PowerPoint Presentation - Adobe Acrobat Reader DC (32-bit)

File Edit View Sign Window Help

Home Tools PowerPoint Present... Sign In

12 / 39 90.5%

Definitions

- **Computer Security** - generic name for the collection of tools designed to protect data and to thwart hackers
- **Network Security** - measures to protect data during their transmission
- **Internet Security** - measures to protect data during their transmission over a collection of interconnected networks

Cryptography

- **Cryptography** – *Secret writing*

  from the Greek for "secret writing" is the mathematical "scrambling" of data so that only someone with the necessary ***key*** can "unscramble" it.

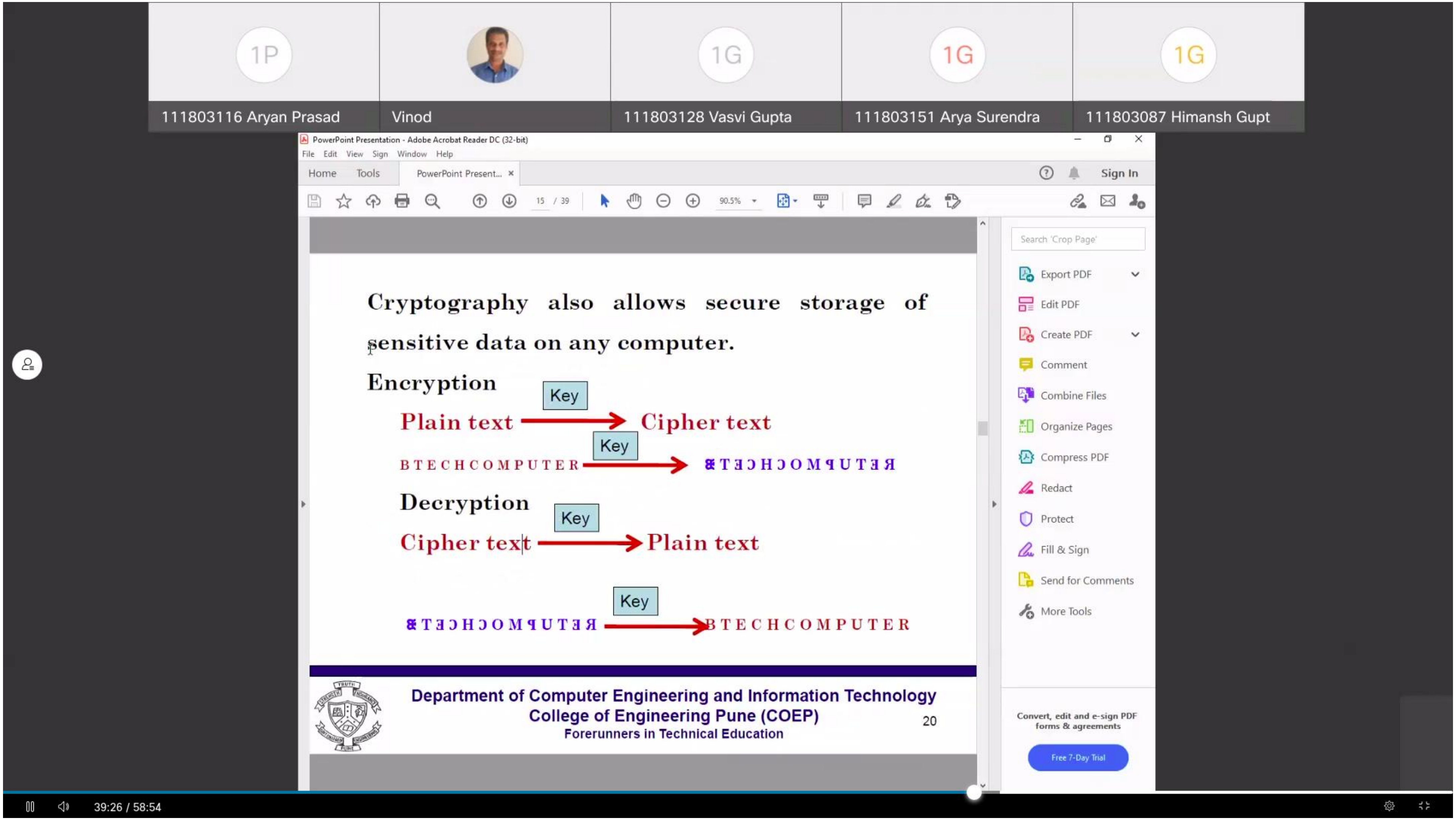
- Cryptography allows secure transmission of private information over insecure channels

Plaintext – A message in its natural format readable by an attacker (Original message/data)

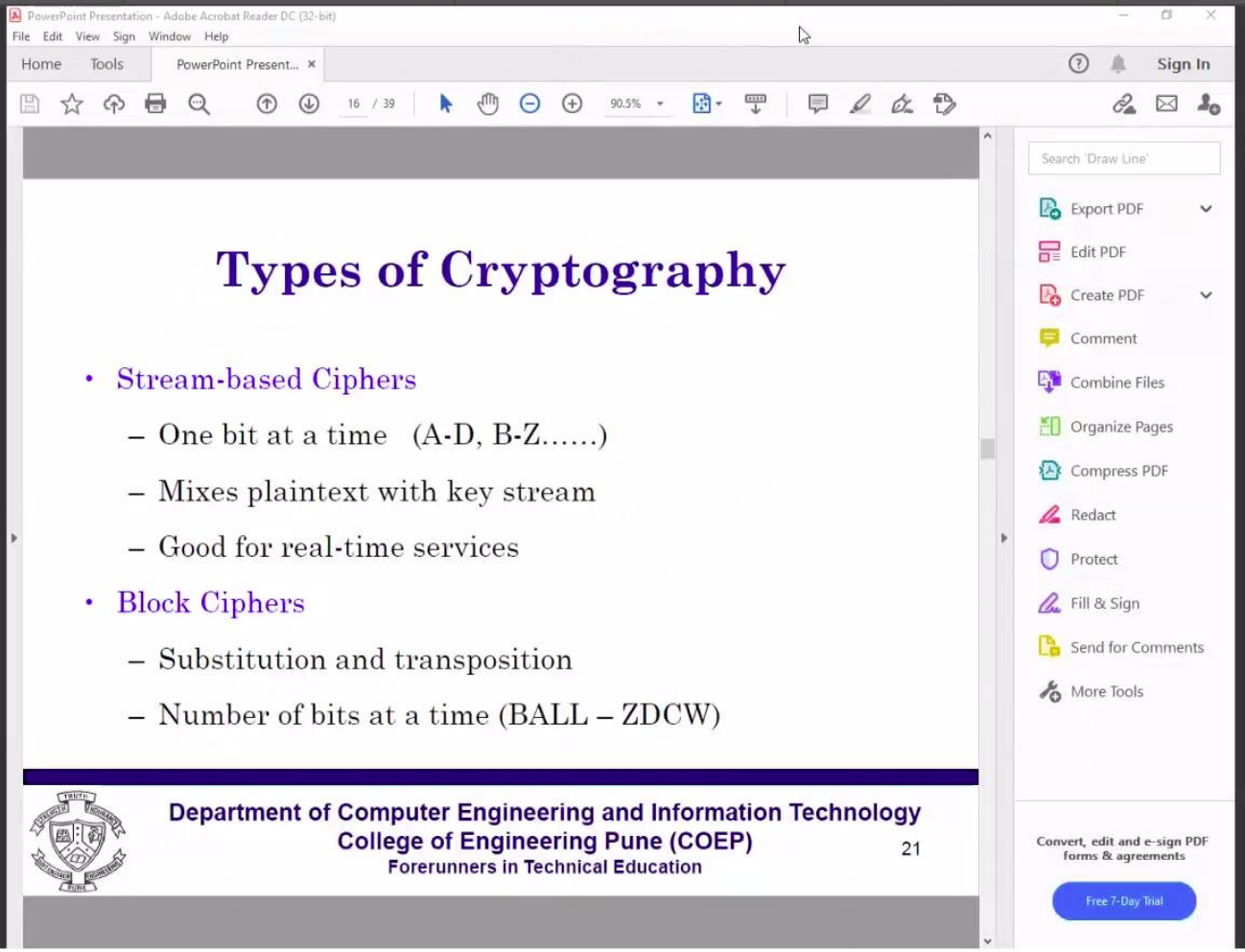
Ciphertext – Message altered to be unreadable by anyone except the intended recipients (Encoded message/data)

Key – Sequence that controls the operation and behavior of the cryptographic algorithm (Password)

Keyspace – Total number of possible values of keys in a crypto algorithm (ex. Suppose the key is binary and the key size is 3 then keyspace is 2^3.)


111803116 Aryan Prasad
Vinod
111803128 Vasvi Gupta
111803151 Arya Surendra
111803087 Himansh Gupt
PowerPoint Presentation - Adobe Acrobat Reader DC (32-bit)
Cryptography also allows secure storage of sensitive data on any computer.
Encryption
Key
Plain text → Cipher text
Key
BTECHCOMPUTER → ꓭTƎƆHƆOMꟼUTƎЯ
Decryption
Key
Cipher text → Plain text
Key
ꓭTƎƆHƆOMꟼUTƎЯ → BTECHCOMPUTER
Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education
20
39:26 / 58:54

1A	1M	1B	1S	1M
111803034 Aditya Abhan	111803072 Shaunak Mah	111803038 YOGESHWARI	111803095 Tejas Sakre	111803176 Yash Gajanan



1A	1M		1S	1M
111803034 Aditya Abhan	111803072 Shaunak Mah	Vinod	111803095 Tejas Sakre	111803176 Yash Gajanan

PowerPoint Presentation - Adobe Acrobat Reader DC (32-bit)

File Edit View Sign Window Help

Home Tools PowerPoint Present... Sign In

16 / 39 90.5%

Types of Cryptography

- Stream-based Ciphers
  - One bit at a time (A-D, B-Z……)
  - Mixes plaintext with key stream
  - Good for real-time services
- Block Ciphers
  - Substitution and transposition
  - Number of bits at a time (BALL – ZDCW)

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

21

Search 'Draw Line'

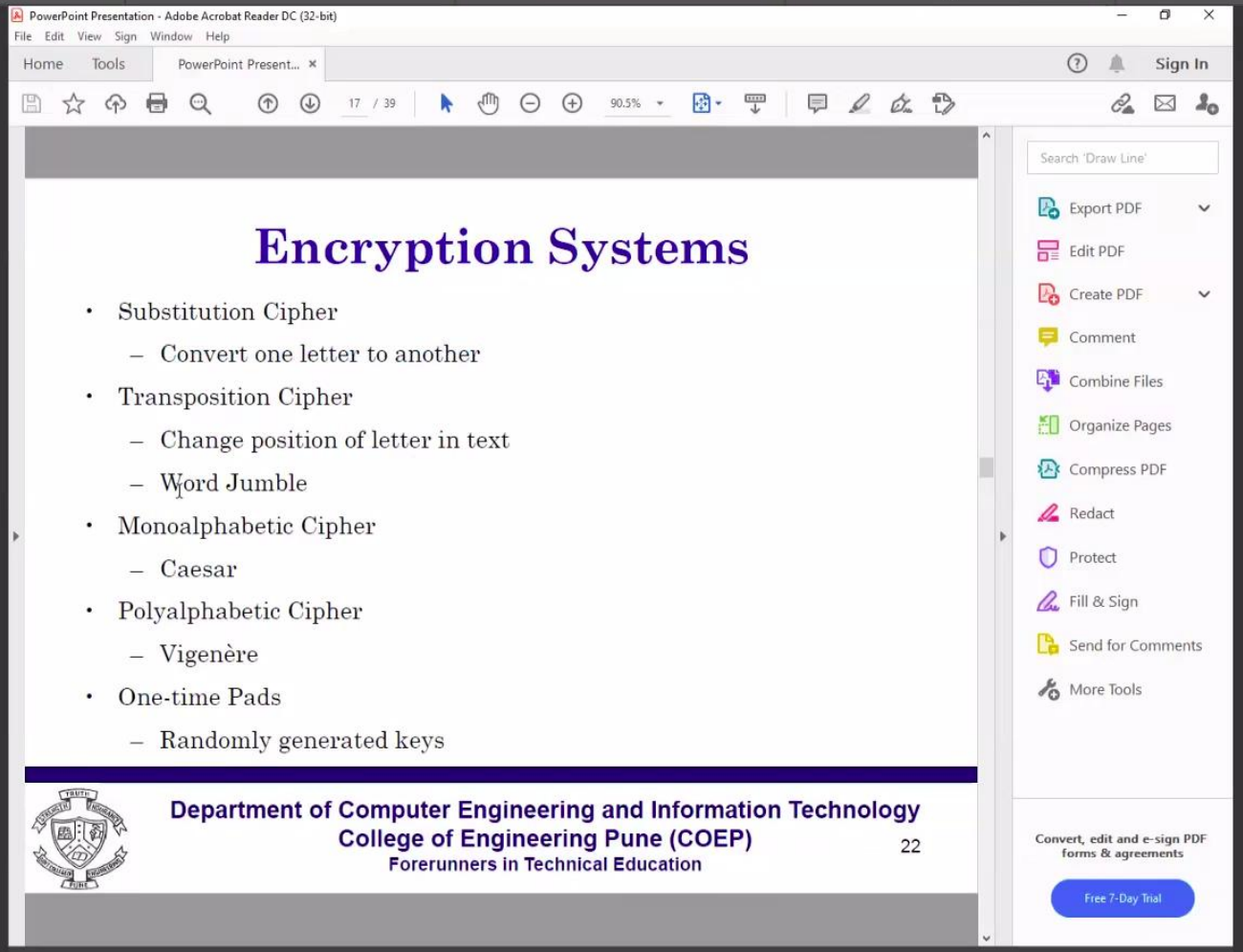
Export PDF
Edit PDF
Create PDF
Comment
Combine Files
Organize Pages
Compress PDF
Redact
Protect
Fill & Sign
Send for Comments
More Tools

Convert, edit and e-sign PDF forms & agreements

Free 7-Day Trial

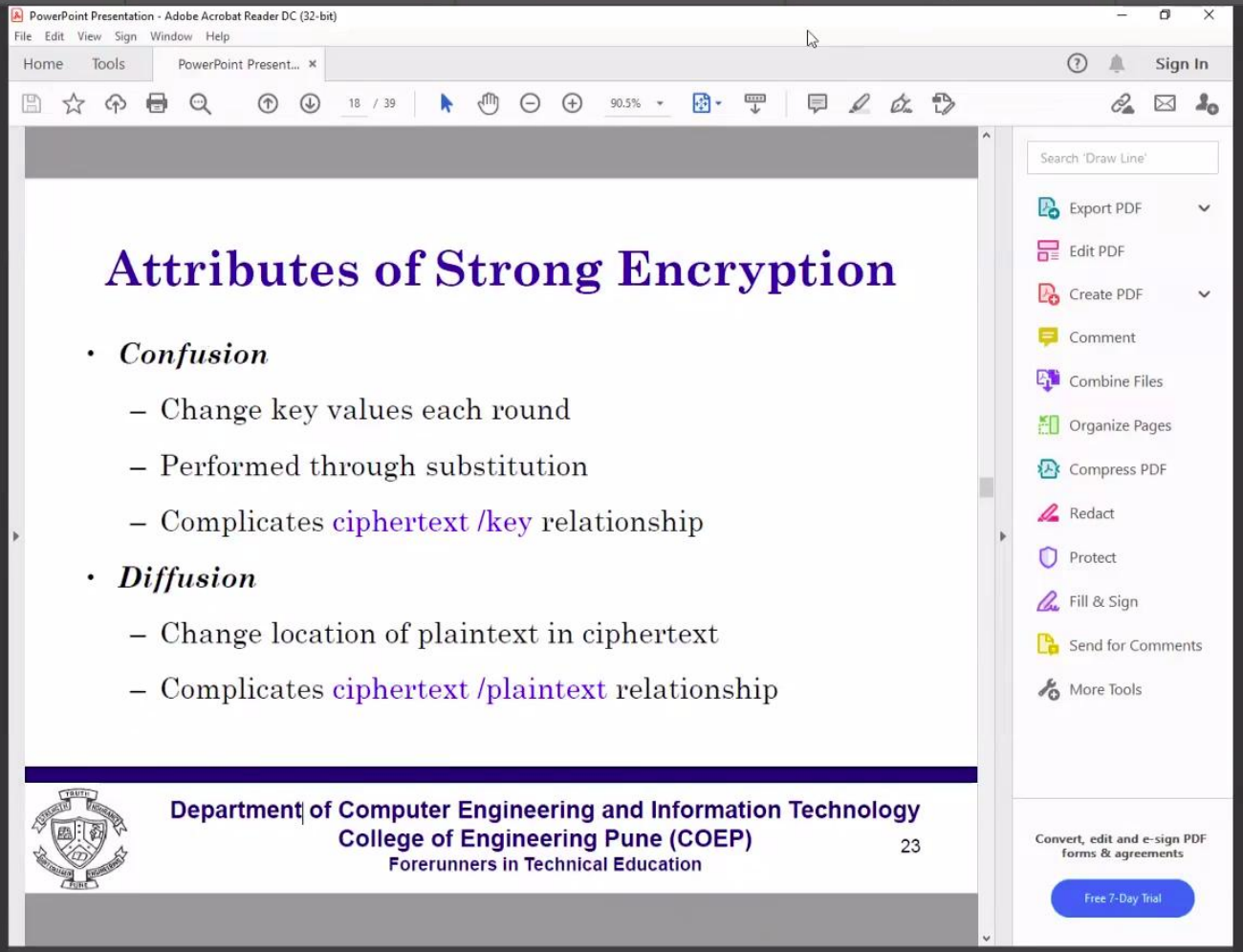
+60

1A	1M		1S	1M
111803034 Aditya Abhan	111803072 Shaunak Mah	Vinod	111803095 Tejas Sakre	111803176 Yash Gajanan



+69

1A	1M		1S	1M
111803034 Aditya Abhan	111803072 Shaunak Mah	Vinod	111803095 Tejas Sakre	111803176 Yash Gajanan



+75

Hashing Algorithms

- **MD5**
  - Computes 128-bit hash value
  - Widely used for file integrity checking
- **SHA-1**
  - Computes 160-bit hash value
  - NIST approved message digest algorithm
- **RIPEMD-160**
  - Developed in Europe published in 1996
  - Patent-free

Three Aspects of Information Security

- Security attack
- Security mechanism
- Security service

1A	1J		1S	1D
111803034 Aditya Abhan	111803142 ATHARVA MU	Vinod	111803095 Tejas Sakre	141803013 Trupti Namde

Press Esc to exit full screen

PowerPoint Presentation - Adobe Acrobat Reader DC (32-bit)

File Edit View Sign Window Help

Home Tools PowerPoint Present... Sign In

21 / 39 90.5%

Security Service

- is something that enhances the security of the data processing systems and the information transfers of an organization
- intended to counter security attacks
- make use of one or more security mechanisms to provide the service
- eg. have signatures, dates; need protection from disclosure, tampering, or destruction; be notarized or witnessed; be recorded or licensed

+108

Security Mechanism

- a mechanism that is designed to detect, prevent, or recover from a security attack
- no single mechanism that will support all functions required
- however one particular element underlies many of the security mechanisms in use: **cryptographic techniques**

1A	1J		1S	1D
111803034 Aditya Abhan	111803142 ATHARVA MU	Vinod	111803095 Tejas Sakre	141803013 Trupti Namde

Press Esc to exit full screen

PowerPoint Presentation - Adobe Acrobat Reader DC (32-bit)

File Edit View Sign Window Help

Home Tools PowerPoint Present... Sign In

23 / 39 90.5%

Security Attack

- any action that compromises the security of information
- information security is about how to prevent attacks, or failing that, to detect attacks on information-based systems

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

28

Search 'Draw Line'

Export PDF
Edit PDF
Create PDF
Comment
Combine Files
Organize Pages
Compress PDF
Redact
Protect
Fill & Sign
Send for Comments
More Tools

Convert, edit and e-sign PDF forms & agreements

Free 7-Day Trial

+111

1D	1J		1S	1D
111803111 Atharva Kailas	111803142 ATHARVA MU	Vinod	111803095 Tejas Sakre	111803049 Vrushali Pram

PowerPoint Presentation - Adobe Acrobat Reader DC (32-bit)

File Edit View Sign Window Help

Home Tools PowerPoint Present... Sign In

26 / 39 90.5%

Security Services

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

31

Search 'Draw Line'

Export PDF
Edit PDF
Create PDF
Comment
Combine Files
Organize Pages
Compress PDF
Redact
Protect
Fill & Sign
Send for Comments
More Tools

Convert, edit and e-sign PDF forms & agreements

Free 7-Day Trial

25:07 / 01:03:32

Authentication

- assurance that the communicating entity is the one claimed
  - **Peer Entity Authentication**: Used in association with a logical connection to provide confidence in the identity of the entities connected.
  - **Data Origin Authentication**: In a connectionless transfer, provides assurance that the source of received data is as claimed.

Data Confidentiality

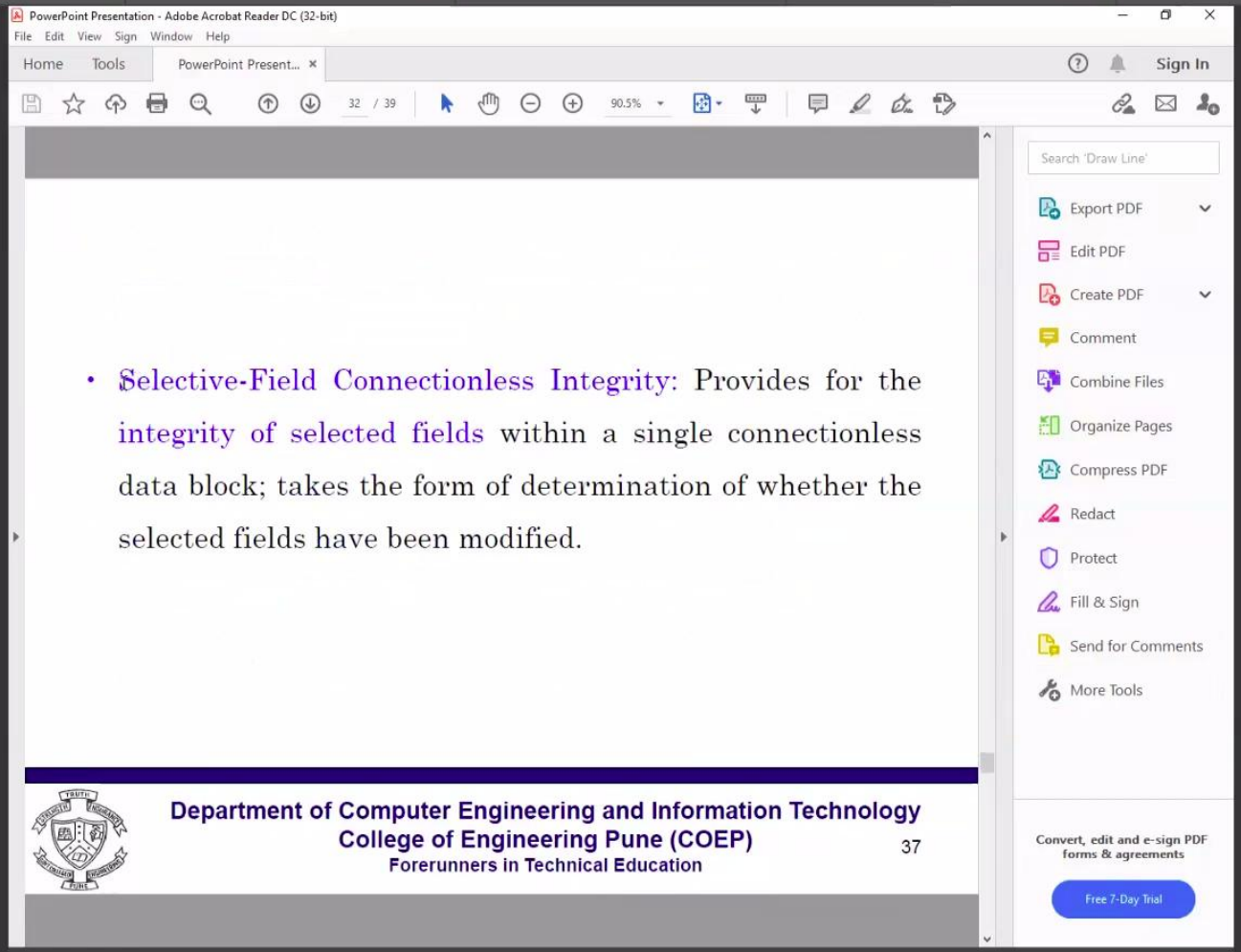
- protection of data from unauthorized disclosure
  - **Connection Confidentiality**: The protection of all user data on a connection.
  - **Connectionless Confidentiality**: The protection of all user data in a single data block
  - **Selective-Field Confidentiality**: The confidentiality of selected fields within the user data on a connection or in a single data block.
  - **Traffic Flow Confidentiality**: The protection of the information that might be derived from observation of traffic flows.

Data Integrity

- assurance that data received is as sent by an authorized entity
- i.e., contain no modification, insertion, deletion, or replay
  - Connection Integrity with Recovery: Provides for the integrity of all user data on a connection and detects any modification, insertion, deletion, or replay of any data within an entire data sequence, with recovery attempted.
  - Connection Integrity without Recovery: As above, but provides only detection without recovery.

- Selective-Field Connection Integrity: Provides for the integrity of selected fields within the user data of a data block transferred over a connection and takes the form of determination of whether the selected fields have been modified, inserted, deleted, or replayed.
- Connectionless Integrity: Provides for the integrity of a single connectionless data block and may take the form of detection of data modification. Additionally, a limited form of replay detection may be provided.

1D	1J		1S	1D
111803111 Atharva Kailas	111803142 ATHARVA MU	Vinod	111803095 Tejas Sakre	111803049 Vrushali Pram



+117

Non-Repudiation

- protection against denial by one of the parties in a communication
  - Non-repudiation, Origin: Proof that the message was sent by the specified party
  - Non-repudiation, Destination: Proof that the message was received by the specified party

Non-Repudiation

- protection against denial by one of the parties in a communication
  - Non-repudiation, Origin: Proof that the message was sent by the specified party.
  - Non-repudiation, Destination: Proof that the message was received by the specified party

Security Mechanisms (X.800)

- Specific security mechanisms:
  - encipherment, digital signatures, access controls, data integrity, authentication exchange, traffic padding, routing control
- Pervasive security mechanisms:
  - trusted functionality, security labels, event detection, security audit trails, security recovery

Vinod | 111803049 Vrushali Pram | 111803142 ATHARVA MU | 111803095 Tejas Sakre | 111803166 Rutvik Ganesh

Press Esc to exit full screen

AutoSave Off | Lect-II | 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

1 Classical Encryption Techniques
2 Symmetric Encryption
3 Asymmetric Encryption
4 Basic Terminology
5 Symmetric Cipher Model
6 Types of Cryptanalytic Attacks
7 Brute Force Search
8 Classical Substitution Ciphers

Classical Encryption Techniques

Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education
1

Click to add notes

Slide 1 of 67 | English (India) | Notes | 97%

+119

1D	1J	1S	1M
Vinod	111803049 Vrushali Pram	111803142 ATHARVA MU	111803095 Tejas Sakre	111803166 Rutvik Ganesh

Symmetric Encryption

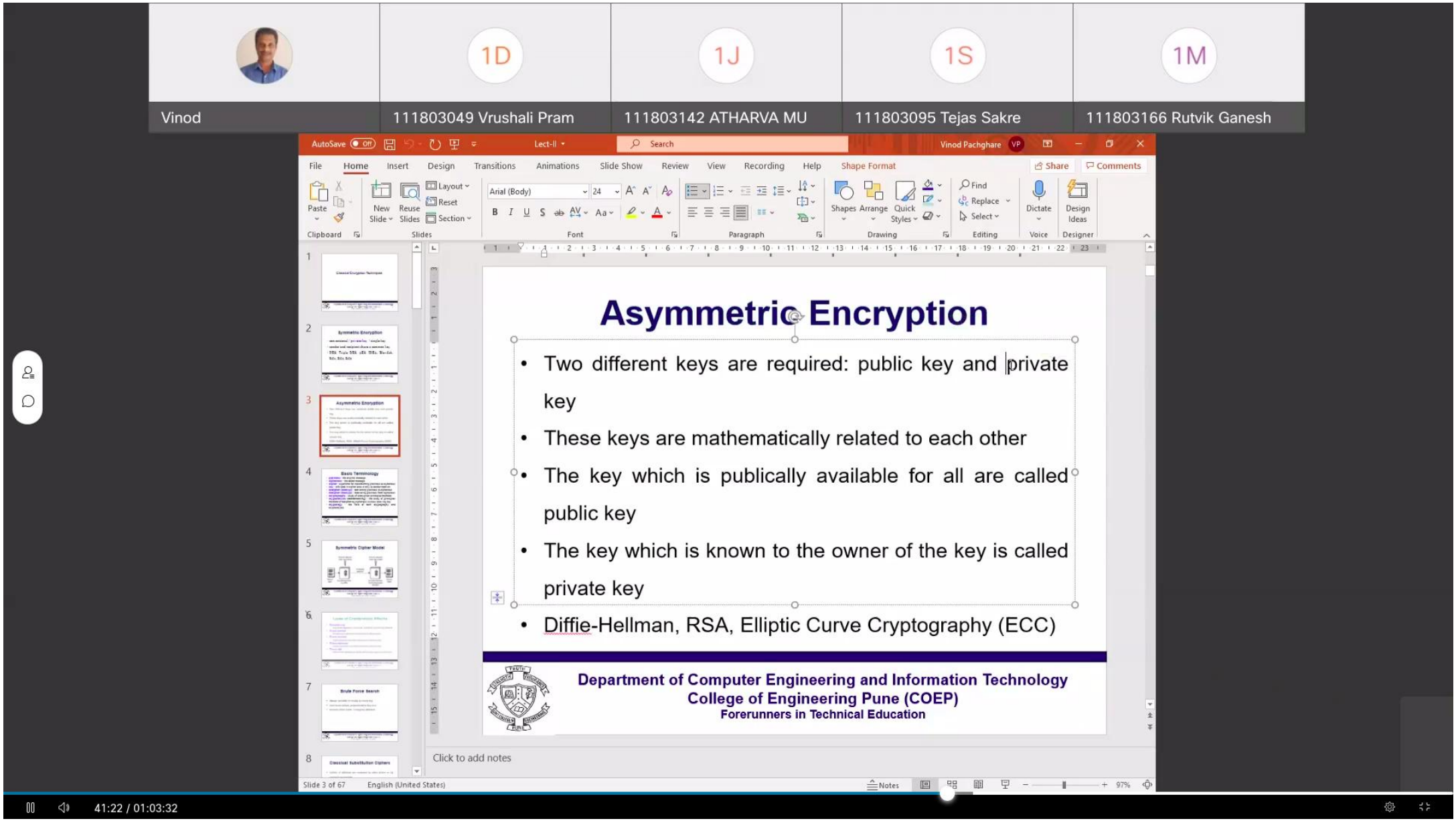
- conventional / private-key / single-key
- sender and recipient share a common key
- DES, Triple DES, AES, IDEA, Blowfish, RC4, RC5, RC6

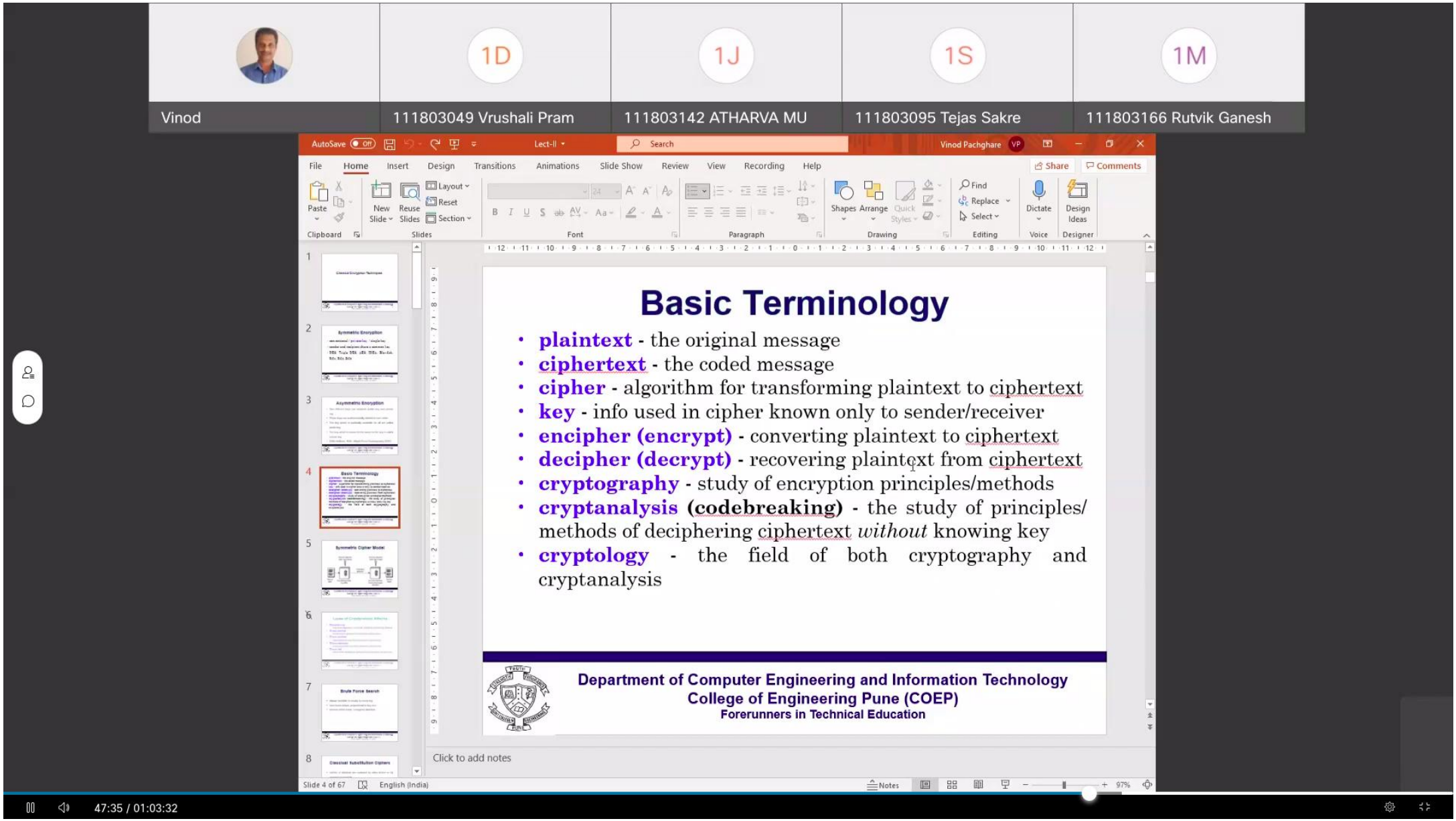
Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education

Click to add notes

Slide 2 of 67 English (United States)

+117


Vinod
1D
111803049 Vrushali Pram
1J
111803142 ATHARVA MU
1S
111803095 Tejas Sakre
1M
111803166 Rutvik Ganesh
Asymmetric Encryption
Two different keys are required: public key and private key
These keys are mathematically related to each other
The key which is publically available for all are called public key
The key which is known to the owner of the key is called private key
Diffie-Hellman, RSA, Elliptic Curve Cryptography (ECC)
Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education
Click to add notes
41:22 / 01:03:32


1D
1J
1S
1M
Vinod
111803049 Vrushali Pram
111803142 ATHARVA MU
111803095 Tejas Sakre
111803166 Rutvik Ganesh
Basic Terminology
plaintext - the original message
ciphertext - the coded message
cipher - algorithm for transforming plaintext to ciphertext
key - info used in cipher known only to sender/receiver
encipher (encrypt) - converting plaintext to ciphertext
decipher (decrypt) - recovering plaintext from ciphertext
cryptography - study of encryption principles/methods
cryptanalysis (codebreaking) - the study of principles/ methods of deciphering ciphertext without knowing key
cryptology - the field of both cryptography and cryptanalysis
Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education
Click to add notes
47:35 / 01:03:32

1D

1J

1S

1M

Vinod | 111803049 Vrushali Pram | 111803142 ATHARVA MU | 111803095 Tejas Sakre | 111803166 Rutvik Ganesh

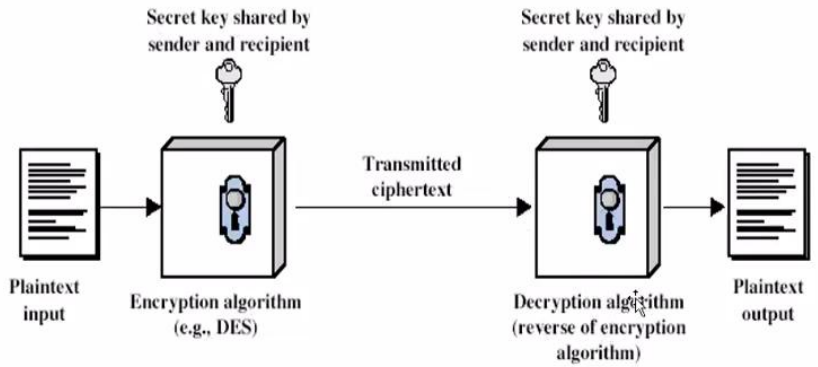
AutoSave Off | Lect-II | Search | Vinod Pachghare

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

1 2 3 4 5 6 7 8

Symmetric Cipher Model



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

Click to add notes

Slide 5 of 67 | English (India) | Notes | 97%

+118

1D	1J	1S	1M
Vinod	111803049 Vrushali Pram	111803142 ATHARVA MU	111803095 Tejas Sakre	111803166 Rutvik Ganesh

Types of Cryptanalytic Attacks

- **Ciphertext only**
  - only know algorithm / ciphertext, statistical, can identify plaintext
- **Known plaintext**
  - know/suspect plaintext & ciphertext to attack cipher
- **Chosen plaintext**
  - select plaintext and obtain ciphertext to attack cipher
- **Chosen ciphertext**
  - select ciphertext and obtain plaintext to attack cipher
- **Chosen text**
  - select either plaintext or ciphertext to en/decrypt to attack cipher

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

Click to add notes

Slide 6 of 67 English (Australia)

+119

1D	1J	1S	1M
Vinod	111803049 Vrushali Pram	111803142 ATHARVA MU	111803095 Tejas Sakre	111803166 Rutvik Ganesh

AutoSave Off | Lect-II | Search | Vinod Pachghare

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

Paste | New Slide | Reuse Slides | Layout | Reset | Section | Arial (Body) | 24 | Shapes | Arrange | Quick Styles | Find | Replace | Select | Dictate | Design Ideas

Clipboard | Slides | Font | Paragraph | Drawing | Editing | Voice | Designer

1 2 3 4 5 6 7 8

Brute Force Search

- always possible to simply try every key
- most basic attack, proportional to key size
- assume either know / recognise plaintext

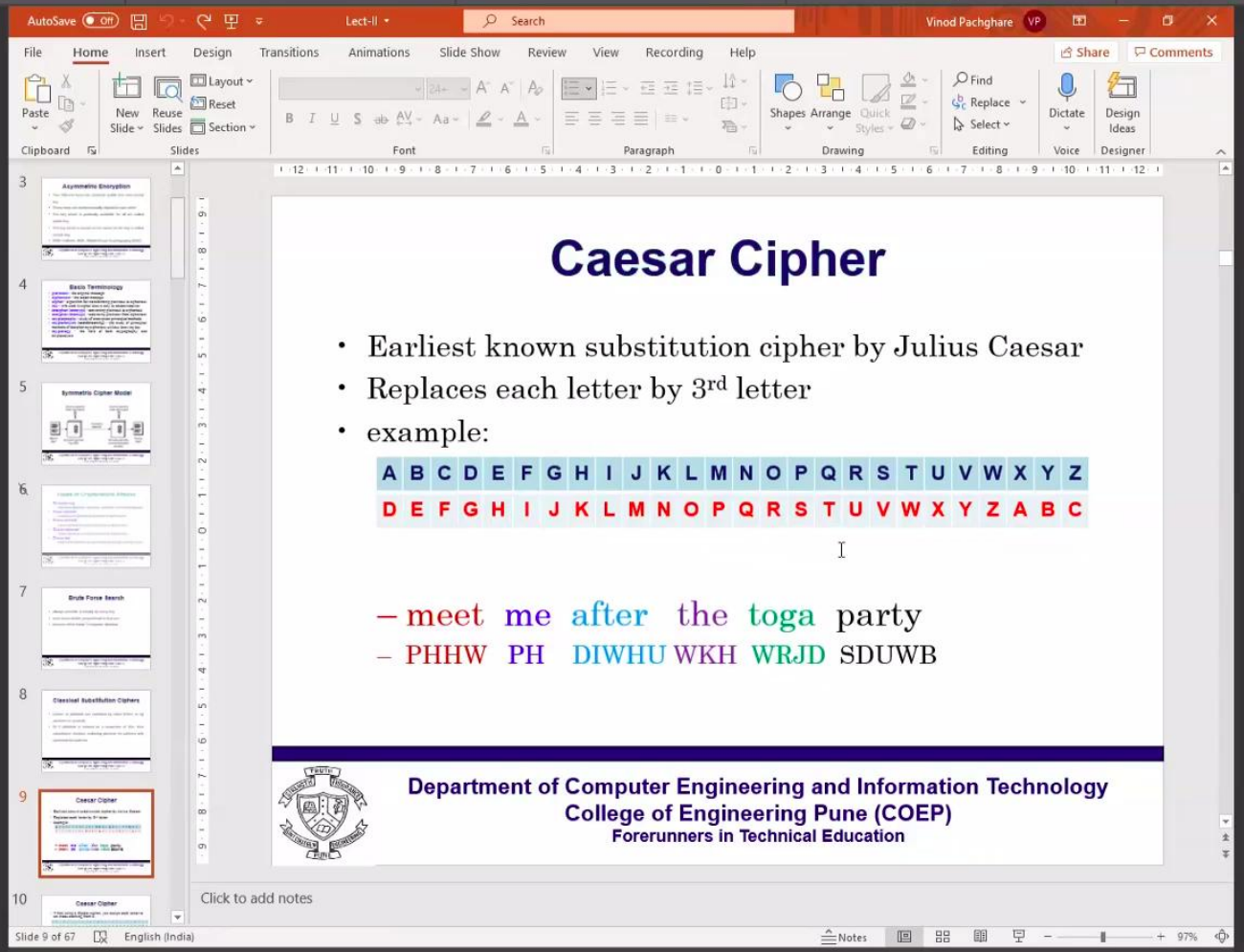
Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education

Click to add notes

Slide 7 of 67 | English (Australia) | Notes | 97%

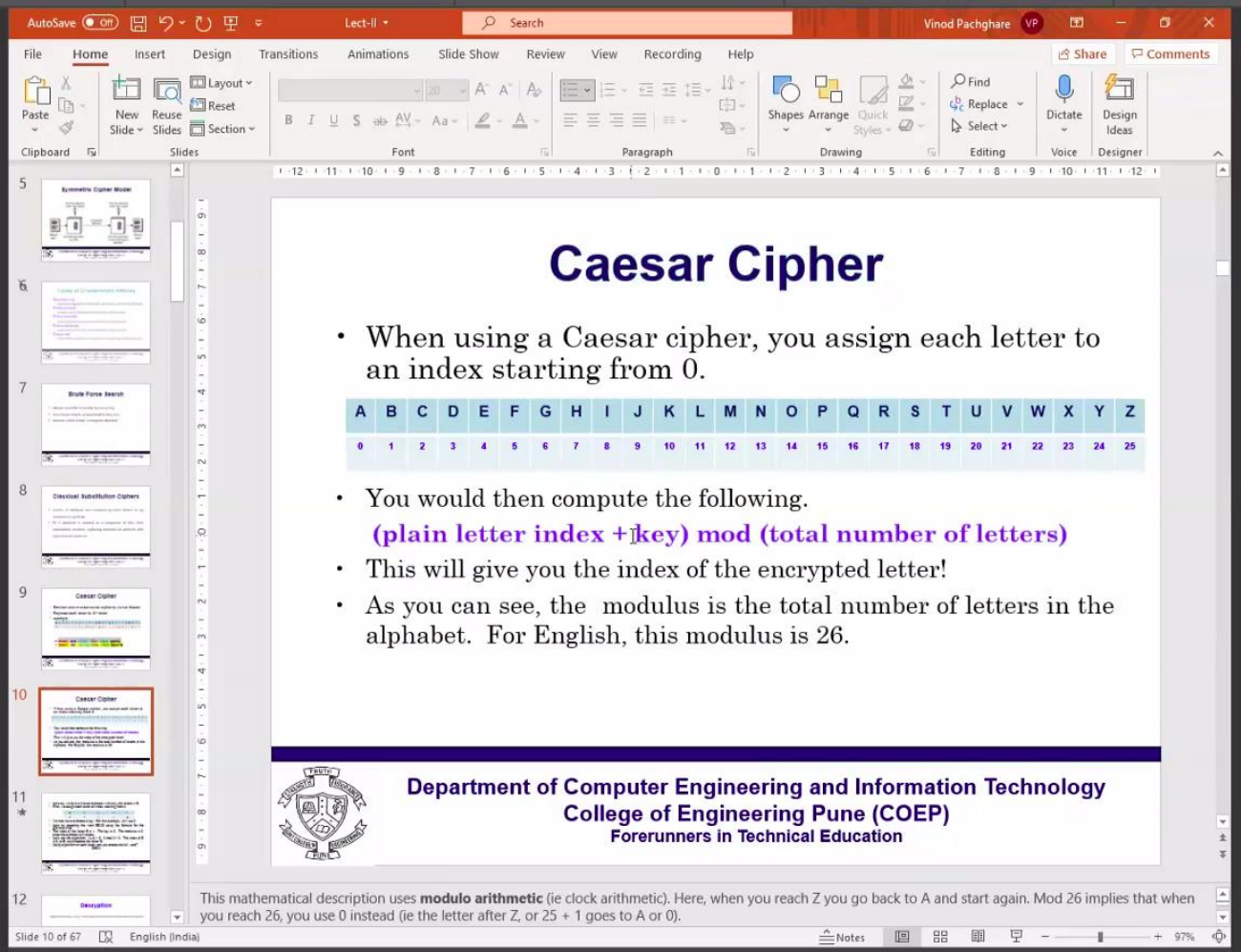
+117

1D	1J	1S	1M
Vinod	111803049 Vrushali Pram	111803142 ATHARVA MU	111803095 Tejas Sakre	111803166 Rutvik Ganesh



+116

1D	1J	1S	1M
Vinod	111803049 Vrushali Pram	111803142 ATHARVA MU	111803095 Tejas Sakre	111803166 Rutvik Ganesh



+117

1D	1J	1S	1M
Vinod	111803049 Vrushali Pram	111803142 ATHARVA MU	111803095 Tejas Sakre	111803166 Rutvik Ganesh

AutoSave Off | Lect-II | 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

- Let's say we have a 5 letter alphabet with only the letters A-E
- First, we assign each letter an index, starting from 0.

A	B	C	D	E
0	1	2	3	4

- We then have to choose a key. For this example, we'll use 2.
- Let's try encoding the word BEAD using the formula for the previous slide.
- The index of the letter B is 1. The key is 2. The modulus is 5, since the alphabet is 5 letters.
- Let's use the algorithm: (1+2) = 3. 3 mod 5 = 3. The index of D is 3, so B would become the letter D.
- Using algorithm on each letter, can you encode the full word?

DBCA

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

Click to add notes

Slide 11 of 67 | English (India) | Notes | 97%

01:00:53

01:01:02 / 01:03:32

1G	4B	1K	1B
Vinod	141903005 Kajol Gaikwad	46_111803038 YOGESH	111803126 Simran Kuche	111803136 Siddhika Sant

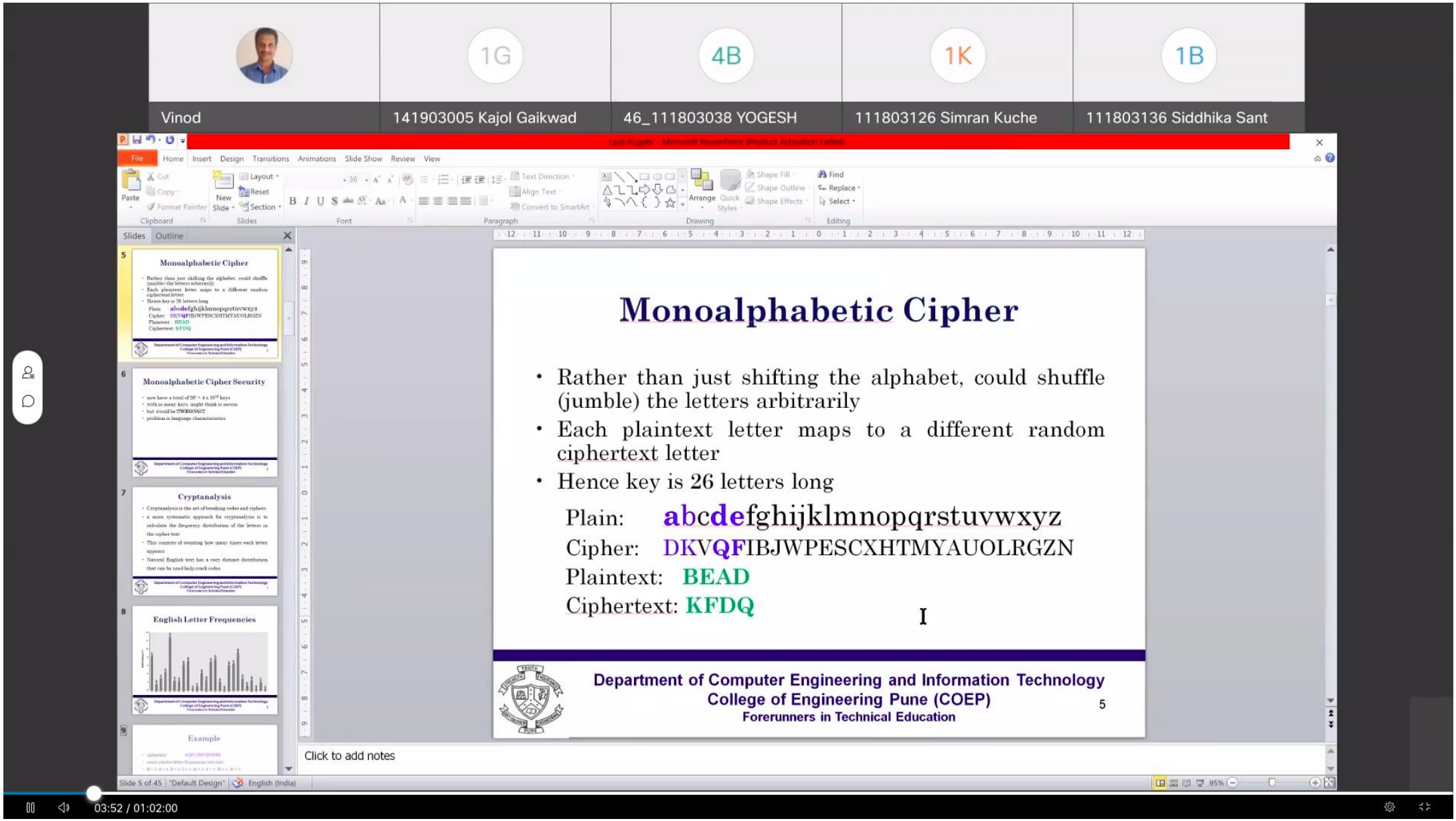
- ***Advantages***
  - This cipher (encryption algorithm) is easy to implement.
- ***Disadvantages***
  - Brute force attack is easily possible.
  - Its observable pattern helps the attacker to find out plaintext easily.
  - Maximum number of keyspace (total number of keys) are 25 which can be easily found out

Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education
4

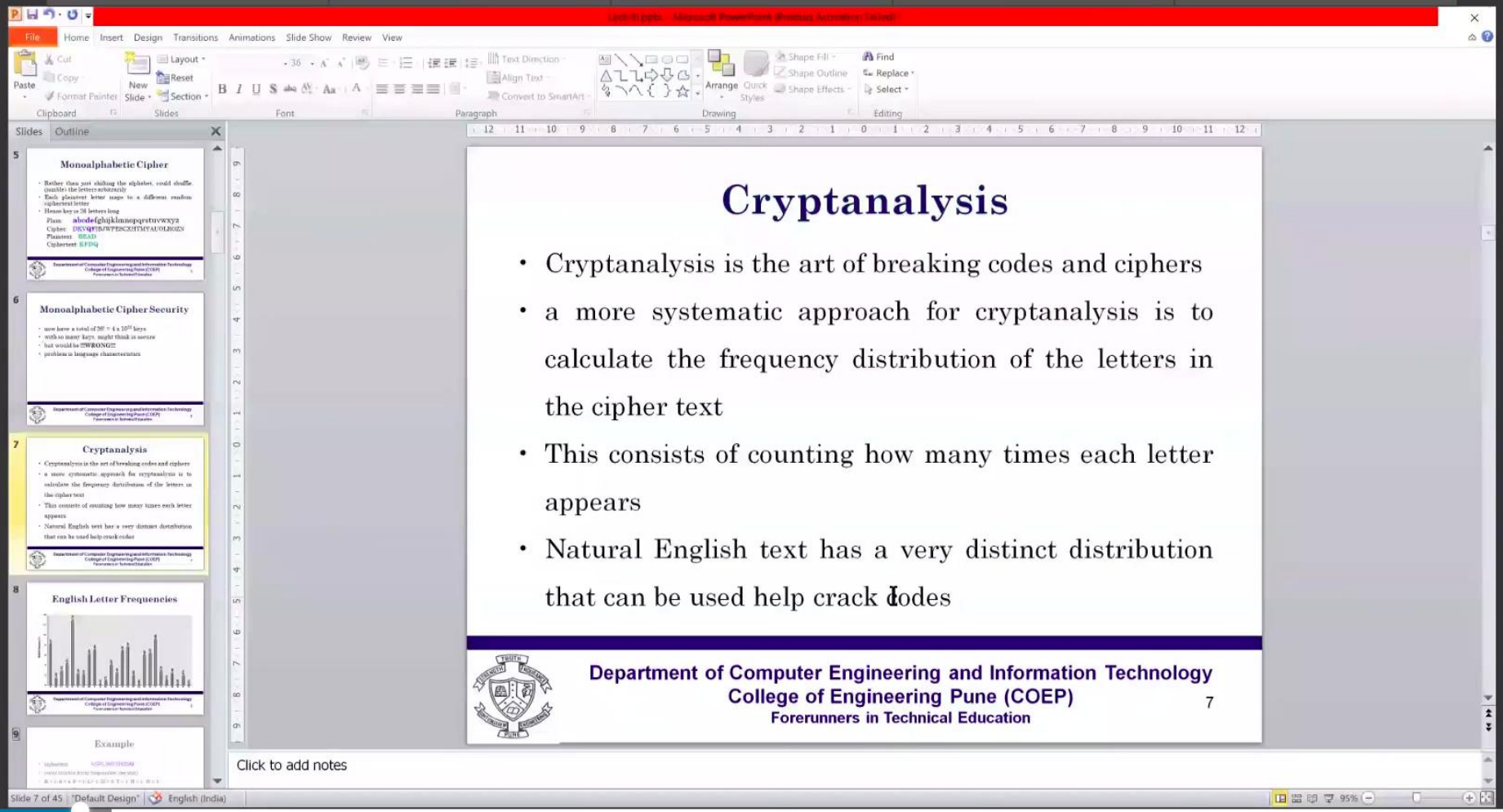
Click to add notes

Slide 4 of 45 | "Default Design" | English (India)

+55


Vinod
1G
141903005 Kajol Gaikwad
4B
46_111803038 YOGESH
1K
111803126 Simran Kuche
1B
111803136 Siddhika Sant
Monoalphabetic Cipher
Rather than just shifting the alphabet, could shuffle (jumble) the letters arbitrarily
Each plaintext letter maps to a different random ciphertext letter
Hence key is 26 letters long
Plain: abcdefghijklmnopqrstuvwxyz
Cipher: DKVQFIBJWPESCXHTMYAUOLRGZN
Plaintext: BEAD
Ciphertext: KFDQ
Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education
5
Click to add notes
03:52 / 01:02:00

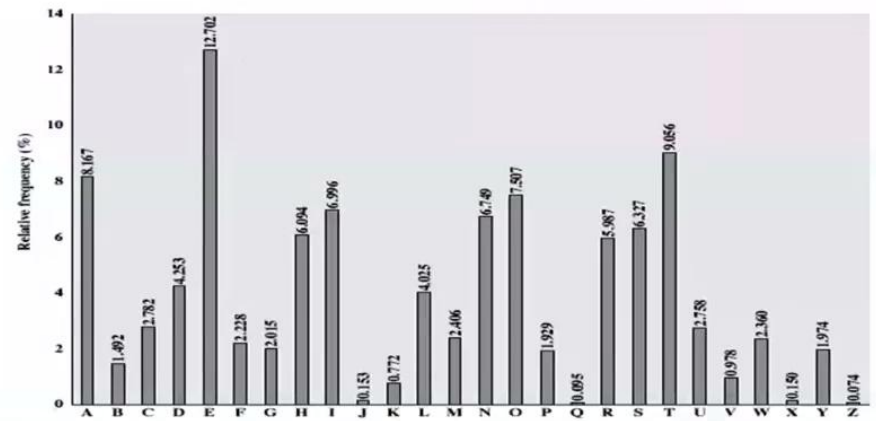
Vinod	141903005 Kajol Gaikwad	46_111803038 YOGESH	111803126 Simran Kuche	111803136 Siddhika Sant



07:24 / 01:02:00

Vinod	141903005 Kajol Gaikwad	46_111803038 YOGESH	111803126 Simran Kuche	111803136 Siddhika Sant

English Letter Frequencies



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

8

Click to add notes

Slide 8 of 45 | "Default Design" | English (India)

08:14 / 01:02:00

	1G	4B	1K	1B
Vinod	141903005 Kajol Gaikwad	46_111803038 YOGESH	111803126 Simran Kuche	111803136 Siddhika Sant

+115

1G	4B	1K	1B
Vinod	141903005 Kajol Gaikwad	46_111803038 YOGESH	111803126 Simran Kuche	111803136 Siddhika Sant

Monoalphabetic Cipher Security

- now have a total of 26! = 4 x 10^{26} keys
- with so many keys, might think is secure
- but would be **!!!WRONG!!!**
- problem is language characteristics

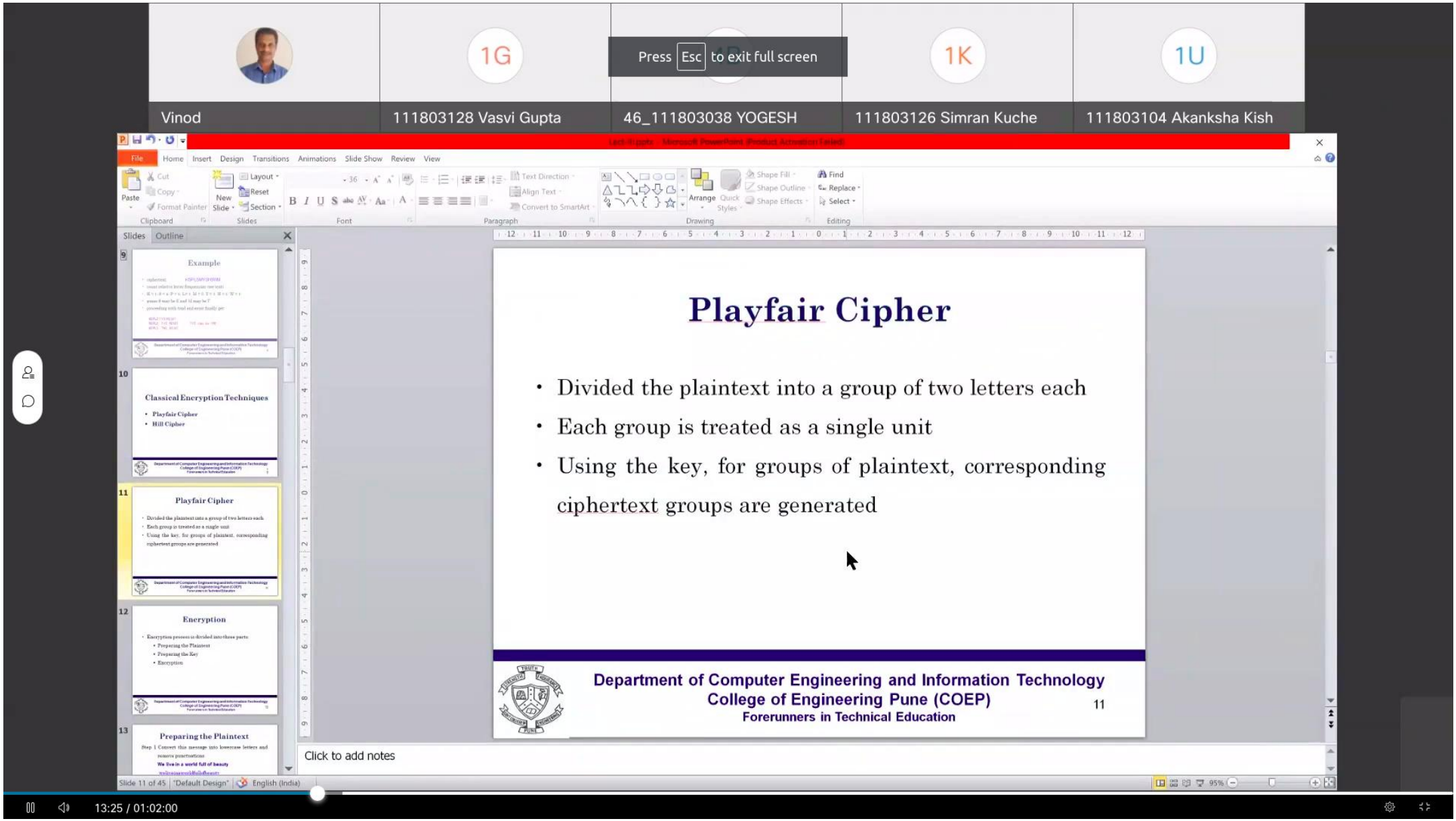
Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education

6

Click to add notes

Slide 7 of 45 | "Default Design" | English (India)

11:59 / 01:02:00


Press Esc to exit full screen
Vinod
111803128 Vasvi Gupta
46_111803038 YOGESH
111803126 Simran Kuche
111803104 Akanksha Kish
Playfair Cipher
Divided the plaintext into a group of two letters each
Each group is treated as a single unit
Using the key, for groups of plaintext, corresponding ciphertext groups are generated
Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education
11
Click to add notes
13:25 / 01:02:00

	1G	4B	1K	1U
Vinod	111803128 Vasi Gupta	46_111803038 YOGESH	111803126 Simran Kuche	111803104 Akanksha Kish

Preparing the Plaintext

Step 1 Convert this message into lowercase letters and remove punctuations.

We live in a world full of beauty

weliveinaworldfullofbeauty

Step 2 Split the text into a pair of two.

we li ve in aw or ld fu ll of be au ty

If the last group is having only one letter, then append any one letter in that group to make a pair

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

13

Click to add notes

Slide 13 of 45 | "Default Design" | English (India)

+118

1G

Press Esc to exit full screen

1K

1P

Vinod | 111803128 Vasvi Gupta | 46_111803038 YOGESH | 111803126 Simran Kuche | 111803155 VIREN RAJES

File Home Insert Design Transitions Animations Slide Show Review View

Slides Outline

13 Preparing the Plaintext

14

15

16

17 Preparing the Key

Click to add title

- Step 3 Now, write the groups such that in one row 5 pairs are there as shown below:
- If j is present all j are replaced with i. (or any letter)

we	li	ve	in	aw
or	ld	fu	lx	lo
fb	ea	ut	yz	

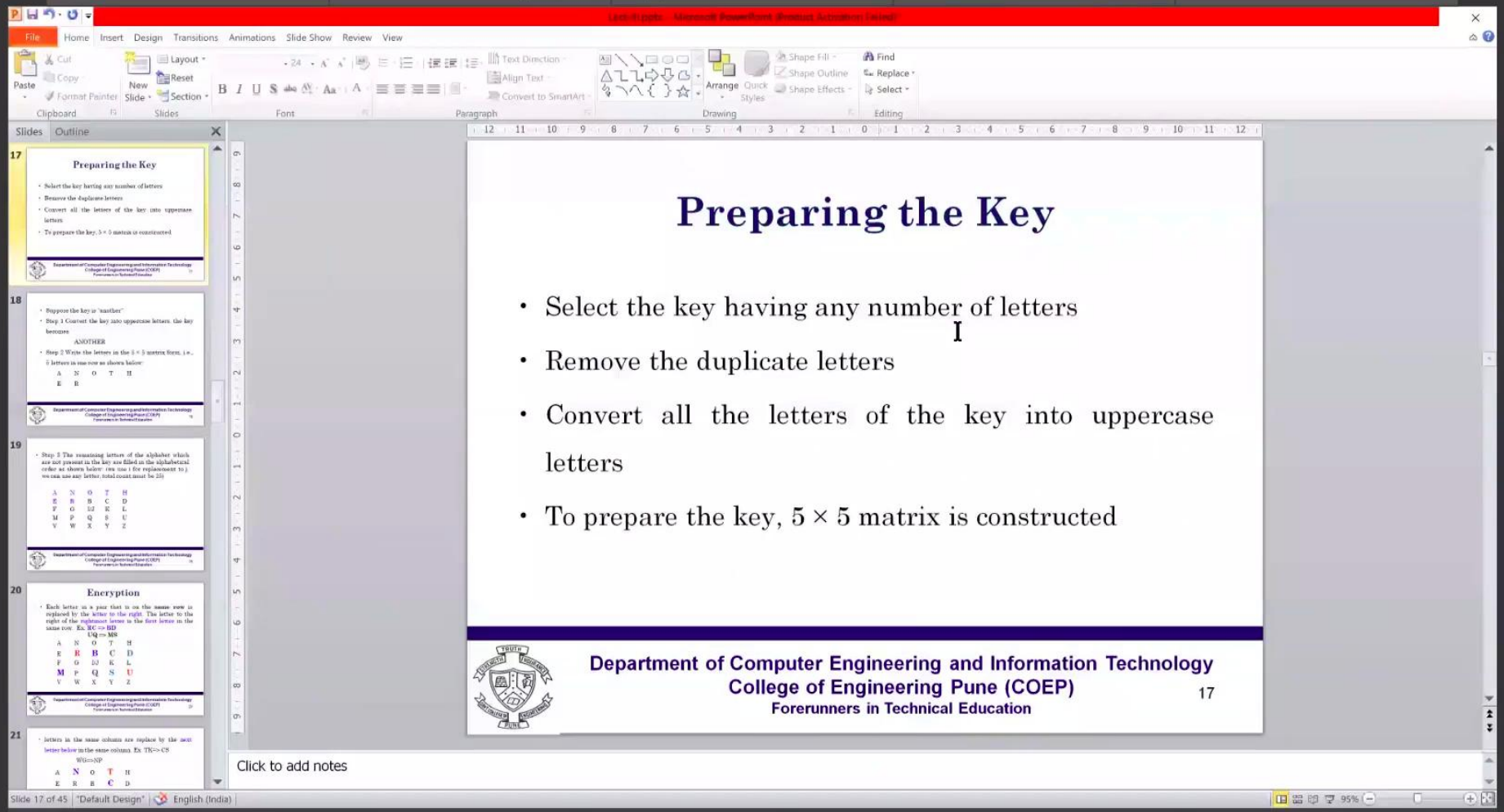
Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education
16

Click to add notes

Slide 16 of 45 "Default Design" English (India)

+124

	1G	4B	1K	1P
Vinod	111803128 Vasi Gupta	46_111803038 YOGESH	111803126 Simran Kuche	111803155 VIREN RAJES



+124

1G	4B	1K	1P
Vinod	111803128 Vasvi Gupta	46_111803038 YOGESH	111803126 Simran Kuche	111803155 VIREN RAJES

- Suppose the key is “another”
- Step 1 Convert the key into uppercase letters, the key becomes

  ANOTHER
- Step 2 Write the letters in the 5 × 5 matrix form, i.e., 5 letters in one row as shown below:

A	N	O	T	H
E	R			

Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education
18

Click to add notes

Slide 18 of 45 | "Default Design" | English (India) | 95%

20:45 / 01:02:00

- Step 3 The remaining letters of the alphabet which are not present in the key are filled in the alphabetical order as shown below: (we use i for replacement to j, we can use any letter, total count must be 25)

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

1G	1B	1K	1P
Vinod	111803128 Vasvi Gupta	111803143 Rohini Bhonga	111803126 Simran Kuche	111803155 VIREN RAJES

Encryption

- Each letter in a pair that is on the **same row** is replaced by the letter to the right. The letter to the right of the rightmost letter is the first letter in the same row. Ex. **RC => BD**

UQ => MS

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

- letters in the same column are replace by the next letter below in the same column. Ex. TK=> CS

WG=>NP

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

- when the letters are neither in the same row nor column, the substitution is based upon their intersection
- first move across (left or right), and then up or down.

Ex. **WE => VR**
CZ => DY

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

1G	1B	1K	1P
Vinod	111803128 Vasvi Gupta	111803143 Rohini Bhonga	111803126 Simran Kuche	111803155 VIREN RAJES

Encryption

- Each letter in a pair that is on the **same row** is replaced by the letter to the right. The letter to the right of the rightmost letter is the first letter in the same row. Ex. **RC => BD**

UQ => MS

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

1G	1B	1K	1P
Vinod	111803128 Vasvi Gupta	111803143 Rohini Bhonga	111803126 Simran Kuche	111803155 VIREN RAJES

- letters in the same column are replace by the next letter below in the same column. Ex. TK=> CS

WG=>NP

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

Activities Brave Web Browser Wed Sep 1 11:39:47 PM 91 %

Course: Object Oriented Mod | CNS-odd-sem-21-22: Lecture F | Cisco Webex Meetings | WhatsApp

coep.webex.com/recordingservice/sites/coep/recording/39b9b0aae23d1039b7ed005056818831/playback

Imported fro... Programming Inbox (4,357) -... Meet – csk-shd... Inspect with C...

CNS Theory Pachghare-20210818 1030-1

	1G	1B	1K	1P
Vinod	111803128 Vasvi Gupta	111803143 Rohini Bhonga	111803126 Simran Kuche	111803155 VIREN RAJES

PT:- WE LI VE IN AW OR LD FU LX LO FB EA UT YZ

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

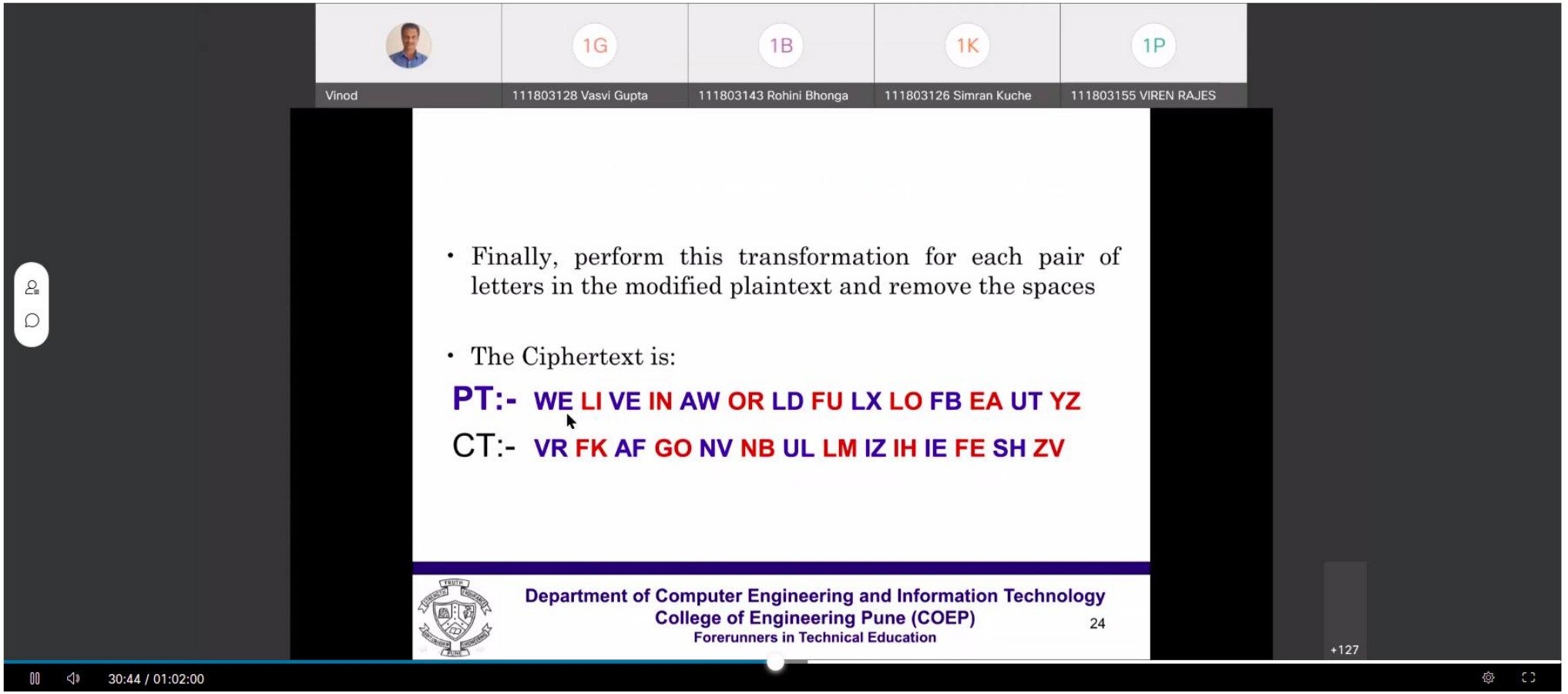
CT:- VR FK AF GO NV NB UL LM IZ IH IE FE SH ZV

Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education
23

+126

29:02 / 01:02:00

CNS Theory Pachghare-20210818 1030-1



Activities Brave Web Browser Wed Sep 1 11:40:11 PM 92 %

Course: Object Oriented Mod | CNS-odd-sem-21-22: Lecture F | Cisco Webex Meetings | WhatsApp

coep.webex.com/recordingservice/sites/coep/recording/39b9b0aae23d1039b7ed005056818831/playback

Imported fro... Programming Inbox (4,357) -... Meet – csk-shd... Inspect with C...

CNS Theory Pachghare-20210818 1030-1

	1G	1B	1K	1P
Vinod	111803128 Vasvi Gupta	111803143 Rohini Bhonga	111803126 Simran Kuche	111803155 VIREN RAJES

Decryption

- To decrypt the message, simply reverse the entire process. Break the ciphertext into pairs of letters:

VR FK AF GO NV
NB UL LM IZ IH
IE FE SH ZV

Write down the alphabet square with the key:

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

+126

31:30 / 01:02:00

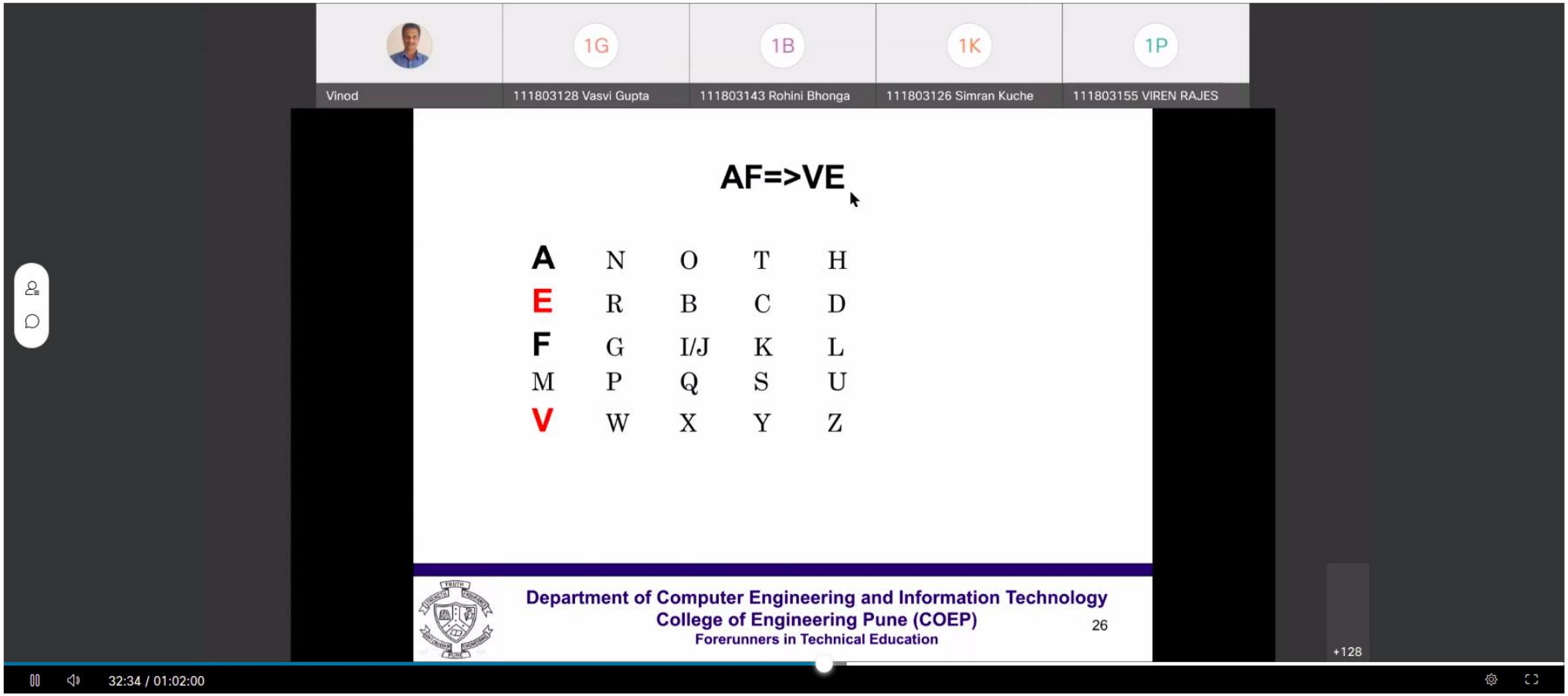
Activities Brave Web Browser Wed Sep 1 11:40:20 PM 92 %

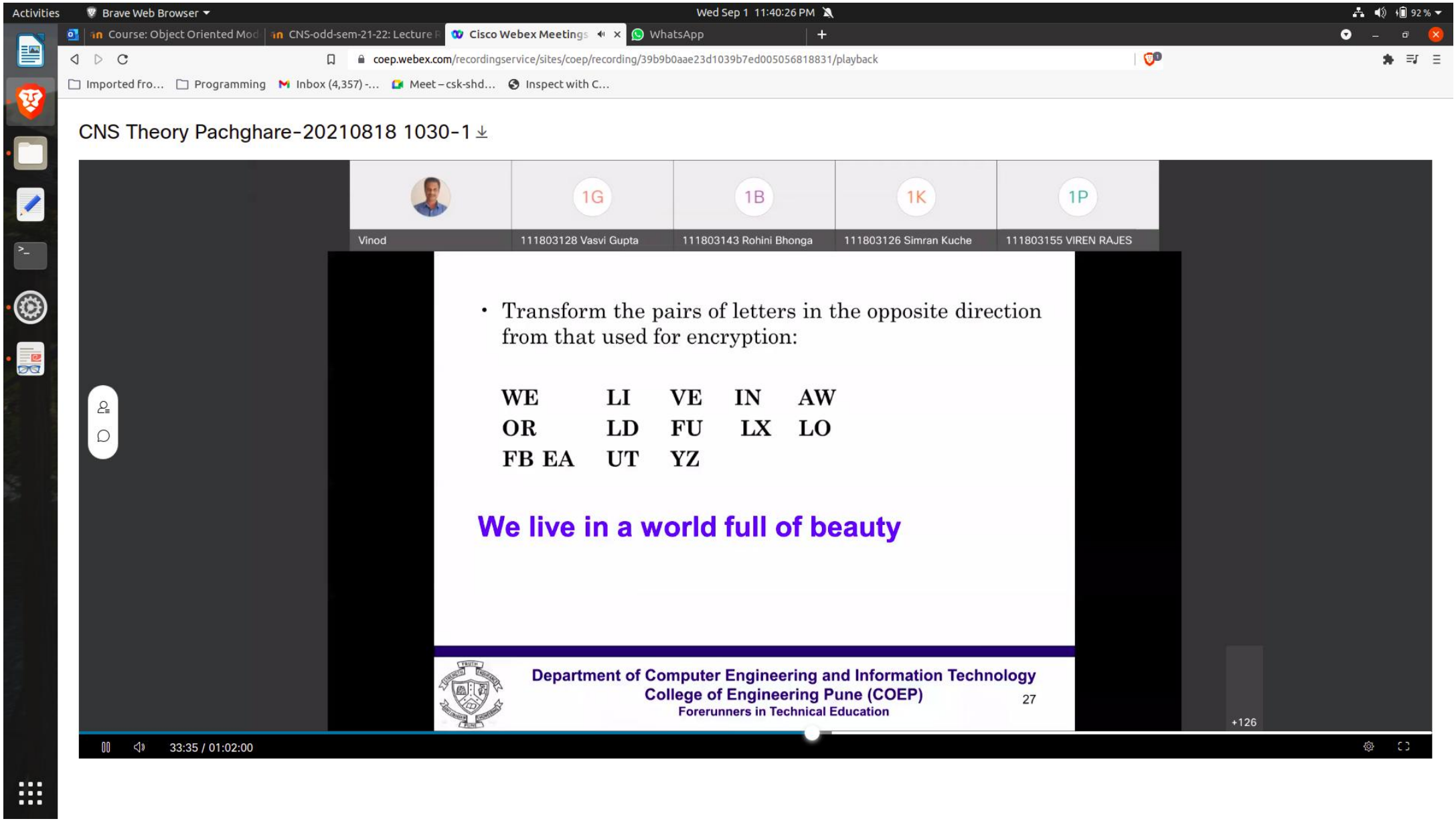
Course: Object Oriented Mod | CNS-odd-sem-21-22: Lecture F | Cisco Webex Meetings | WhatsApp

coep.webex.com/recordingservice/sites/coep/recording/39b9b0aae23d1039b7ed005056818831/playback

Imported fro... Programming Inbox (4,357) -... Meet – csk-shd... Inspect with C...

CNS Theory Pachghare-20210818 1030-1




Activities
Brave Web Browser
Wed Sep 1 11:40:26 PM
92 %
Course: Object Oriented Mod
CNS-odd-sem-21-22: Lecture F
Cisco Webex Meetings
WhatsApp
coep.webex.com/recordingservice/sites/coep/recording/39b9b0aae23d1039b7ed005056818831/playback
Imported fro...
Programming
Inbox (4,357) -...
Meet – csk-shd...
Inspect with C...
CNS Theory Pachghare-20210818 1030-1
1G
1B
1K
1P
Vinod
111803128 Vasvi Gupta
111803143 Rohini Bhonga
111803126 Simran Kuche
111803155 VIREN RAJES
• Transform the pairs of letters in the opposite direction from that used for encryption:
WE LI VE IN AW
OR LD FU LX LO
FB EA UT YZ
We live in a world full of beauty
Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education
27
+126
33:35 / 01:02:00

Activities Brave Web Browser Wed Sep 1 11:40:36 PM 92 %

Course: Object Oriented Mod | CNS-odd-sem-21-22: Lecture F | Cisco Webex Meetings | WhatsApp

coep.webex.com/recordingservice/sites/coep/recording/39b9b0aae23d1039b7ed005056818831/playback

Imported fro... Programming Inbox (4,357) -... Meet – csk-shd... Inspect with C...

CNS Theory Pachghare-20210818 1030-1

Vinod	111803128 Vasvi Gupta	111803143 Rohini Bhonga	111803126 Simran Kuche	111803155 VIREN RAJES
	1G	1B	1K	1P

The Hill Cipher

- The Hill cipher is a polygraphic substitution cipher based on linear algebra
- Each letter is treated as a digit in base 26: A = 0, B =1, and so on.

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

- Consider the message 'COE', and the key below (or "ANOTGERBZ" in letters):
- Ciphertext = Key x Plaintext mod 26

  C = KP mod 26

Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education
29

+126

34:20 / 01:02:00

Activities Brave Web Browser Wed Sep 1 11:40:55 PM 92 %

Course: Object Oriented Mod | CNS-odd-sem-21-22: Lecture F | Cisco Webex Meetings | WhatsApp

coep.webex.com/recordingservice/sites/coep/recording/39b9b0aae23d1039b7ed005056818831/playback

Imported fro... Programming Inbox (4,357) -... Meet – csk-shd... Inspect with C...

CNS Theory Pachghare-20210818 1030-1

	1G	1B	1K	1P
Vinod	111803128 Vasvi Gupta	111803143 Rohini Bhonga	111803126 Simran Kuche	111803155 VIREN RAJES

Encryption

Encryption process is divided into three parts:

- Preparing the Plaintext
- Preparing the Key
- Encryption

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

30

+127

37:31 / 01:02:00

Activities Brave Web Browser Wed Sep 1 11:41:02 PM 92 %

Course: Object Oriented Mod | CNS-odd-sem-21-22: Lecture F | Cisco Webex Meetings | WhatsApp

coep.webex.com/recordingservice/sites/coep/recording/39b9b0aae23d1039b7ed005056818831/playback

Imported fro... Programming Inbox (4,357) -... Meet – csk-shd... Inspect with C...

CNS Theory Pachghare-20210818 1030-1

	1G	1B	1K	1P
Vinod	111803128 Vasvi Gupta	111803143 Rohini Bhonga	111803126 Simran Kuche	111803155 VIREN RAJES

Preparing the Plaintext

- First each letter in the message is converted into numbers such as a = 0, b = 1 and so on.
- Then the numbers should be written in columnar form. The number of letters in each column depends on the size of the key matrix.

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

31

+127

38:12 / 01:02:00

Activities Brave Web Browser Wed Sep 1 11:41:13 PM 92 %

Course: Object Oriented Mod | CNS-odd-sem-21-22: Lecture F | Cisco Webex Meetings | WhatsApp

coep.webex.com/recordingservice/sites/coep/recording/39b9b0aae23d1039b7ed005056818831/playback

Imported fro... Programming Inbox (4,357) -... Meet – csk-shd... Inspect with C...

CNS Theory Pachghare-20210818 1030-1

	1G	1B	1K	1P
Vinod	111803128 Vasvi Gupta	111803143 Rohini Bhonga	111803126 Simran Kuche	111803155 VIREN RAJES

- Suppose the key matrix is 2 × 2, then each column of plaintext has two elements only.
- Suppose the key matrix is 3 × 3 matrix, then each column of plaintext has three elements only.
- If the last column contains less elements then append necessary numbers to complete the last column.

Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education
32

+128

40:04 / 01:02:00

Activities Brave Web Browser Wed Sep 1 11:41:22 PM 92 %

Course: Object Oriented Mod | CNS-odd-sem-21-22: Lecture F | Cisco Webex Meetings | WhatsApp

coep.webex.com/recordingservice/sites/coep/recording/39b9b0aae23d1039b7ed005056818831/playback

Imported fro... Programming Inbox (4,357) -... Meet – csk-shd... Inspect with C...

CNS Theory Pachghare-20210818 1030-1

	1G	1B	1K	1P
Vinod	111803128 Vasvi Gupta	111803143 Rohini Bhonga	111803126 Simran Kuche	111803155 VIREN RAJES

Preparing the Key

- Key matrix should be a square matrix.
- i,.e. the size of the key must be a square value.
- For example, size of a matrix should be 4 or 9 or 16 etc.
- Every letter in the key is also assigning the number like message.

+128

40:56 / 01:02:00

Activities Brave Web Browser Wed Sep 1 11:41:30 PM 92 %

Course: Object Oriented Mod | CNS-odd-sem-21-22: Lecture F | Cisco Webex Meetings | WhatsApp

coep.webex.com/recordingservice/sites/coep/recording/39b9b0aae23d1039b7ed005056818831/playback

Imported fro... Programming Inbox (4,357) -... Meet – csk-shd... Inspect with C...

CNS Theory Pachghare-20210818 1030-1

	1G	1B	1K	1P
Vinod	111803128 Vasvi Gupta	111803143 Rohini Bhonga	111803126 Simran Kuche	111803155 VIREN RAJES

- The numbers should be written in row wise.
- The number of letters in each row depends on the size of the key matrix.
- Suppose, the key matrix is 2 × 2, then each row having two elements only.
- The key matrix is always a square matrix

like message.

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

+127

41:39 / 01:02:00

Activities Brave Web Browser Wed Sep 1 11:41:39 PM 92 %

Course: Object Oriented Mod | CNS-odd-sem-21-22: Lecture F | Cisco Webex Meetings | WhatsApp

coep.webex.com/recordingservice/sites/coep/recording/39b9b0aae23d1039b7ed005056818831/playback

Imported fro... Programming Inbox (4,357) -... Meet – csk-shd... Inspect with C...

CNS Theory Pachghare-20210818 1030-1

	1G	1B	1K	1P
Vinod	111803128 Vasvi Gupta	111803143 Rohini Bhonga	111803126 Simran Kuche	111803155 VIREN RAJES

Consider the message 'COE'.

- Since 'C' is 2, 'O' is 14 and 'E' is 4, the message is the vector:

$$P = \begin{bmatrix} 2 \\ 14 \\ 4 \end{bmatrix}$$

+127

43:26 / 01:02:00

Activities Brave Web Browser Wed Sep 1 11:41:45 PM 92 %

Course: Object Oriented Mod | CNS-odd-sem-21-22: Lecture F | Cisco Webex Meetings | WhatsApp

coep.webex.com/recordingservice/sites/coep/recording/39b9b0aae23d1039b7ed005056818831/playback

Imported fro... Programming Inbox (4,357) -... Meet – csk-shd... Inspect with C...

CNS Theory Pachghare-20210818 1030-1

	1G	1B	1K	1P
Vinod	111803128 Vasi Gupta	111803143 Rohini Bhonga	111803126 Simran Kuche	111803155 VIREN RAJES

Encryption

Ciphertext = Key x Plaintext mod 26

C = KP mod 26

$$C = \begin{bmatrix} 0 & 13 & 14 \\ 19 & 6 & 4 \\ 17 & 1 & 25 \end{bmatrix} \begin{bmatrix} 2 \\ 14 \\ 4 \end{bmatrix} = \begin{bmatrix} 238 \\ 138 \\ 148 \end{bmatrix} \bmod 26$$

$$C = \begin{bmatrix} 4 \\ 8 \\ 18 \end{bmatrix}$$

Here the numbers are reconverted into the letters, so, 4 = E, 8 = I, 18 = S. So the ciphertext is 'EIS'.

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

37

+127

44:18 / 01:02:00

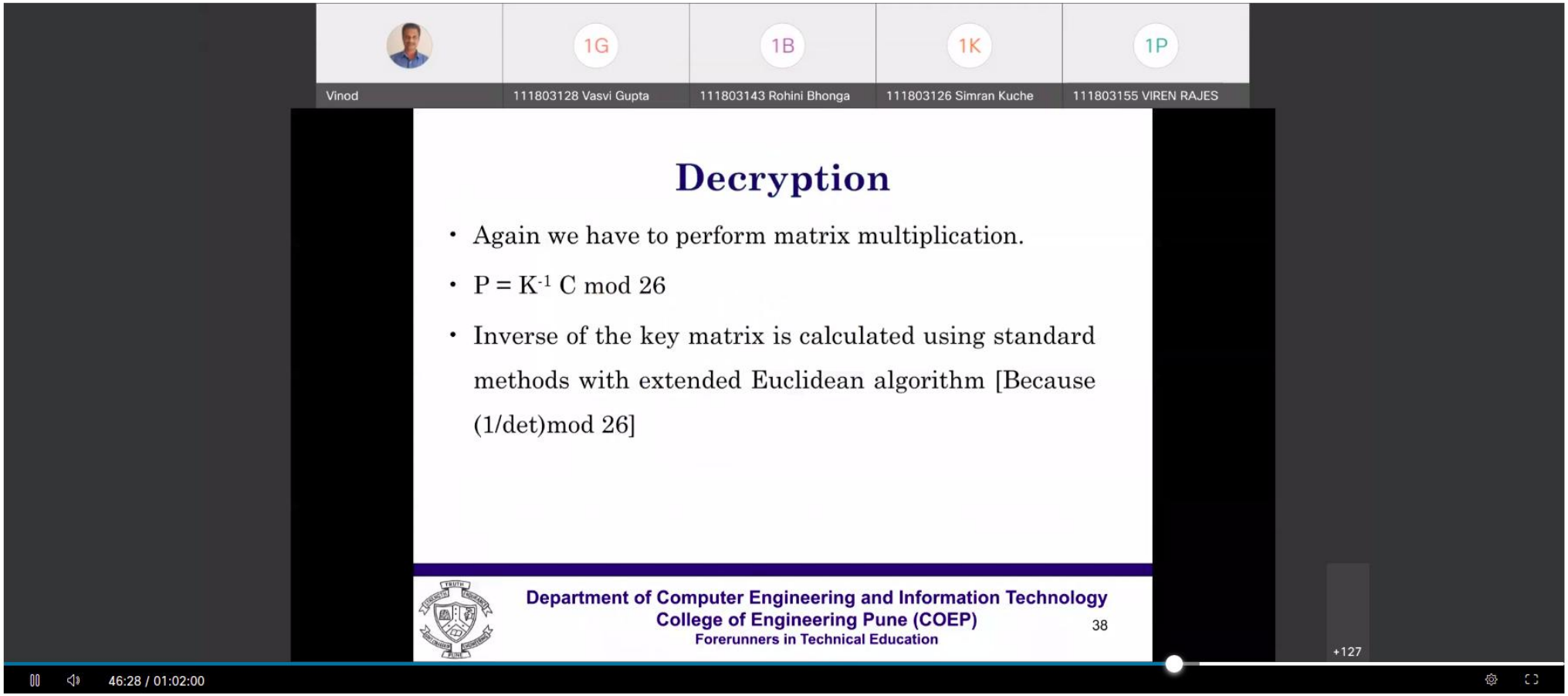
Activities Brave Web Browser Wed Sep 1 11:41:55 PM 92 %

Course: Object Oriented Mod | CNS-odd-sem-21-22: Lecture F | Cisco Webex Meetings | WhatsApp

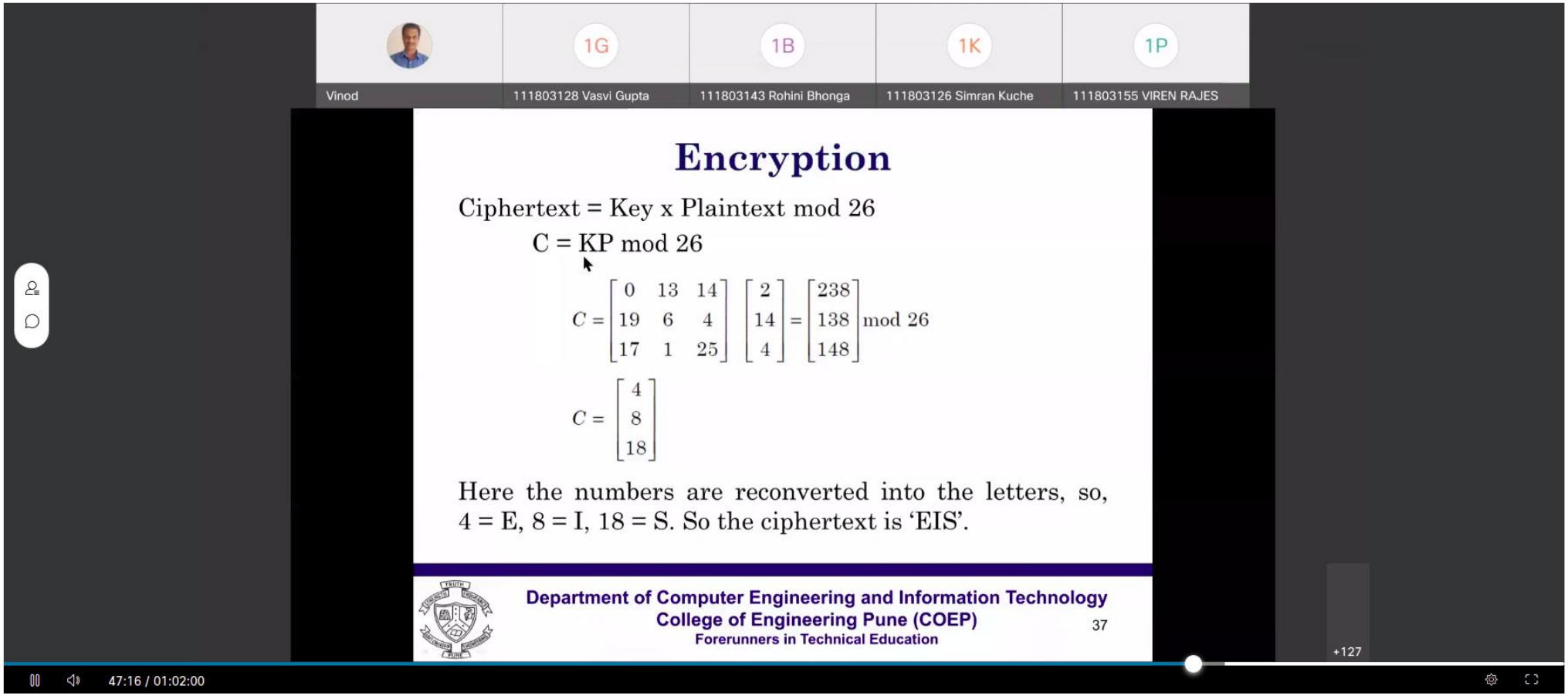
coep.webex.com/recordingservice/sites/coep/recording/39b9b0aae23d1039b7ed005056818831/playback

Imported fro... Programming Inbox (4,357) -... Meet – csk-shd... Inspect with C...

CNS Theory Pachghare-20210818 1030-1



CNS Theory Pachghare-20210818 1030-1



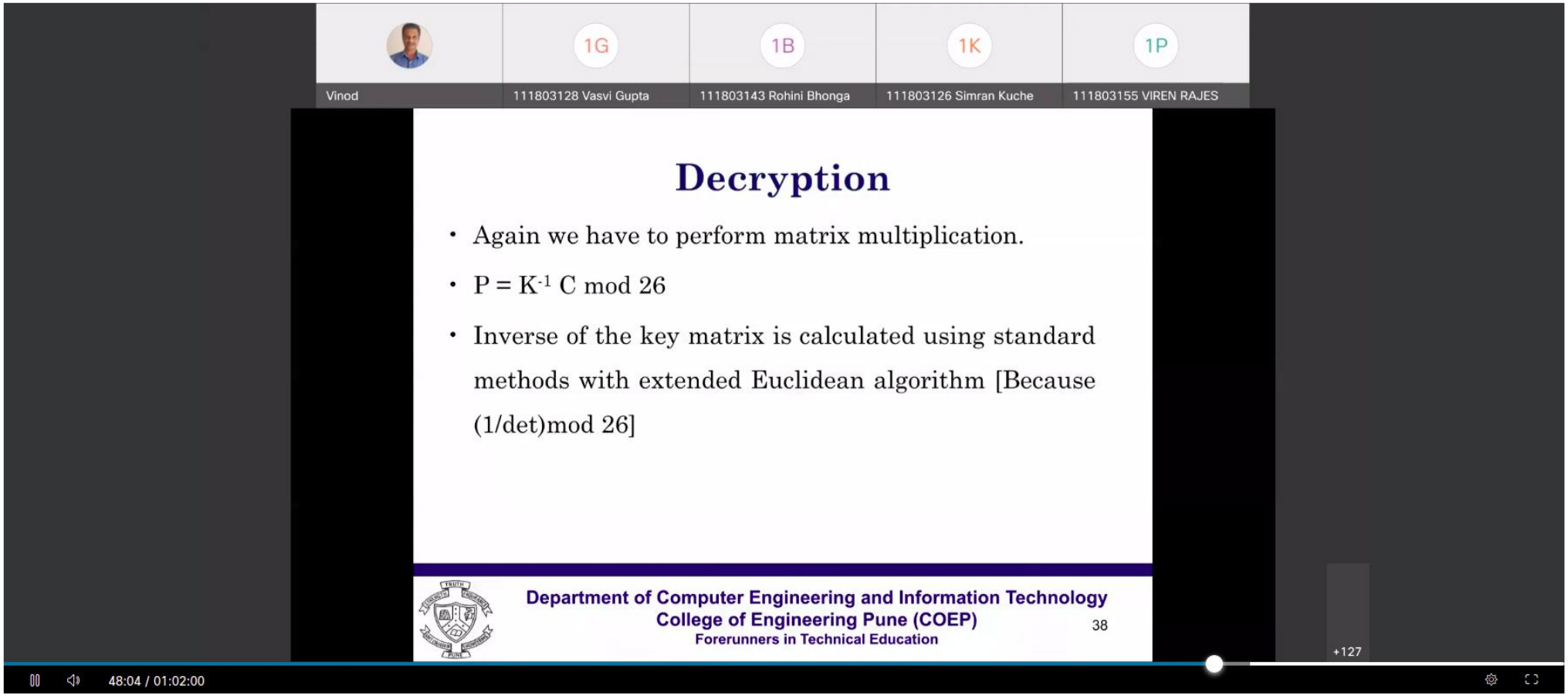
Activities Brave Web Browser Wed Sep 1 11:42:06 PM 92 %

Course: Object Oriented Mod | CNS-odd-sem-21-22: Lecture F | Cisco Webex Meetings | WhatsApp

coep.webex.com/recordingservice/sites/coep/recording/39b9b0aae23d1039b7ed005056818831/playback

Imported fro... Programming Inbox (4,357) -... Meet – csk-shd... Inspect with C...

CNS Theory Pachghare-20210818 1030-1



Activities Brave Web Browser Wed Sep 1 11:42:25 PM 93 %

Course: Object Oriented Mod | CNS-odd-sem-21-22: Lecture F | Cisco Webex Meetings | WhatsApp

coep.webex.com/recordingservice/sites/coep/recording/39b9b0aae23d1039b7ed005056818831/playback

Imported fro... Programming Inbox (4,357) -... Meet – csk-shd... Inspect with C...

CNS Theory Pachghare-20210818 1030-1

	1G	1B	1K	1P
Vinod	111803128 Vasvi Gupta	111803143 Rohini Bhonga	111803126 Simran Kuche	111803155 VIREN RAJES

$$P = K^{-1} \times \mathrm{C} \bmod 26$$

$$K^{-1} = \frac{1}{6453}\begin{bmatrix} -146 & 311 & 32 \\ 407 & 238 & -266 \\ 83 & -211 & 247 \end{bmatrix} \bmod 26$$

$$K^{-1} = \frac{1}{6453}\begin{bmatrix} -16 & 25 & 6 \\ 17 & 4 & -6 \\ 5 & -3 & 13 \end{bmatrix} \bmod 26$$

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

+124

52:59 / 01:02:00

Activities Brave Web Browser Wed Sep 1 11:42:34 PM 93 %

Course: Object Oriented Mod | CNS-odd-sem-21-22: Lecture F | Cisco Webex Meetings | WhatsApp

coep.webex.com/recordingservice/sites/coep/recording/39b9b0aae23d1039b7ed005056818831/playback

Imported fro... Programming Inbox (4,357) -... Meet – csk-shd... Inspect with C...

CNS Theory Pachghare-20210818 1030-1

	1G	1B	1K	1P
Vinod	111803128 Vasi Gupta	111803143 Rohini Bhonga	111803126 Simran Kuche	111803155 VIREN RAJES

Here first compute 6453 mod 26 = 5, then find the multiplicative inverse of 5 such that 5 d mod 26 = 1, where d is the multiplicative inverse of 5.

$$K^{-1} = \frac{1}{5}\begin{bmatrix} -16 & 25 & 6 \\ 17 & 4 & -6 \\ 5 & -3 & 13 \end{bmatrix} \bmod 26$$

+124

53:50 / 01:02:00

Activities Brave Web Browser Wed Sep 1 11:42:38 PM 93 %

Course: Object Oriented Mod | CNS-odd-sem-21-22: Lecture F | Cisco Webex Meetings | WhatsApp

coep.webex.com/recordingservice/sites/coep/recording/39b9b0aae23d1039b7ed005056818831/playback

Imported fro... Programming Inbox (4,357) -... Meet – csk-shd... Inspect with C...

CNS Theory Pachghare-20210818 1030-1

	1G	1B	1K	1P
Vinod	111803128 Vasvi Gupta	111803143 Rohini Bhonga	111803126 Simran Kuche	111803155 VIREN RAJES

Extended Euclidean algorithm

Find out the multiplicative inverse of 5 mod 26

$26 = 5(5) + 1$ $\qquad$ $1 = 26 - 5(5)$

$1 = 26 - 5(5)$
$1 = 26 + 5(-5)]$

-5 is the multiplicative inverse of 5 mod 26 which is equal to (-5 + 26) mod 26 = 21 mod 26

So, 21 is the multiplicative inverse of 5 mod 26

+123

54:49 / 01:02:00

Activities Brave Web Browser Wed Sep 1 11:42:53 PM 93 %

Course: Object Oriented Mod | CNS-odd-sem-21-22: Lecture F | Cisco Webex Meetings | WhatsApp

coep.webex.com/recordingservice/sites/coep/recording/39b9b0aae23d1039b7ed005056818831/playback

Imported fro... Programming Inbox (4,357) -... Meet – csk-shd... Inspect with C...

CNS Theory Pachghare-20210818 1030-1

	1G	1B	1K	1P
Vinod	111803128 Vasvi Gupta	111803143 Rohini Bhonga	111803126 Simran Kuche	111803155 VIREN RAJES

Now replace (1/5) by 21

$$K^{-1} = 21 \begin{bmatrix} -16 & 25 & 6 \\ 17 & 4 & -6 \\ 5 & -3 & 13 \end{bmatrix} \bmod 26$$

$$K^{-1} = \begin{bmatrix} -24 & 5 & 22 \\ 19 & 6 & -22 \\ 1 & -11 & 13 \end{bmatrix} \bmod 26$$

$$K^{-1} = \begin{bmatrix} 2 & 5 & 22 \\ 19 & 6 & 4 \\ 1 & 15 & 13 \end{bmatrix} \bmod 26$$

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

42

+123

57:16 / 01:02:00

Activities Brave Web Browser Wed Sep 1 11:42:58 PM 93 %

Course: Object Oriented Mod | CNS-odd-sem-21-22: Lecture F | Cisco Webex Meetings | WhatsApp

coep.webex.com/recordingservice/sites/coep/recording/39b9b0aae23d1039b7ed005056818831/playback

Imported fro... Programming Inbox (4,357) -... Meet – csk-shd... Inspect with C...

CNS Theory Pachghare-20210818 1030-1

	1G	1B	1K	1P
Vinod	111803128 Vasvi Gupta	111803143 Rohini Bhonga	111803126 Simran Kuche	111803155 VIREN RAJES

Advantages

- The ciphertext letter generated for a letter in plaintext is not dependent upon only a single plaintext letter but it is a combination of many letters.
- This helps to avoid the letter frequency problem. It is therefore difficult for cryptanalysis and provides more security.

+122

58:16 / 01:02:00

Activities Brave Web Browser Wed Sep 1 11:43:06 PM 93 %

Course: Object Oriented Mod | CNS-odd-sem-21-22: Lecture F | Cisco Webex Meetings | WhatsApp

coep.webex.com/recordingservice/sites/coep/recording/39b9b0aae23d1039b7ed005056818831/playback

Imported fro... Programming Inbox (4,357) -... Meet – csk-shd... Inspect with C...

CNS Theory Pachghare-20210818 1030-1

	1G	1C	1S	1P
Vinod	111803128 Vasi Gupta	111807076 Swebert Nich	111803127 Vasu Sharma	111803155 VIREN RAJES

Disadvantage

- This cipher uses linear algebra, which makes easy for a known plaintext attack

+113

01:00:16 / 01:02:00