

1P



1G

1G

1G

111803116 Aryan Prasad

Vinod

111803128 Vasvi Gupta

111803151 Arya Surendra

111803087 Himansh Gupt

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

File Edit View Sign Window Help

Home Tools PowerPoint Present... 12 / 39 90.5% Search 'Crop Page'

Export PDF

Edit PDF

Create PDF

Comment

Combine Files

Organize Pages

Compress PDF

Redact

Protect

Fill & Sign

Send for Comments

More Tools

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

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

17

Convert, edit and e-sign PDF forms & agreements

Free 7-Day Trial

1P



1G

111803116 Aryan Prasad

Vinod

1G

111803128 Vasvi Gupta

111803151 Arya Surendra

1G

111803087 Himansh Gupt

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

File Edit View Sign Window Help

Home Tools PowerPoint Present... 13 / 39 90.5% Search 'Crop Page'

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

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

18

Convert, edit and e-sign PDF forms & agreements

Free 7-Day Trial

1P		1G	1G	1G
111803116 Aryan Prasad	Vinod	111803128 Vasvi Gupta	111803151 Arya Surendra	111803087 Himansh Gupt

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

File Edit View Sign Window Help

Home Tools PowerPoint Present... 14 / 39 90.5% Search 'Crop Page'

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 .)

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

19

Convert, edit and e-sign PDF forms & agreements

Free 7-Day Trial



1P



1G

1G

1G

111803116 Aryan Prasad

Vinod

111803128 Vasvi Gupta

111803151 Arya Surendra

111803087 Himansh Gupt

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

File Edit View Sign Window Help

Home Tools PowerPoint Present... 15 / 39 90.5% Search 'Crop Page'

Cryptography also allows secure storage of sensitive data on any computer.

Encryption

Plain text → Cipher text

B TECH COMPUTER → ⚡ TECH COMPUTER

Decryption

Cipher text → Plain text

⚡ TECH COMPUTER → B TECH COMPUTER

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

Convert, edit and e-sign PDF forms & agreements

Free 7-Day Trial



1A

1M

1B

1S

1M

111803034 Aditya Abhan

111803072 Shaunak Mah

111803038 YOGESHWARI

111803095 Tejas Sakre

111803176 Yash Gajanan

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

File Edit View Sign Window Help

Home Tools PowerPoint Present... x

16 / 39 90.5% 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 26 27 28 29 30 31 32 33 34 35 36 37 38 39

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

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

Convert, edit and e-sign PDF
forms & agreements

Free 7-Day Trial



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... x

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

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

+60

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... 17 / 39 90.5% 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

Encryption Systems

- Substitution Cipher
 - Convert one letter to another
- Transposition Cipher
 - Change position of letter in text
 - Word Jumble
- Monoalphabetic Cipher
 - Caesar
- Polyalphabetic Cipher
 - Vigenère
- One-time Pads
 - Randomly generated keys

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

22

Convert, edit and e-sign PDF forms & agreements

Free 7-Day Trial

+69

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... x

18 / 39 90.5% ↕

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

Attributes of Strong Encryption

- **Confusion**
 - Change key values each round
 - Performed through substitution
 - Complicates **ciphertext /key** relationship
- **Diffusion**
 - Change location of plaintext in ciphertext
 - Complicates **ciphertext /plaintext** relationship

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

23

+75

1A

1J

1S

1M

111803034 Aditya Abhan

111803142 ATHARVA MU

Vinod

111803095 Tejas Sakre

111803176 Yash Gajanan

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



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



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

24

Convert, edit and e-sign PDF
forms & agreements

Free 7-Day Trial

1A

1J

1S

1M

111803034 Aditya Abhan

111803142 ATHARVA MU

Vinod

111803095 Tejas Sakre

111803176 Yash Gajanan

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



Three Aspects of Information Security

I

- Security attack
- Security mechanism
- Security service



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

25

Convert, edit and e-sign PDF
forms & agreements

Free 7-Day Trial

+105

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



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

26

Convert, edit and e-sign PDF
forms & agreements

Free 7-Day Trial

+108

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

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**



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

27

Convert, edit and e-sign PDF forms & agreements

Free 7-Day Trial

+109

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...

23

/ 39

90.5%

+

-

0

1

2

3

4

5

6

7

8

9

0

?

Sign In

Q

E

M

S

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

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... 26 / 39 90.5% Sign In

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

Security Services

Non-Repudiation

Authentication

Access Control

Data Confidentiality

Data Integrity

Security Services

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

31

25:07 / 01:03:32

1D

1J

1S

1D

111803111 Atharva Kailas

111803142 ATHARVA MU

Press Esc to exit full screen

111803095 Tejas Sakre

111803049 Vrushali Pram

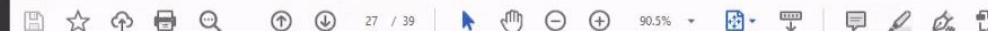
PowerPoint Presentation - Adobe Acrobat Reader DC (32-bit)

File Edit View Sign Window Help

Home Tools

PowerPoint Present...

? Sign In



27 / 39

90.5%



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.



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

32

Convert, edit and e-sign PDF
forms & agreements

Free 7-Day Trial

1D

1J

1S

1D

111803111 Atharva Kailas

111803142 ATHARVA MU

Vinod

111803095 Tejas Sakre

111803049 Vrushali Pram

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



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.



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

34

Convert, edit and e-sign PDF
forms & agreements

Free 7-Day Trial

+118

1D

1J

1S

1D

111803111 Atharva Kailas

111803142 ATHARVA MU

Vinod

111803095 Tejas Sakre

111803049 Vrushali Pram

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

30 / 39

90.5%

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.



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

35

Convert, edit and e-sign PDF
forms & agreements

Free 7-Day Trial



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... x

?

Sign In

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

- 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.

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

36

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... x

?

Sign In

Export PDF

Edit PDF

Create PDF

Comment

Combine Files

Organize Pages

Compress PDF

Redact

Protect

Fill & Sign

Send for Comments

More Tools

Search 'Draw Line'

32 / 39 | 90.5% |

- **Selective-Field Connectionless Integrity:** Provides for the integrity of selected fields within a single connectionless data block; takes the form of determination of whether the selected fields have been modified.

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

37

Convert, edit and e-sign PDF forms & agreements

Free 7-Day Trial

+117

1D

1J

1S

1D

111803111 Atharva Kailas

111803142 ATHARVA MU

Vinod

111803095 Tejas Sakre

111803049 Vrushali Pram

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



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

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



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

38

+118

1D

1J

1S

1D

111803111 Atharva Kailas

111803142 ATHARVA MU

Vinod

111803095 Tejas Sakre

111803049 Vrushali Pram

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



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

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



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

38

+117

1D

1J

1S

1D

111803111 Atharva Kailas

111803142 ATHARVA MU

Vinod

111803095 Tejas Sakre

111803049 Vrushali Pram

Press Esc to exit full screen

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

File Edit View Sign Window Help

Home Tools

PowerPoint Present... x

?

Sign In



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



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

39

Convert, edit and e-sign PDF
forms & agreements

Free 7-Day Trial

+117



Vinod

1D

Press Esc to exit full screen

1S

1M

111803049 Vrushali Pram

111803142 ATHARVA MU

111803095 Tejas Sakre

111803166 Rutvik Ganesh

AutoSave Off

Lect-II

Search

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

Vinod Pachghare VP

Clipboard Slides

Font Paragraph Drawing Editing Voice Designer

1 Classical Encryption Techniques

2 Asymmetric Encryption

3 Asymmetric Encryption

4 Basic Terminology

5 Symmetric Cipher Model

6 Cases of Cryptographic 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

Click to add notes

Slide 1 of 67 English (India)

Vinod

1D

1J

1S

1M

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

Vinod

1D

1J

1S

1M

111803049 Vrushali Pram

111803142 ATHARVA MU

111803095 Tejas Sakre

111803166 Rutvik Ganesh

Lect-II

Search

Vinod Pachghare VP

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

Clipboard Slides

Font Paragraph Drawing Editing Voice Designer

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23

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

Slide 3 of 67 English (United States)

Notes

97%

Vinod

1D

1J

1S

1M

111803049 Vrushali Pram

111803142 ATHARVA MU

111803095 Tejas Sakre

111803166 Rutvik Ganesh

AutoSave Lect-II

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

Vinod Pachhare VP

Clipboard Slides

Font Paragraph Drawing Editing Voice Designer

1 2 3 4 5 6 7 8 9 10 11 12

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

Slide 4 of 67 English (India)



Vinod

1D

1J

1S

1M

111803049 Vrushali Pram

111803142 ATHARVA MU

111803095 Tejas Sakre

111803166 Rutvik Ganesh

Lect-II

Search

AutoSave

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

Vinod Pachghare VP

Clipboard Slides

Font Paragraph Drawing Editing Voice Designer

1 2 3 4 5 6 7 8 9 10 11 12

1 2 3 4 5 6 7 8 9 10 11 12

Symmetric Cipher Model

Secret key shared by sender and recipient

Secret key shared by sender and recipient

Plaintext input → Encryption algorithm (e.g., DES) → Transmitted ciphertext → Decryption algorithm (reverse of encryption algorithm) → Plaintext output

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)

+118

Vinod

1D

1J

1S

1M

111803049 Vrushali Pram

111803142 ATHARVA MU

111803095 Tejas Sakre

111803166 Rutvik Ganesh

AutoSave Lect-II

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

Clipboard Slides

Font Paragraph Drawing Editing Voice Designer

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23

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)

Notes

+119

Vinod

1D

1J

1S

1M

111803049 Vrushali Pram

111803142 ATHARVA MU

111803095 Tejas Sakre

111803166 Rutvik Ganesh

AutoSave Lect-II

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

Paste New Slide Reset Slides Section

Font Paragraph Drawing Editing Voice Designer

Brute Force Search

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

I

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)



Vinod

1D

1J

1S

1M

111803049 Vrushali Pram

111803142 ATHARVA MU

111803095 Tejas Sakre

111803166 Rutvik Ganesh

AutoSave Lect-II

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

Vinod Pachghare VP

Clipboard Slides

Font Paragraph Drawing Editing Voice Designer

Shapes Arrange Quick Styles Find Replace Select Dictate Design Ideas

Caesar Cipher

- Earliest known substitution cipher by Julius Caesar
- Replaces each letter by 3rd letter
- example:

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

— meet me after the toga party

— PHHW PH DIWHU WKH WRJD SDUWB

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

Click to add notes

Slide 9 of 67 English (India)

Vinod

1D

1J

1S

1M

111803049 Vrushali Pram

111803142 ATHARVA MU

111803095 Tejas Sakre

111803166 Rutvik Ganesh

AutoSave Lect-II

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

Vinod Pachghare VP

Clipboard Slides

Font Paragraph Drawing Editing Voice Designer

Shapes Arrange Quick Styles Select Dictate Design Ideas

Find Replace Select Dictate Design Ideas

Caesar Cipher

- When using a Caesar cipher, you assign each letter to an index starting from 0.
- You would then compute the following.
(plain letter index + key) mod (total number of letters)
- This will give you the index of the encrypted letter!
- As you can see, the modulus is the total number of letters in the alphabet. For English, this modulus is 26.

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

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

This mathematical description uses **modulo arithmetic** (ie clock arithmetic). Here, when you reach Z you go back to A and start again. Mod 26 implies that when you reach 26, you use 0 instead (ie the letter after Z, or 25 + 1 goes to A or 0).

Slide 10 of 67 English (India)

+117

Vinod

1D

1J

1S

1M

111803049 Vrushali Pram

111803142 ATHARVA MU

111803095 Tejas Sakre

111803166 Rutvik Ganesh

AutoSave Lect-II Vinod Pachghare Share

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

Clipboard Slides

Font Paragraph Drawing Editing Voice 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: $(1+2) = 3$. $3 \text{ mod } 5 = 3$. 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

Slide 11 of 67 English (India)

01:01:02 / 01:03:32 01:00:53



Vinod

1G

4B

1K

1B

141903005 Kajol Gaikwad

46_111803038 YOGESH

111803126 Simran Kuche

111803136 Siddhika Sant

Lectures - Recently Published Presentations (2)

File Home Insert Design Transitions Animations Slide Show Review View

Cut Copy Format Painter New Reset Slide Section

Clipboard Slides

Font Paragraph Drawing Editing

1 Cryptography and Network Security Session 3 Date: 18 August 2021 V. K. Pachghare

2 Classical Encryption Techniques

3 Caesar Cipher

4 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

Click to add notes

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

TRUTH
KNOWLEDGE
CHARACTER
PINE

4

Slide 4 of 45 | Default Design | English (India) | +55



Vinod

1G

4B

1K

1B

141903005 Kajol Gaikwad

46_111803038 YOGESH

111803126 Simran Kuche

111803136 Siddhika Sant

Lecture 10 - Monoalphabetic Ciphers (Part 1)

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: DSVQFJWPESCXHTMYAUOLRGZN
Plaintext: BEAD
Ciphertext: KFDQ

Plain: abcdefghijklmnopqrstuvwxyz
Cipher: DKVQFIBJWPESCXHTMYAUOLRGZN
Plaintext: BEAD
Ciphertext: KFDQ

I

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

Click to add notes

Slide 5 of 45 | Default Design | English (India) | 95% | 03:52 / 01:02:00



Vinod

1G

4B

1K

1B

141903005 Kajol Gaikwad

46_111803038 YOGESH

111803126 Simran Kuche

111803136 Siddhika Sant

Lecture 10 - Advanced Cryptanalysis: Frequency Analysis

File Home Insert Design Transitions Animations Slide Show Review View

Cut Copy Paste Format Painter New Reset Slide Section Clipboard Slides Font Paragraph Drawing Editing

Slides Outline

5 Monoalphabetic Cipher

- Rather than just shifting the alphabet, could shuffle (mix) the letters randomly
- Each letter maps to a different random ciphertext letter
- Same key for all letters to map

Plain: abcdefghijklmnopqrstuvwxyz
Cipher: DESQVJWATPENXKTHAIVULBZON
Plaintext: BEAN
Ciphertext: RFPQ

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

6 Monoalphabetic Cipher Security

- use have a total of $26 = 4 \times 10^6$ keys
- with so many keys, might think as secure
- but would be **INSECURE**
- problem is language characteristics

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

7 Cryptanalysis

- Cryptanalysis is the art of breaking codes and ciphers
- a more systematic approach for cryptanalysis is to calculate the frequency distribution of the letters in the cipher text

This consists of counting how many times each letter appears

- Natural English text has a very distinct distribution that can be used help crack codes

English Letter Frequencies

Click to add notes

Cryptanalysis

- Cryptanalysis is the art of breaking codes and ciphers
- a more systematic approach for cryptanalysis is to calculate the frequency distribution of the letters in the cipher text

This consists of counting how many times each letter appears

- Natural English text has a very distinct distribution that can be used help crack codes

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

Example

1. Substitution: ASDFJLK; 2. Vertical: ABCDEFGHIJKLMNOPQRSTUVWXYZ; 3. Horizontal: ABCDEFGHIJKLMNOPQRSTUVWXYZ

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



Vinod

1G

Press Esc to exit full screen

1K

1B

141903005 Kajol Gaikwad

46_111803038 YOGESH

111803126 Simran Kuche

111803136 Siddhika Sant

Lectures in progress. Automatically powerpoint slides advance automatically (every 5s).

File Home Insert Design Transitions Animations Slide Show Review View

Cut Copy Paste Format Painter New Reset Slide Section Clipboard Slides

Font Paragraph Drawing Editing

Slides Outline

5 Monoalphabetic Cipher

- Rather than just shifting the alphabet, could shuffle (permute) the letters arbitrarily
- So, each letter maps to a different random ciphertext letter
- Hence key is as long as the plaintext

Plain text: abcdefghijklmnopqrstuvwxyz
Cipher: DESNPQTRUPENCXMTMAYAUOLBZGN
Plaintext: HEAD
Ciphertext: RPNQ

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

6 Monoalphabetic Cipher Security

- we have a total of $26 = 4 \times 10^3$ keys
- with so many keys, might think it's 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

7 Cryptanalysis

- Cryptanalysis is the art of breaking codes and ciphers
- a more systematic approach for cryptanalysis is to calculate the frequency distribution of the letters in the cipher text
- This consists of counting how many times each letter appears
- Natural English text has a very distinct distribution that can be used to crack codes

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

8 English Letter Frequencies

A bar chart titled "English Letter Frequencies" showing the relative frequency of each letter in the English alphabet. The y-axis represents "Relative frequency (%)" from 0 to 14. The x-axis lists the letters A through Z. The frequencies are as follows:

Letter	Relative Frequency (%)
A	8.167
B	1.492
C	2.782
D	4.253
E	12.702
F	2.228
G	2.015
H	6.094
I	6.96
J	0.153
K	0.772
L	4.025
M	2.406
N	6.49
O	7.597
P	1.929
Q	0.095
R	5.987
S	6.327
T	9.086
U	2.758
V	0.978
W	2.360
X	0.150
Y	1.974
Z	0.074

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

Click to add notes

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

8:14 / 01:02:00

95%



Vinod

1G

4B

1K

1B

141903005 Kajol Gaikwad

46_111803038 YOGESH

111803126 Simran Kuche

111803136 Siddhika Sant

Lecture 10 - Advanced Cryptanalysis: Frequency Analysis

File Home Insert Design Transitions Animations Slide Show Review View

Cut Copy Paste Format Painter New Reset Slide Section Clipboard Slides Font Paragraph Drawing Editing

Slides Outline

8 English Letter Frequencies

9 Example

10 Classical Encryption Techniques

- Playfair Cipher
- Hill Cipher

11 Playfair Cipher

- Divide 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 ciphered groups are generated

12 Encryption

- Encryption process is divided into three parts:
 - Preparing the Plaintext
 - Prepare the Key

Example

- ciphertext: KSPLSMYSHSWM
- count relative letter frequencies (see text)
- K = 1; S = 4; P = 1; L = 1; M = 2; Y = 1; H = 1; W = 1;
- guess S may be E and M may be T
- proceeding with trial and error finally get:
I
KEPLETYEHEWT
KEPLE TYE HEWT TYE may be THE
KEPLE THE HEWT

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

Click to add notes

Slide 9 of 45 | Default Design | English (India) | 95% | +115



Vinod

1G

4B

1K

1B

141903005 Kajol Gaikwad

46_111803038 YOGESH

111803126 Simran Kuche

111803136 Siddhika Sant

Lecture 10 - Monoalphabetic Cipher Security, Substitution Ciphers, Vigenere Cipher

File Home Insert Design Transitions Animations Slide Show Review View

Cut Copy New Reset Slide Section

Font Paragraph Drawing Editing

Slides Outline

6 Monoalphabetic Cipher Security

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

Monoalphabetic Cipher Security

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

English Letter Frequencies

Example

plaintext: ciphertext: frequency (approx.)
our: rjgsvy (approx. 12%)
and: qkxwv (approx. 12%)
the: pbfm (approx. 12%)
is: oqz (approx. 12%)
you: vjw (approx. 12%)
of: ntu (approx. 12%)
and: qkxwv (approx. 12%)
for: sly (approx. 12%)
the: pbfm (approx. 12%)
is: oqz (approx. 12%)
a: m (approx. 12%)
n: l (approx. 12%)
t: k (approx. 12%)
e: j (approx. 12%)
s: i (approx. 12%)
d: h (approx. 12%)
o: g (approx. 12%)
r: f (approx. 12%)
w: e (approx. 12%)
l: d (approx. 12%)
u: c (approx. 12%)
v: b (approx. 12%)
x: a (approx. 12%)
y: z (approx. 12%)
z: y (approx. 12%)
possibility: for it to be 26 keys? No!
processing note: total number of possibilities: 26!

Classical Encryption Techniques

- Playfair Cipher
- Hill Cipher

Playfair Cipher

- Divided the plaintext into a group of two letters each
- Each group is treated as a single unit
- Use the key, for array of plaintext, corresponding

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

Click to add notes

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



Vinod

1G

Press Esc to exit full screen

1K

1U

111803128 Vasvi Gupta

46_111803038 YOGESH

111803126 Simran Kuche

111803104 Akanksha Kish

Lect-11.pptx Microsoft PowerPoint (Presented, AutoFormat Applied)

File Home Insert Design Transitions Animations Slide Show Review View

Cut Copy Format Painter New Slide Section

Clipboard Slides

Font Paragraph Drawing Editing

Slides Outline

9 Example

- ciphering
- invert relative letter frequency (one test)
- $M = 1, R = 2, S = 3, T = 4, U = 5, V = 6, W = 7$
- assume if 'E' has 1, 'M' has 2, etc.
- processing with first and last family per
- $M = 1, R = 2, S = 3, T = 4, U = 5, V = 6, W = 7$
- $E = 8, D = 9, C = 10, B = 11, A = 12$

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

10 Classical Encryption Techniques

- Playfair Cipher
- Hill Cipher

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

11 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

12 Encryption

- Encryption process is divided into these parts
 - Preparing the Plaintext
 - Preparing the Key
 - Encryption

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

13 Preparing the Plaintext

Step 1 Convert the message into lowercase letters and remove punctuation

We live in a world full of beauty
yalavane@fullhouse.in

Click to add notes

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

Slide 11 of 45 | Default Design | English (India) 95%



Vinod

1G

4B

1K

1U

111803128 Vasvi Gupta

46_111803038 YOGESH

111803126 Simran Kuche

111803104 Akanksha Kish

Lect-13(Notes - Substitution cipher and Vigenere cipher)

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

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

Step 3 Now write the groups such that in one row 3 pairs are there as shown below.

If it is present all 'y' are replaced with 'z' (any letter)

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

Preparing the Key

Select the key having no. of letters
Leave the duplicate letters

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

Click to add notes

Slide 13 of 45 | Default Design | English (India) | 95% | +118



Vinod

1G

Press Esc to exit full screen

1K

1P

111803128 Vasvi Gupta

46_111803038 YOGESH

111803126 Simran Kuche

111803155 VIREN RAJES

Lecture 10 - Caesar cipher and Vigenere cipher

File Home Insert Design Transitions Animations Slide Show Review View

Cut Copy New Reset Slide Section

Format Painter

Clipboard Slides

Font Paragraph Drawing Editing

12 11 10 9 8 7 6 5 4 3 2 1 0 1 2 3 4 5 6 7 8 9 10 11 12

Slides Outline

13 Preparing the Plaintext

Step 1 Convert the message into lowercase letters and remove punctuation.

We live in a world full of beauty.

We live in a world full of beauty.

Step 2 Split the text into a pair of two.

We live in a world full of beauty.

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

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

14

- If both the letters in a pair same, then split that pair by adding any letter in between the letters and rearrange the groups.
- In this example, we have 'ee'. If 'e' is by 'e', then 'ee' is 'ea'. If 'e' is by 'l', then 'ee' is 'el'.
- In this example, one of the pairs having same letters 'll' (shown in bold). Add letter 'y' in between the letters, so the group is 'ly'. But the group should be of two letters, so shift the last letters of this group to the right by one position and rearrange the groups again.

We live in a world full of beauty.

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

15

- If the last group is having only one letter, as append one more letter to complete the pair. Here we append 'x' with the last letter 'y' as shown below:

We live in a world full of beauty.

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

16

- 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	

I

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)

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

17 Preparing the Key

Select the key having any number of letters.

Never the duplicate letters.

Click to add notes

Slide 16 of 45 | Default Design | English (India) | +124



Vinod

1G

4B

1K

1P

111803128 Vasvi Gupta

46_111803038 YOGESH

111803126 Simran Kuche

111803155 VIREN RAJES

Prepared by: Savitri Damerla, Department of Computer Engineering and Information Technology, College of Engineering Pune (COEP), Forerunners in Technical Education.

File Home Insert Design Transitions Animations Slide Show Review View

Cut Copy New Reset Slide Section

Format Painter

Clipboard Slides

Font Paragraph Drawing Editing

17 Preparing the Key

- Select the key having any number of letters
- Remove the duplicate letters
- Convert all the letters of the key into uppercase letters
- To prepare the key, 5×5 matrix is constructed

18 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

19 Step 3 The remaining letters of the alphabet which are not present in the key are filled in the alphabetical order as shown below (the letter 'I' is not replaced by 'J' as we can use any letter, total count must be 25)
A N O T H
E R B C D
F G D E L
H V Q S U
Y W X Y Z

20 Encryption

Each letter in a pair that is in 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. TQ-> MS

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

21 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

Click to add notes

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

Slide 17 of 45 | Default Design | English (India) | +124



Vinod

1G

4B

1K

1P

111803128 Vasvi Gupta

46_111803038 YOGESH

111803126 Simran Kuche

111803155 VIREN RAJES

File Home Insert Design Animations Slide Show Review View

Cut Copy Format Painter Paste New Reset Slide Section Clipboard Slides

Font Paragraph Drawing Editing

17 Preparing the Key

- Select the key having set number of letters
- Remove the duplicate letters
- Convert all the letters of the key into uppercase letters
- To prepare the key, 5×5 matrix is constructed.

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

18 Suppose the key is "another"

- Step 1 Convert the key into uppercase letters, the key becomes ANOTHER
- Step 2 Write the letters in the 3×5 matrix form, i.e., 5 letters in one row as shown below:

A	N	O	T	H
E	R	B	C	D
F	G	I	K	L

5 letters in one row as shown below:

ANOTHER

- Step 3 The remaining letters of the alphabet which are not present in the key are filled in the alphabetical order starting from A to Z (for replacement to). We can use any letter, total count must be 25.

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

19 Encryption

Each letter in a pair that is in 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. TQ-> MS

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

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

WG->NP

A	N	O	T	H
E	R	B	C	D

Click to add notes

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

18

Slide 18 of 45 | Default Design | English (India) | 95% | 20:45 / 01:02:00



Vinod

1G

4B

1K

1P

111803128 Vasvi Gupta

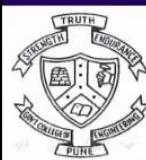
46_111803038 YOGESH

111803126 Simran Kuche

111803155 VIREN RAJES

- 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



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

19

+126



Vinod

1G

1B

1K

1P

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



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

20



Vinod

1G

1B

1K

1P

111803128 Vasvi Gupta

111803143 Rohini Bhonga

111803126 Simran Kuche

111803155 VIREN RAJES

- letters in the same column are replaced 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





Vinod

1G

1B

1K

1P

111803128 Vasvi Gupta

111803143 Rohini Bhonga

111803126 Simran Kuche

111803155 VIREN RAJES

- 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



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

22



Vinod

1G

1B

1K

1P

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





Vinod

1G

1B

1K

1P

111803128 Vasvi Gupta

111803143 Rohini Bhonga

111803126 Simran Kuche

111803155 VIREN RAJES

- letters in the same column are replaced 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



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

21

+128

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

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

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

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

CNS Theory Pachghare-20210818 1030-1

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

PT:- WE LIVE 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

00 29:02 / 01:02:00

Activities Brave Web Browser ▾ Wed Sep 1 11:40:04 PM

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

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

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

CNS Theory Pachghare-20210818 1030-1 ↴

The screenshot shows a Cisco Webex meeting interface. At the top, there's a participant list with five entries: Vinod, 1G, 1B, 1K, and 1P. Below the list, the names of the participants are displayed: 111803128 Vasvi Gupta, 111803143 Rohini Bhonga, 111803126 Simran Kuche, and 111803155 VIREN RAJES. The main content area contains a presentation slide with the following text:

- Finally, perform this transformation for each pair of letters in the modified plaintext and remove the spaces
- The Ciphertext is:

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

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

At the bottom of the slide, there's a logo of the College of Engineering Pune (COEP) and the text: "Department of Computer Engineering and Information Technology, College of Engineering Pune (COEP), Forerunners in Technical Education". The slide also includes a page number "24" and a link "+127". The video player at the bottom shows the current time as 30:44 / 01:02:00.

Activities Brave Web Browser ▾ Wed Sep 1 11:40:11 PM

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

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

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

CNS Theory Pachghare-20210818 1030-1 ↴

The screenshot shows a video recording interface from coep.webex.com. At the top, there's a participant list with five entries: Vinod (1G), 111803128 Vasvi Gupta (1B), 111803143 Rohini Bhonga (1K), 111803126 Simran Kuche (1P), and 111803155 VIREN RAJES. Below the list, the slide content is displayed.

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

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

25 +126

31:30 / 01:02:00

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

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

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

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

CNS Theory Pachghare-20210818 1030-1

Vinod 1G 1B 1K 1P

111803128 Vasvi Gupta 111803143 Rohini Bhonga 111803126 Simran Kuche 111803155 VIREN RAJES

AF=>VE

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

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

26 +128

00 32:34 / 01:02:00

Activities Brave Web Browser ▾ Wed Sep 1 11:40:26 PM

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

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

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

CNS Theory Pachghare-20210818 1030-1 ↴

Vinod	1G	1B	1K	1P
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

00 33:35 / 01:02:00

Activities Brave Web Browser ▾

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

Wed Sep 1 11:40:36 PM

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

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

CNS Theory Pachghare-20210818 1030-1 ↴

Vinod 1G 1B 1K 1P

111803128 Vasvi Gupta 111803143 Rohini Bhonga 111803126 Simran Kuche 111803155 VIREN RAJES

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	1	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

$$C = KP \text{ mod } 26$$

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

29 +126

00 34:20 / 01:02:00

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

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

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

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

CNS Theory Pachghare-20210818 1030-1 ↴

The screenshot shows a video player interface. At the top, there's a navigation bar with icons for back, forward, and search, followed by the URL 'coep.webex.com/recording/service/sites/coep/recording/39b9b0aae23d1039b7ed005056818831/playback'. Below the URL is a toolbar with icons for imported files, programming, inbox, and inspecting with C++. The main content area displays a presentation slide. The slide has a dark background with a grid of five circular icons at the top labeled '1G', '1B', '1K', and '1P'. Below the icons, names are listed: 'Vinod' (with a profile picture), '111803128 Vasvi Gupta', '111803143 Rohini Bhonga', '111803126 Simran Kuche', and '111803155 VIREN RAJES'. The title 'Encryption' is centered in large, bold, blue serif font. Below the title, a text block states: 'Encryption process is divided into three parts:' followed by a bulleted list: '• Preparing the Plaintext', '• Preparing the Key', and '• Encryption'. In the bottom right corner of the slide, there's a small watermark-like text '+127'. The bottom of the screen shows a video control bar with icons for volume, brightness, and other controls, and a progress bar indicating the video is at 37:31 / 01:02:00.

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

00 37:31 / 01:02:00

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

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

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

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

CNS Theory Pachghare-20210818 1030-1 ↴

Vinod 1G 1B 1K 1P

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

00 38:12 / 01:02:00

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

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

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

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

CNS Theory Pachghare-20210818 1030-1 ↴

Vinod	1G	1B	1K	1P
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

00 40:04 / 01:02:00

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

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

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

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

CNS Theory Pachghare-20210818 1030-1 ↴

Vinod	1G	1B	1K	1P
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.

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

34 +128

00 40:56 / 01:02:00

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

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

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

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

CNS Theory Pachghare-20210818 1030-1 ↴

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

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

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

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

CNS Theory Pachghare-20210818 1030-1 ↴

Vinod	1G	1B	1K	1P
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:

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

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

33 +127

00 43:26 / 01:02:00

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

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

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

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

CNS Theory Pachghare-20210818 1030-1 ↴

Vinod 111803128 Vasvi Gupta 111803143 Rohini Bhonga 111803126 Simran Kuche 111803155 VIREN RAJES

Encryption

Ciphertext = Key x Plaintext mod 26

$$C = KP \text{ mod } 26$$
$$C = \begin{bmatrix} 0 & 13 & 14 \\ 19 & 6 & 4 \\ 17 & 1 & 25 \end{bmatrix} \begin{bmatrix} 2 \\ 14 \\ 4 \end{bmatrix} = \begin{bmatrix} 238 \\ 138 \\ 148 \end{bmatrix} \text{ mod } 26$$
$$C = \begin{bmatrix} 4 \\ 8 \\ 18 \end{bmatrix}$$

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

00 44:18 / 01:02:00

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

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

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

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

CNS Theory Pachghare-20210818 1030-1 ↴

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

Decryption

- Again we have to perform matrix multiplication.
- $P = K^{-1} C \text{ mod } 26$
- Inverse of the key matrix is calculated using standard methods with extended Euclidean algorithm [Because $(1/\det) \text{mod } 26$]

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

38 +127

46:28 / 01:02:00

Activities Brave Web Browser ▾ Wed Sep 1 11:41:59 PM

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

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

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

CNS Theory Pachghare-20210818 1030-1 ↴

Vinod 111803128 Vasvi Gupta 111803143 Rohini Bhonga 111803126 Simran Kuche 111803155 VIREN RAJES

Encryption

Ciphertext = Key x Plaintext mod 26

$$C = KP \text{ mod } 26$$
$$C = \begin{bmatrix} 0 & 13 & 14 \\ 19 & 6 & 4 \\ 17 & 1 & 25 \end{bmatrix} \begin{bmatrix} 2 \\ 14 \\ 4 \end{bmatrix} = \begin{bmatrix} 238 \\ 138 \\ 148 \end{bmatrix} \text{ mod } 26$$
$$C = \begin{bmatrix} 4 \\ 8 \\ 18 \end{bmatrix}$$

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

00 47:16 / 01:02:00

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

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

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

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

CNS Theory Pachghare-20210818 1030-1 ↴

The screenshot shows a video player interface. At the top, there's a navigation bar with icons for back, forward, and search, followed by the URL 'coep.webex.com/recording/service/sites/coep/recording/39b9b0aae23d1039b7ed005056818831/playback'. Below the URL is a toolbar with various icons. The main content area displays a presentation slide. The slide has a dark background with a grid of five circular icons at the top labeled '1G', '1B', '1K', and '1P'. Below the icons, there are names: 'Vinod', '111803128 Vasvi Gupta', '111803143 Rohini Bhonga', '111803126 Simran Kuche', and '111803155 VIREN RAJES'. The title of the slide is 'Decryption'. Below the title is a bulleted list of points:

- Again we have to perform matrix multiplication.
- $P = K^{-1} C \text{ mod } 26$
- Inverse of the key matrix is calculated using standard methods with extended Euclidean algorithm [Because $(1/\det) \text{mod } 26$]

At the bottom of the slide, there's a footer with the COEP logo and text: 'Department of Computer Engineering and Information Technology', 'College of Engineering Pune (COEP)', 'Forerunners in Technical Education', '38', and '+127'. The video player also shows a progress bar at the bottom with the time '48:04 / 01:02:00'.

Activities Brave Web Browser ▾

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

Wed Sep 1 11:42:25 PM

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

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

CNS Theory Pachghare-20210818 1030-1

Vinod 1G 1B 1K 1P

111803128 Vasvi Gupta 111803143 Rohini Bhonga 111803126 Simran Kuche 111803155 VIREN RAJES

$P = K^{-1} \times C \text{ MOD } 26$

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

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

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

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

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

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

CNS Theory Pachghare-20210818 1030-1

Vinod 1G 1B 1K 1P

111803128 Vasvi Gupta 111803143 Rohini Bhonga 111803126 Simran Kuche 111803155 VIREN RAJES

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

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

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

40 +124

53:50 / 01:02:00

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

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

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

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

CNS Theory Pachghare-20210818 1030-1 ↴

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

Extended Euclidean algorithm

Find out the multiplicative inverse of 5 mod 26

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

-5 is the multiplicative inverse of 5 mod 26 which is equal to $(-5 + 26) \text{ mod } 26 = 21 \text{ mod } 26$

So, 21 is the multiplicative inverse of 5 mod 26

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

41 +123

00 54:49 / 01:02:00

Activities Brave Web Browser ▾

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

Wed Sep 1 11:42:53 PM

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

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

CNS Theory Pachghare-20210818 1030-1

Vinod 1G 1B 1K 1P

111803128 Vasvi Gupta 111803143 Rohini Bhonga 111803126 Simran Kuche 111803155 VIREN RAJES

Now replace (1/5) by 21

$$K^{-1} = 21 \begin{bmatrix} -16 & 25 & 6 \\ 17 & 4 & -6 \\ 5 & -3 & 13 \end{bmatrix} \text{ mod } 26$$
$$K^{-1} = \begin{bmatrix} -24 & 5 & 22 \\ 19 & 6 & -22 \\ 1 & -11 & 13 \end{bmatrix} \text{ mod } 26$$
$$K^{-1} = \begin{bmatrix} 2 & 5 & 22 \\ 19 & 6 & 4 \\ 1 & 15 & 13 \end{bmatrix} \text{ mod } 26$$

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

42 +123

00 57:16 / 01:02:00

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

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

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

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

CNS Theory Pachghare-20210818 1030-1 ↴

Vinod	1G	1B	1K	1P
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.

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

44 +122

58:16 / 01:02:00

Activities Brave Web Browser ▾

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

Wed Sep 1 11:43:06 PM

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

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

CNS Theory Pachghare-20210818 1030-1 ↴

Vinod 1G 1C 1S 1P

111803128 Vasvi Gupta 111807076 Swebert Nich 111803127 Vasu Sharma 111803155 VIREN RAJES

Disadvantage ↴

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

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

45 +113

00 01:00:16 / 01:02:00