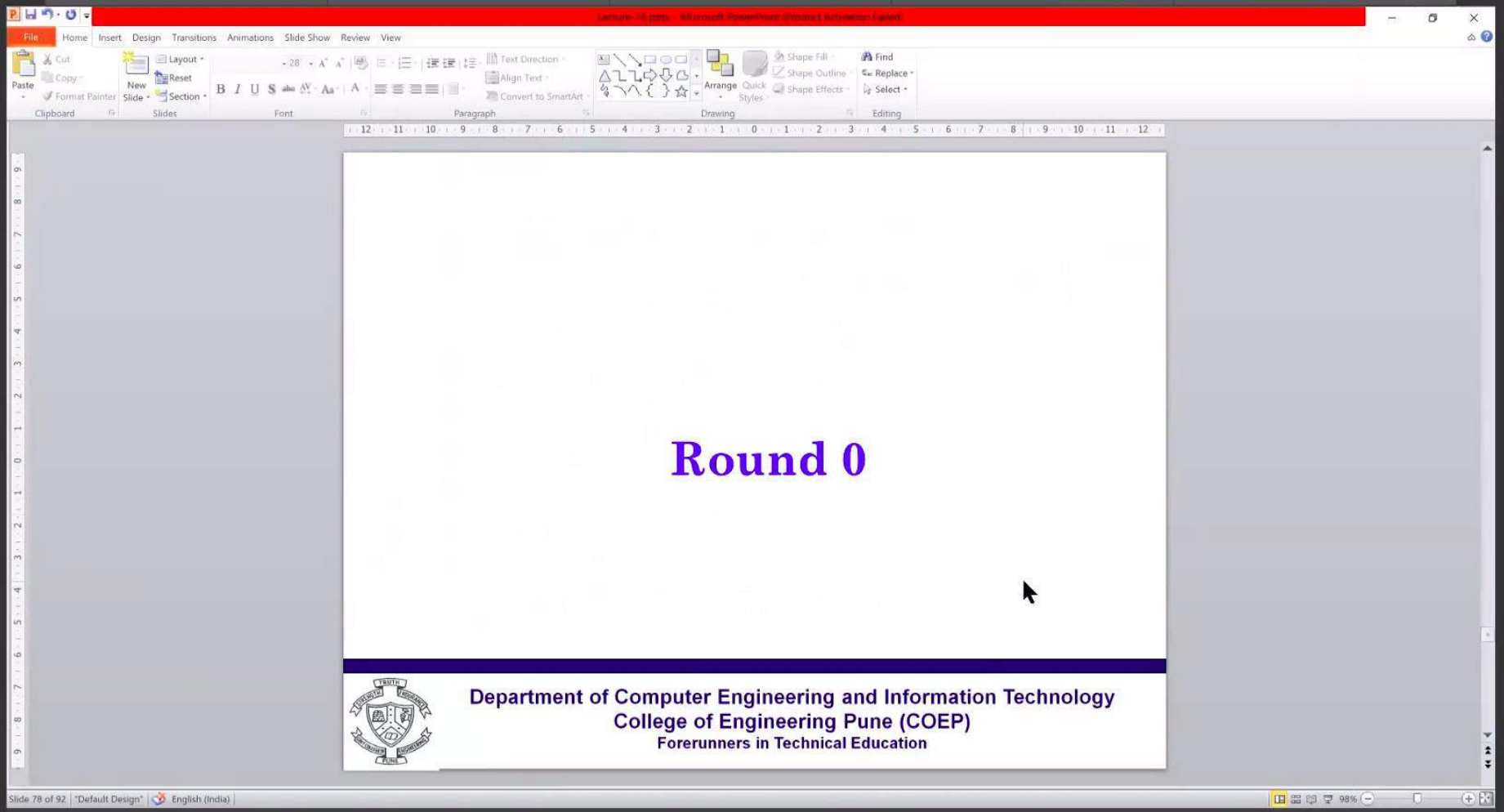
$w_6 = w_2 \oplus w_5 = (B1; 59; E4; E6)$

$w_7 = w_3 \oplus w_6 = (D6; 79; A2; 93)$

First roundkey:

E2 32 FC F1 91 12 91 88 B1 59 E4 E6 D6 79 A2 93

	1A	1S	1A	1P
Vinod	111803037 Urvi Sachin As	141903015 Vaishnavi Raje	111803036 Manish Naray	111803116 Aryan Prasad



+109

1A	1S	1A	1P
Vinod	111803037 Urvi Sachin As	141903015 Vaishnavi Raje	111803036 Manish Naray	111803116 Aryan Prasad

State Matrix and Roundkey 0 Matrix

$$\begin{bmatrix} 54 & 4F & 4E & 20 \\ 77 & 6E & 69 & 54 \\ 6F & 65 & 6E & 77 \\ 20 & 20 & 65 & 6F \end{bmatrix} \oplus \begin{bmatrix} 54 & 73 & 20 & 67 \\ 68 & 20 & 4B & 20 \\ 61 & 6D & 75 & 46 \\ 74 & 79 & 6E & 75 \end{bmatrix} = \begin{bmatrix} 00 & 3C & 6E & 47 \\ 1F & 4E & 22 & 74 \\ 0E & 08 & 1B & 31 \\ 54 & 59 & 0B & 1A \end{bmatrix}$$

State Matrix(Plaintext) *Key*

$$69 \quad 0110 \quad 1001$$

$$\oplus \quad 4B \quad \underline{0100} \quad \underline{1011}$$

$$0010 \quad 0010 = 22$$

Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education

1A	1S	1A	1P
Vinod	111803037 Urvi Sachin As	141903015 Vaishnavi Raje	111803036 Manish Naray	111803116 Aryan Prasad

Round 1

Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education

+106

	1A	1S	1A	1P
Vinod	111803037 Urvi Sachin As	141903015 Vaishnavi Raje	111803036 Manish Naray	111803116 Aryan Prasad

1. Byte substitution (SubBytes)

- Substitute each entry of current state matrix by corresponding entry in AES S-Box
- byte 3C is substituted by entry of S-Box in row 3 and column C, i.e. by EB

Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education

+106

	1A	1S	1A	1P
Vinod	111803037 Urvi Sachin As	141903015 Vaishnavi Raje	111803036 Manish Naray	111803116 Aryan Prasad

	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
1	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
3	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
4	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
5	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
6	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
8	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
A	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
B	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
C	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
D	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
E	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
F	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

2. Shift Rows

$$\begin{bmatrix} 63 & EB & 9F & A0 \\ C0 & 2F & 93 & 92 \\ AB & 30 & AF & C7 \\ 20 & CB & 2B & A2 \end{bmatrix} \rightarrow \begin{bmatrix} 63 & EB & 9F & A0 \\ 2F & 93 & 92 & C0 \\ AF & C7 & AB & 30 \\ A2 & 20 & CB & 2B \end{bmatrix}$$

1A	1S	1A	1P
Vinod	111803037 Urvi Sachin As	141903015 Vaishnavi Raje	111803036 Manish Naray	111803116 Aryan Prasad

3. Mix Column

$$\begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix} \begin{bmatrix} 63 & EB & 9F & A0 \\ 2F & 93 & 92 & C0 \\ AF & C7 & AB & 30 \\ A2 & 20 & CB & 2B \end{bmatrix} = \begin{bmatrix} BA & 84 & E8 & 1B \\ 75 & A4 & 8D & 40 \\ F4 & 8D & 06 & 7D \\ 7A & 32 & 0E & 5D \end{bmatrix}$$

$$(02 \bullet 63) \oplus (03 \bullet 2F) \oplus (01 \bullet AF) \oplus (01 \bullet A2)$$

$$= \quad \text{BA}$$

Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education

	1A	1S	1A	1P
Vinod	111803037 Urvi Sachin As	141903015 Vaishnavi Raje	111803036 Manish Naray	111803116 Aryan Prasad

$$(02 \bullet 63) \oplus (03 \bullet 2F) \oplus (01 \bullet AF) \oplus (01 \bullet A2)$$

2 x 63

63 => 0110 0011

Shift left-> 1100 0110

3 x 2F = 2F XOR (2 x 2F)

2 x 2F = 0010 1111

Shift Left => 0101 1110

XOR 2F => 0010 1111

---

3 x 2F 0 111 0001

Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education

4. Add Subkey (AddRoundKey)

State Matrix and Roundkey No. 1 Matrix

$$\begin{bmatrix} BA & 84 & E8 & 1B \\ 75 & A4 & 8D & 40 \\ F4 & 8D & 06 & 7D \\ 7A & 32 & 0E & 5D \end{bmatrix} \oplus \begin{bmatrix} E2 & 91 & B1 & D6 \\ 32 & 12 & 59 & 79 \\ FC & 91 & E4 & A2 \\ F1 & 88 & E6 & 93 \end{bmatrix} = \begin{bmatrix} 58 & 15 & 59 & CD \\ 47 & B6 & D4 & 39 \\ 08 & 1C & E2 & DF \\ 8B & BA & E8 & CE \end{bmatrix}$$

Output after round 1

58 47 08 8B 15 B6 1C BA 59 D4 E2 E8 CD 39 DF CE

1A	1S	1A	1P
Vinod	111803037 Urvi Sachin As	141903015 Vaishnavi Raje	111803036 Manish Naray	111803116 Aryan Prasad

Comparison of AES with DES

	AES	DES
Block size (in bits)	128	64
Key size (in bits)	128, 192, 256	56
Speed	High	Low
Encryption primitives	Substitution, shift, bit mixing	Substitution, permutation
Cryptographic primitives	Confusion, Diffusion	Confusion, Diffusion

1A	1S	1A	1P
Vinod	111803037 Urvi Sachin As	141903015 Vaishnavi Raje	111803036 Manish Naray	111803116 Aryan Prasad

Confusion

- Confusion seeks to make the relationship between the statistics of the ciphertext and the value of the encryption key as complex as possible

Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education

+101

1D		1P	1P	1K
111803111 Atharva Kailas	Vinod	111803155 VIREN RAJES	111803161 Rohan Pravin	111803059 Sakshi Kaleka

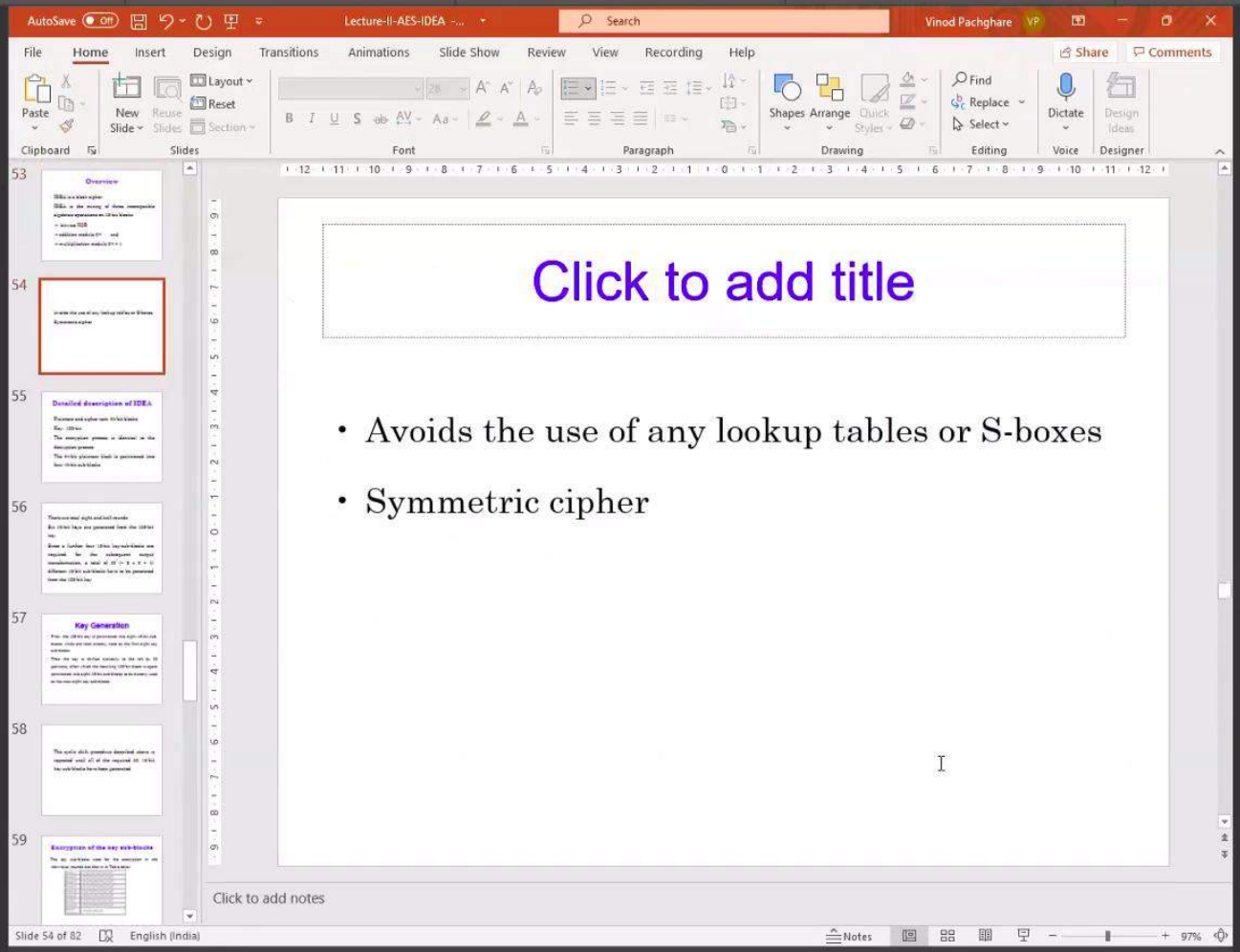
Overview

- IDEA is a block cipher
- IDEA is the mixing of three incompatible algebraic operations on 16-bit blocks:
  - bitwise XOR
  - addition modulo 2^{16} and
  - multiplication modulo $2^{16} + 1$

Click to add notes

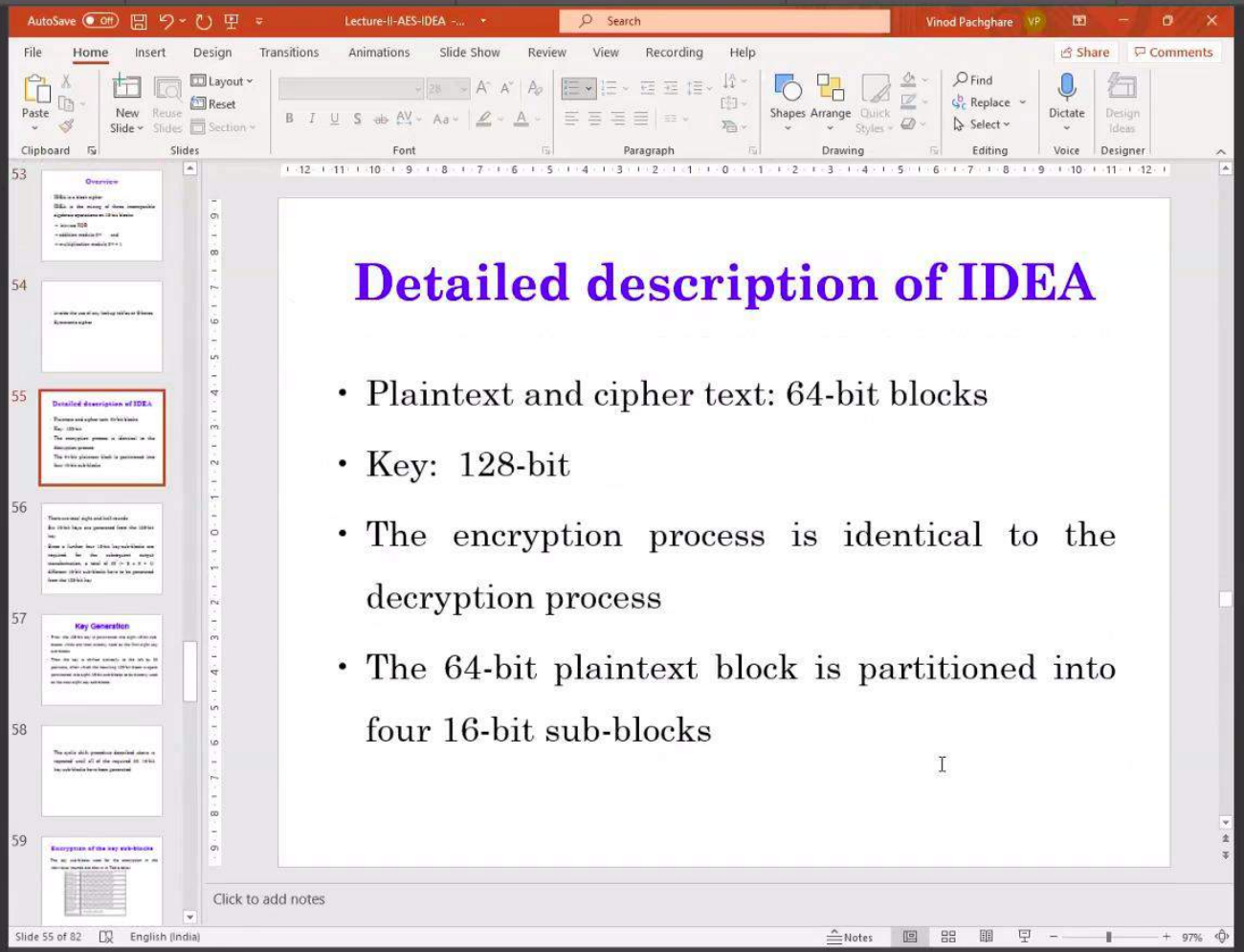
Slide 53 of 82 English (United States)

1D		1P	1P	1K
111803111 Atharva Kailas	Vinod	111803155 VIREN RAJES	111803161 Rohan Pravin	111803059 Sakshi Kaleka

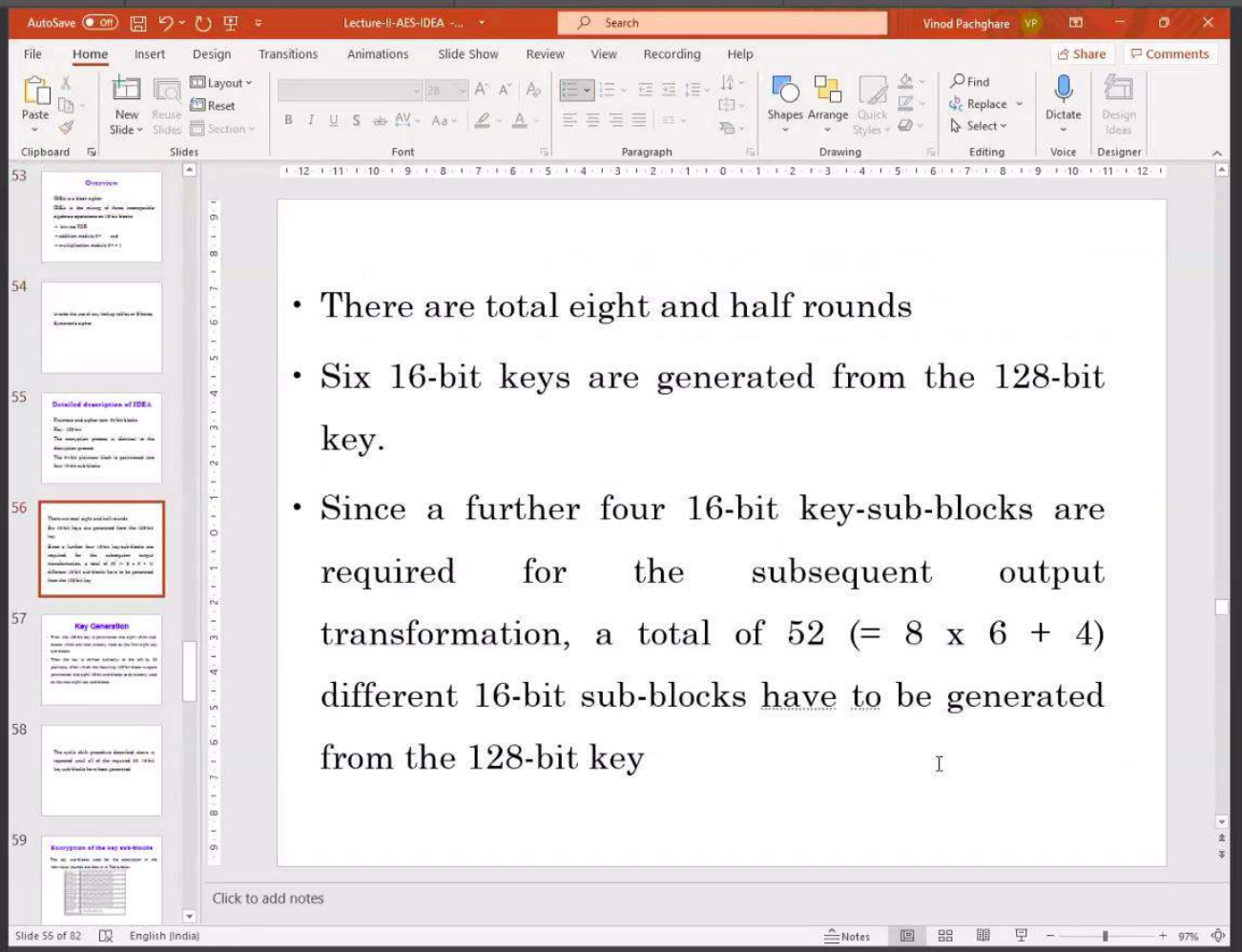


+116

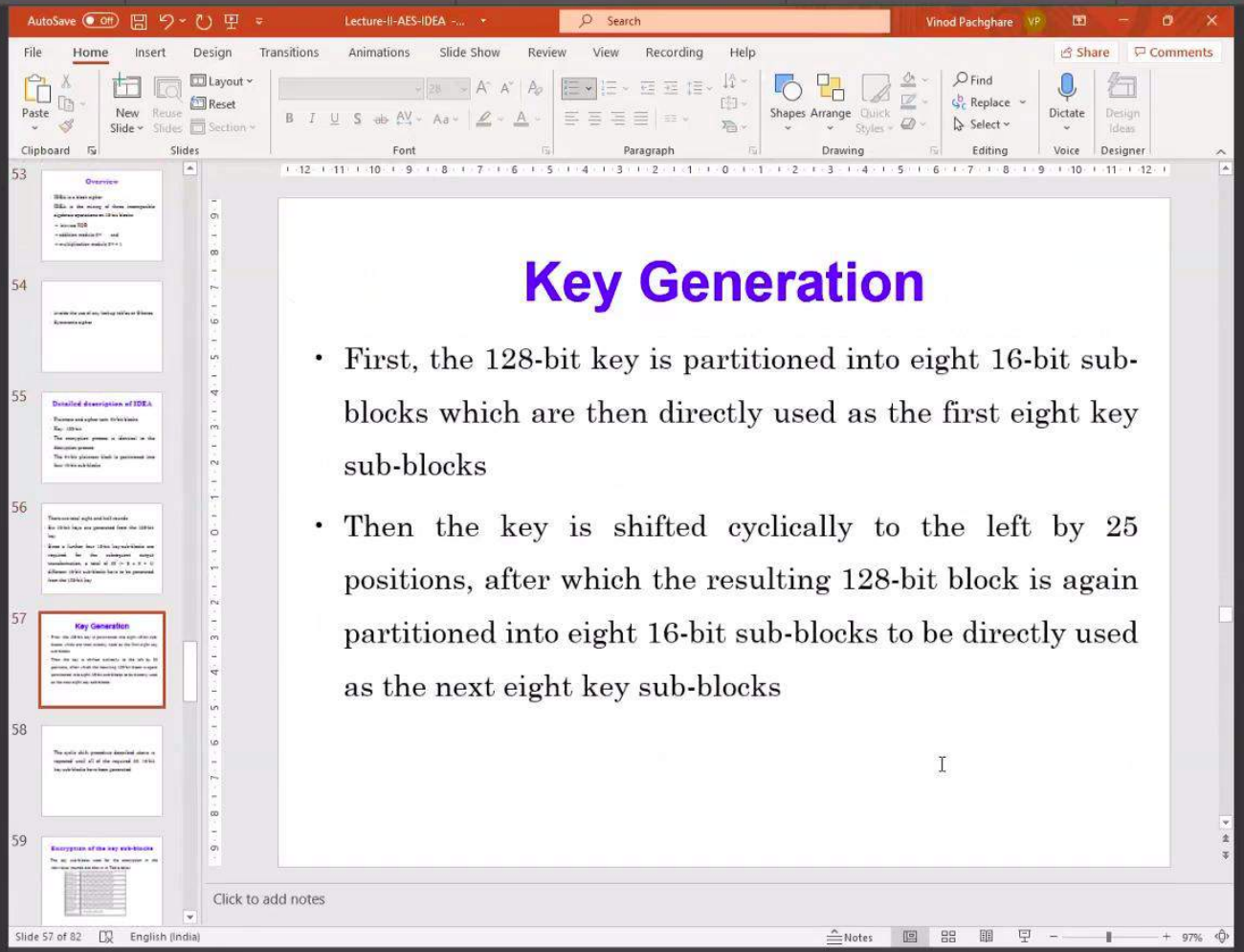
1D		1P	1P	1K
111803111 Atharva Kailas	Vinod	111803155 VIREN RAJES	111803161 Rohan Pravin	111803059 Sakshi Kaleka



+116

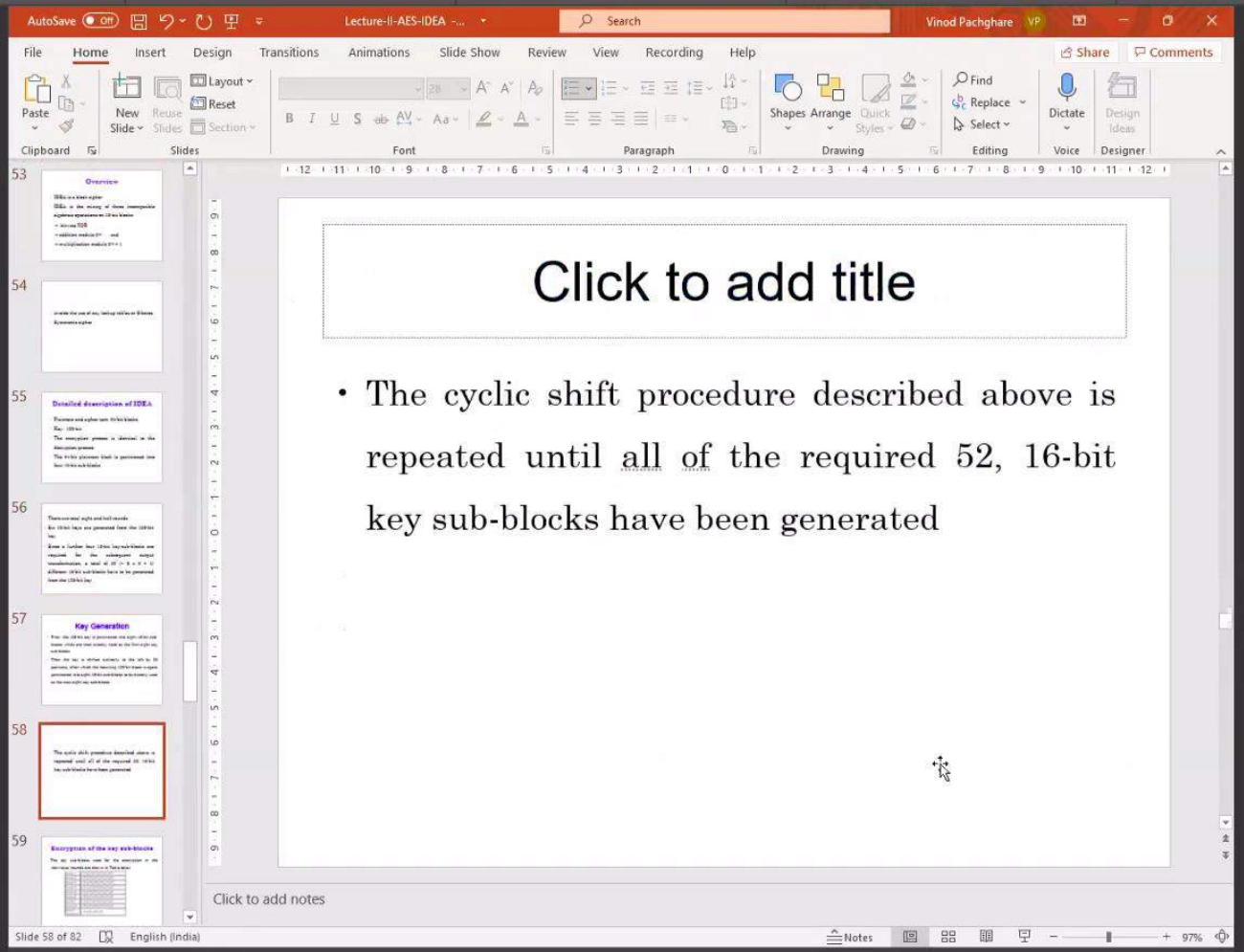


1D		1P	1P	1K
111803111 Atharva Kailas	Vinod	111803155 VIREN RAJES	111803161 Rohan Pravin	111803059 Sakshi Kaleka



+116

1D		1P	1P	1K
111803111 Atharva Kailas	Vinod	111803155 VIREN RAJES	111803161 Rohan Pravin	111803059 Sakshi Kaleka



+116

1D		1P	1P	1K
111803111 Atharva Kailas	Vinod	111803155 VIREN RAJES	111803161 Rohan Pravin	111803059 Sakshi Kaleka

+116

1D		1P	1P	1K
111803111 Atharva Kailas	Vinod	111803155 VIREN RAJES	111803161 Rohan Pravin	111803059 Sakshi Kaleka

AutoSave Lecture-II-AES-IDEA -... Search Vinod Pachghare

File Home Insert Design Transitions Animations Slide Show Review View Recording Help Share Comments

Paste New Slide Layout Reset Section Clipboard Slides Font Paragraph Shapes Arrange Quick Styles Find Replace Select Dictate Design Ideas Voice Designer Drawing Editing

55 56 57 58 59 60 61

Encryption

- The first four 16-bit key sub-blocks are combined with two of the 16-bit plaintext blocks using addition modulo 2^{16}, and with the other two plaintext blocks using multiplication modulo $2^{16} + 1$
- At the end of the first encryption round four 16-bit values are produced which are used as input to the second encryption round
- The process is repeated in each of the subsequent 7 encryption rounds
- The four 16-bit values produced at the end of the 8th encryption round are combined with the last four of the 52 key sub-blocks using addition modulo 2^{16} and multiplication modulo $2^{16} + 1$ to form the resulting four 16-bit ciphertext blocks

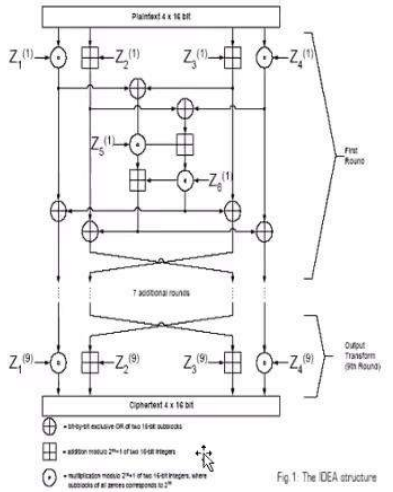


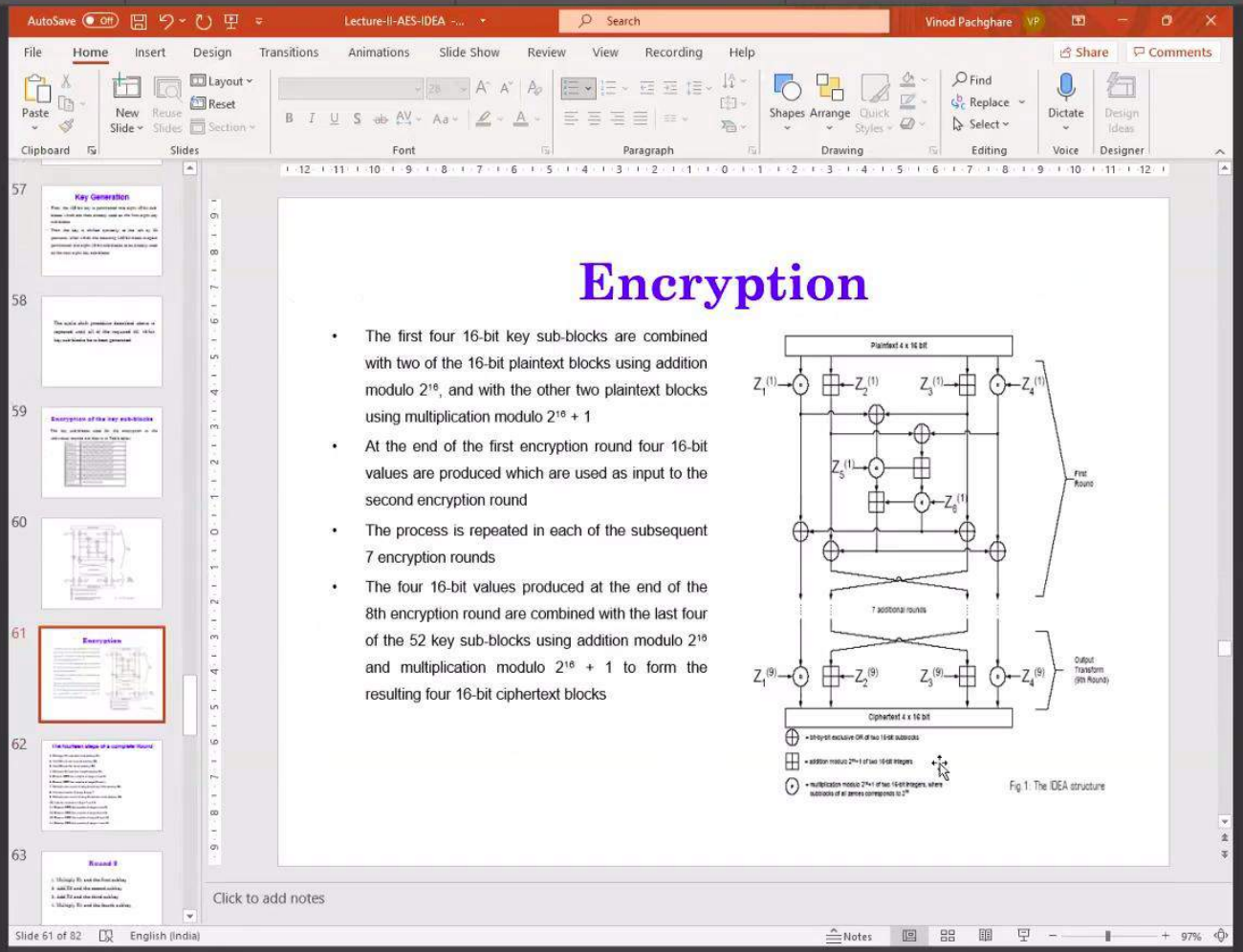
Fig.1 The IDEA structure

Click to add notes

Slide 61 of 82 English (India) Notes 97%

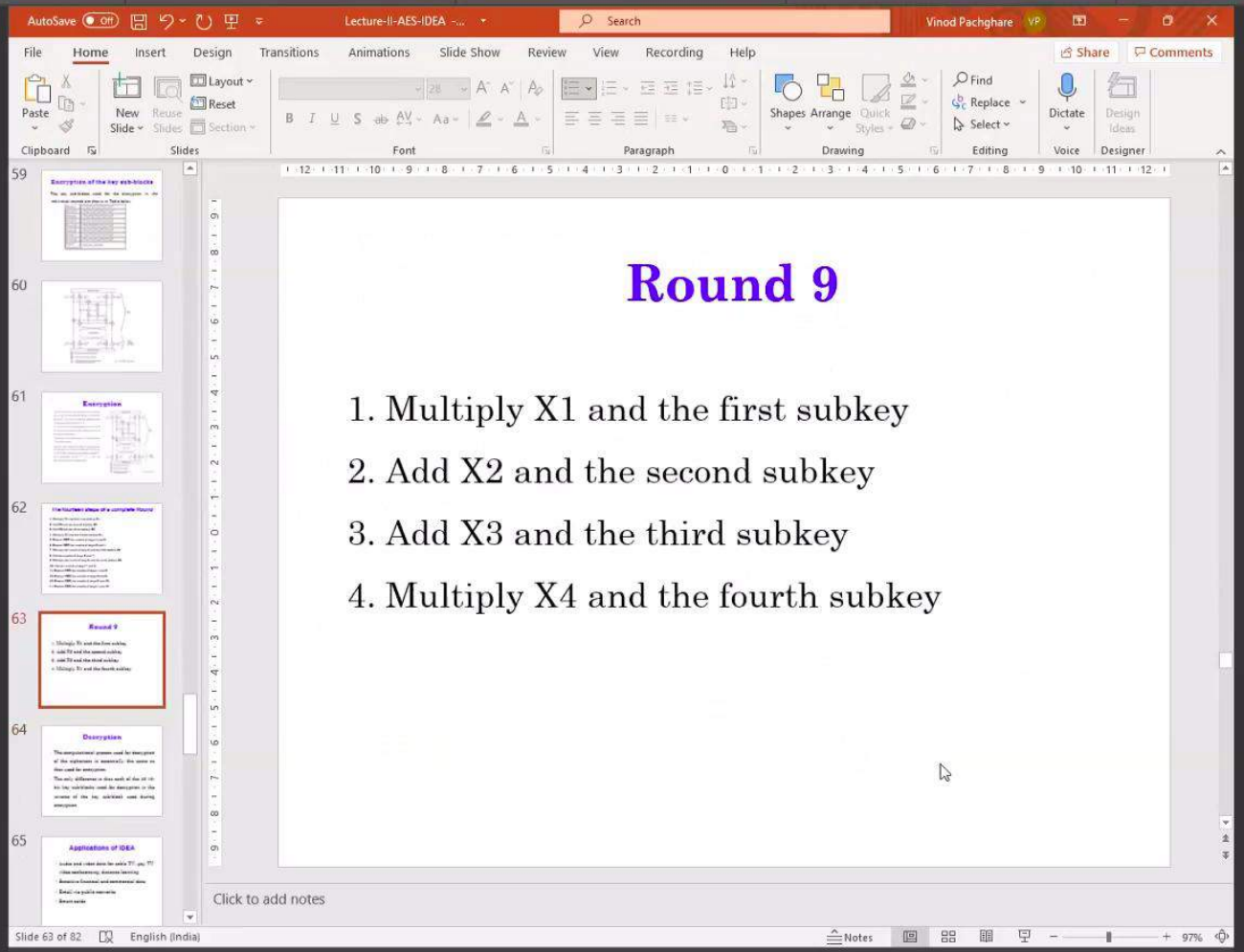
+116

1D		1P	1P	1K
111803111 Atharva Kailas	Vinod	111803155 VIREN RAJES	111803161 Rohan Pravin	111803059 Sakshi Kaleka

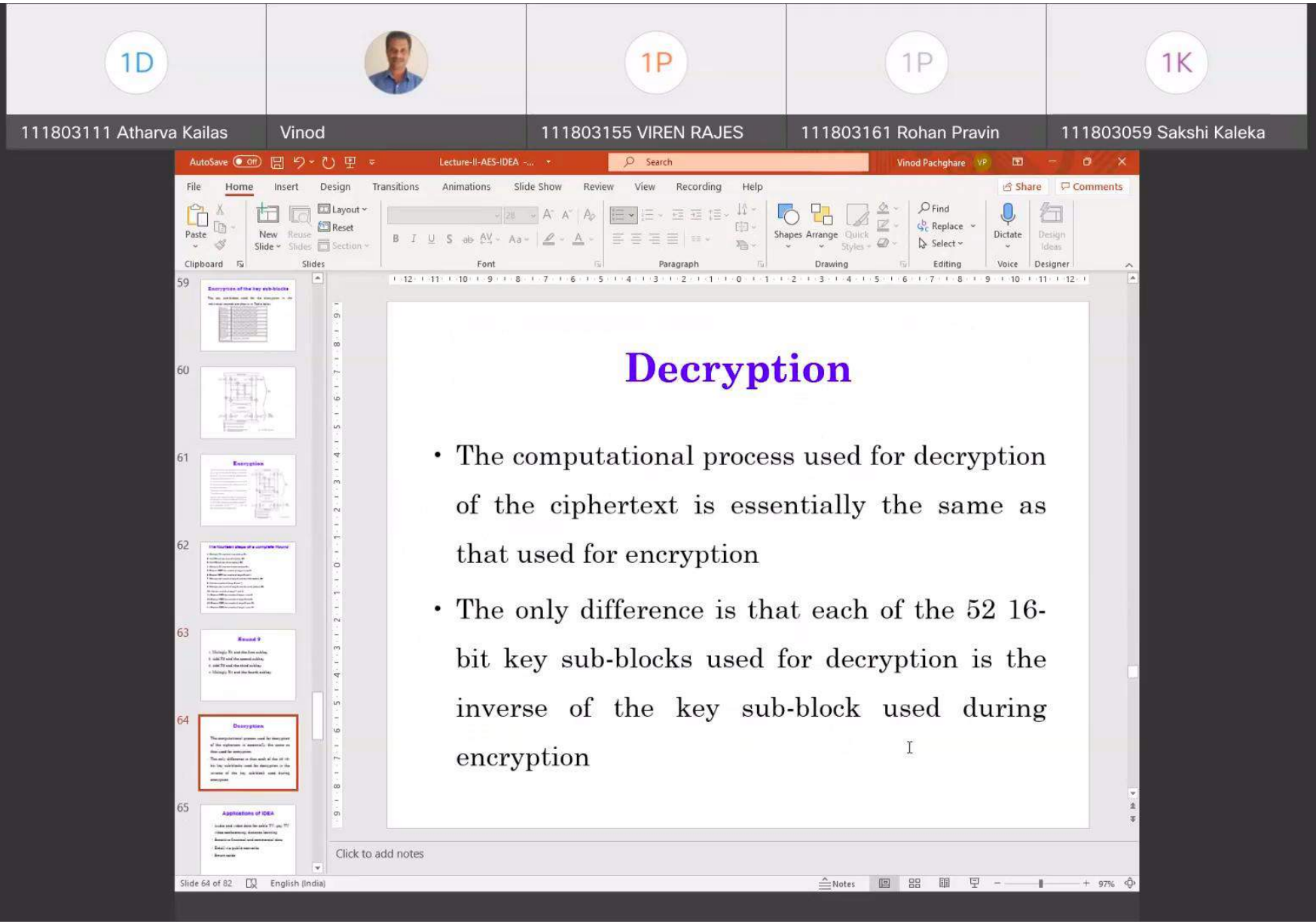


+116

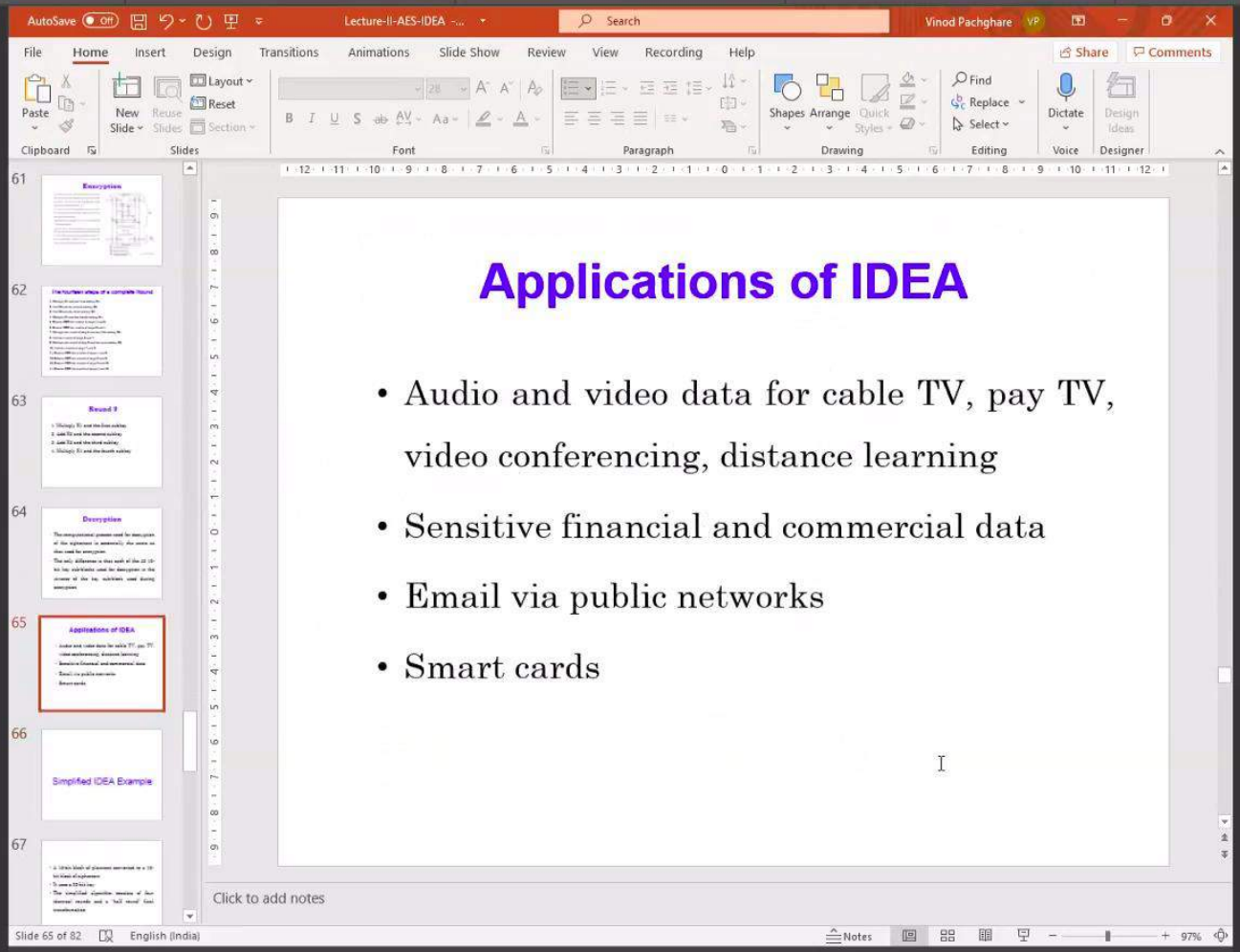
1D		1P	1P	1K
111803111 Atharva Kailas	Vinod	111803155 VIREN RAJES	111803161 Rohan Pravin	111803059 Sakshi Kaleka



+116

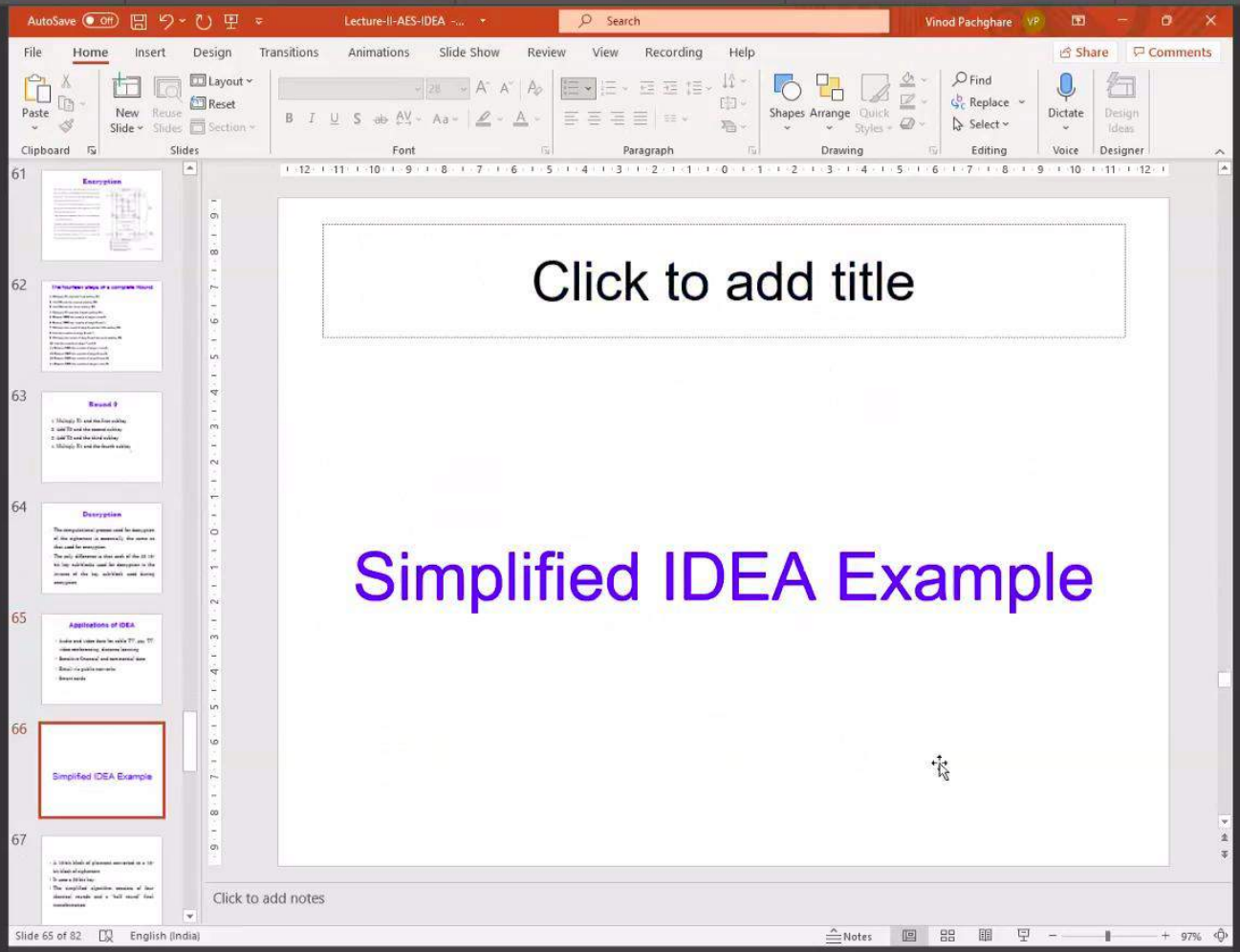

1D
111803111 Atharva Kailas
Vinod
1P
111803155 VIREN RAJES
1P
111803161 Rohan Pravin
1K
111803059 Sakshi Kaleka
Lecture-II-AES-IDEA -...
Search
Vinod Pachghare
File Home Insert Design Transitions Animations Slide Show Review View Recording Help
Share Comments
Clipboard Slides Font Paragraph Drawing Editing Voice Designer
Decryption
• The computational process used for decryption of the ciphertext is essentially the same as that used for encryption
• The only difference is that each of the 52 16-bit key sub-blocks used for decryption is the inverse of the key sub-block used during encryption
Click to add notes
Slide 64 of 82
English (India)
Notes
97%
+116

1D		1P	1P	1K
111803111 Atharva Kailas	Vinod	111803155 VIREN RAJES	111803161 Rohan Pravin	111803059 Sakshi Kaleka



+116

1D		1P	1P	1K
111803111 Atharva Kailas	Vinod	111803155 VIREN RAJES	111803161 Rohan Pravin	111803059 Sakshi Kaleka



+116

1D		1P	1P	1K
111803111 Atharva Kailas	Vinod	111803155 VIREN RAJES	111803161 Rohan Pravin	111803059 Sakshi Kaleka

AutoSave Off | Lecture-II-AES-IDEA -... | Search | Vinod Pachghare VP

File Home Insert Design Transitions Animations Slide Show Review View Recording Help | Share | Comments

Paste | New Slide | Layout | Reset | Section | Clipboard | Slides | Font | Paragraph | Shapes | Arrange | Quick Styles | Find | Replace | Select | Editing | Dictate | Voice | Design Ideas | Designer

63 Round 3

64 Decryption

65 Applications of IDEA

66 Simplified IDEA Example

67

68

69

Click to add title

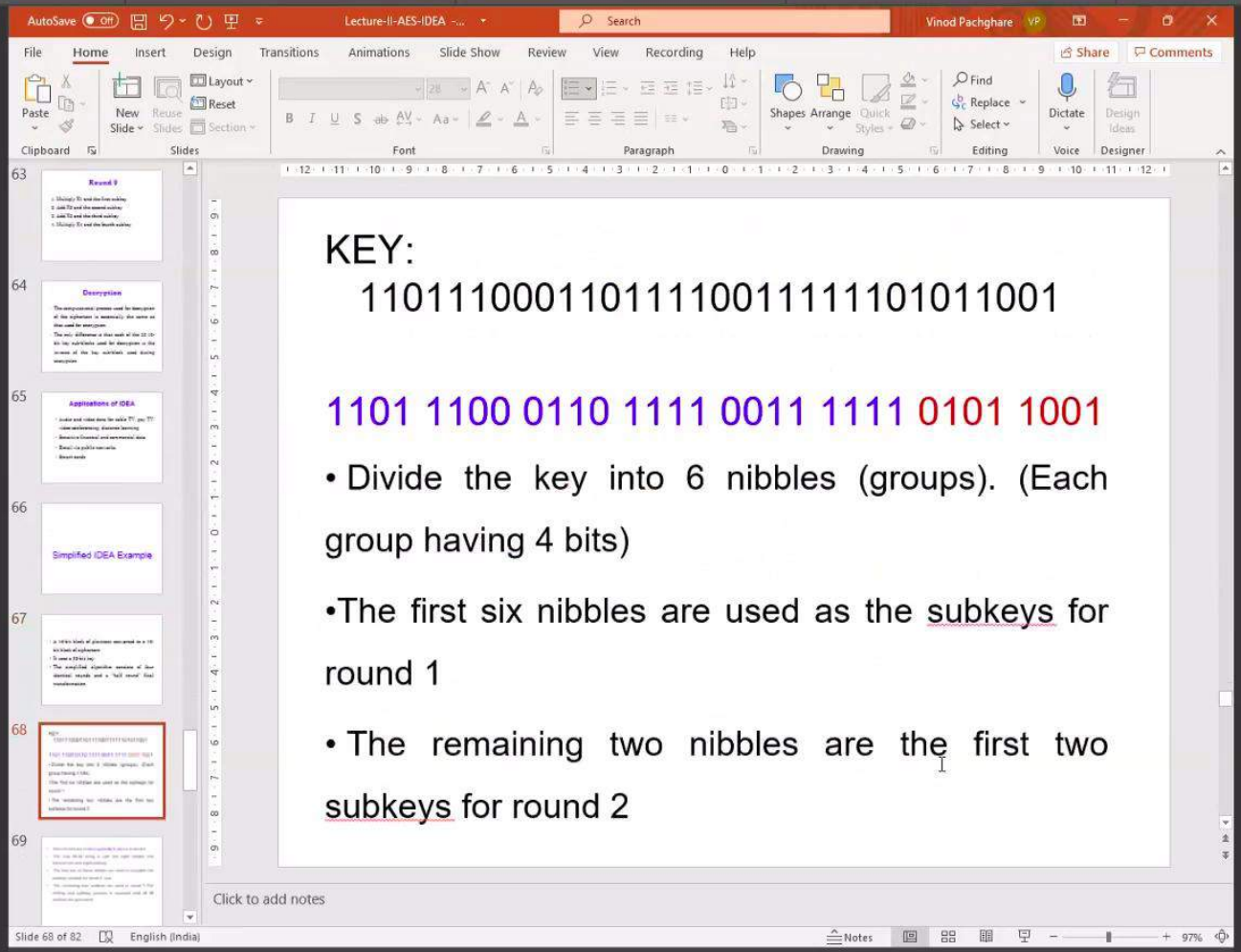
- A 16-bit block of plaintext converted to a 16-bit block of ciphertext
- It uses a 32-bit key
- The simplified algorithm consists of four identical rounds and a "half round" final transformation

Click to add notes

Slide 67 of 82 | English (India) | Notes | 97%

+116

1D		1P	1P	1K
111803111 Atharva Kailas	Vinod	111803155 VIREN RAJES	111803161 Rohan Pravin	111803059 Sakshi Kaleka



+116

1D		1P	1P	1K
111803111 Atharva Kailas	Vinod	111803155 VIREN RAJES	111803161 Rohan Pravin	111803059 Sakshi Kaleka

AutoSave Off | Lecture-II-AES-IDEA -... | Search | Vinod Pachghare VP

File Home Insert Design Transitions Animations Slide Show Review View Recording Help | Share | Comments

Paste | New Slide | Layout | Reset | Section | Clipboard | Slides | Font | Paragraph | Shapes | Arrange | Quick Styles | Find | Replace | Select | Editing | Dictate | Voice | Design Ideas | Designer

65 Applications of IDEA

66 Simplified IDEA Example

67

68

69

70

71 Key Generation

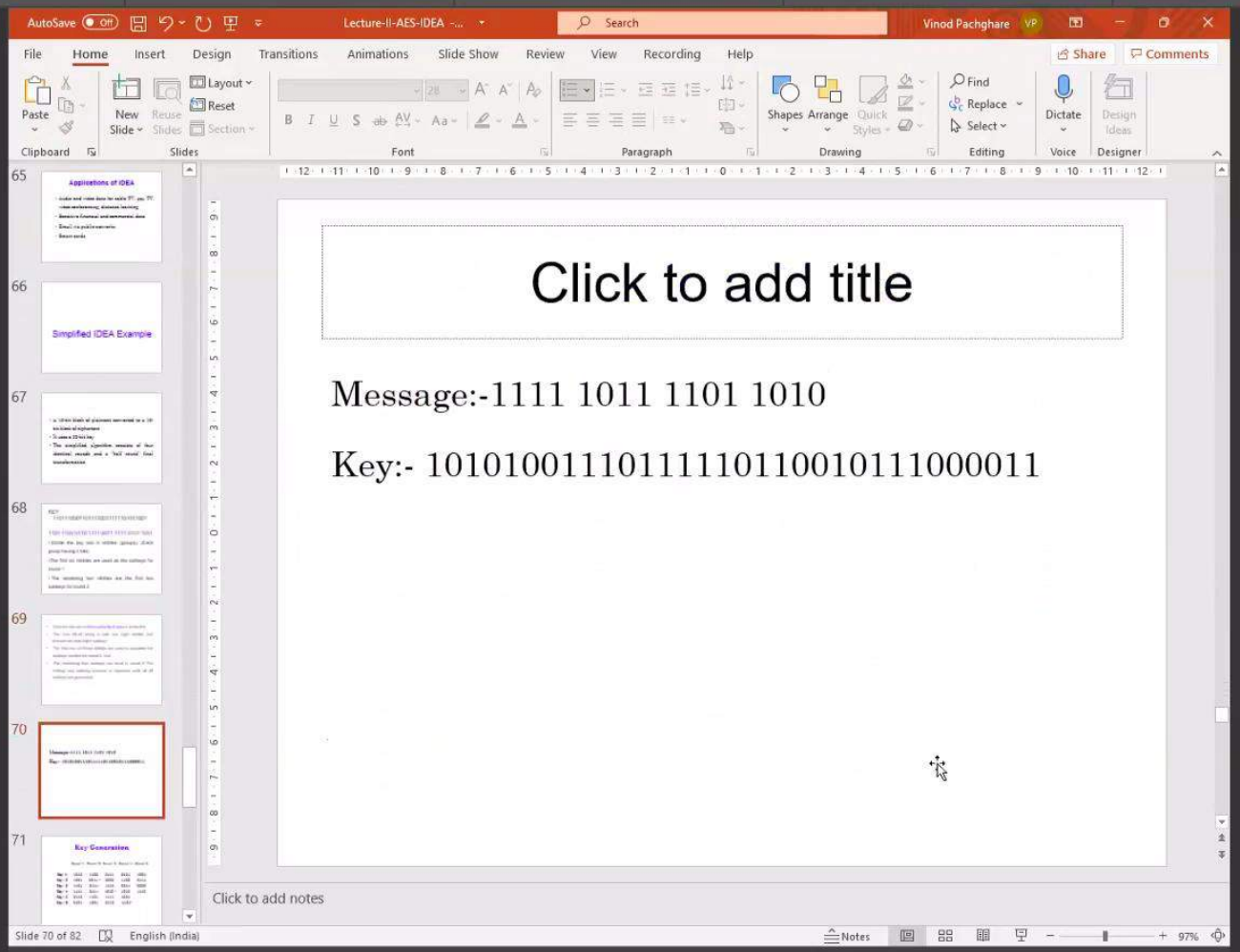
- Then the bits are shifted cyclically 6 places to the left
- The new 32-bit string is split into eight nibbles that become the next eight subkeys
- The first four of these nibbles are used to complete the subkeys needed for round 2, and
- The remaining four subkeys are used in round 3 The shifting and splitting process is repeated until all 28 subkeys are generated

Click to add notes

Slide 69 of 82 | English (India) | Notes | 97%

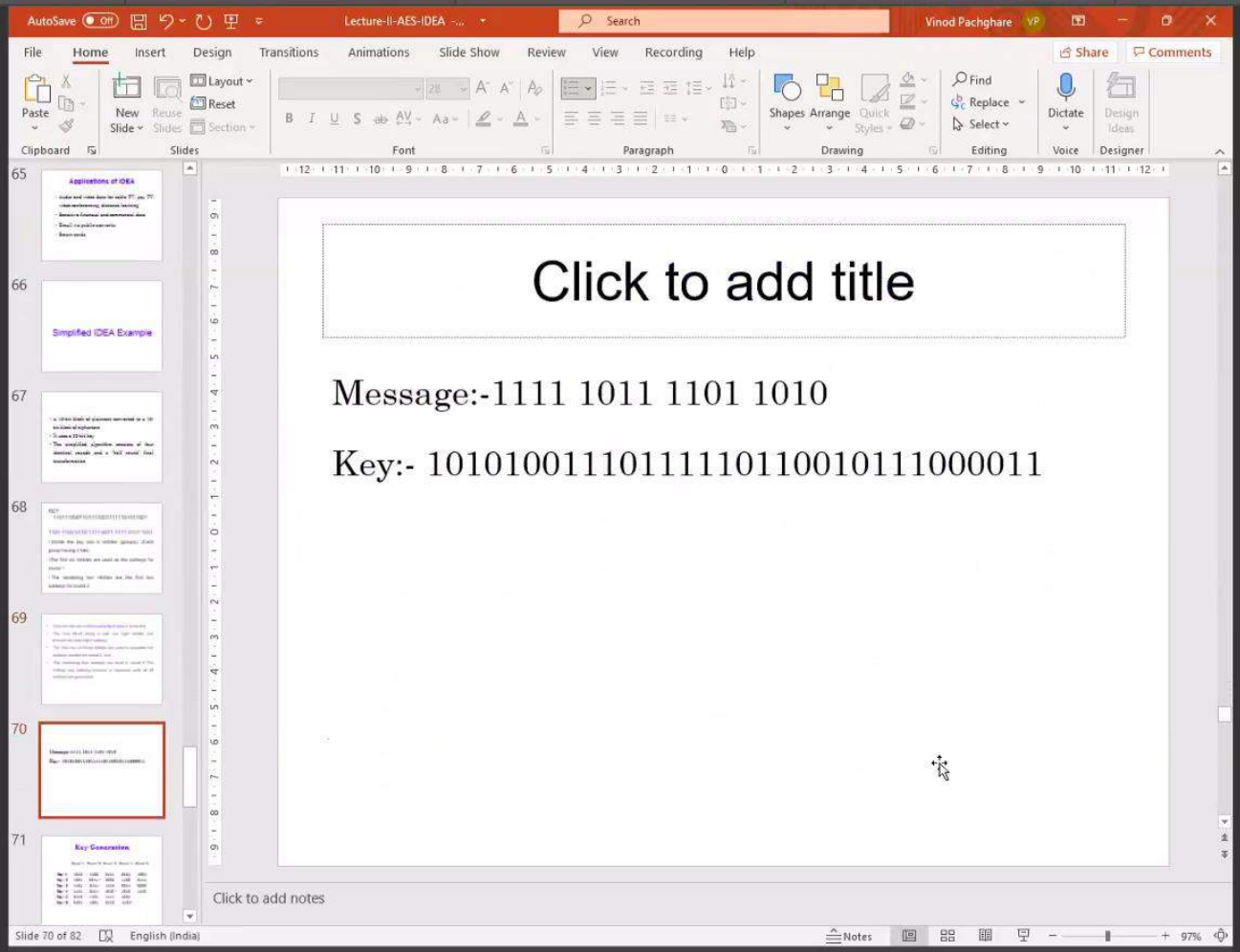
+116

1D		1P	1P	1K
111803111 Atharva Kailas	Vinod	111803155 VIREN RAJES	111803161 Rohan Pravin	111803059 Sakshi Kaleka



+116

1D		1P	1P	1K
111803111 Atharva Kailas	Vinod	111803155 VIREN RAJES	111803161 Rohan Pravin	111803059 Sakshi Kaleka



+116

1D		1P	1P	1K
111803111 Atharva Kailas	Vinod	111803155 VIREN RAJES	111803161 Rohan Pravin	111803059 Sakshi Kaleka

AutoSave Off | Lecture-II-AES-IDEA -... | Search | Vinod Pachghare

File Home Insert Design Transitions Animations Slide Show Review View Recording Help | Share | Comments

Paste | New Slide | Reuse Slides | Layout | Reset | Section | Clipboard | Slides | Font | Paragraph | Shapes | Arrange | Quick Styles | Find | Replace | Select | Editing | Dictate | Voice | Design Ideas | Designer

Simplified IDEA Example

67

68

69

70

71

72

73

Key Generation

	Round -1	Round - 2	Round - 3	Round - 4	Round -5
Key -1	1010	1100	0111	0101	1001
Key - 2	1001	0011 *	0000	1100	0111
Key - 3	1101	0111	1110	0011	0000
Key - 4	1111	0111	1010 *	1010	1110
Key - 5	0110	1101	1111	1001	
Key - 6	0101	1001	0110	1101*	

Click to add notes

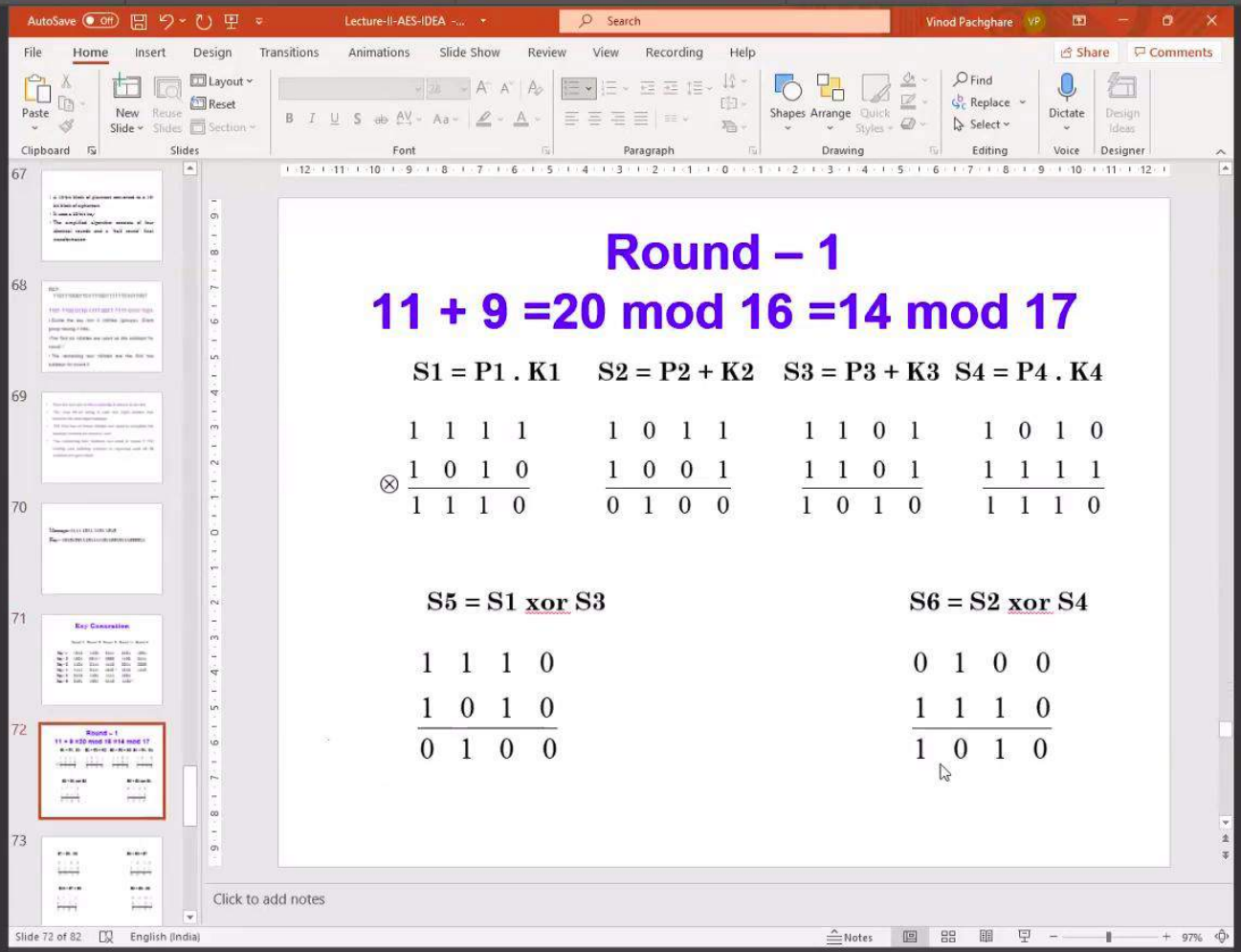
Slide 71 of 82 | English (India) | Notes | 97%

+116

Key Generation

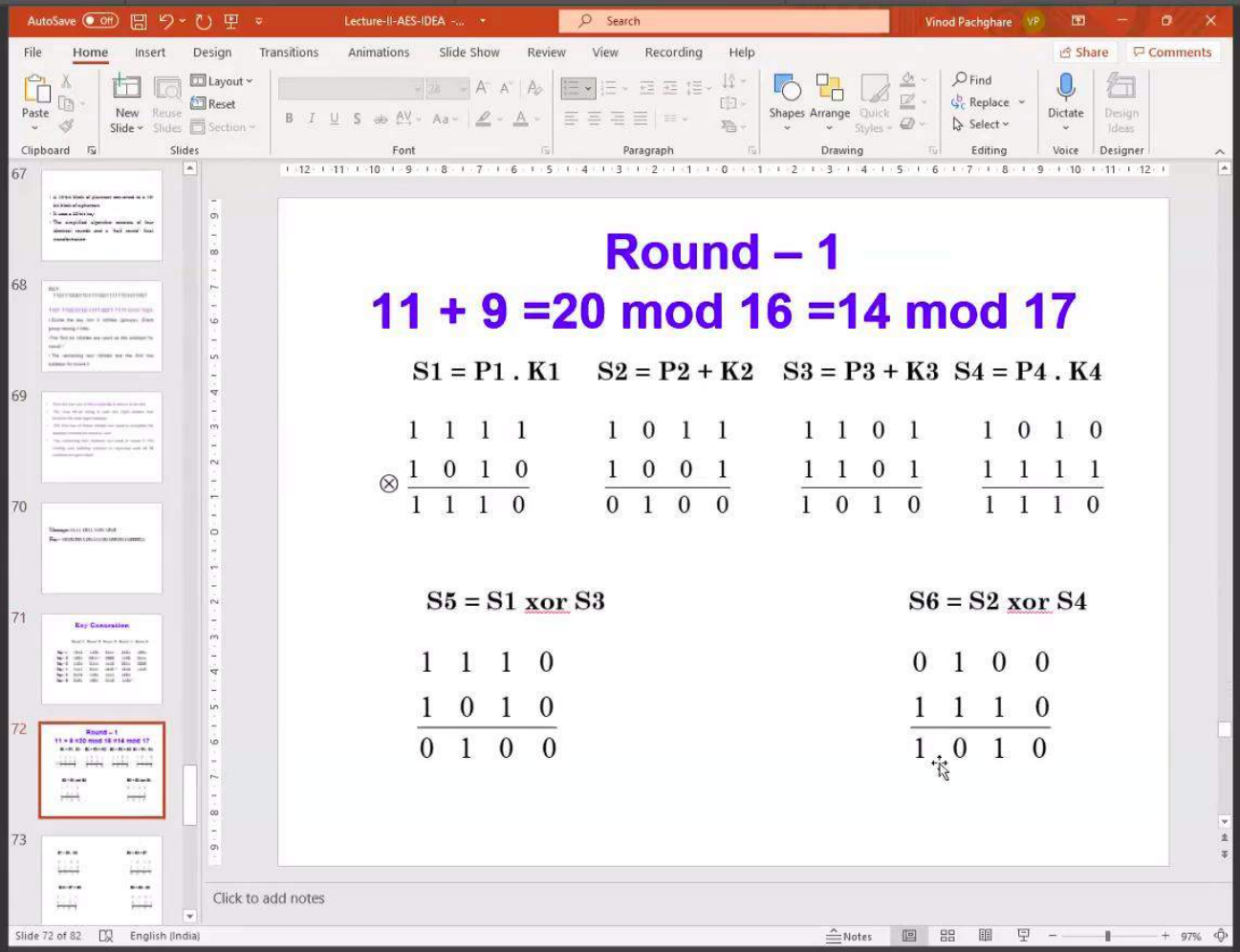
	Round -1	Round - 2	Round - 3	Round - 4	Round -5
Key -1	1010	1100	0111	0101	1001
Key - 2	1001	0011 *	0000	1100	0111
Key - 3	1101	0111	1110	0011	0000
Key - 4	1111	0111	1010 *	1010	1110
Key - 5	0110	1101	1111	1001	
Key - 6	0101	1001	0110	1101*	

1D		1P	1P	1K
111803111 Atharva Kailas	Vinod	111803155 VIREN RAJES	111803161 Rohan Pravin	111803059 Sakshi Kaleka

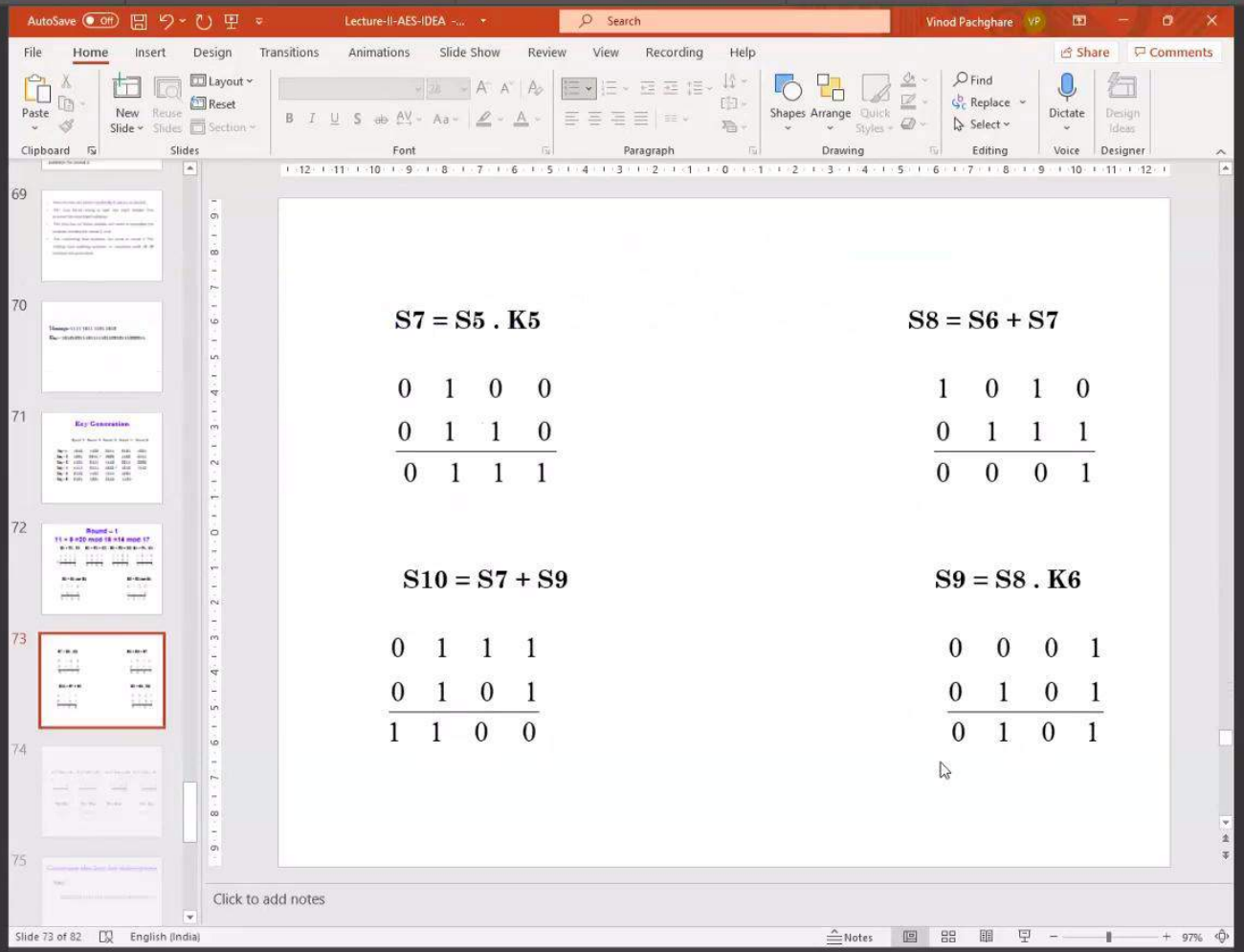


+116

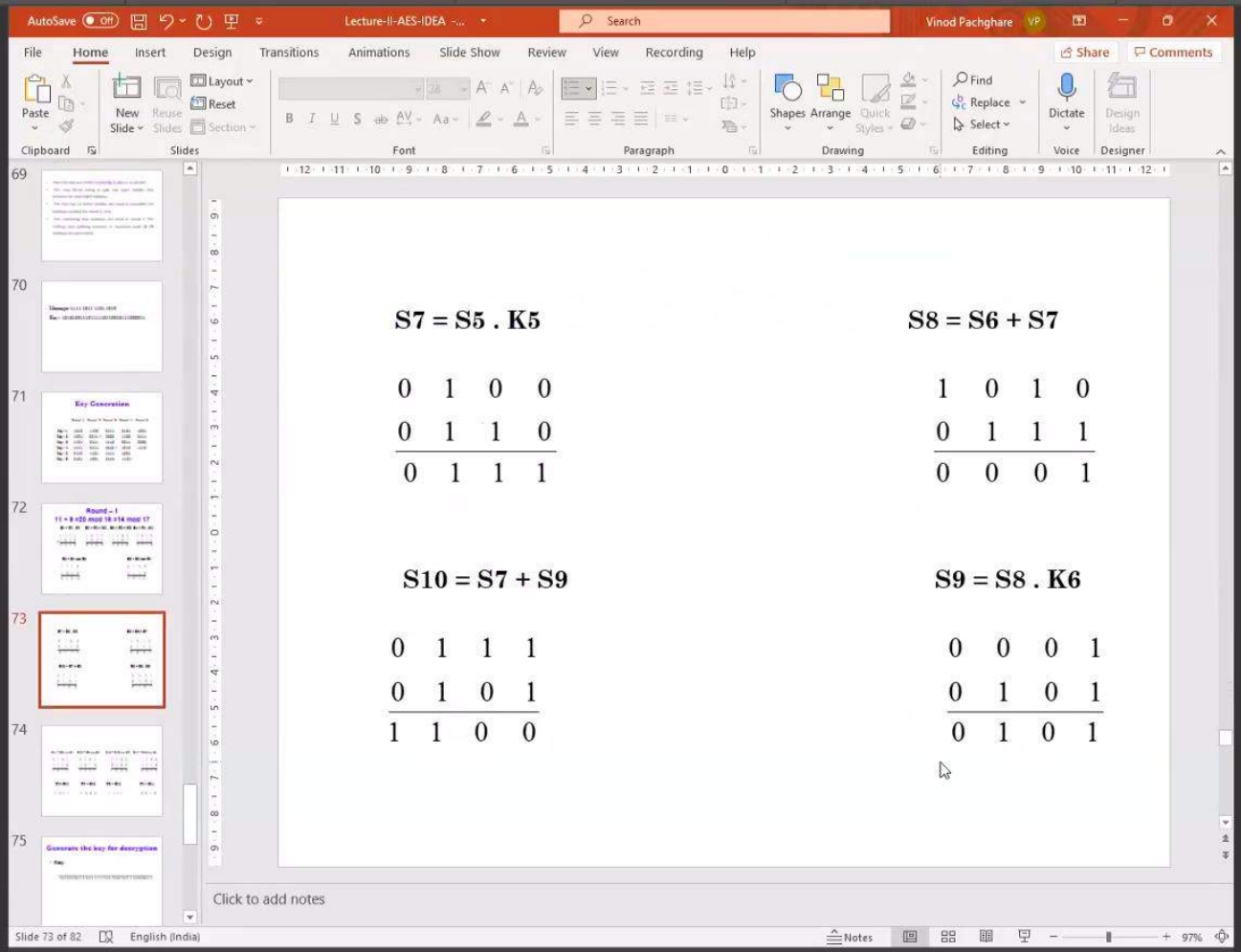
1D		1P	1P	1K
111803111 Atharva Kailas	Vinod	111803155 VIREN RAJES	111803161 Rohan Pravin	111803059 Sakshi Kaleka



+116

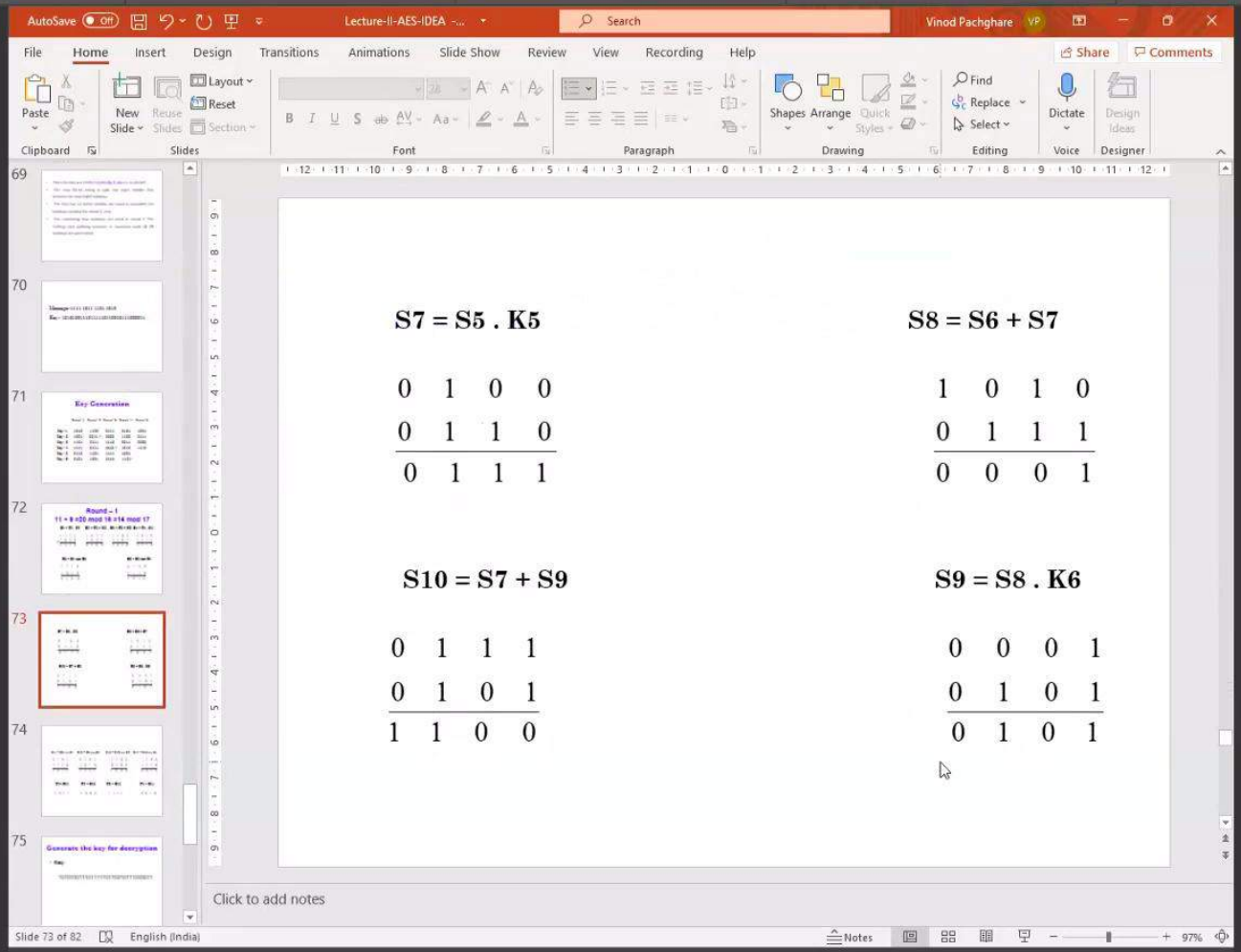


1D		1P	1P	1K
111803111 Atharva Kailas	Vinod	111803155 VIREN RAJES	111803161 Rohan Pravin	111803059 Sakshi Kaleka



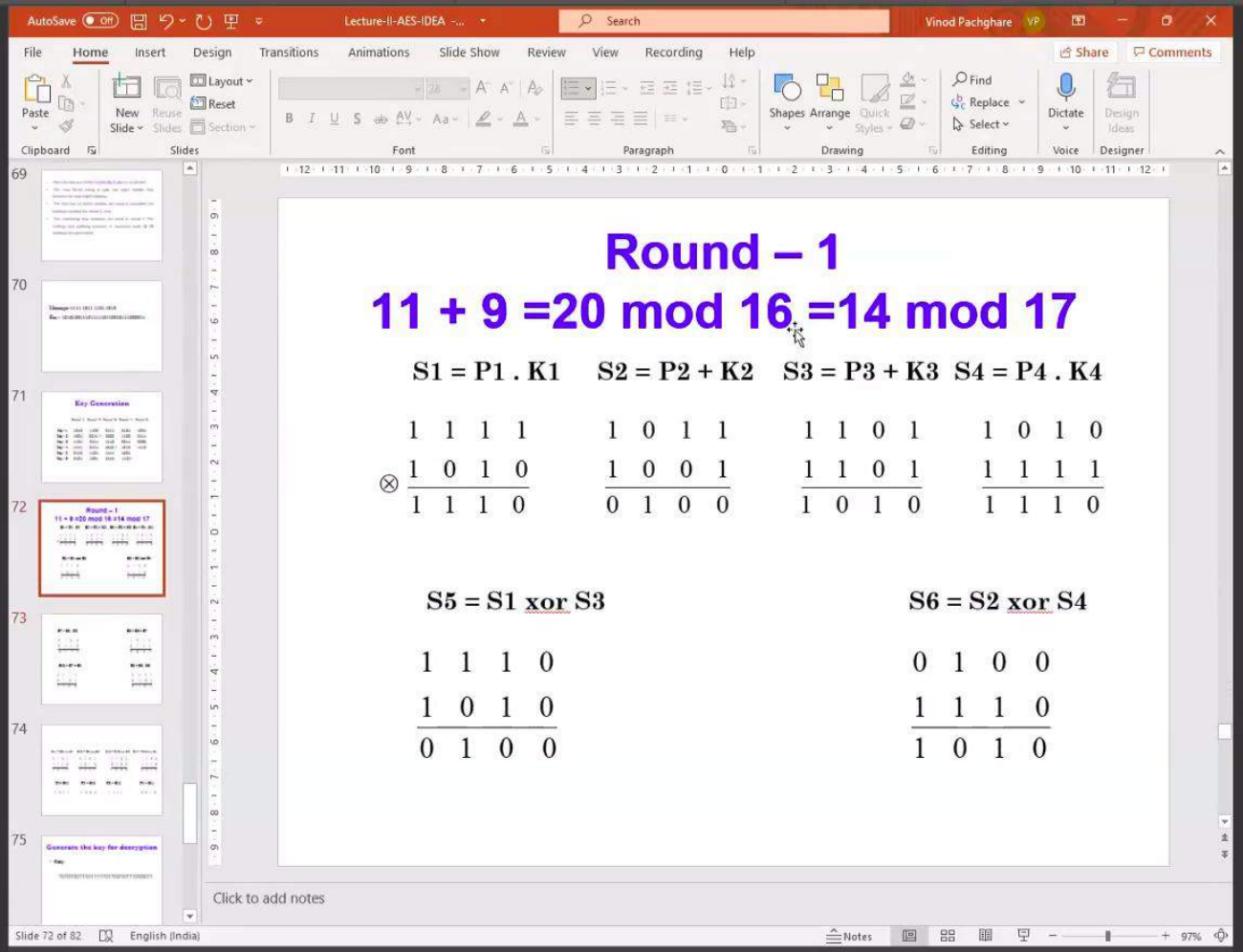
+116

1D		1P	1P	1K
111803111 Atharva Kailas	Vinod	111803155 VIREN RAJES	111803161 Rohan Pravin	111803059 Sakshi Kaleka



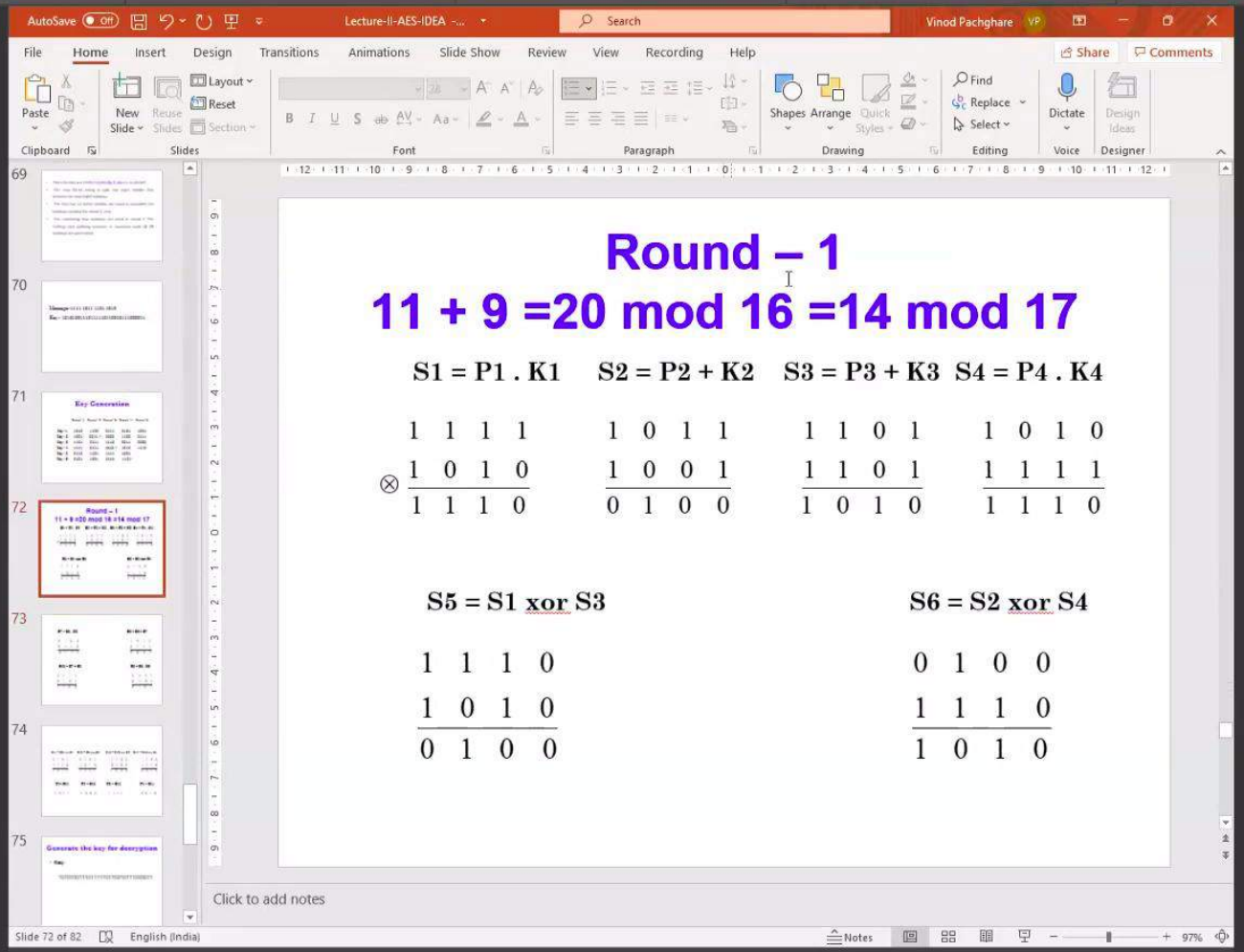
+116

1D		1P	1P	1K
111803111 Atharva Kailas	Vinod	111803155 VIREN RAJES	111803161 Rohan Pravin	111803059 Sakshi Kaleka



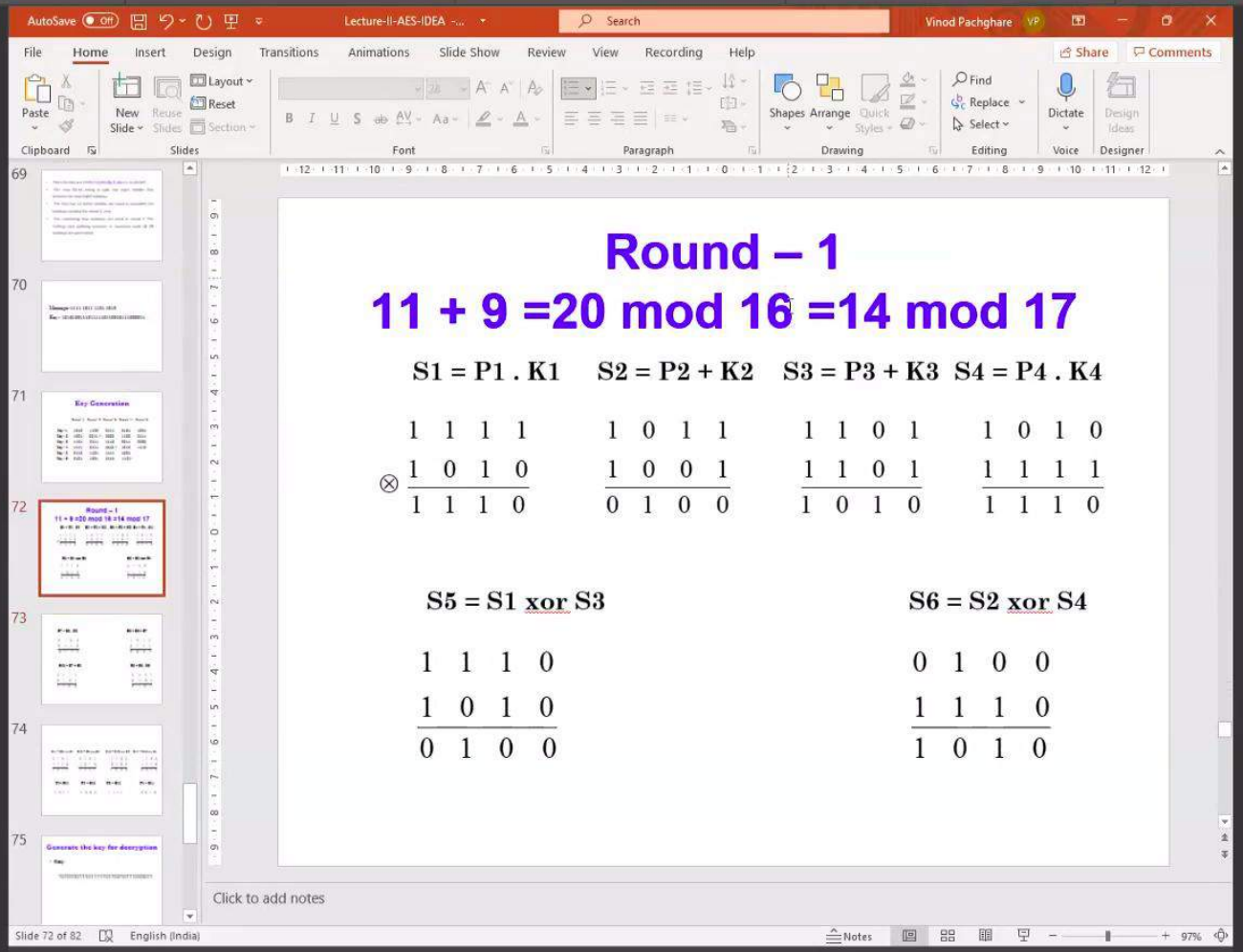
+116

1D		1P	1P	1K
111803111 Atharva Kailas	Vinod	111803155 VIREN RAJES	111803161 Rohan Pravin	111803059 Sakshi Kaleka



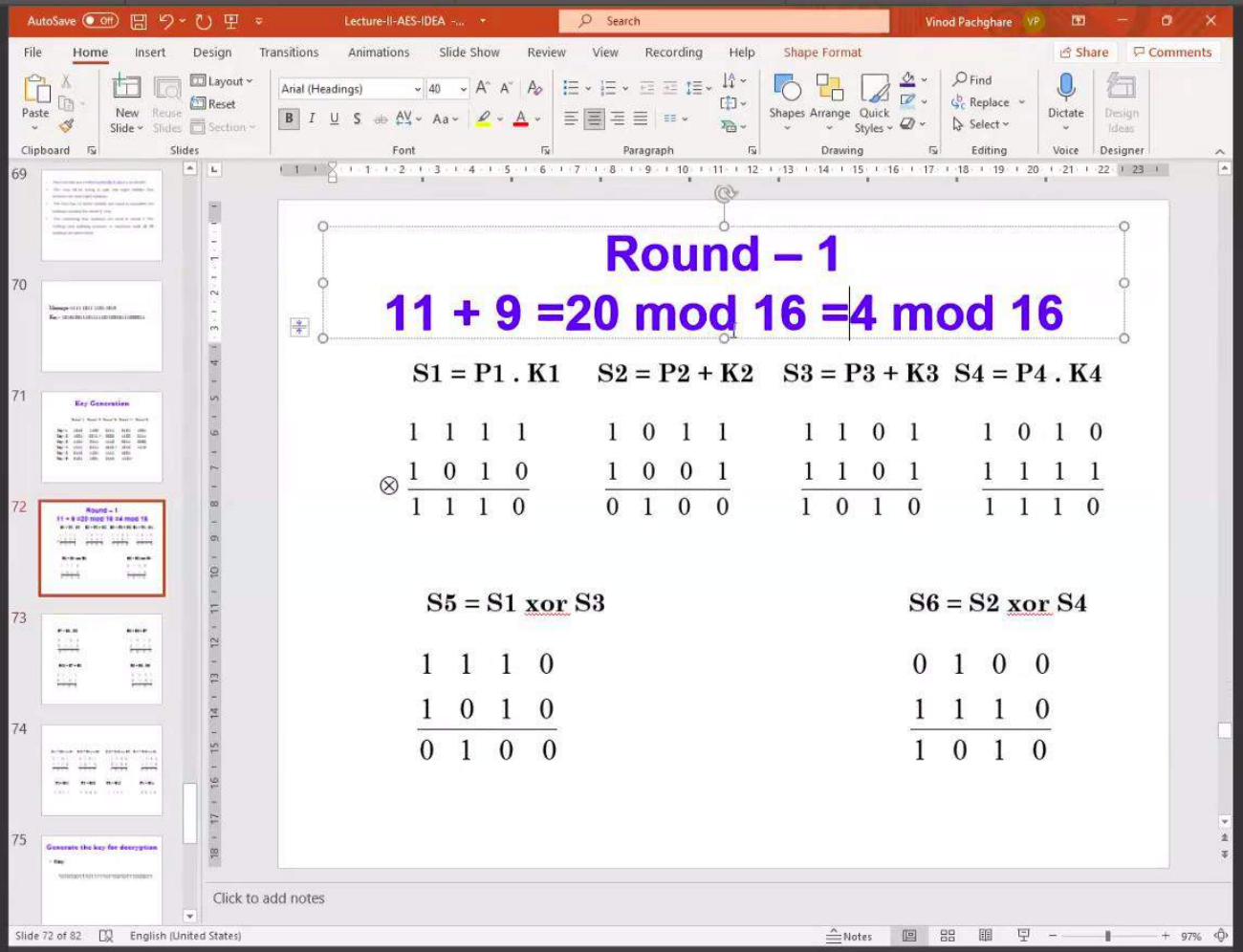
+116

1D		1P	1P	1K
111803111 Atharva Kailas	Vinod	111803155 VIREN RAJES	111803161 Rohan Pravin	111803059 Sakshi Kaleka



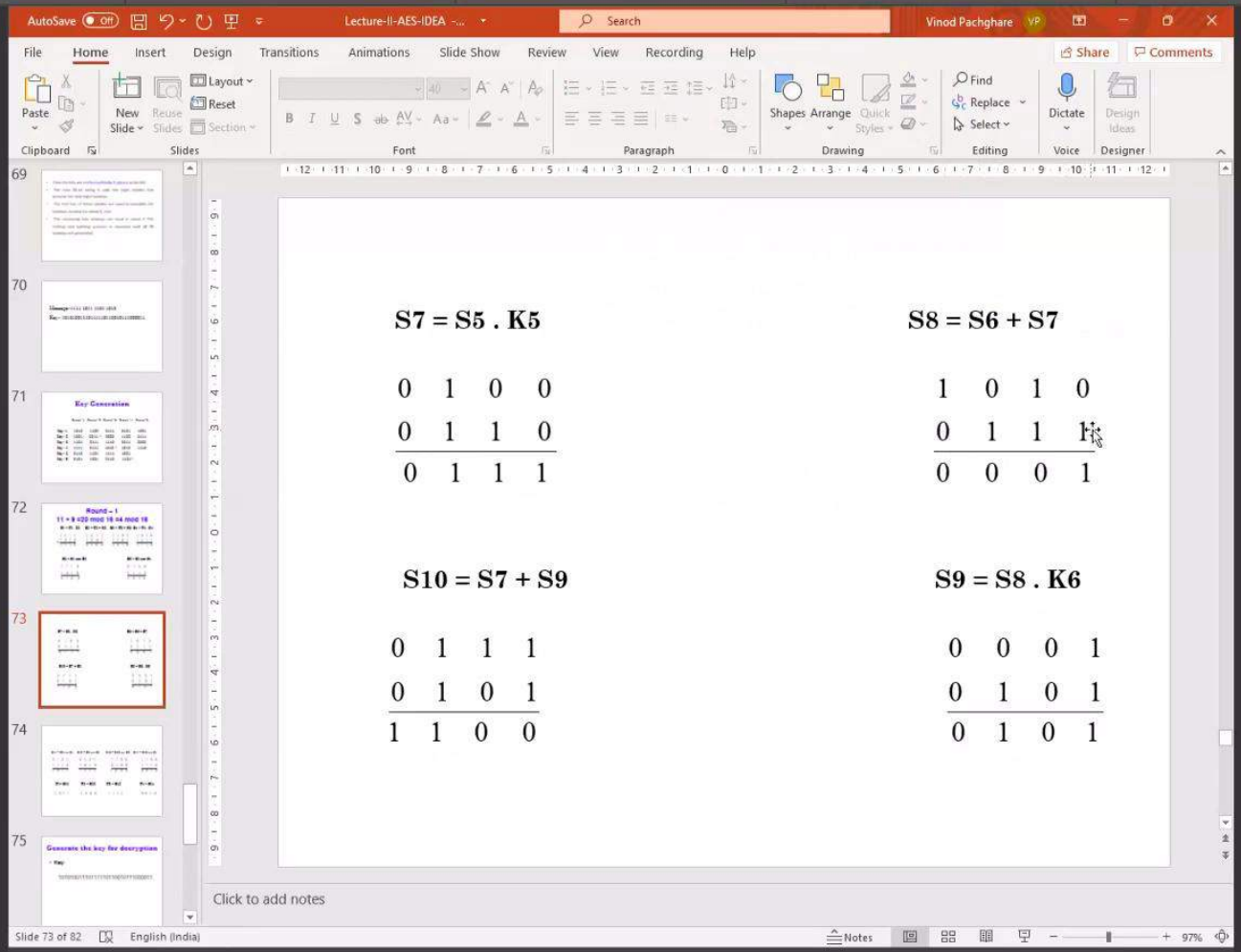
+116

1D		1P	1P	1K
111803111 Atharva Kailas	Vinod	111803155 VIREN RAJES	111803161 Rohan Pravin	111803059 Sakshi Kaleka



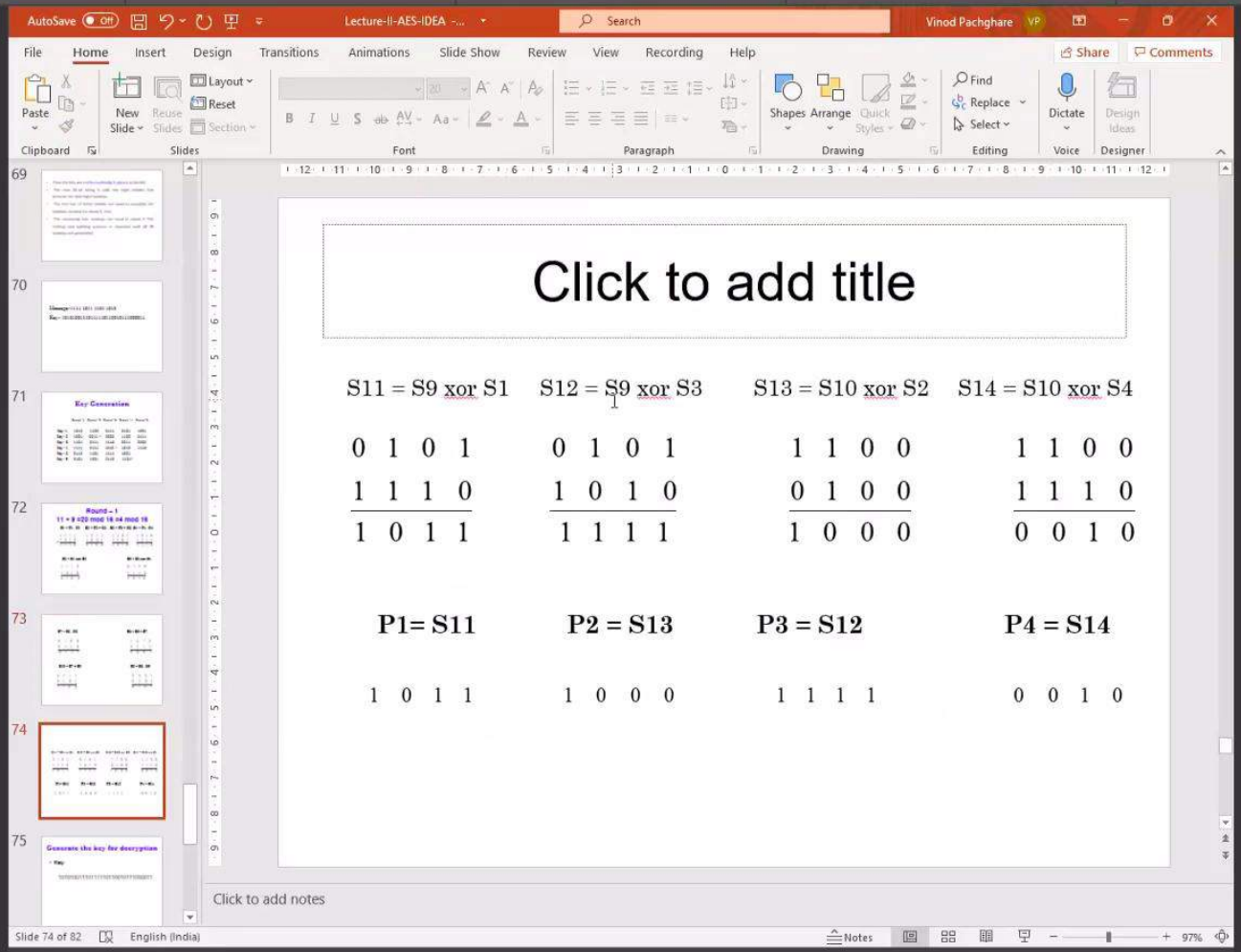
+116

1D		1P	1P	1K
111803111 Atharva Kailas	Vinod	111803155 VIREN RAJES	111803161 Rohan Pravin	111803059 Sakshi Kaleka

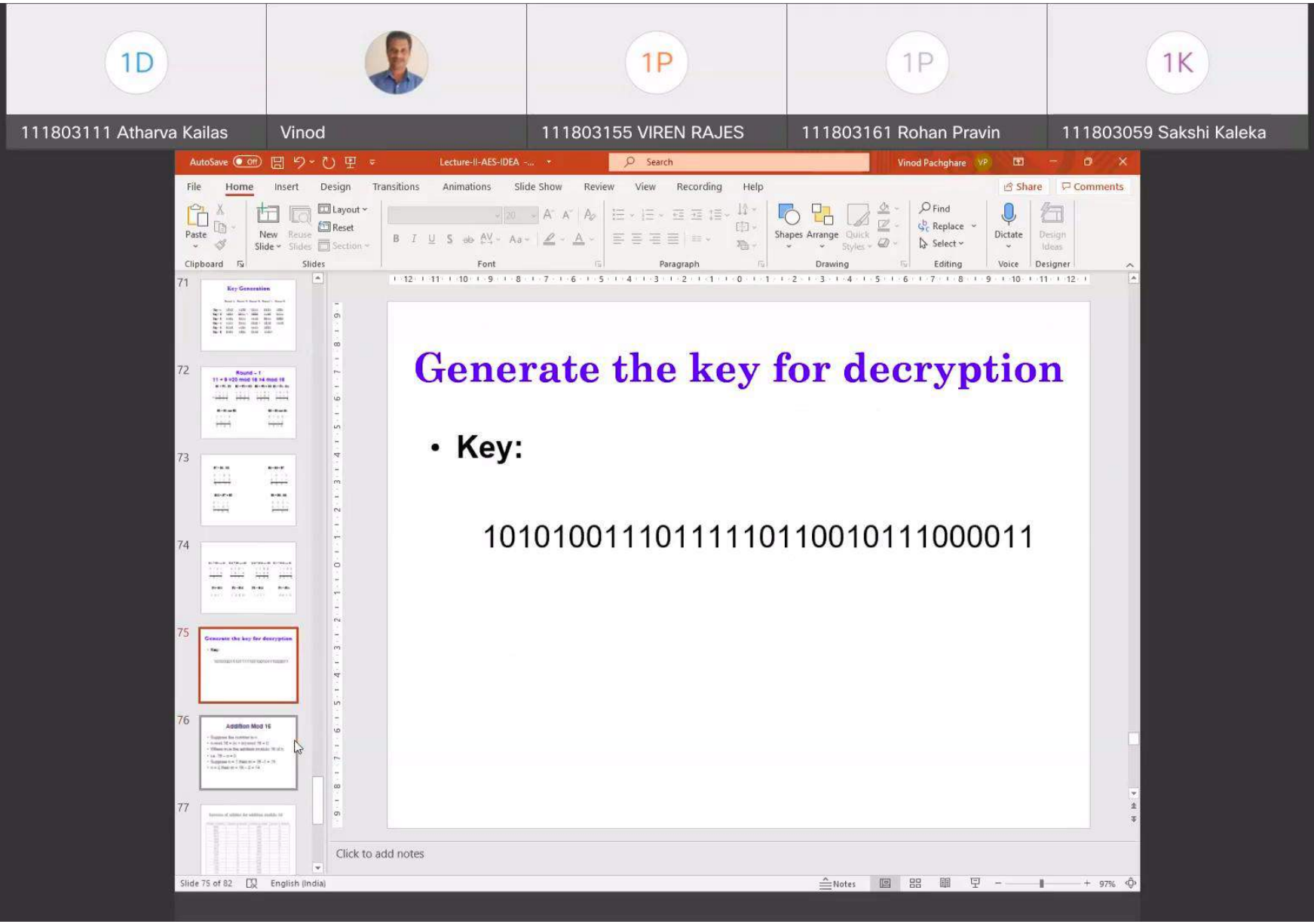


+114

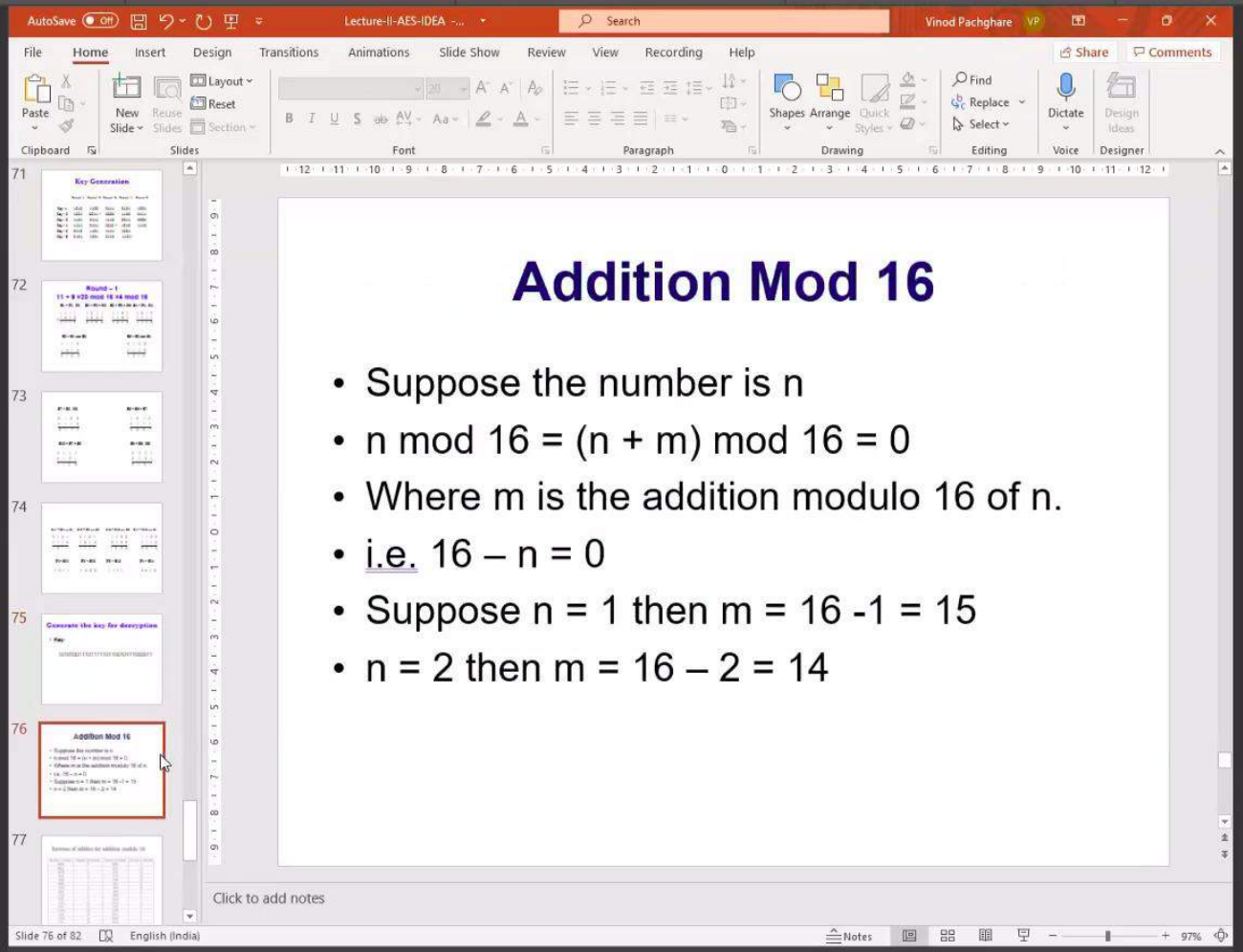
1D		1P	1P	1K
111803111 Atharva Kailas	Vinod	111803155 VIREN RAJES	111803161 Rohan Pravin	111803059 Sakshi Kaleka



+114


1D
111803111 Atharva Kailas
Vinod
1P
111803155 VIREN RAJES
1P
111803161 Rohan Pravin
1K
111803059 Sakshi Kaleka
Lecture-II-AES-IDEA -...
Search
Vinod Pachghare
File Home Insert Design Transitions Animations Slide Show Review View Recording Help
Share Comments
Generate the key for decryption
• Key:
10101001110111110110010111000011
Click to add notes
Slide 75 of 82
English (India)
Notes
97%
+114

1D		1P	1P	1K
111803111 Atharva Kailas	Vinod	111803155 VIREN RAJES	111803161 Rohan Pravin	111803059 Sakshi Kaleka



+114

1D		1P	1P	1K
111803111 Atharva Kailas	Vinod	111803155 VIREN RAJES	111803161 Rohan Pravin	111803059 Sakshi Kaleka

AutoSave Off | Lecture-II-AES-IDEA -... | Search | Vinod Pachghare VP

File Home Insert Design Transitions Animations Slide Show Review View Recording Help | Share | Comments

Paste | New Slide | Layout | Reset | Section | Reuse Slides | Clipboard | Slides | Font | Paragraph | Shapes | Arrange | Quick Styles | Drawing | Find | Replace | Select | Editing | Dictate | Voice | Design Ideas | Designer

73 74 75 76 77 78 79

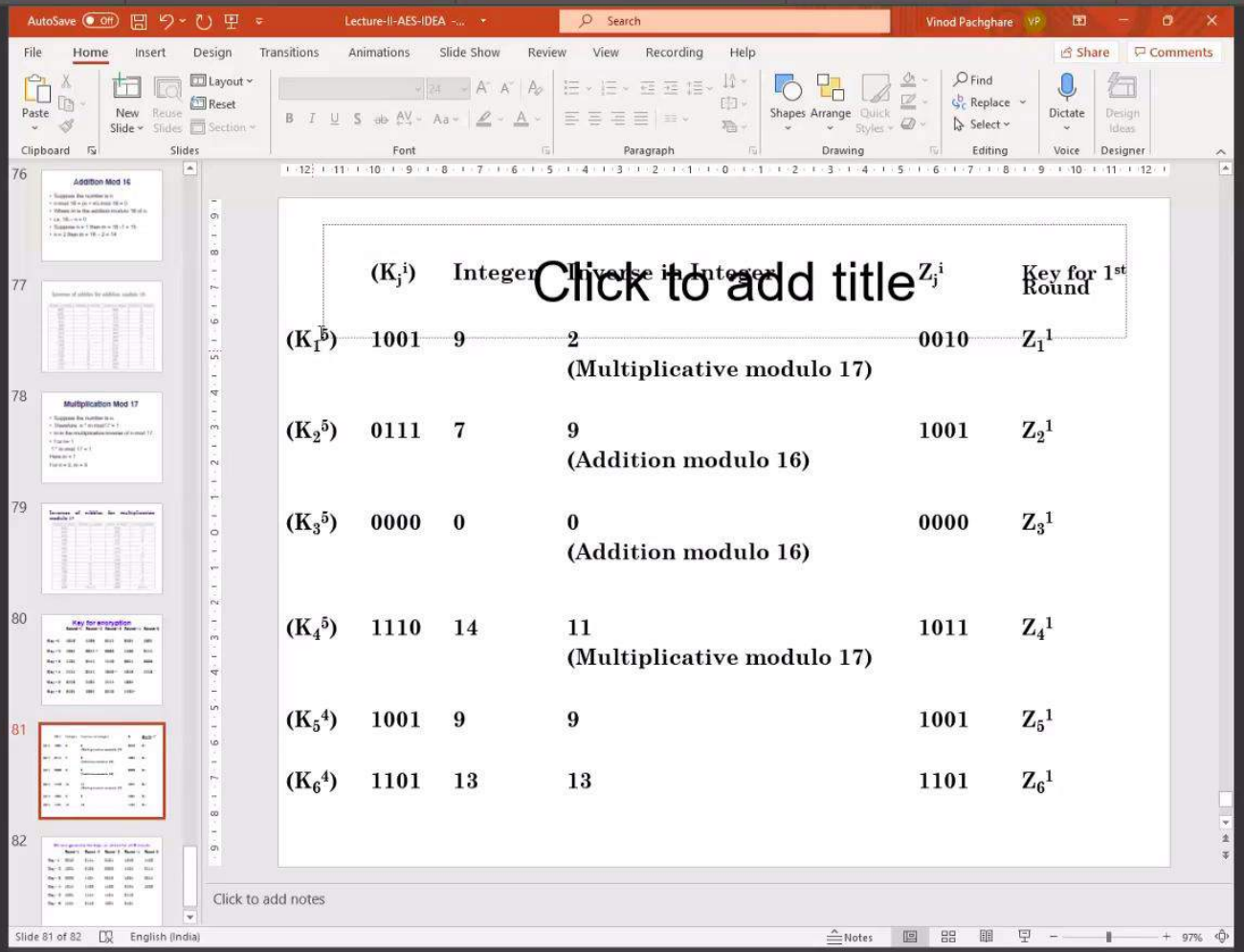
Inverses of nibbles for addition modulo 16:

Number in binary	Number in decimal	Inverse in binary	Inverse in decimal
0000	0	0000	0
0001	1	1111	15
0010	2	1110	14
0011	3	1101	13
0100	4	1100	12
0101	5	1011	11
0110	6	1010	10
0111	7	1001	9
1000	8	1000	8
1001	9	0111	7
1010	10	0110	6
1011	11	0101	5
1100	12	0100	4
1101	13	0011	3
1110	14	0010	2
1111	15	0001	1

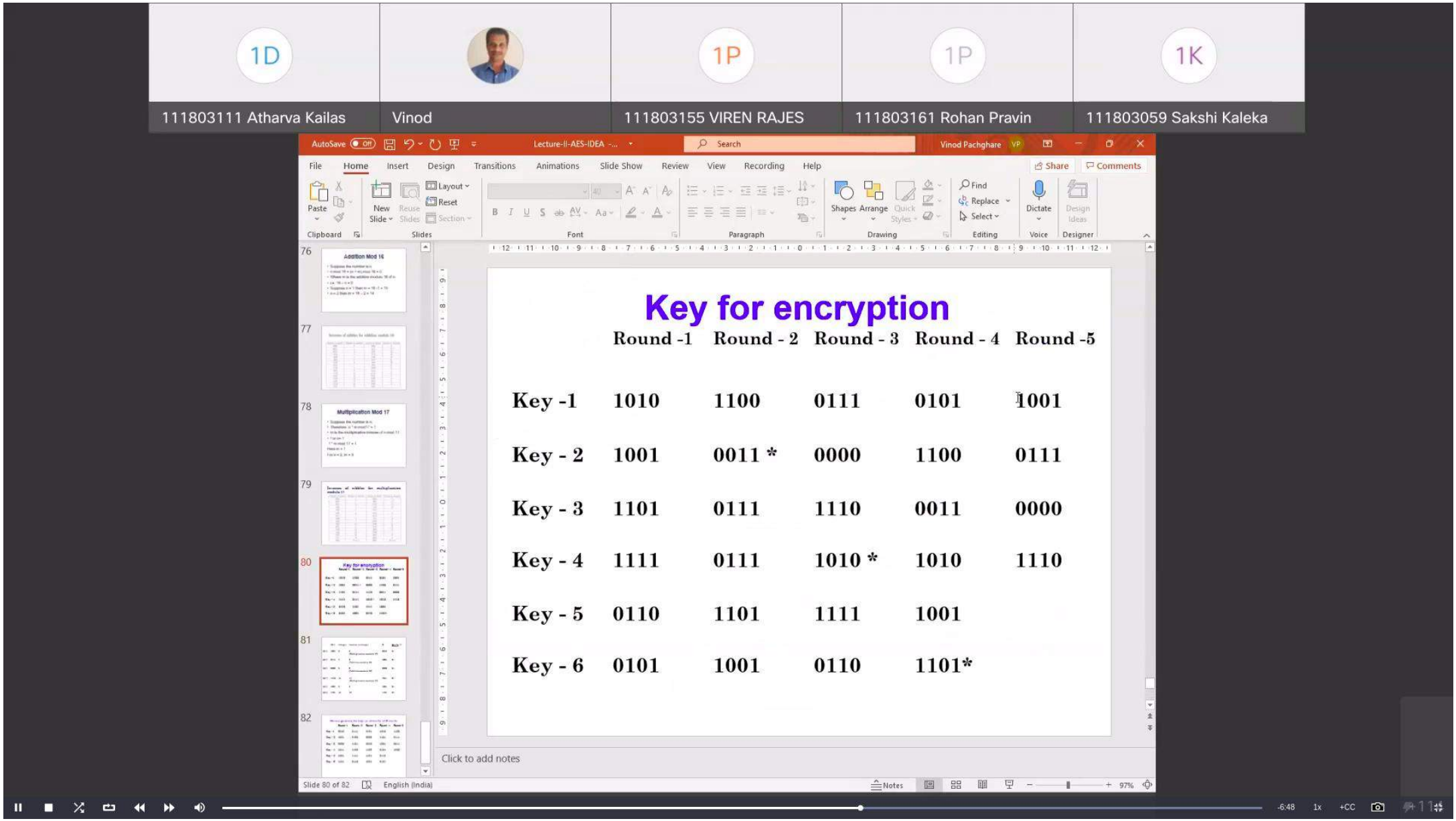
Click to add notes

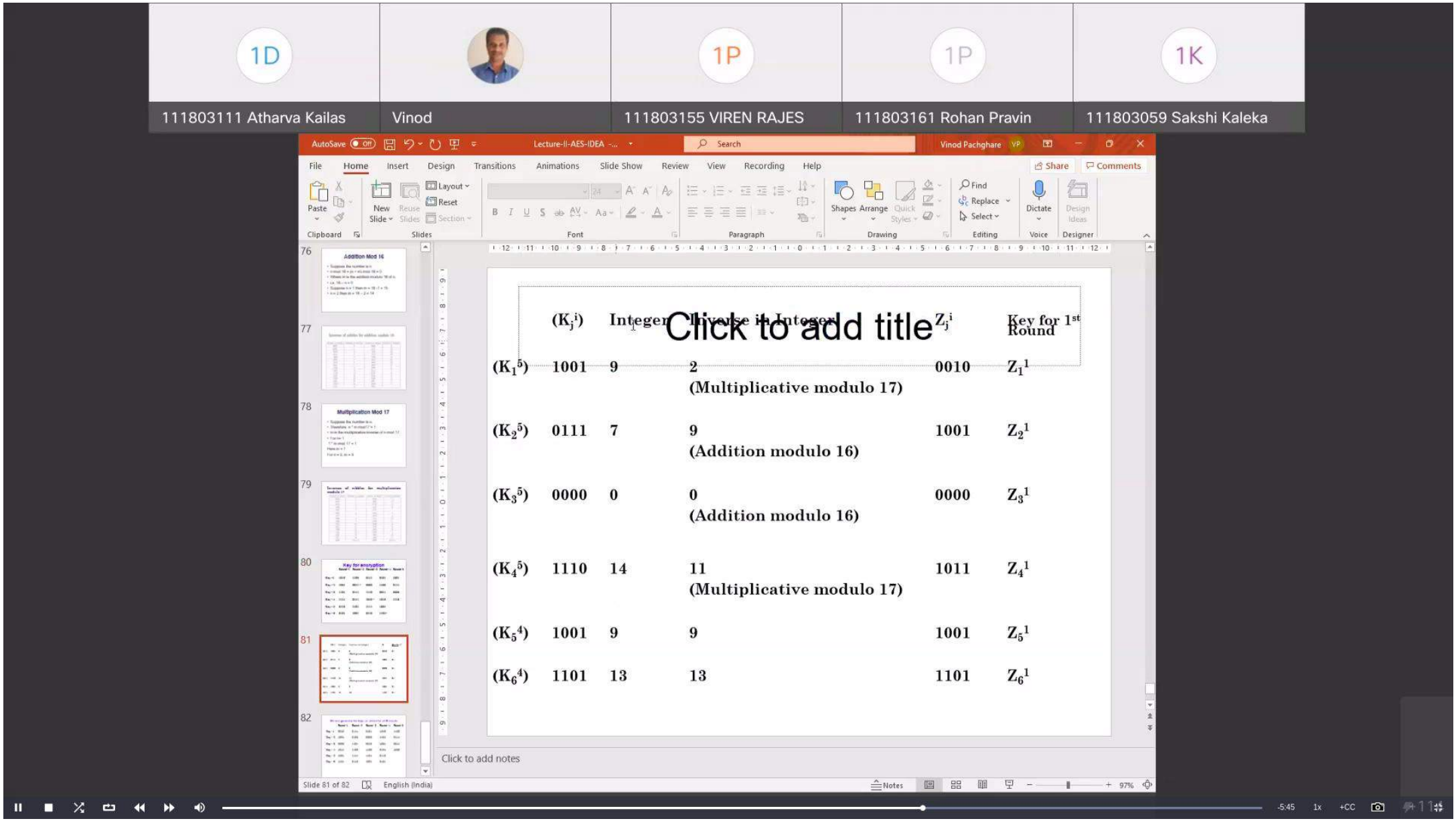
Slide 77 of 82 | English (India) | Notes | 97%

+114

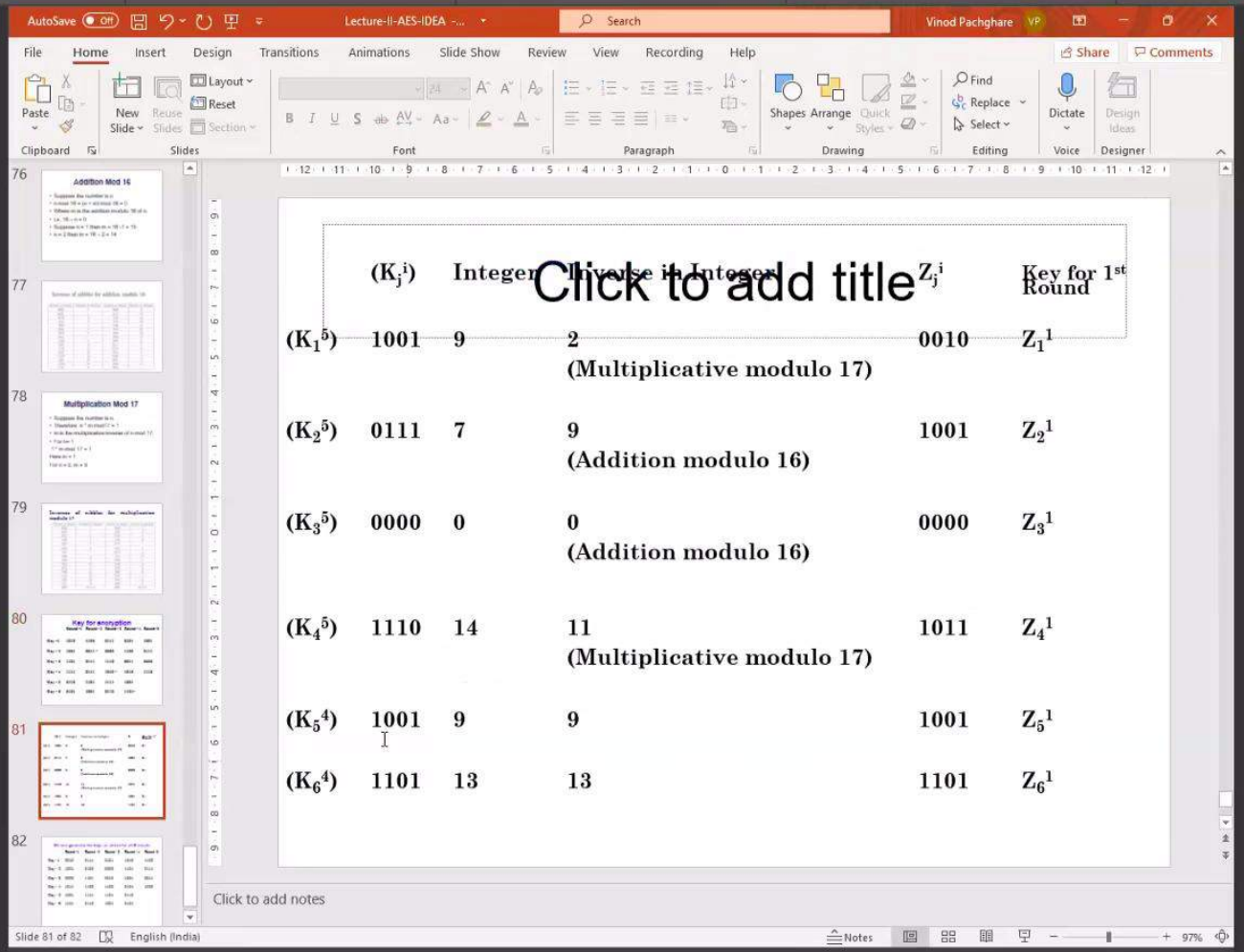


	(K_j^i)	Integer	Inverse in Integer	Z_j^i	Key for 1st Round
(K_1^5)	1001	9	2 (Multiplicative modulo 17)	0010	Z_1^1
(K_2^5)	0111	7	9 (Addition modulo 16)	1001	Z_2^1
(K_3^5)	0000	0	0 (Addition modulo 16)	0000	Z_3^1
(K_4^5)	1110	14	11 (Multiplicative modulo 17)	1011	Z_4^1
(K_5^4)	1001	9	9	1001	Z_5^1
(K_6^4)	1101	13	13	1101	Z_6^1


1D
1P
1P
1K
111803111 Atharva Kailas
Vinod
111803155 VIREN RAJES
111803161 Rohan Pravin
111803059 Sakshi Kaleka
Lecture-II-AES-IDEA -...
Search
Vinod Pachghare
File Home Insert Design Transitions Animations Slide Show Review View Recording Help
Share Comments
Paste Clipboard
New Slide Reuse Slides Layout Reset Section Slides
Font
Paragraph
Shapes Arrange Quick Styles Drawing
Find Replace Select Editing
Dictate Voice
Design Ideas Designer
Key for encryption
Round -1 Round - 2 Round - 3 Round - 4 Round -5
Key -1 1010 1100 0111 0101 1001
Key - 2 1001 0011 * 0000 1100 0111
Key - 3 1101 0111 1110 0011 0000
Key - 4 1111 0111 1010 * 1010 1110
Key - 5 0110 1101 1111 1001
Key - 6 0101 1001 0110 1101*
Click to add notes
Slide 80 of 82
English (India)
Notes
97%
-6:48
1x
+CC

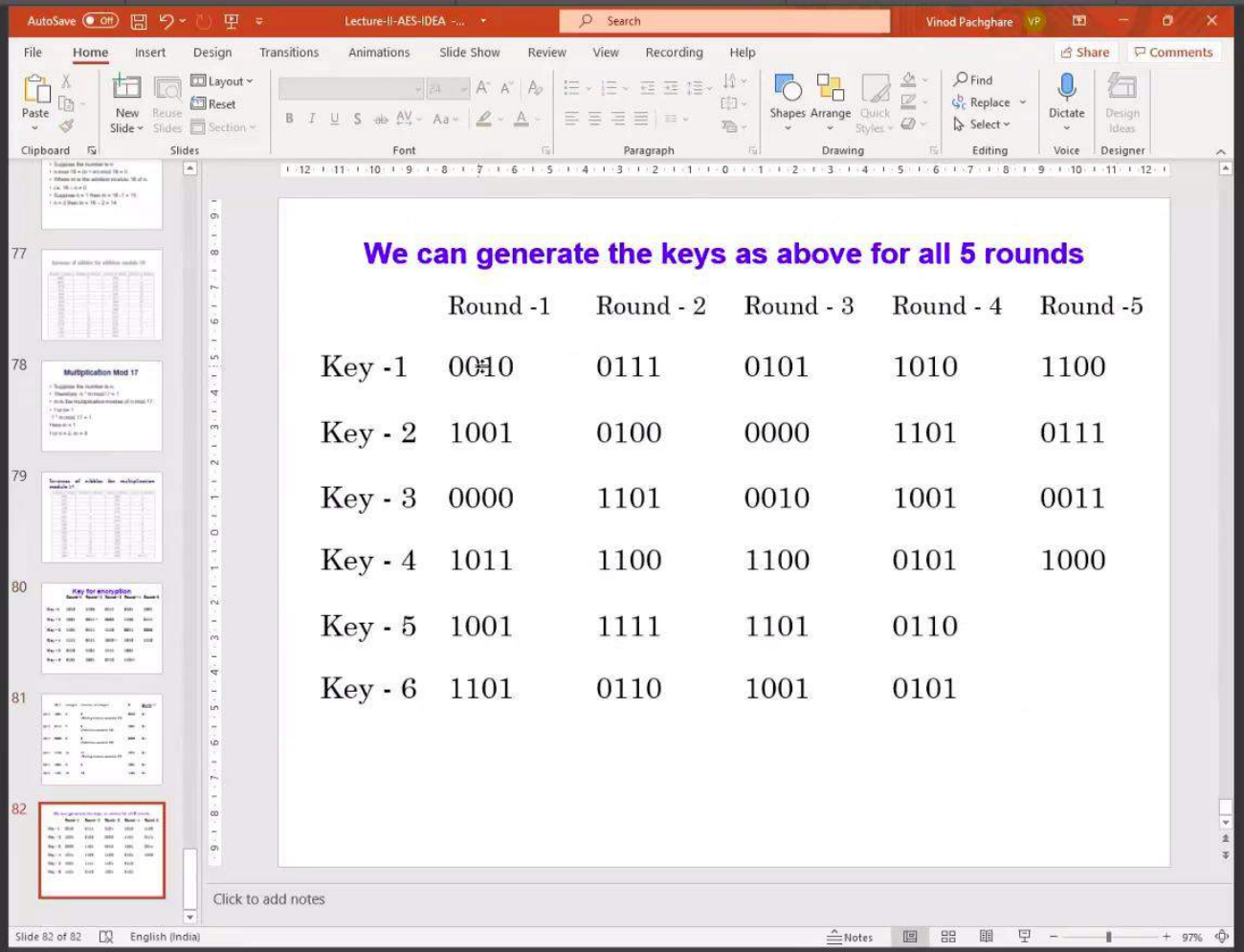


	(K_j^i)	Integer	Inverse in Integer	Z_j^i	Key for 1st Round
(K_1^5)	1001	9	2 (Multiplicative modulo 17)	0010	Z_1^1
(K_2^5)	0111	7	9 (Addition modulo 16)	1001	Z_2^1
(K_3^5)	0000	0	0 (Addition modulo 16)	0000	Z_3^1
(K_4^5)	1110	14	11 (Multiplicative modulo 17)	1011	Z_4^1
(K_5^4)	1001	9	9	1001	Z_5^1
(K_6^4)	1101	13	13	1101	Z_6^1



	(K_j^i)	Integer	Inverse in Integer	Z_j^i	Key for 1st Round
(K_1^5)	1001	9	2 (Multiplicative modulo 17)	0010	Z_1^1
(K_2^5)	0111	7	9 (Addition modulo 16)	1001	Z_2^1
(K_3^5)	0000	0	0 (Addition modulo 16)	0000	Z_3^1
(K_4^5)	1110	14	11 (Multiplicative modulo 17)	1011	Z_4^1
(K_5^4)	1001	9	9	1001	Z_5^1
(K_6^4)	1101	13	13	1101	Z_6^1

1D		1P	1P	1K
111803111 Atharva Kailas	Vinod	111803155 VIREN RAJES	111803161 Rohan Pravin	111803059 Sakshi Kaleka



+114