

Vinod

1D

1U

1M

1K

111803111 Atharva Kailas

111803104 Akanksha Kish

111803078 Prathamesh U

111803058 Omkar Anand

AutoSave Lect-VI

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

Century Schoolbook 28 A A A A B I U S AV Aa AV Aa Shapes Arrange Quick Styles Find Replace Select Dictate Voice Designer

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

1. Engineering and Network Security
2. Classical Encryption Techniques
3. Polyalphabetic Ciphers
4. Polyalphabetic Cipher
5. Playfair cipher
6. Vigenere cipher
7. Hill cipher
8. DES cipher

Classical Encryption Techniques

- Polyalphabetic Ciphers
- Transposition ciphers

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

Click to add notes

Slide 2 of 52 English (United States)

Notes

00 01:17 / 57:24 97%

Vinod

1D

1U

1M

1K

111803111 Atharva Kailas

111803104 Akanksha Kish

111803078 Prathamesh U

111803058 Omkar Anand

Lect-VI

Search

Vinod Pachghare

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

AutoSave Off

Clipboard Slides

Font Paragraph Drawing Editing Voice Designer

Shapes Arrange Quick Styles Select Dictate Design Ideas

Find Replace Select Dictate Design Ideas

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

Polyalphabetic Ciphers

- The keyspace consists of all ordered permutations of the alphabet called a Vigenere square.
- There are 26 rows that can be used as keys, each numbered with the amount they are shifted.

I

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

Click to add notes

Slide 3 of 52 English (India)

Notes

97%

1D

1U

1M

1K

Vinod

111803111 Atharva Kailas

111803104 Akanksha Kish

111803078 Prathamesh U

111803058 Omkar Anand

A screenshot of a Microsoft PowerPoint presentation. The slide number is 4 of 52. The slide title is "Lect-VI" and the subtitle is "Vidyalayam and Network Security".
The main content of the slide is a large matrix table with 5 rows labeled 'a' through 'e' and 26 columns labeled with letters from 'a' to 'z'. The table is mostly empty, with some cells containing letters from the sets 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.
At the bottom of the slide, there is a footer with the text: "Department of Computer Engineering and Information Technology, College of Engineering Pune (COEP), Forerunners in Technical Education". There is also a small logo of the college seal.

Vinod

1D

1U

1M

1K

111803111 Atharva Kailas

111803104 Akanksha Kish

111803078 Prathamesh U

111803058 Omkar Anand

AutoSave Lect-VI Search

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

Vinod Pachghare

Clipboard Slides

Font Paragraph Drawing Editing Voice Designer

Shapes Arrange Quick Styles Select Dictate Design Ideas

Find Replace Select Dictate Design Ideas

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

- Create a master-key that specifies which order the keys (or rows) are to be used in. This does not have to include all rows.
- For example we could use $k = (5, 2, 16)$ and then cycle through these three keys. This would mean every third letter is encrypted with the same key.
- For each single letter, you are using only 1 key and encryption and decryption works as with monoalphabetic ciphers.

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

Click to add notes

Slide 5 of 52 English (India)

Notes

00 05:54 / 57:24

5

Vinod

1D

1U

1M

1K

111803111 Atharva Kailas

111803104 Akanksha Kish

111803078 Prathamesh U

111803058 Omkar Anand

AutoSave (Off) Lect-VI Search

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

Vinod Pachghare

Clipboard Slides

Font Paragraph Drawing Editing Voice Designer

Key: ant
Plaintext: technology

ant ant ant a (Row)
t e c h n o l o g y (Column)
T R V H A H L B Z Y

Plaintext											
		c	e	g	h	l	n	o	t	y	
KEY	a	C	E	G	H	L	N	O	T	Y	
	n	P	R	T	U	Y	A	B	G	L	
	t	V	X	Z	A	E	G	H	M	R	

Ciphertext is TRVHAHLBZY

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

Click to add notes

Slide 7 of 52 English (India)

Notes

97%

Vinod

1S

1U

1M

1K

111803109 Akanksha Sha

111803104 Akanksha Kish

111803078 Prathamesh U

111803058 Omkar Anand

AutoSave Lect-VI Vinod Pachghare

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

Clipboard Slides

Font Paragraph Drawing Editing Voice Designer

Click to add title

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

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

Slide 8 of 52 English (India)



Vinod

1S

1U

1M

1K

111803109 Akanksha Sha

111803104 Akanksha Kish

111803078 Prathamesh U

111803058 Omkar Anand

AutoSave Lect-VI Vinod Pachghare

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

Clipboard Slides

Font Paragraph Drawing Editing Voice Designer

Decryption

Keyword: Ianoth erano theran nothe ranot heran

Ciphertext: SUSBZ ZVRLV TWTPA ARULE LTVTN SKZRY

PT: sheis veryh appya ndbea utifu lgirl

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	
a	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
e	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	D
h	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
n	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
o	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
r	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
t	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	

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

Click to add notes

Slide 10 of 52 English (India)

Vinod

1S

1U

1M

1K

111803109 Akanksha Sha

111803104 Akanksha Kish

111803078 Prathamesh U

111803058 Omkar Anand

Lect-VI

Search

Vinod Pachhare

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

AutoSave Off

Clipboard Slides

Font Paragraph Drawing Editing Voice Designer

Shapes Arrange Quick Styles Find Replace Select Dictate Design Ideas

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

Advantages

- For the same plaintext letter, there are multiple ciphertext.
- This helps to avoid the frequency analysis of the cipher.
- For example, in the above plaintext there are 3 e's that they have been encrypted by 'S,' 'V,' 'L', respectively.
- Plaintext: sheis veryh appya ndbea utifu lgirl
CT: SU**S**BZ Z**V**RLV TWTPA AR**U**LE LTVTN SKZRY

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

Click to add notes

Slide 11 of 52 English (India)

Notes

+108



Vinod

1S

1U

1M

1K

111803109 Akanksha Sha

111803104 Akanksha Kish

111803078 Prathamesh U

111803058 Omkar Anand

AutoSave Lect-VI

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

Vinod Pachhare

Clipboard Slides

Font Paragraph Drawing Editing Voice Designer

Paragraph

Click to add title

• This helps to hide the count of occurrence of e in the plaintext.

• So, it makes frequency analysis of the letters in the plaintext difficult.

• The implementation of this cipher is easy.

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

Slide 12 of 52 English (India)

Vinod

1S

1U

1M

1K

111803109 Akanksha Sha

111803104 Akanksha Kish

111803078 Prathamesh U

111803058 Omkar Anand

AutoSave Lect-VI

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

Vinod Pachhare

Clipboard Slides

Font Paragraph Drawing Editing Voice Designer

Paragraph

Disadvantages

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

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

Slide 13 of 52 English (India)





Vinod

1S

1U

1M

1K

111803109 Akanksha Sha

111803104 Akanksha Kish

111803078 Prathamesh U

111803058 Omkar Anand

Lect-VI

Search

Vinod Pachghare

AutoSave (off)

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

Paste New Slide Slides Section

Clipboard Slides

Font Paragraph Drawing Editing Voice Designer

Shapes Arrange Quick Styles Select Dictate Design Ideas

Find Replace Select Dictate Design Ideas

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

9

10

11

12

13

14

15

16

Transposition ciphers

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

14

Click to add notes

Slide 14 of 52 English (India)

Notes

+108



Vinod

1S

1U

1M

1K

111803109 Akanksha Sha

111803104 Akanksha Kish

111803078 Prathamesh U

111803058 Omkar Anand

Lect-VI

Search

Vinod Pachghare

AutoSave (off)

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

Clipboard Slides

Font Paragraph Drawing Editing Voice Designer

Shapes Arrange Quick Styles

Find Replace Select Dictate Design Ideas

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

Transposition ciphers

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

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

15

Click to add notes

Slide 15 of 52 English (India)

Notes

+108

Vinod

1S

1U

1M

1K

111803109 Akanksha Sha

111803104 Akanksha Kish

111803078 Prathamesh U

111803058 Omkar Anand

AutoSave (Off) Lect-VI Vinod Pachghare

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

Clipboard Slides

Font Paragraph Drawing Editing Voice Designer

17 Preparing the Key

18

19

20

21

22

23

24

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

Preparing the Key

- Suppose the key is '**another**'.
- We can assign the number to each letter in this key.
- The first letter 'a' is numbered 1.
- There are no 'B', 'C' or 'D', so the next letter to be numbered is the 'e'. So e is numbered 2, followed by h, and so on.

I

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

Slide 17 of 52 English (India)



Vinod

1S

1U

1M

1K

111803109 Akanksha Sha

111803104 Akanksha Kish

111803078 Prathamesh U

111803058 Omkar Anand

AutoSave (Off) Lect-VI Search

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

Vinod Pachghare Share Comments

Clipboard Slides

Font Paragraph Drawing Editing Voice Designer

17
18
19
20
21
22
23
24

Click to add title

a n o t h e r
1

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

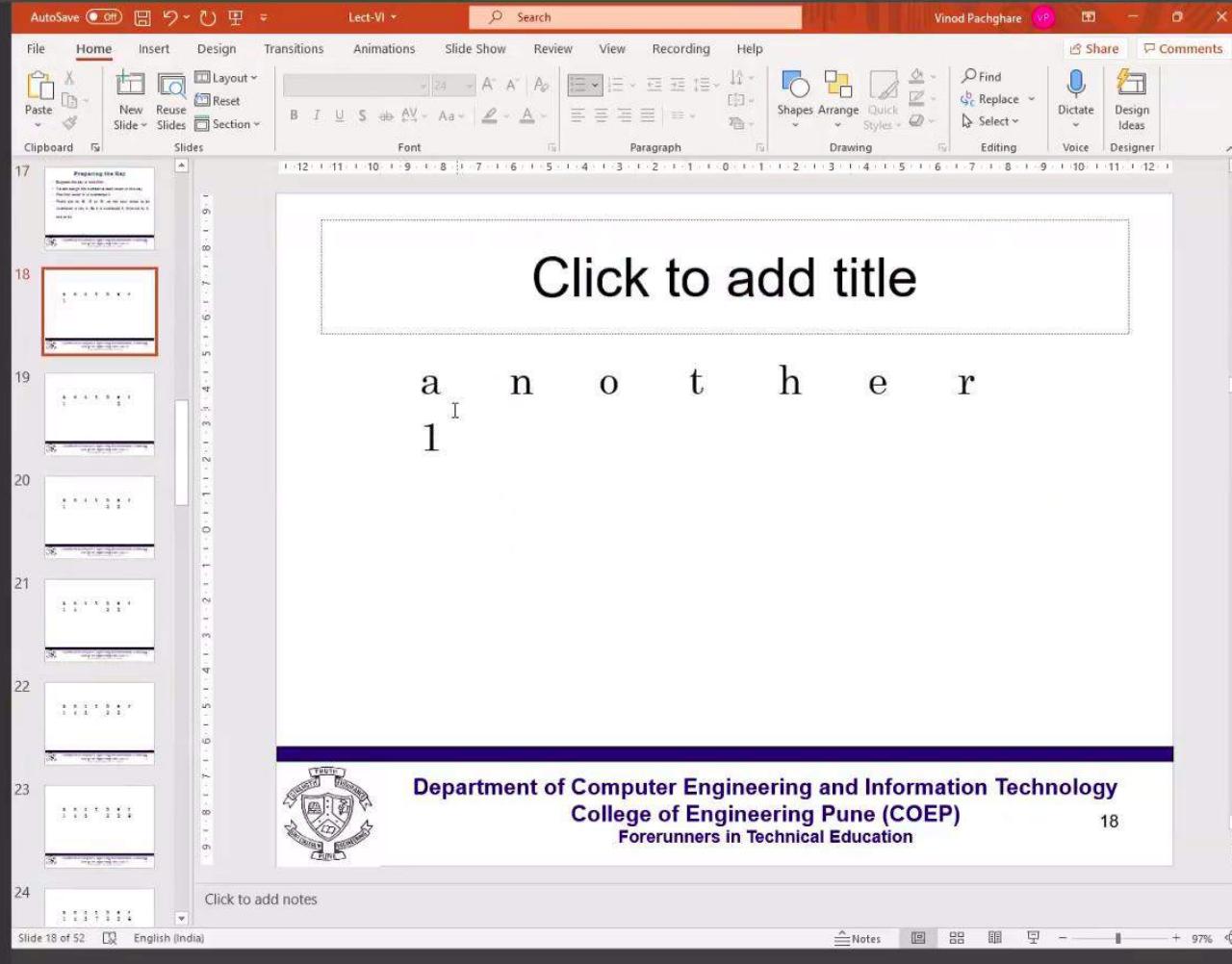
18

Click to add notes

Slide 18 of 52 English (India)

Notes - + 97%

+112





Vinod

1S

1U

1M

1K

111803109 Akanksha Sha

111803104 Akanksha Kish

111803078 Prathamesh U

111803058 Omkar Anand

AutoSave Lect-VI

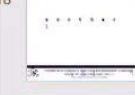
File Home Insert Design Transitions Animations Slide Show Review View Recording Help

Vinod Pachghare

Clipboard Slides

Font Paragraph Drawing Editing Voice Designer

17 

18 

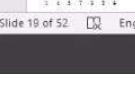
19 

20 

21 

22 

23 

24 

Click to add title

I a n o t h e r

1 2

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

19

Slide 19 of 52 English (India)

Notes

+114



Vinod

1S

1U

1M

1K

111803109 Akanksha Sha

111803104 Akanksha Kish

111803078 Prathamesh U

111803058 Omkar Anand

AutoSave Lect-VI

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

Vinod Pachghare

Clipboard Slides

Font Paragraph Drawing Editing Voice Designer

17 Processing the file

18

19

20

21

22

23

24

Click to add title

a n o t h e r

1 3 2

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

20

Click to add notes

Slide 20 of 52 English (India)

Notes

+114



Vinod

1S

1U

1M

1K

111803109 Akanksha Sha

111803104 Akanksha Kish

111803078 Prathamesh U

111803058 Omkar Anand

AutoSave Lect-VI

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

Vinod Pachghare

Clipboard Slides

Font Paragraph Drawing Editing Voice Designer

Shapes Arrange Quick Styles Select Dictate Design Ideas

17 Processing the file
Report on the file
The file has been processed.
The file has been processed.
The file has been processed.

18

19

20

21

22

23

24

Click to add title

a n o t h e r

1 4 3 2

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

21

Click to add notes

Slide 21 of 52 English (India)

Notes

+114



Vinod

1S

1U

1M

1K

111803109 Akanksha Sha

111803104 Akanksha Kish

111803078 Prathamesh U

111803058 Omkar Anand

AutoSave Lect-VI

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

Vinod Pachghare

Clipboard Slides

Font Paragraph Drawing Editing Voice Designer

17 Processing the file

18

19

20

21

22

23

24

Click to add title

a n o t h e r

1 4 5 3 2

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

Slide 22 of 52 English (India)

Notes

+114



Vinod

1S

1U

1M

1K

111803109 Akanksha Sha

111803104 Akanksha Kish

111803078 Prathamesh U

111803058 Omkar Anand

AutoSave Lect-VI

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

Vinod Pachghare

Clipboard Slides

Font Paragraph Drawing Editing Voice Designer

Shapes Arrange Quick Styles Find Replace Select Dictate Design Ideas

19

20

21

22

23

24

25

26

Click to add title

a n o t h e r
1 4 I 5 7 3 2 6

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

24

Click to add notes

Slide 24 of 52 English (India)

Notes

+114



Vinod

1S

1U

1M

1K

111803109 Akanksha Sha

111803104 Akanksha Kish

111803078 Prathamesh U

111803058 Omkar Anand

AutoSave Lect-VI Vinod Pachhare

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

Paste New Reuse Slides Reset Clipboard Slides

Font Paragraph Drawing Editing Voice Designer

19
20
21
22
23
24
25
26

• In the key word if the same letter is occurred more than one time, it should be numbered 1, 2, 3 etc. from left to write for ex. Key word is **heaven**

h e a v e n
4 2 1 6 3 5

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

Click to add notes

Slide 25 of 52 English (India)

Notes

+114



Vinod

1S

1U

1M

1K

111803109 Akanksha Sha

111803104 Akanksha Kish

111803078 Prathamesh U

111803058 Omkar Anand

AutoSave (Off) Lect-VI Search

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

Vinod Pachghare

Clipboard Slides

Font Paragraph Drawing Editing Voice Designer

Font Size: 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

Numbered keyword: 21, 22, 23, 24, 25, 26, 27, 28

Plaintext: "We are the best" written in rows under the numbered keyword

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

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

Click to add notes

Slide 27 of 52 English (India)

Notes + 97%

Vinod

1S

1U

1M

1K

111803109 Akanksha Sha

111803104 Akanksha Kish

111803078 Prathamesh U

111803058 Omkar Anand

AutoSave Lect-VI Vinod Pachhare

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

Century Schoolbook 24 A A A B I U S AV Aa AV Aa Shapes Arrange Quick Styles Find Replace Select Dictate Design Ideas

Clipboard Slides Font Paragraph Drawing Editing Voice Designer

21 22 23 24 25 26 27 28

• In the key word if the same letter is occurred more than one time, it should be numbered 1, 2, 3 etc. from left to write for ex. Key word is **heaven**

h e a v e n
4 2 1 6 3 5

Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education 25

Click to add notes

Slide 25 of 52 English (United States)

Notes

+114

Vinod

1S

1U

1M

1K

111803109 Akanksha Sha

111803104 Akanksha Kish

111803078 Prathamesh U

111803058 Omkar Anand

AutoSave (Off) Lect-VI Search Share Comments

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

Clipboard Slides

Font Paragraph Drawing Editing Voice Designer

15 16 17 18 19 20 21 22

Transposition ciphers

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

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

Slide 15 of 52 English (India)

Notes



Vinod

1S

1U

1M

1K

111803109 Akanksha Sha

111803104 Akanksha Kish

111803078 Prathamesh U

111803058 Omkar Anand

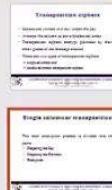
AutoSave Lect-VI

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

Vinod Pachghare

Clipboard Slides

Font Paragraph Drawing Editing Voice Designer

15 

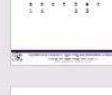
16 

17 

18 

19 

20 

21 

22 

Single columnar transposition

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

I

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

Slide 16 of 52 English (India)

Notes

+118

Vinod

1S

1U

1M

1K

111803109 Akanksha Sha

111803104 Akanksha Kish

111803078 Prathamesh U

111803058 Omkar Anand

AutoSave (Off) Lect-VI Search

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

Vinod Pachghare

Clipboard Slides Slides

Font Paragraph Drawing Editing Voice Designer

21

22

23

24

25

26 Preparing the Plaintext

27

28

• Next the plaintext “We are the best” is written in rows under the numbered keyword

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

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

Click to add notes

Slide 27 of 52 English (India)

Notes + 97%



Vinod

1S

1U

1M

1K

111803109 Akanksha Sha

111803104 Akanksha Kish

111803078 Prathamesh U

111803058 Omkar Anand

AutoSave Lect-VI Vinod Pachghare

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

Clipboard Slides

Font Paragraph

Shapes Arrange Quick Styles Drawing Editing Voice Designer

21

22

23

24

25

26

27

28

• Next the plaintext “We are the best” is written in rows under the numbered keyword

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

• AB EE ES WH TT RE

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

Click to add notes

Slide 27 of 52 English (United States)

Notes

+117



Vinod

1S

1U

1M

1K

111803109 Akanksha Sha

111803104 Akanksha Kish

111803078 Prathamesh U

111803058 Omkar Anand

AutoSave Lect-VI Vinod Pachghare

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

Clipboard Slides

Font Paragraph Drawing Editing Voice Designer

Century Schoolbook 20 A A A B I U S AV Aa Aa AV Aa Aa Aa Aa

Font Paragraph Drawing Editing Voice Designer

Shapes Arrange Quick Styles Find Replace Select Dictate Design Ideas

21

22

23

24

25

26

27

28

• Next the plaintext “We are the best” is written in rows under the numbered keyword

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

• ABEEESWHTTRE

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

Click to add notes

Slide 27 of 52 English (United States)

Notes

+118

Vinod

1S

1U

1M

1K

111803109 Akanksha Sha

111803104 Akanksha Kish

111803078 Prathamesh U

111803058 Omkar Anand

AutoSave Lect-VI Vinod Pachghare

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

Clipboard Slides

Font Paragraph Drawing Editing Voice Designer

23

24

25

26 Preparing the Plaintext

27

28 Encryption

29

30

23 24 25 26 27 28 29 30

Encryption

Read

Encryption

- Now, arrange the above message written in rows under the numbered letters of the key as per ascending order of the numbers at the top of the plaintext letters.

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

- Then the letters are copied down column wise from top to bottom. The result is ciphertext, i.e.,
AB EE ES WH TT RE

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

Slide 28 of 52 English (India)

Vinod

1S

1U

1M

1K

111803109 Akanksha Sha

111803104 Akanksha Kish

111803078 Prathamesh U

111803058 Omkar Anand

AutoSave Lect-VI Vinod Pachhare

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

Clipboard Slides

Font Paragraph Drawing Editing Voice Designer

23

24

25

26 Preparing the Planlet

27

28

29

30

• The ciphertext is
AB EE ES WH TT RE

Decryption-

h	e	a	v	e	n
4	2	1	6	3	5

A
B

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

Click to add notes

Slide 29 of 52 English (India)

Vinod

1S

1U

1M

1K

111803109 Akanksha Sha

111803104 Akanksha Kish

111803078 Prathamesh U

111803058 Omkar Anand

AutoSave (Off) Vinod Pachghare

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

Font Paragraph Drawing Editing Voice Designer

Clipboard Slides

Century Schoolbook 24 A A A A A A A A

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24

29

The ciphertext is AB EE ES WH TT RE

Decryption-

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

Read

Plaintext: WEARETHEBEST
WE ARE THE BEST

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



34

Click to add notes

Slide 34 of 52 English (United States)

97%

+118



Vinod

1S

1U

1M

1K

111803109 Akanksha Sha

111803104 Akanksha Kish

111803078 Prathamesh U

111803058 Omkar Anand

AutoSave Lect-VI Vinod Pachghare

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

Clipboard Slides

Font Paragraph Drawing Editing Voice Designer

Shapes Arrange Quick Styles Select Dictate Design Ideas

Find Replace Select Dictate Design Ideas

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

29
30
31
32
33
34
35
36

Double Columnar Transposition

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

Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education 35

Click to add notes

Slide 35 of 52 English (India)

Vinod

1S

1U

1M

1K

111803109 Akanksha Sha

111803104 Akanksha Kish

111803078 Prathamesh U

111803058 Omkar Anand

AutoSave Lect-VI Vinod Pachghare

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

Century Schoolbook 20 A A A B I U S AV Aa A Paragraph

Clipboard Slides Shapes Arrange Quick Styles Find Replace Select Dictate Design Ideas

Font Paragraph Drawing Editing Voice Designer

27

28

29

30

31

32

33

34

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

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

• ABE EEN ES WHO TT RE

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

Slide 27 of 52 English (United States)

+121

Vinod

1S

1B

1A

1K

111803109 Akanksha Sha

111803118 Karan Bhat

111803037 Urvi Sachin As

111803058 Omkar Anand

AutoSave (On) Lect-VI Search Vinod Pachghare

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

Clipboard Slides

Font Paragraph Drawing Editing Voice Designer

Century Schoolbook 24 A A A A A A A A

B I U S A A A A A A A A A A A A A A

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24

27
28
29
30
31
32
33
34

The ciphertext is 15/6 = 3 ROW HAVING 3 LETTERS

ABE EEN ES WHO TT RE

Decryption-

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

WEARETHEBESTONE

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

29

Slide 29 of 52 English (United States)

Click to add notes



Vinod

1S

1B

1A

1K

111803109 Akanksha Sha

111803118 Karan Bhat

111803037 Urvi Sachin As

111803058 Omkar Anand

AutoSave Lect-VI Vinod Pachhare

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

Paste New Slide Slides Reset Clipboard Slides

Font Paragraph Drawing Editing Voice Designer

Shapes Arrange Quick Styles Select Dictate Design Ideas

Find Replace

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

29
30
31
32
33
34
35
36

Double Columnar Transposition

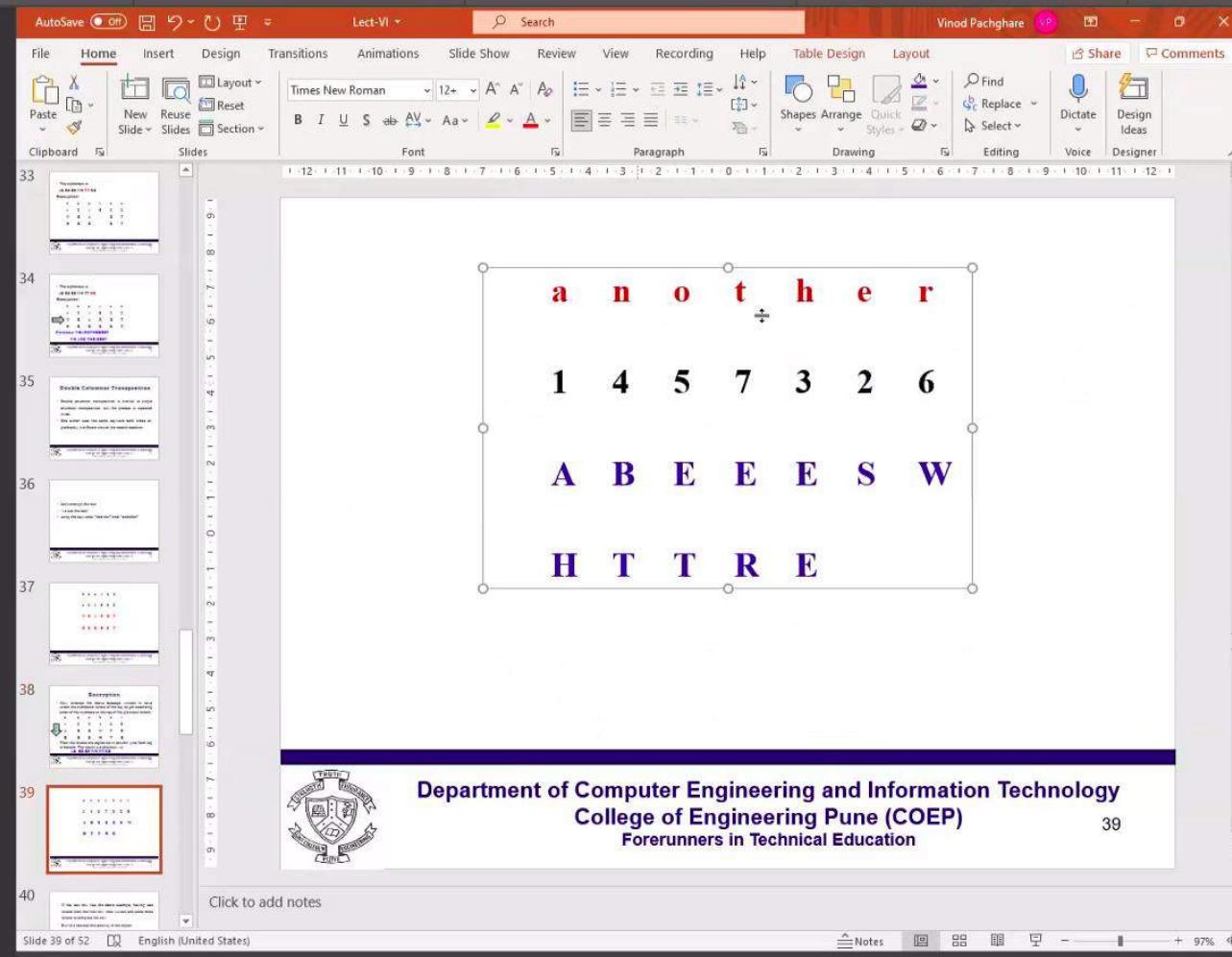
- Double columnar transposition is similar to single columnar transposition, but the process is repeated twice. I
- One either uses the same keyword both times or, preferably, a different one on the second occasion.

Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education 35

Click to add notes

Slide 35 of 52 English (India)

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



The screenshot shows a Microsoft PowerPoint slide titled 'Lect-VI' in the ribbon. The slide contains a word search puzzle. The words hidden in the grid are:

- Across: annote, 14, 5, 7, 3, 2, 6, BEETERS, HOTTIE
- Down: Anote, 4, 5, 7, 3, 2, 6, ABEETERS, HOTTIE
- Diagonals: Anote (top-left to bottom-right), BEETERS (top-right to bottom-left)
- Verticals: 1, 4, 5, 7, 3, 2, 6, ABEETERS, HOTTIE

The slide footer includes the text 'Department of Computer Engineering and Information Technology, College of Engineering Pune (COEP), Forerunners in Technical Education, 39'.

1S

Press Esc to exit full screen

1A

1K

Vinod

111803109 Akanksha Sha

111803118 Karan Bhat

111803037 Urvi Sachin As

111803058 Omkar Anand

A Microsoft PowerPoint slide titled "Lect-VI" showing a word cloud diagram. The slide includes a navigation bar with slides 33 through 40, a search bar, and a ribbon menu.

The main content area displays a word cloud diagram with the following text elements:

- Top row: a n o t h e r
- Middle row: 1 4 5 7 3 2 6
- Second row from bottom: A B E E E S W
- Bottom row: H T T R E
- Bottom-most row: AB EE ES WH TT RE

The slide footer contains the text:

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

Slide 39 of 52

Click to add notes

39:38 / 57:24

English (United States)

Notes

97%

Vinod

1S

1B

1A

1K

111803109 Akanksha Sha

111803118 Karan Bhat

111803037 Urvi Sachin As

111803058 Omkar Anand

AutoSave Lect-VI Search

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

Vinod Pachghare Share Comments

Clipboard Slides

Font Paragraph Drawing Editing Voice Designer

35

36

37

38

39

40

41

42

Read

a	e	h	n	o	r	t
1	2	3	4	5	6	7
A	S	E	B	E	W	E
H		E	T	T		R

Ciphertext: AHSEEBTETWER

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

Slide 41 of 52 English (India)

Notes + 97%



Vinod

1S

1B

1A

1K

111803109 Akanksha Sha

111803118 Karan Bhat

111803037 Urvi Sachin As

111803058 Omkar Anand

AutoSave Lect-VI Vinod Pachghare

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

Clipboard Slides

Font Paragraph Drawing Editing Voice Designer

Steganography

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

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

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

Click to add notes

Slide 48 of 52 English (India)



Vinod

1S

1B

1A

1K

111803109 Akanksha Sha

111803118 Karan Bhat

111803037 Urvi Sachin As

111803058 Omkar Anand

AutoSave Lect-VI

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

Vinod Pachghare

Clipboard Slides

Font Paragraph Drawing Editing Voice Designer

Click to add title

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

43
44
45
46
47
48
49
50

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

49

Slide 49 of 52 English (India)

Notes + 97%



Vinod

1S

1B

1A

1K

111803109 Akanksha Sha

111803118 Karan Bhat

111803037 Urvi Sachin As

111803058 Omkar Anand

AutoSave Lect-VI Vinod Pachghare

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

Clipboard Slides

Font Paragraph Drawing Editing Designer

Shapes Arrange Quick Styles Select Dictate Design Ideas

Find Replace

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

45
46
47
48
49
50
51
52

Question

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

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

Slide 50 of 52 English (India)



Vinod

1S

1B

1A

1K

111803109 Akanksha Sha

111803118 Karan Bhat

111803037 Urvi Sachin As

111803058 Omkar Anand

AutoSave Lect-VI

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

Vinod Pachhare

Clipboard Slides

Font Paragraph Drawing Editing Voice Designer

Answer

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

The Cryptography exam key is in PO Box 1212.

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

Slide 51 of 52 English (India)

Vinod

1A

Press Esc to exit full screen

1S

1K

111803037 Urvi Sachin As

111803118 Karan Bhat

111803109 Akanksha Sha

111803058 Omkar Anand

AutoSave Lect-III

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

Slide 30 of 40 English (India)

Click to add notes

30 One-Time Pad or Vernam Cipher

31

32

33

34

35

36

37

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

30 0

+107

The screenshot shows a Microsoft PowerPoint presentation in full-screen mode. The slide title is "One-Time Pad or Vernam Cipher". Below the title, there is a footer for the Department of Computer Engineering and Information Technology, College of Engineering Pune (COEP), and the text "Forerunners in Technical Education". The slide number is 30 of 40. The ribbon menu at the top includes tabs like File, Home, Insert, Design, Transitions, Animations, Slide Show, Review, View, Recording, and Help. The Home tab is selected. The ribbon also displays the name "Vinod Pachghare" and his initials "VP". The left sidebar shows a thumbnail view of the first 17 slides, which appear to be related to the topic of encryption. The status bar at the bottom indicates the slide number, language, and zoom level.

1A

Press Esc to exit full screen

1S

1K

Vinod

111803037 Urvi Sachin As

111803118 Karan Bhat

111803109 Akanksha Sha

111803058 Omkar Anand

• Different messages are encrypted by different key streams.

Three essential properties are:

- The number of possible keys is equal to the number of possible plaintexts
- The key is selected at random
- The key should be used only once

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

Slide 31 of 40 English (India)

+107

The screenshot shows a Microsoft PowerPoint slide titled 'Lect-III' with the subtitle 'Stream Ciphers'. The slide contains a bulleted list: '• Different messages are encrypted by different key streams.' Below this, under the heading 'Three essential properties are:', there is another bulleted list: '• The number of possible keys is equal to the number of possible plaintexts', '• The key is selected at random', and '• The key should be used only once'. At the bottom of the slide, there is a footer with the text 'Department of Computer Engineering and Information Technology', 'College of Engineering Pune (COEP)', 'Forerunners in Technical Education', and the number '31'. The slide also includes a navigation bar with icons for notes, search, and other presentation controls.



Vinod

1A

1B

1S

1K

111803037 Urvi Sachin As

111803118 Karan Bhat

111803109 Akanksha Sha

111803058 Omkar Anand

AutoSave Lect-III Vinod Pachghare

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

Clipboard Slides

Font Paragraph Drawing Editing Voice Designer

Shapes Arrange Quick Styles Select Dictate Design Ideas

Find Replace Select Dictate Design Ideas

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

30
31
32
33
34
35
36
37

CT = $(PT \oplus K) \text{ mod } 26$

OR

• Click icon to add table

PT	K	CT = PT \oplus K
0	10	0
0	1	1
1	0	1
1	1	0

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

Click to add notes

Slide 32 of 40 English (India)

Notes

+107

Vinod

1A

1B

1S

1K

111803037 Urvi Sachin As

111803118 Karan Bhat

111803109 Akanksha Sha

111803058 Omkar Anand

AutoSave Lect-III Vinod Pachghare

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

Century Schoolbook 24 A⁺ A⁻ B I U S AV Aa A Drawing Editing Voice Designer

Font Paragraph Numbered List Bulleted List Alignment Text Direction Orientation Spacing Paragraph Spacing

Clipboard Slides

Shapes Arrange Quick Styles Find Replace Select Dictate Design Ideas

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

30
31
32
33
34
35
36
37

EXAMPLE

Message: WE LIVE IN A WORLD FULL OF BEAUTY

Key: ABCDEFGHIJKLMNOPQRSTUVWXYZ

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

Slide 33 of 40 English (United States)

The slide is titled "Encryption". It contains a table with the following data:

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

The ciphertext is "WFNLZJOUIFYCXQTJBCGYVZWRRX"

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



1A

Vinod

111803154 Hrishikesh Jay

Cryptography and Network Security
Unit-III

Date: 15 Sept 2021

Dr. V. K. Pachghare

ENCRYPTION TECHNIQUES

Advanced Encryption Standard (AES)

Introduction

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

Click to add notes

Cryptography and Network Security
Unit-III

Date: 15 Sept 2021

Dr. V. K. Pachghare

Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)



Slide 1 of 92 | "Default Design" | English (India) | 00:45 / 01:06:11 | 98% |  

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

Introduction

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

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



Slide 4 of 92 | "Default Design" | English (India) | +27

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

vinod-16.com - Microsoft PowerPoint - Default Design - Microsoft PowerPoint

File Home Insert Design Transitions Animations Slide Show Review View

Cut Copy Format Painter New Slide Section Reset Layout Font Paragraph Drawing Editing

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

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

Slide 5 of 92 | "Default Design" | English (India) | 98% +74

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

vinod-16.com - Microsoft PowerPoint - Microsoft Activation Key.txt

File Home Insert Design Transitions Animations Slide Show Review View

Cut Copy Format Painter New Slide Section Reset Layout 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

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

I

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

Slide 7 of 92 | "Default Design" | English (India) | 98% | +74



Vinod

1A

1S

1N

1P

111803154 Hrishikesh Jay

141903015 Vaishnavi Raje

111803158 Ruhee Rajesh

111803116 Aryan Prasad

Document 16 - Microsoft PowerPoint - Default Design.pptx

File Home Insert Design Transitions Animations Slide Show Review View

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

This transformation forms a state.

A state defines the current condition of the block during encryption.

A state is nothing but the block of 4×4 matrix of bytes which is currently being processed on.

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

Slide 8 of 92 | "Default Design" | English (India) | 98% | 11:31 / 01:06:11



Vinod

1A

1S

1N

1P

111803154 Hrishikesh Jay

141903015 Vaishnavi Raje

111803158 Ruhee Rajesh

111803116 Aryan Prasad

vinod-16.com - Microsoft PowerPoint - Default Design.htm - Microsoft PowerPoint

Terminology

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

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

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



Slide 9 of 92 | "Default Design" | English (India) | 98% | Navigation icons



Vinod

1A

1S

1N

1P

111803154 Hrishikesh Jay

141903015 Vaishnavi Raje

111803158 Ruhee Rajesh

111803116 Aryan Prasad

vinod-16.com - Microsoft PowerPoint - AES and Activation Function

File Home Insert Design Transitions Animations Slide Show Review View

Cut Copy Format Painter New Slide Reset Section B I U S A Aa Aa Aa Aa Convert to SmartArt

Clipboard Slides Font Paragraph Drawing Editing

AES

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

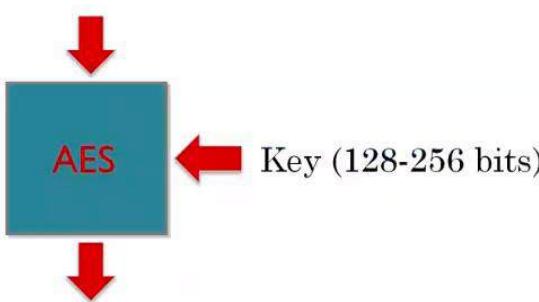
Key Size [bits]	Number of Rounds
128	10
192	12
I 256	14

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

Slide 10 of 92 | "Default Design" | English (India) | 98% | +90

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

AES Conceptual Scheme



```

graph TD
    A[Plaintext (128 bits)] --> B[AES]
    C[Key (128-256 bits)] --> B
    B --> D[Ciphertext (128 bits)]
  
```

Plaintext (128 bits)

AES

Key (128-256 bits)

Ciphertext (128 bits)

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

Slide 11 of 92 | "Default Design" | English (India) | +96

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

Structure of AES

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

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





Vinod

1A

1S

1N

1P

111803154 Hrishikesh Jay

141903015 Vaishnavi Raje

111803158 Ruhee Rajesh

111803116 Aryan Prasad

vinod-16.com - Microsoft PowerPoint - Microsoft Activation Key.txt

File Home Insert Design Transitions Animations Slide Show Review View

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

Key expansion Subkeys are generated from original key for each round

Initial round XOR operation between the state and the round key

Rounds 1 to 9 Each round has four steps: byte substitution shift rows, mix columns, add subkey

Final round This round has three steps: byte substitution, shift rows, add subkey

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

Slide 12 of 92 | "Default Design" | English (India) | 98% +96

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

Each round consists of four stages

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

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

Slide 13 of 92 | "Default Design" | English (India) | +106



Vinod

1A

1S

1N

1P

111803154 Hrishikesh Jay

141903015 Vaishnavi Raje

111803158 Ruhee Rajesh

111803116 Aryan Prasad

Untitled-16.pptx Microsoft PowerPoint Microsoft Animation Layer

File Home Insert Design Transitions Animations Slide Show Review View

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

Clipboard Slides

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

```
graph TD; State1[State] --> Sub[Byte substitution]; Sub --> State2[State]; State2 --> Shift[Shift rows]; Shift --> State3[State]; State3 --> Mix[Mix columns]; Mix --> State4[State]; State4 --> Add[Add subkey]; Add --> State5[State]
```

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

Slide 14 of 92 | "Default Design" | English (India) | +108

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

1. Byte substitution (SubBytes)

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

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

Slide 15 of 92 | "Default Design" | English (India) | +108



Vinod

1A

1S

1N

1P

111803037 Urvi Sachin As

141903015 Vaishnavi Raje

111803158 Ruhee Rajesh

111803116 Aryan Prasad

username-16.cppx - Microsoft PowerPoint - Microsoft Animation Browser

File Home Insert Design Animations Slide Show Review View

Cut Copy Format Painter

New Slide Section

Font Paragraph Drawing Editing

Clipboard Slides

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

S-box

	y															
	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	18	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	P9	02	7F	50	3C	9F	A8
7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

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



Vinod

1A

1S

1N

1P

111803037 Urvi Sachin As

141903015 Vaishnavi Raje

111803158 Ruhee Rajesh

111803116 Aryan Prasad

username-16.cppx - Microsoft PowerPoint - Inv_S-box_Decryption.pptx

File Home Insert Design Transitions Animations Slide Show Review View

Cut Copy Format Painter New Slide Reset Section B I U S A Aa A Aa Aa Aa Aa Aa Convert to SmartArt 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

Inv. S-box (Decryption)

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

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



Slide 17 of 92 | "Default Design" | English (India) | +109



Vinod

1A

1S

1N

1P

111803037 Urvi Sachin As

141903015 Vaishnavi Raje

111803158 Ruhee Rajesh

111803116 Aryan Prasad

vinod-16.com - Microsoft PowerPoint - D:\mca2\Autonav\Index.pptx

File Home Insert Design Transitions Animations Slide Show Review View

Cut Copy Format Painter New Slide Reset Section B I U S A A A A A A Convert to SmartArt 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

Byte substitution (SubBytes)

The SubBytes and Inv SubBytes transformations are inverses of each other

State

$$\begin{bmatrix} 00 & 12 & 0C & 08 \\ 04 & 04 & 00 & 23 \\ 12 & 12 & 13 & 19 \\ 14 & 00 & 11 & 19 \end{bmatrix}$$

SubByte

State

$$\begin{bmatrix} 63 & C9 & FE & 30 \\ F2 & F2 & 63 & 26 \\ C9 & C9 & 7D & D4 \\ FA & 63 & 82 & D4 \end{bmatrix}$$

InvSubByte

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

Slide 18 of 92 | Default Design | English (India) | 98% | +111



Vinod

1A

Press Esc to exit full screen

1N

1P

111803037 Urvi Sachin As

141903015 Vaishnavi Raje

111803158 Ruhee Rajesh

111803116 Aryan Prasad

username-16.cppx - Microsoft PowerPoint - Microsoft Activation License

File Home Insert Design Transitions Animations Slide Show Review View

Cut Copy Format Painter New Slide Reset Section B I U S A Aa Aa Aa Convert to SmartArt 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

2. Shift Rows

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

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



Slide 19 of 92 | "Default Design" | English (India) | +114



Vinod

1A

1S

1N

1P

111803037 Urvi Sachin As

141903015 Vaishnavi Raje

111803158 Ruhee Rajesh

111803116 Aryan Prasad

vinod-16.com - Microsoft PowerPoint - Default Design - Microsoft PowerPoint

File Home Insert Design Transitions Animations Slide Show Review View

Cut Copy Format Painter New Slide Reset Section Convert to SmartArt

Clipboard Slides Font Paragraph Drawing Editing

Shift Row

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

Before Shift

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

Slide 21 of 92 | "Default Design" | English (India) | +115



Vinod

1A

1S

1N

1P

111803037 Urvi Sachin As

141903015 Vaishnavi Raje

111803158 Ruhee Rajesh

111803116 Aryan Prasad

vinod-16.cppx Microsoft PowerPoint - [Autosave] Activation banner

File Home Insert Design Transitions Animations Slide Show Review View

Cut Copy Format Painter New Slide Section Reset Layout B I U S Aa Aa Aa Aa Convert to SmartArt 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

Shift Row

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

Before Shift *After Shift*

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



Vinod

1A

1S

1N

1P

111803037 Urvi Sachin As

141903015 Vaishnavi Raje

111803158 Ruhee Rajesh

111803116 Aryan Prasad

File Home Insert Design Transitions Animations Slide Show Review View

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

Shift Row

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

Before Shift After Shift

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

Speed 2x

Slide 25 of 92 | Default Design | English (India)



Vinod

1A

1S

1N

1P

111803037 Urvi Sachin As

141903015 Vaishnavi Raje

111803158 Ruhee Rajesh

111803116 Aryan Prasad

document 16.pptx Microsoft PowerPoint - Default Design - Untitled - 1

File Home Insert Design Transitions Animations Slide Show Review View

Cut Copy Format Painter New Slide Section Reset Layout Font Paragraph Drawing Editing

Font Size: 32 30 28 26 24 22 20 18 16 14 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

3. Mix Columns

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

I

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

Slide 26 of 92 | "Default Design" | English (India) | 98% +116



Vinod

1A

1S

1N

1P

111803037 Urvi Sachin As

141903015 Vaishnavi Raje

111803158 Ruhee Rajesh

111803116 Aryan Prasad

Lecture-16.pptx Microsoft PowerPoint Microsoft Automation based.

File Home Insert Design Transitions Animations Slide Show Review View

Cut Copy Format Painter New Slide Section Reset Layout B I U S Aa Aa Aa Aa Convert to SmartArt 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

3. Mix Columns

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

I

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

Slide 26 of 92 | Default Design | English (India)

33:03 / 01:06:11 98%



Vinod

1A

1S

1N

1P

111803037 Urvi Sachin As

141903015 Vaishnavi Raje

111803158 Ruhee Rajesh

111803116 Aryan Prasad

username-16.cppx - Microsoft PowerPoint - Microsoft Animation Browser

File Home Insert Design Transitions Animations Slide Show Review View

Cut Copy Format Painter

New Slide Section

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

$$\begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix}$$

Multiplication Matrix

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

State Matrix

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

Slide 27 of 92 | "Default Design" | English (India) | 98% | +116



Vinod

1A

1S

1N

1P

111803037 Urvi Sachin As

141903015 Vaishnavi Raje

111803158 Ruhee Rajesh

111803116 Aryan Prasad

vinod-16.com - Microsoft PowerPoint - Default Design - Untitled - 1

Click to add title

b1 = (b1 * 2) XOR (b2*3) XOR (b3*1) XOR (b4*1)
b2 = (b1 * 1) XOR (b2*2) XOR (b3*3) XOR (b4*1)
b3 = (b1 * 1) XOR (b2*1) XOR (b3*2) XOR (b4*3)
b4 = (b1 * 3) XOR (b2*1) XOR (b3*1) XOR (b4*2)


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

Slide 28 of 92 | "Default Design" | English (India) |  +116



Vinod

1A

1S

1N

1P

111803037 Urvi Sachin As

141903015 Vaishnavi Raje

111803158 Ruhee Rajesh

111803116 Aryan Prasad

username-16.cppx - Microsoft PowerPoint - Microsoft PowerPoint

File Home Insert Design Transitions Animations Slide Show Review View

Cut Copy Format Painter

New Slide Section

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

Galois Field Multiplication

- Multiplication of a value by 02 can be implemented as
 - Shift all the bits to the left by 1 position
 - If bit B_7 is 0, then bit B_0 is 0

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

Slide 30 of 92 | "Default Design" | English (India) | 36:27 / 01:06:11 | 98% | Full Screen



Vinod

1A

Press Esc to exit full screen

1N

1P

111803037 Urvi Sachin As

141903015 Vaishnavi Raje

111803158 Ruhee Rajesh

111803116 Aryan Prasad

File Home Insert Design Transitions Animations Slide Show Review View

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

Galois Field Multiplication

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

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



Slide 31 of 92 | "Default Design" | English (India) | 98% | +116



Vinod

1A

1S

1N

1P

111803037 Urvi Sachin As

141903015 Vaishnavi Raje

111803158 Ruhee Rajesh

111803116 Aryan Prasad

username-16.com - Microsoft PowerPoint - Default Design - Untitled Document - Microsoft PowerPoint

File Home Insert Design Transitions Animations Slide Show Review View

Cut Copy Format Painter New Reset Slide Section 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

Click to add title

- Multiplication of a value by 03 to N can be implemented as
- $N \oplus 02 \cdot N$

I

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

Slide 32 of 92 | "Default Design" | English (India) | 98% | 38:28 / 01:06:11



Vinod

1A

1S

1N

1P

111803037 Urvi Sachin As

141903015 Vaishnavi Raje

111803158 Ruhee Rajesh

111803116 Aryan Prasad

For Ex:- $02 * 87$ Shift left by 1 bit position and $B_0 = 0$ $0000\ 1110$ 



Vinod

1A

1S

1N

1P

111803037 Urvi Sachin As

141903015 Vaishnavi Raje

111803158 Ruhee Rajesh

111803116 Aryan Prasad

Lecture-16.pptx Microsoft PowerPoint Microsoft Animation (Presentation)

File Home Insert Design Transitions Animations Slide Show Review View

Cut Copy Format Painter Paste New Slide Section Reset Layout 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

03 . 6E can be written as
6E \oplus {02 * 6E}
I

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

Slide 37 of 92 | "Default Design" | English (India) | +112



Vinod

1A

1S

1N

1P

111803037 Urvi Sachin As

141903015 Vaishnavi Raje

111803158 Ruhee Rajesh

111803116 Aryan Prasad

03 . 6E can be written as

$$6E \oplus \{02 * 6E\}$$
$$6E = 0110 \quad 1110$$
$$\{02 * 6E\} = 0110 \quad 1110$$

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

$$1101 \quad 1100$$

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

Slide 41 of 92 | "Default Design" | English (U.S.) | 98% | +113

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

03 . 6E can be written as

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

$$\begin{array}{r}
 0110 \ 1110 \ \oplus \ 11011100 \\
 0110 \ 1110 \ \quad (6E) \\
 \oplus \ 1101 \ 1100 \ \quad (02 * 6E) \\
 \hline
 1011 \ 0010
 \end{array}$$

$$03 . 6E = 1011 \ 0010 \ [B2]$$


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

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

vinod-16.com - Microsoft PowerPoint - Default Design - Microsoft PowerPoint

File Home Insert Design Transitions Animations Slide Show Review View

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

Font Size: 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

4. Add Subkey (AddRoundKey)

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

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

Slide 45 of 92 | "Default Design" | English (India) | +113



Vinod

1A

1S

1N

1P

111803037 Urvi Sachin As

141903015 Vaishnavi Raje

111803158 Ruhee Rajesh

111803116 Aryan Prasad

username-16.cpp - Microsoft PowerPoint - Simultaneous Activation License

File Home Insert Design Transitions Animations Slide Show Review View

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

An iteration of the above steps 1 to 4 is called a round.

The amount of rounds of the algorithm depends on the key size.

The only exception being that in the last round the Mix Column step is not performed, to make the algorithm reversible during decryption

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

Slide 46 of 92 | "Default Design" | English (India) | 98% +113



Vinod

1A

1S

1N

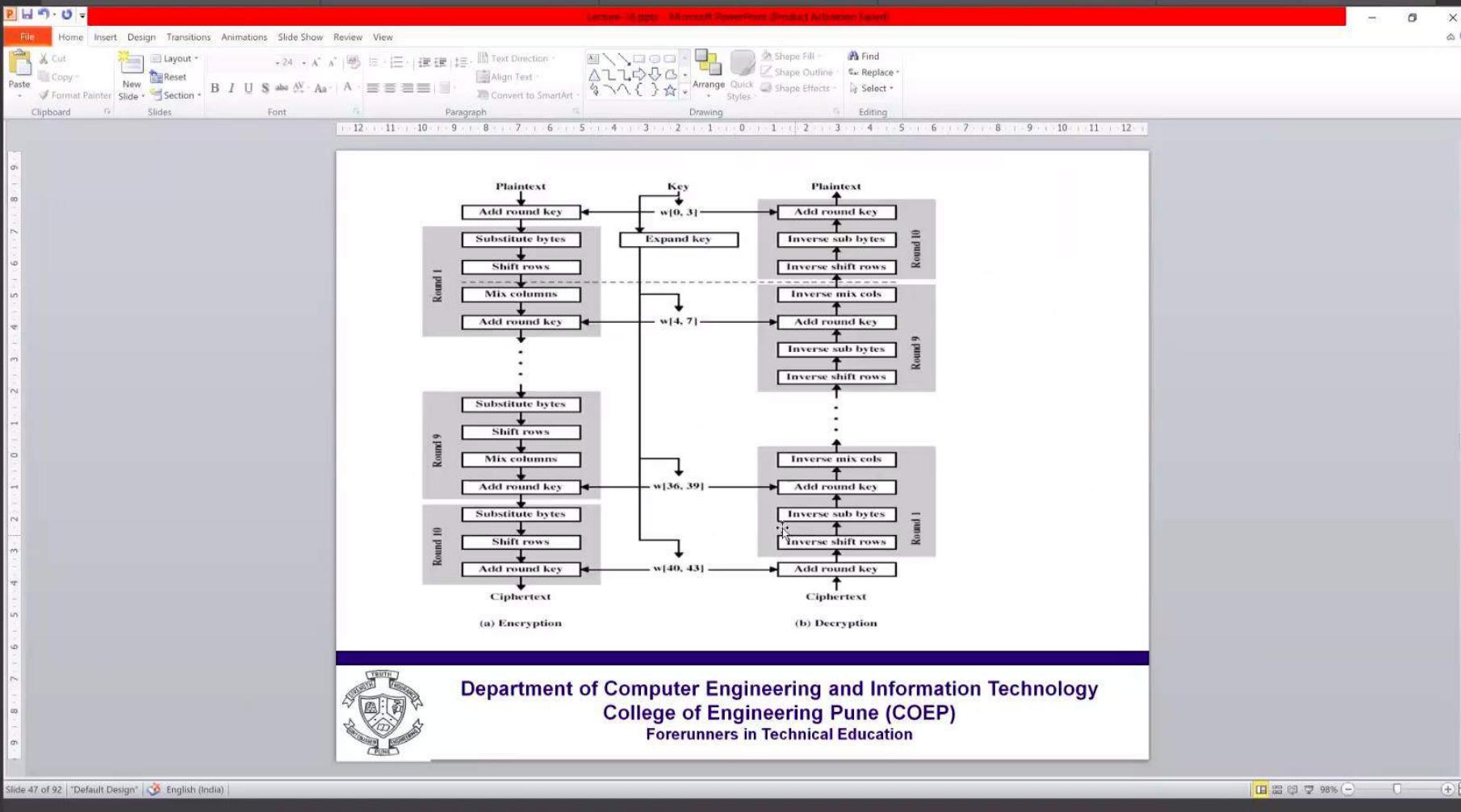
1P

111803037 Urvi Sachin As

141903015 Vaishnavi Raje

111803158 Ruhee Rajesh

111803116 Aryan Prasad



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

Lecture-18.pptx Microsoft PowerPoint Product Activation Required

File Home Insert Design Transitions Animations Slide Show Review View

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

Key Generation

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

Slide 48 of 92 | "Default Design" | English (India) | +114



Vinod

1A

1S

1A

1P

111803037 Urvi Sachin As

141903015 Vaishnavi Raje

111803036 Manish Naray

111803116 Aryan Prasad

username-16.cppx - Microsoft PowerPoint - Microsoft Activation License

File Home Insert Design Transitions Animations Slide Show Review View

Cut Copy Format Painter

New Slide Section

Font Paragraph

Drawing Editing

Clipboard Slides

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

Click to add title

- One key has 128 bits or 16 bytes
- These subkeys will never be reused.
- The logic of subkey generation is designed in such a way that, changes in one bit of a key affects the subkeys of the several rounds.

I

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

Slide 54 of 92 | "Default Design" | English (India)

45:53 / 01:06:11

98%

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

Document - 16 copy - Microsoft PowerPoint - Default Design - Untitled - Microsoft PowerPoint

File Home Insert Design Transitions Animations Slide Show Review View

Cut Copy Format Painter New Slide Section Reset Layout Font Paragraph Drawing Editing

Steps for subkeys generation

Step 1

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

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

Slide 51 of 92 | "Default Design" | English (India) | 98% | +115



Vinod

1A

1S

1A

1P

111803037 Urvi Sachin As

141903015 Vaishnavi Raje

111803036 Manish Naray

111803116 Aryan Prasad

File Home Insert Design Transitions Animations Slide Show Review View

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

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

$$[w_0 \quad w_1 \quad w_2 \quad w_3]$$

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

Slide 62 of 92 | "Default Design" | English (India) | +115

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

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

$$w_0 = (b_0; b_1; b_2; b_3)$$

$$w_1 = (b_4; b_5; b_6; b_7)$$

$$w_2 = (b_8; b_9; b_{10}; b_{11})$$

$$w_3 = (b_{12}; b_{13}; b_{14}; b_{15})$$

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



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

	1A	1S	1A	1P
Vinod	111803037 Urvi Sachin As	141903015 Vaishnavi Raje	111803036 Manish Naray	111803116 Aryan Prasad
<p>Step 2:</p> <p>Calculate $g[w_3]$ using following steps.</p> <ul style="list-style-type: none">a) Perform circular left shift of the bytes of w_3 (fourth word of a key).b) Perform substitution of the bytes using S-box.c) Add round constant <p> Department of Computer Engineering and Information Technology College of Engineering Pune (COEP) Forerunners in Technical Education</p>				

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

username-16.cppx - Microsoft PowerPoint - Microsoft PowerPoint

File Home Insert Design Transitions Animations Slide Show Review View

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

Step 2:

Calculate $g[w_3]$ using following steps.

- a) Perform circular left shift of the bytes of w_3 (fourth word of a key).
- b) Perform substitution of the bytes using S-box.
- c) Add round constant

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

Slide 64 of 92 | "Default Design" | English (India) | 98% | +113



Vinod

1A

1S

1A

1P

111803037 Urvi Sachin As

141903015 Vaishnavi Raje

111803036 Manish Naray

111803116 Aryan Prasad

File Home Insert Design Transitions Animations Slide Show Review View

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

S-Box for Key Generation

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

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



Slide 65 of 92 | "Default Design" | English (India) | +115



Vinod

1A

1S

1A

1P

111803037 Urvi Sachin As

141903015 Vaishnavi Raje

111803036 Manish Naray

111803116 Aryan Prasad

vinod-16.com - Microsoft PowerPoint - Default Design - Microsoft PowerPoint

File Home Insert Design Transitions Animations Slide Show Review View

Cut Copy Format Painter New Slide Reset Section Slide Section

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

Round Constant (RCon)

- RCon is a word in which the three rightmost bytes are zero
- It is different for each round and defined as:
$$RCon[j] = (RCon[j], 0, 0, 0)$$
where $RCon[1] = 1$, $RCon[j] = 2 * RCon[j-1]$
- Multiplication is defined over $GF(2^8)$ but can be implemented in Lookup Table

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

confusion

Slide 66 of 92 | "Default Design" | English (India) | 98% | +115



Vinod

1A

1S

1A

1P

111803037 Urvi Sachin As

141903015 Vaishnavi Raje

111803036 Manish Naray

111803116 Aryan Prasad

vinod-16.com - Microsoft PowerPoint - Default Design - Microsoft PowerPoint

File Home Insert Design Transitions Animations Slide Show Review View

Cut Copy Format Painter New Slide Section Reset Layout 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

Round	Constant (RCon)	Round	Constant (RCon)
1	<u>(01 00 00 00)₁₆</u>	6	<u>(20 00 00 00)₁₆</u>
2	<u>(02 00 00 00)₁₆</u>	7	<u>(40 00 00 00)₁₆</u>
3	<u>(04 00 00 00)₁₆</u>	8	<u>(80 00 00 00)₁₆</u>
4	<u>(08 00 00 00)₁₆</u>	9	<u>(1B 00 00 00)₁₆</u>
5	<u>(10 00 00 00)₁₆</u>	10	<u>(36 00 00 00)₁₆</u>

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

Slide 67 of 92 | "Default Design" | English (India) | 98% | +115

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

File Home Insert Design Transitions Animations Slide Show Review View

Cut Copy Format Painter

New Slide Section

Font Paragraph

Drawing Editing

Click to add title

Step 3

Generation of round key for first round.

$w_4 = w_0 \text{ XOR } g(w_3)$

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

Slide 68 of 92 | "Default Design" | English (India) | 98% | +114

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

vinod-16.com - Microsoft PowerPoint - Default Design - Microsoft PowerPoint

File Home Insert Design Transitions Animations Slide Show Review View

Cut Copy Format Painter

Clipboard Slides New Section

Font Paragraph Drawing Editing

Text Direction Align Text Convert to SmartArt

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

$w_4 = w_0 \text{ XOR } g(w_3)$

$w_5 = w_1 \text{ XOR } w_4$

$w_6 = w_2 \text{ XOR } w_5$

$w_7 = w_3 \text{ XOR } w_6$

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



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

Slide 69 of 92 | "Default Design" | English (India) | +114



Vinod

1A

Press Esc to exit full screen

1A

1P

111803037 Urvi Sachin As

141903015 Vaishnavi Raje

111803036 Manish Naray

111803116 Aryan Prasad

File Home Insert Design Transitions Animations Slide Show Review View

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

Subkey 2

$w_0 = w_4$

$w_1 = w_5$ I

$w_2 = w_6$

$w_3 = w_7$

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

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

Slide 70 of 92 | "Default Design" | English (India) | 98% +115

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

AES Example

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

Slide 71 of 92 | "Default Design" | English (India) | 98% | +113

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

Key in Hex (128 bits):

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

Plaintext in Hex (128 bits):

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



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



Vinod

1A

1S

1A

1P

111803037 Urvi Sachin As

141903015 Vaishnavi Raje

111803036 Manish Naray

111803116 Aryan Prasad

File Home Insert Design Transitions Animations Slide Show Review View Drawing Tools
Cut Copy Paste Format Painter New Section... Layout... Century Schoolbook - 24pt A A¹ Text Direction... Align Text... Convert to SmartArt... Drawing Editing
Clipboard Slides Font Paragraph
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23

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

Plaintext in Hex (128 bits):
54 77 6F 20 4F 6E 65 20 4E 69 6E 65 20 54 77 6F

I

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



Slide 72 of 92 | "Default Design" | English (U.S.) | 98% | +109



Vinod

1A

1S

1A

1P

111803037 Urvi Sachin As

141903015 Vaishnavi Raje

111803036 Manish Naray

111803116 Aryan Prasad

vinod-16 copy Microsoft PowerPoint Product Activation Layout

File Home Insert Design Transitions Animations Slide Show Review View

Cut Copy Format Painter New Slide Reset Section B I U S also A A A A Convert to SmartArt

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

Click to add title

$$\begin{bmatrix} 54 & 73 & 20 & 67 \\ 68 & 20 & 4B & 20 \\ 61 & 6D & 75 & 46 \\ 74 & 79 & 6E & 75 \\ w_0 & w_1 & w_2 & w_3 \end{bmatrix}$$

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

Slide 74 of 92 | "Default Design" | English (India) | 98% | 56:15 / 01:06:11

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

vinod-16.pptx Microsoft PowerPoint Microsoft PowerPoint

File Home Insert Design Transitions Animations Slide Show Review View

Cut Copy Format Painter New Slide Section Reset Layout B I U S also A A A A Convert to SmartArt Clipboard Slides Font Paragraph Drawing Editing

Roundkey Generation

Key in Hex (128 bits):

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

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

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

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

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

I

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

Slide 75 of 92 | "Default Design" | English (India) | 98% +109



Vinod

1A

Press Esc to exit full screen

1A

1P

111803037 Urvi Sachin As

141903015 Vaishnavi Raje

111803036 Manish Naray

111803116 Aryan Prasad

File Home Insert Design Transitions Animations Slide Show Review View Drawing Tools

C:\Users\16-computer\Microsoft PowerPoint Product Activation Key.txt

Clipboard Slides Font Paragraph Drawing Editing

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

g(w₃):
circular byte left shift of w₃:
(20; 46; 75; 67)

Byte Substitution (S-Box): →
(B7; 5A; 9D; 85)

Adding round constant
(01; 00; 00; 00) gives:
g(w₃) = (B6; 5A; 9D; 85)

0111
0001 0110
0110

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

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

Slide 76 of 92 | "Default Design" | English (U.S.) | +109



Vinod

1A

1S

1A

1P

111803037 Urvi Sachin As

141903015 Vaishnavi Raje

111803036 Manish Naray

111803116 Aryan Prasad

vinod-16.com Microsoft PowerPoint Document Activation Required

File Home Insert Design Transitions Animations Slide Show Review View

Cut Copy Format Painter New Slide Section Reset Layout B I U S A Aa A Convert to SmartArt 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

$w_0 \oplus g(w_3) \oplus w_4 \rightarrow$

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

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

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

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

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

First roundkey:

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

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

Slide 77 of 92 | "Default Design" | English (India) | 98% | +110

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

username-16.com - Microsoft PowerPoint - Default Design - Untitled - 1

File Home Insert Design Transitions Animations Slide Show Review View

Cut Copy Format Painter New Slide Section Reset Layout 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

Round 0

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

Slide 78 of 92 | "Default Design" | English (India) | 98% | +109



Vinod

1A

1S

1A

1P

111803037 Urvi Sachin As

141903015 Vaishnavi Raje

111803036 Manish Naray

111803116 Aryan Prasad

username-16.com - Microsoft PowerPoint - Default Design - Untitled - 1.pptx

File Home Insert Design Transitions Animations Slide Show Review View

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

State Matrix and Roundkey 0 Matrix

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

State Matrix(Plaintext) Key

$$\begin{array}{ccc} 69 & 0110 & 1001 \\ \oplus & 4B & \hline 0100 & 1011 \\ & 0010 & 0010 = 22 \end{array}$$

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

Slide 79 of 92 | "Default Design" | English (India) | 98% | +109

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

vinod-16.com - Microsoft PowerPoint Default Activation Layout

File Home Insert Design Transitions Animations Slide Show Review View

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

Round 1

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

Slide 81 of 92 | "Default Design" | English (India) | +106

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

vinod-16.com - Microsoft PowerPoint - Default Design - Microsoft PowerPoint

File Home Insert Design Transitions Animations Slide Show Review View

Cut Copy Format Painter New Slide Section Reset Layout Font Paragraph Drawing Editing

1. Byte substitution (SubBytes)

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

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

Slide 82 of 92 | "Default Design" | English (India) | 98% | +106

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

File Home Insert Design Transitions Animations Slide Show Review View

Cut Copy Format Painter New Slides Section Layout Reset

Clipboard Slides Font Paragraph Text Direction Align Text Convert to SmartArt

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

Click to add title

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

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

Slide 83 of 92 | "Default Design" | English (India) | +106

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

2. Shift Rows

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

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

Slide 85 of 92 | "Default Design" | English (India) | +106

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

File Home Insert Design Transitions Animations Slide Show Review View

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

Clipboard Slides 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

3. Mix Column

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

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

$$= BA$$

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

Slide 86 of 92 | "Default Design" | English (India) | 98% | +106

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

File Home Insert Design Transitions Animations Slide Show Review View

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

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

2 x 63

63 => 0110 0011

Shift left-> 1100 0110

3 x 2F

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

2 x 2F = 0010 1111

Shift Left => 0101 1110

XOR 2F => 0010 1111

3 x 2F 0 111 0001

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

Slide 87 of 92 | "Default Design" | English (India) | 98% | +106



Vinod

1A

1S

1A

1P

111803037 Urvi Sachin As

141903015 Vaishnavi Raje

111803036 Manish Naray

111803116 Aryan Prasad

vinod-16.com - Microsoft PowerPoint - Default Design - Activation Required

File Home Insert Design Transitions Animations Slide Show Review View

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

BA 84 E8 1B
75 A4 8D 40
F4 8D 06 7D
7A 32 0E 5D

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

⊕ =

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

Output after round 1

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

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

Slide 89 of 92 | "Default Design" | English (India) | 98% | +103

Vinod

1A

1S

1A

1P

111803037 Urvi Sachin As

141903015 Vaishnavi Raje

111803036 Manish Naray

111803116 Aryan Prasad

username-16.com - Microsoft PowerPoint - Default Design - Microsoft PowerPoint

File Home Insert Design Transitions Animations Slide Show Review View

Cut Copy Format Painter New Slide Section Layout Reset Font Paragraph Drawing Editing

Font Size: 24 11 10 9 8 7 6 5 4 3 2 1 0 1 2 3 4 5 6 7 8 9 10 11 12

Comparison of AES with DES

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

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

Slide 90 of 92 | "Default Design" | English (India) | 98% | +103



Vinod

1A

1S

1A

1P

111803037 Urvi Sachin As

141903015 Vaishnavi Raje

111803036 Manish Naray

111803116 Aryan Prasad

File Home Insert Design Transitions Animations Slide Show Review View

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

Confusion

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

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

Slide 92 of 92 | "Default Design" | English (India) | +101

1D



1P

1P

1K

111803111 Atharva Kailas

Vinod

111803155 VIREN RAJES

111803161 Rohan Pravin

111803059 Sakshi Kaleka

The screenshot shows a Microsoft PowerPoint presentation window. The title bar indicates the file is titled "Lecture-II-AES-IDEA". The main slide, slide 53, is titled "Overview" in large blue font. Below the title is a small circular logo with a gear symbol. The slide contains a bulleted list:

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

The left sidebar shows thumbnails for slides 53 through 59, each containing a brief description of a specific aspect of the IDEA cipher. The status bar at the bottom shows "Slide 53 of 82" and "English (United States)".

1D



1P

1P

1K

111803111 Atharva Kailas

Vinod

111803155 VIREN RAJES

111803161 Rohan Pravin

111803059 Sakshi Kaleka

AutoSave (off) Lecture-II-AES-IDEA

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

Vinod Pachghare VP

Clipboard Slides

Font Paragraph Drawing Editing Voice Designer

Font: 28 A⁺ A⁻ A₊ A₋ Paragraph: 12pt 11pt 10pt 9pt 8pt 7pt 6pt 5pt 4pt 3pt 2pt 1pt 0pt Drawing: 1pt 2pt 3pt 4pt 5pt 6pt 7pt 8pt 9pt 10pt 11pt 12pt Editing: 1pt 2pt 3pt 4pt 5pt 6pt 7pt 8pt 9pt 10pt 11pt 12pt Voice: 1pt 2pt 3pt 4pt 5pt 6pt 7pt 8pt 9pt 10pt 11pt 12pt Designer: 1pt 2pt 3pt 4pt 5pt 6pt 7pt 8pt 9pt 10pt 11pt 12pt

53 Overview
IDEA is a cipher.
IDEA is the acronym for International Data Encryption Algorithm.
IDEA has 128 bit key size.
IDEA has 10 rounds.
IDEA has 32 bit block size.
IDEA has 8 S-boxes.

54 Create the code of any cipher and use it in IDEA.
IDEA is a symmetric cipher.

55 Detailed description of IDEA
IDEA is a symmetric cipher.
IDEA has 128 bit key size.
The encryption process is divided in the following phases:
1. Initial permutation
2. Key generation
3. Main processing loop (10 times)
4. Final permutation

56 There are eight initial rounds.
The initial keys are generated from the 128 bit key.
There are four initial keys.
The four initial keys are required for the subsequent steps.
The total number of keys is 108 = 8 + 4 + 80.
The total number of keys is 108 = 8 + 4 + 80.
The total number of keys is 108 = 8 + 4 + 80.

57 Key Generation
For the 128 bit key, there are eight initial keys.
The initial keys are generated from the 128 bit key.
The initial keys are generated from the 128 bit key.
The initial keys are generated from the 128 bit key.
The initial keys are generated from the 128 bit key.

58 This part shows the detailed steps of the algorithm.
The algorithm consists of 10 iterations.
The algorithm consists of 10 iterations.
The algorithm consists of 10 iterations.

59 Encryption of the key sub-blocks
The 10 sub-blocks are for the iteration in 10.
The 10 sub-blocks are for the iteration in 10.

Click to add title

Click to add notes

Slide 54 of 82 English (India) 97%

1D



1P

1P

1K

111803111 Atharva Kailas

Vinod

111803155 VIREN RAJES

111803161 Rohan Pravin

111803059 Sakshi Kaleka

Lecture-II-AES-IDEA

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

Share Comments

AutoSave Off

Search

53 Overview

IDEA is the acronym for International Data Encryption Algorithm. It is a symmetric block cipher developed by Daewan Kim and Sungjin Lee at Daewoo Electronics.

54 Create the user of any key size and then generate the key.

55 Detailed description of IDEA

Plaintext and cipher text: 64-bit blocks
Key: 128-bit
The encryption process is identical to the decryption process
The initial process that is performed first is called initialisation.

56 There are eight initial rounds.
The initial keys are generated from the initial key.
Given a 128-bit key, 16 subkeys are required for the subsequent stages.
The total number of subkeys is 16 = 8 + 8 = 16 different 16-bit subkeys are generated from the 128-bit key.

57 Key Generation

For the 128-bit key, there are eight initial subkeys. These are then broken down into two 64-bit subkeys each.
These are further broken down into four 32-bit subkeys each.
These are then further broken down into eight 16-bit subkeys each.

58 This 64-bit plaintext is divided into four 16-bit sub-blocks.

59 Encryption of the key sub-blocks

The 16-bit plaintext used for the encryption is 00000000000000000000000000000000

Click to add notes

Slide 55 of 82 English (India)

Notes

97%

+116

1D



1P

1P

1K

111803111 Atharva Kailas

Vinod

111803155 VIREN RAJES

111803161 Rohan Pravin

111803059 Sakshi Kaleka

AutoSave (Off) Lecture-II-AES-IDEA Search Vinod Pachghare VP

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

Clipboard Slides

Font Paragraph Drawing Editing Voice Designer

Font: 28 A⁺ A⁻ A₊ A₋ Paragraph: 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: 53 54 55 56 57 58 59

• There are total eight and half rounds

• Six 16-bit keys are generated from the 128-bit key.

• Since a further four 16-bit key-sub-blocks are required for the subsequent output transformation, a total of 52 ($= 8 \times 6 + 4$) different 16-bit sub-blocks have to be generated from the 128-bit key

Click to add notes

Slide 55 of 82 English (India)

1D



1P

1P

1K

111803111 Atharva Kailas

Vinod

111803155 VIREN RAJES

111803161 Rohan Pravin

111803059 Sakshi Kaleka

Lecture-II-AES-IDEA

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

Vinod Pachghare VP

Key Generation

- First, the 128-bit key is partitioned into eight 16-bit sub-blocks which are then directly used as the first eight key sub-blocks
- Then the key is shifted cyclically to the left by 25 positions, after which the resulting 128-bit block is again partitioned into eight 16-bit sub-blocks to be directly used as the next eight key sub-blocks

Click to add notes

Slide 57 of 82 English (India)

+116

1D



1P

1P

1K

111803111 Atharva Kailas

Vinod

111803155 VIREN RAJES

111803161 Rohan Pravin

111803059 Sakshi Kaleka

AutoSave (off) Home Insert Design Transitions Animations Slide Show Review View Recording Help

Clipboard Slides New Slide Reuse Slides Reset Section

Font Paragraph Drawing Editing Voice Designer

Font: A⁺ A⁻ A⁰ Paragraph: B I U S A¹ A² A³ A⁴ A⁵ A⁶ A⁷ A⁸ A⁹ A¹⁰ A¹¹ A¹²

Paragraph: Alignment: Top Center Bottom Justify Spacing: 1.5 2x 3x 4x 5x 6x 7x 8x 9x 10x 11x 12x

Editing: Find Replace Select Dictate Design Ideas

Designer: Share Comments

Slide 53: Overview of IDEA algorithm.

Slide 54: Detailed description of IDEA.

Slide 55: Key Generation process.

Slide 56: Key schedule generation.

Slide 57: Key generation details.

Slide 58: Key schedule generation details.

Slide 59: Encryption of the key sub-blocks.

Click to add title

Click to add notes

Slide 58 of 82 English (India)

1D



1P

1P

1K

111803111 Atharva Kailas

Vinod

111803155 VIREN RAJES

111803161 Rohan Pravin

111803059 Sakshi Kaleka

Lecture-II-AES-IDEA

Encryption of the key sub-blocks

The key sub-blocks used for the encryption in the individual rounds are shown in Table below

Round 1	$Z_1^{(1)} Z_2^{(1)} Z_3^{(1)} Z_4^{(1)} Z_5^{(1)} Z_6^{(1)}$
Round 2	$Z_1^{(2)} Z_2^{(2)} Z_3^{(2)} Z_4^{(2)} Z_5^{(2)} Z_6^{(2)}$
Round 3	$Z_1^{(3)} Z_2^{(3)} Z_3^{(3)} Z_4^{(3)} Z_5^{(3)} Z_6^{(3)}$
Round 4	$Z_1^{(4)} Z_2^{(4)} Z_3^{(4)} Z_4^{(4)} Z_5^{(4)} Z_6^{(4)}$
Round 5	$Z_1^{(5)} Z_2^{(5)} Z_3^{(5)} Z_4^{(5)} Z_5^{(5)} Z_6^{(5)}$
Round 6	$Z_1^{(6)} Z_2^{(6)} Z_3^{(6)} Z_4^{(6)} Z_5^{(6)} Z_6^{(6)}$
Round 7	$Z_1^{(7)} Z_2^{(7)} Z_3^{(7)} Z_4^{(7)} Z_5^{(7)} Z_6^{(7)}$
Round 8	$Z_1^{(8)} Z_2^{(8)} Z_3^{(8)} Z_4^{(8)} Z_5^{(8)} Z_6^{(8)}$
Output Transform	$Z_1^{(9)} Z_2^{(9)} Z_3^{(9)} Z_4^{(9)}$

Click to add notes

Slide 59 of 82 English (India)

1D



1P

1P

1K

111803111 Atharva Kailas

Vinod

111803155 VIREN RAJES

111803161 Rohan Pravin

111803059 Sakshi Kaleka

Lecture-II-AES-IDEA

Encryption

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

Fig 1. The IDEA structure

Legend:

- ⊕ shift exclusive OR of two 16-bit words
- addition modulo $2^{16} + 1$ of two 16-bit integers
- multiplication modulo $2^{16} + 1$ of two 16-bit integers, where each of all entries corresponds to 2^8

Notes

Slide 61 of 82 English (India)

Click to add notes

97%

1D



1P

1P

1K

111803111 Atharva Kailas

Vinod

111803155 VIREN RAJES

111803161 Rohan Pravin

111803059 Sakshi Kaleka

Lecture-II-AES-IDEA

The slide shows the structure of the IDEA cipher. It starts with a **Plaintext 4 x 16 bit** input. This is processed through a **First Round**, which consists of four 16-bit key sub-blocks ($Z_1^{(1)}, Z_2^{(1)}, Z_3^{(1)}, Z_4^{(1)}$) and eight S-boxes. The output of the first round is then processed through **7 additional rounds**. Each round consists of four 16-bit key sub-blocks ($Z_1^{(i)}, Z_2^{(i)}, Z_3^{(i)}, Z_4^{(i)}$) and eight S-boxes. The final output is a **Ciphertext 4 x 16 bit**. A legend at the bottom defines the symbols: a circle with a plus sign for **shift exclusive OR (the 16-bit sub-blocks)**; a square with a plus sign for **addition modulo 2^{16} of two 16-bit integers**; and a circle with a cross for **multiplication modulo $2^{16} + 1$ of two 16-bit integers where sub-blocks of all j entries corresponds to 2^j** .

Encryption

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

Click to add notes

Slide 61 of 82 English (India)

1D



1P

1P

1K

111803111 Atharva Kailas

Vinod

111803155 VIREN RAJES

111803161 Rohan Pravin

111803059 Sakshi Kaleka

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

Vinod Pachghare VP

Search

Clipboard Slides

Font Paragraph Drawing Editing Voice Designer

Shapes Arrange Quick Styles

Find Replace Select Dictate Design Ideas

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

Vinod Pachghare VP

Search

Clipboard Slides

Font Paragraph Drawing Editing Voice Designer

Shapes Arrange Quick Styles

Find Replace Select Dictate Design Ideas

59 Encryption of the key sub-blocks

60

61

62

63 Round 9

1. Multiply X1 and the first subkey
2. Add X2 and the second subkey
3. Add X3 and the third subkey
4. Multiply X4 and the fourth subkey

64 Description

65 Applications of IDEA

Click to add notes

Slide 63 of 82 English (India)

1D



1P

1P

1K

111803111 Atharva Kailas

Vinod

111803155 VIREN RAJES

111803161 Rohan Pravin

111803059 Sakshi Kaleka

AutoSave

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

Clipboard Slides

Font Paragraph Drawing Editing Voice Designer

Shapes Arrange Quick Styles

Find Replace Select Dictate Design Ideas

59

60

61

62

63

64

65

Click to add notes

Slide 64 of 82 English (India) 97%

Decryption

- The computational process used for decryption of the ciphertext is essentially the same as that used for encryption
- The only difference is that each of the 52 16-bit key sub-blocks used for decryption is the inverse of the key sub-block used during encryption

1D



1P

1P

1K

111803111 Atharva Kailas

Vinod

111803155 VIREN RAJES

111803161 Rohan Pravin

111803059 Sakshi Kaleka

Lecture-II-AES-IDEA

Applications of IDEA

- Audio and video data for cable TV, pay TV, video conferencing, distance learning
- Sensitive financial and commercial data
- Email via public networks
- Smart cards

Slide 65 of 82 English (India)

+116

1D



1P

1P

1K

111803111 Atharva Kailas

Vinod

111803155 VIREN RAJES

111803161 Rohan Pravin

111803059 Sakshi Kaleka

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

Search Vinod Pachghare VP

Clipboard Slides

Font Paragraph Drawing Editing Voice Designer

Shapes Arrange Quick Styles Select Dictate Design Ideas

Find Replace

Clipboard New Reuse Slide Slides Section

61 Encryption

62 The rounds takes a complete round.

63 Round 9

64 Decryption

65 Applications of IDEA

66 Simplified IDEA Example

67 A simplified version of IDEA.

Click to add title

Simplified IDEA Example

Click to add notes

Slide 65 of 82 English (India)

1D



1P

1P

1K

111803111 Atharva Kailas

Vinod

111803155 VIREN RAJES

111803161 Rohan Pravin

111803059 Sakshi Kaleka

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

Search Vinod Pachghare VP

Clipboard Slides

Font Paragraph Drawing Editing Voice Designer

Shapes Arrange Quick Styles Find Replace Select Dictate Design Ideas

Slide 67 of 82 English (India)

Click to add title

• A 16-bit block of plaintext converted to a 16-bit block of ciphertext

• It uses a 32-bit key

• The simplified algorithm consists of four identical rounds and a “half round” final transformation

1D



1P

1P

1K

111803111 Atharva Kailas

Vinod

111803155 VIREN RAJES

111803161 Rohan Pravin

111803059 Sakshi Kaleka

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

Search Vinod Pachghare VP

Clipboard Slides

Font Paragraph Drawing Editing Voice Designer

Shapes Arrange Quick Styles Find Replace Select Dictate Design Ideas

Slide 63 of 82 English (India)

KEY:
11011100011011110011111101011001

1101 1100 0110 1111 0011 1111 0101 1001

- Divide the key into 6 nibbles (groups). (Each group having 4 bits)
- The first six nibbles are used as the subkeys for round 1
- The remaining two nibbles are the first two subkeys for round 2

Click to add notes

Notes

+116

1D



1P

1P

1K

111803111 Atharva Kailas

Vinod

111803155 VIREN RAJES

111803161 Rohan Pravin

111803059 Sakshi Kaleka

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

Search Vinod Pachghare

Clipboard Slides

Font Paragraph Drawing Editing Voice Designer

Shapes Arrange Quick Styles Select Dictate Design Ideas

Find Replace

Slide 65: Applications of IDEA

Slide 66: Simplified IDEA Example

Slide 67: IDEA Subkey Generation

Slide 68: IDEA Subkey Generation

Slide 69: IDEA Subkey Generation

Slide 70: Message 01111111111111111111111111111111

Slide 71: Key Generation

Click to add notes

Slide 69 of 82 English (India)

Notes

+116

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

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

AutoSave Lecture-II-AES-IDEA Search

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

Clipboard Slides

Font Paragraph Drawing Editing Voice Designer

Shapes Arrange Quick Styles

Find Replace Select Dictate Design Ideas

Slide Number: 65

Applications of IDEA

- Index and search done for web pages
- Video watermarking, compression, decoding
- Image watermarking, compression, decoding
- Secure communication
- Biometric authentication

Slide Number: 66

Simplified IDEA Example

Slide Number: 67

A 1024x768 pixel image is converted into 100x70 pixels.
The original file size is 1 MB.
The compressed file size is 10 KB.
The compressed file size is 10 times smaller than the original file.

Slide Number: 68

IDEA
IDEA stands for Iterated Discrete Cosine Transform Algorithm.
IDEA is a lossy compression technique.
It compresses the image by removing some of the less important information.
The compressed file size is 10 times smaller than the original file.
The compressed file size is 10 times smaller than the original file.

Slide Number: 69

IDEA
IDEA stands for Iterated Discrete Cosine Transform Algorithm.
The core of IDEA is to use the DCT method.
The DCT method is a lossy compression technique.
The compressed file size is 10 times smaller than the original file.
The compressed file size is 10 times smaller than the original file.

Slide Number: 70

Message (1111 1011 1101 1010)
The message is converted into binary form.

Slide Number: 71

Key Generation

Key 1	Key 2	Key 3	Key 4
1111	1011	1101	1010

Click to add notes

Slide 70 of 82 English (India) 97%

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

AutoSave

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

Clipboard Slides

Font Paragraph Drawing Editing Voice Designer

65
Applications of IDEA
• IDEA and IDEA-based systems play a vital role in security, banking, commerce, and other fields.
• IDEA is used in ATM machines.
• IDEA is used in electronic commerce.
• IDEA is used in secure communication.

66
Simplified IDEA Example
• IDEA and IDEA-based systems play a vital role in security, banking, commerce, and other fields.
• IDEA is used in ATM machines.
• IDEA is used in electronic commerce.
• IDEA is used in secure communication.

67
IDEA Cryptographic Process
• IDEA is a symmetric block cipher developed by X. Rijmen and B. Preneel.
• IDEA uses a 128-bit key and processes data in 64-bit blocks.
• IDEA has three main components: a key scheduler, a message scheduler, and a permutation function.
• The message scheduler takes the 64-bit input and divides it into four 16-bit blocks.
• The key scheduler generates four 16-bit keys from the 128-bit key.
• The permutation function consists of three layers of 16x16-bit S-boxes.

68
IDEA Cryptographic Process
• IDEA is a symmetric block cipher developed by X. Rijmen and B. Preneel.
• IDEA uses a 128-bit key and processes data in 64-bit blocks.
• IDEA has three main components: a key scheduler, a message scheduler, and a permutation function.
• The message scheduler takes the 64-bit input and divides it into four 16-bit blocks.
• The key scheduler generates four 16-bit keys from the 128-bit key.
• The permutation function consists of three layers of 16x16-bit S-boxes.

69
IDEA Cryptographic Process
• IDEA is a symmetric block cipher developed by X. Rijmen and B. Preneel.
• IDEA uses a 128-bit key and processes data in 64-bit blocks.
• IDEA has three main components: a key scheduler, a message scheduler, and a permutation function.
• The message scheduler takes the 64-bit input and divides it into four 16-bit blocks.
• The key scheduler generates four 16-bit keys from the 128-bit key.
• The permutation function consists of three layers of 16x16-bit S-boxes.

70
Message 0111110110111110110010111000011

71
Key Generation
Key 1: 0000000000000000
Key 2: 0000000000000000
Key 3: 0000000000000000
Key 4: 0000000000000000

Click to add title

Message:-1111 1011 1101 1010

Key:- 10101001110111110110010111000011

Click to add notes

Slide 70 of 82 English (India) 97%

1D



1P

1P

1K

111803111 Atharva Kailas

Vinod

111803155 VIREN RAJES

111803161 Rohan Pravin

111803059 Sakshi Kaleka

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

Search Vinod Pachghare VP

Clipboard Slides Simplified IDEA Example

Font Paragraph Drawing Editing Voice Designer

Font: 28 A A' A'' A'''' A''''' Paragraph: 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

Key Generation

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

Click to add notes

Slide 71 of 82 English (India)

Notes

+116

1D



1P

1P

1K

111803111 Atharva Kailas

Vinod

111803155 VIREN RAJES

111803161 Rohan Pravin

111803059 Sakshi Kaleka

Lecture-II-AES-IDEA

Key Generation

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

Slide 71 of 82 English (India)

+116

1D



1P

1P

1K

111803111 Atharva Kailas

Vinod

111803155 VIREN RAJES

111803161 Rohan Pravin

111803059 Sakshi Kaleka

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

Vinod Pachghare VP

Round – 1

$11 + 9 = 20 \text{ mod } 16 = 14 \text{ mod } 17$

$S1 = P1 . K1 \quad S2 = P2 + K2 \quad S3 = P3 + K3 \quad S4 = P4 . K4$

$$\begin{array}{r}
 1 & 1 & 1 & 1 \\
 \times 1 & 0 & 1 & 0 \\
 \hline
 1 & 1 & 1 & 0
 \end{array}
 \quad
 \begin{array}{r}
 1 & 0 & 1 & 1 \\
 1 & 0 & 0 & 1 \\
 \hline
 0 & 1 & 0 & 0
 \end{array}
 \quad
 \begin{array}{r}
 1 & 1 & 0 & 1 \\
 1 & 1 & 0 & 1 \\
 \hline
 1 & 0 & 1 & 0
 \end{array}
 \quad
 \begin{array}{r}
 1 & 0 & 1 & 0 \\
 1 & 1 & 1 & 1 \\
 \hline
 1 & 1 & 1 & 0
 \end{array}$$

$S5 = S1 \text{ xor } S3$

$$\begin{array}{r}
 1 & 1 & 1 & 0 \\
 1 & 0 & 1 & 0 \\
 \hline
 0 & 1 & 0 & 0
 \end{array}$$

$S6 = S2 \text{ xor } S4$

$$\begin{array}{r}
 0 & 1 & 0 & 0 \\
 1 & 1 & 1 & 0 \\
 \hline
 1 & 0 & 1 & 0
 \end{array}$$

Click to add notes

Slide 72 of 82 English (India)

+116

1D



1P

1P

1K

111803111 Atharva Kailas

Vinod

111803155 VIREN RAJES

111803161 Rohan Pravin

111803059 Sakshi Kaleka

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

Search 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

Round – 1

11 + 9 =20 mod 16 =14 mod 17

$$\begin{array}{r} 1 & 1 & 1 & 1 \\ \times 1 & 0 & 1 & 0 \\ \hline 1 & 1 & 1 & 0 \end{array} \quad \begin{array}{r} 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 \\ \hline 0 & 1 & 0 & 0 \end{array} \quad \begin{array}{r} 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 \\ \hline 1 & 0 & 1 & 0 \end{array} \quad \begin{array}{r} 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 \\ \hline 1 & 1 & 1 & 0 \end{array}$$

S1 = P1 . K1 S2 = P2 + K2 S3 = P3 + K3 S4 = P4 . K4

$$\begin{array}{r} 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \\ \hline 0 & 1 & 0 & 0 \end{array} \quad \begin{array}{r} 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ \hline 1 & 0 & 1 & 0 \end{array}$$

S5 = S1 xor S3 S6 = S2 xor S4

$$\begin{array}{r} 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \\ \hline 0 & 1 & 0 & 0 \end{array} \quad \begin{array}{r} 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ \hline 1 & 0 & 1 & 0 \end{array}$$

Slide 72 of 82 English (India)

+116

1D



1P

1P

1K

111803111 Atharva Kailas

Vinod

111803155 VIREN RAJES

111803161 Rohan Pravin

111803059 Sakshi Kaleka

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

Search 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

Slide Number: 69

S7 = S5 . K5

$$\begin{array}{r}
 0 & 1 & 0 & 0 \\
 0 & 1 & 1 & 0 \\
 \hline
 0 & 1 & 1 & 1
 \end{array}$$

Slide Number: 70

S8 = S6 + S7

$$\begin{array}{r}
 1 & 0 & 1 & 0 \\
 0 & 1 & 1 & 1 \\
 \hline
 0 & 0 & 0 & 1
 \end{array}$$

Slide Number: 71

S10 = S7 + S9

$$\begin{array}{r}
 0 & 1 & 1 & 1 \\
 0 & 1 & 0 & 1 \\
 \hline
 1 & 1 & 0 & 0
 \end{array}$$

Slide Number: 72

S9 = S8 . K6

$$\begin{array}{r}
 0 & 0 & 0 & 1 \\
 0 & 1 & 0 & 1 \\
 \hline
 0 & 1 & 0 & 1
 \end{array}$$

Slide Number: 73

Click to add notes

Slide 73 of 82 English (India)

Notes

+116

1D



1P

1P

1K

111803111 Atharva Kailas

Vinod

111803155 VIREN RAJES

111803161 Rohan Pravin

111803059 Sakshi Kaleka

Lecture-II-AES-IDEA

Slide 73: Key Generation

$$S7 = S5 \cdot K5$$

$$\begin{array}{r} 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ \hline 0 & 1 & 1 & 1 \end{array}$$

$$S8 = S6 + S7$$

$$\begin{array}{r} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ \hline 0 & 0 & 0 & 1 \end{array}$$

Slide 74: Round - I

$$S10 = S7 + S9$$

$$\begin{array}{r} 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ \hline 1 & 1 & 0 & 0 \end{array}$$

$$S9 = S8 \cdot K6$$

$$\begin{array}{r} 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ \hline 0 & 1 & 0 & 1 \end{array}$$

Slide 75: Generate the key for description

Click to add notes

Slide 73 of 82

English (India)

Notes

+116

1D



1P

1P

1K

111803111 Atharva Kailas

Vinod

111803155 VIREN RAJES

111803161 Rohan Pravin

111803059 Sakshi Kaleka

Lecture-II-AES-IDEA

Slide 73: Key Generation

Equation: $S7 = S5 \cdot K5$

$$\begin{array}{r}
 0 & 1 & 0 & 0 \\
 0 & 1 & 1 & 0 \\
 \hline
 0 & 1 & 1 & 1
 \end{array}$$

Equation: $S8 = S6 + S7$

$$\begin{array}{r}
 1 & 0 & 1 & 0 \\
 0 & 1 & 1 & 1 \\
 \hline
 0 & 0 & 0 & 1
 \end{array}$$

Equation: $S10 = S7 + S9$

$$\begin{array}{r}
 0 & 1 & 1 & 1 \\
 0 & 1 & 0 & 1 \\
 \hline
 1 & 1 & 0 & 0
 \end{array}$$

Equation: $S9 = S8 \cdot K6$

$$\begin{array}{r}
 0 & 0 & 0 & 1 \\
 0 & 1 & 0 & 1 \\
 \hline
 0 & 1 & 0 & 1
 \end{array}$$

Click to add notes

Slide 73 of 82 English (India)

1D



1P

1P

1K

111803111 Atharva Kailas

Vinod

111803155 VIREN RAJES

111803161 Rohan Pravin

111803059 Sakshi Kaleka

Lecture-II-AES-IDEA

Round – 1

$$11 + 9 = 20 \text{ mod } 16 = 14 \text{ mod } 17$$

$S_1 = P_1 \cdot K_1 \quad S_2 = P_2 + K_2 \quad S_3 = P_3 + K_3 \quad S_4 = P_4 \cdot K_4$

$$\begin{array}{r}
 1 & 1 & 1 & 1 \\
 \times 1 & 0 & 1 & 0 \\
 \hline
 1 & 1 & 1 & 0
 \end{array}
 \quad
 \begin{array}{r}
 1 & 0 & 1 & 1 \\
 + 1 & 0 & 0 & 1 \\
 \hline
 0 & 1 & 0 & 0
 \end{array}
 \quad
 \begin{array}{r}
 1 & 1 & 0 & 1 \\
 + 1 & 1 & 0 & 1 \\
 \hline
 1 & 0 & 1 & 0
 \end{array}
 \quad
 \begin{array}{r}
 1 & 0 & 1 & 0 \\
 + 1 & 1 & 1 & 1 \\
 \hline
 1 & 1 & 1 & 0
 \end{array}$$

$S_5 = S_1 \text{ xor } S_3 \quad S_6 = S_2 \text{ xor } S_4$

$$\begin{array}{r}
 1 & 1 & 1 & 0 \\
 + 1 & 0 & 1 & 0 \\
 \hline
 0 & 1 & 0 & 0
 \end{array}
 \quad
 \begin{array}{r}
 0 & 1 & 0 & 0 \\
 + 1 & 1 & 1 & 0 \\
 \hline
 1 & 0 & 1 & 0
 \end{array}$$

Click to add notes

Slide 72 of 82 English (India)

+116

1D



1P

1P

1K

111803111 Atharva Kailas

Vinod

111803155 VIREN RAJES

111803161 Rohan Pravin

111803059 Sakshi Kaleka

Lecture-II-AES-IDEA

Round – 1

$$11 + 9 = 20 \text{ mod } 16 = 14 \text{ mod } 17$$

$S_1 = P_1 \cdot K_1 \quad S_2 = P_2 + K_2 \quad S_3 = P_3 + K_3 \quad S_4 = P_4 \cdot K_4$

$$\begin{array}{r}
 1 & 1 & 1 & 1 \\
 \times 1 & 0 & 1 & 0 \\
 \hline
 1 & 1 & 1 & 0
 \end{array}
 \quad
 \begin{array}{r}
 1 & 0 & 1 & 1 \\
 + 1 & 0 & 0 & 1 \\
 \hline
 0 & 1 & 0 & 0
 \end{array}
 \quad
 \begin{array}{r}
 1 & 1 & 0 & 1 \\
 + 1 & 1 & 0 & 1 \\
 \hline
 1 & 0 & 1 & 0
 \end{array}
 \quad
 \begin{array}{r}
 1 & 0 & 1 & 0 \\
 + 1 & 1 & 1 & 1 \\
 \hline
 1 & 1 & 1 & 0
 \end{array}$$

$S_5 = S_1 \text{ xor } S_3 \quad S_6 = S_2 \text{ xor } S_4$

$$\begin{array}{r}
 1 & 1 & 1 & 0 \\
 + 1 & 0 & 1 & 0 \\
 \hline
 0 & 1 & 0 & 0
 \end{array}
 \quad
 \begin{array}{r}
 0 & 1 & 0 & 0 \\
 + 1 & 1 & 1 & 0 \\
 \hline
 1 & 0 & 1 & 0
 \end{array}$$

Click to add notes

Slide 72 of 82 English (India)

Notes

+116

1D



1P

1P

1K

111803111 Atharva Kailas

Vinod

111803155 VIREN RAJES

111803161 Rohan Pravin

111803059 Sakshi Kaleka

Lecture-II-AES-IDEA

Round – 1

$$11 + 9 = 20 \text{ mod } 16 = 14 \text{ mod } 17$$

$S_1 = P_1 \cdot K_1 \quad S_2 = P_2 + K_2 \quad S_3 = P_3 + K_3 \quad S_4 = P_4 \cdot K_4$

$$\begin{array}{r}
 1 & 1 & 1 & 1 \\
 \times 1 & 0 & 1 & 0 \\
 \hline
 1 & 1 & 1 & 0
 \end{array}
 \quad
 \begin{array}{r}
 1 & 0 & 1 & 1 \\
 + 1 & 0 & 0 & 1 \\
 \hline
 0 & 1 & 0 & 0
 \end{array}
 \quad
 \begin{array}{r}
 1 & 1 & 0 & 1 \\
 + 1 & 1 & 0 & 1 \\
 \hline
 1 & 0 & 1 & 0
 \end{array}
 \quad
 \begin{array}{r}
 1 & 0 & 1 & 0 \\
 + 1 & 1 & 1 & 1 \\
 \hline
 1 & 1 & 1 & 0
 \end{array}$$

$S_5 = S_1 \text{ xor } S_3 \quad S_6 = S_2 \text{ xor } S_4$

$$\begin{array}{r}
 1 & 1 & 1 & 0 \\
 + 1 & 0 & 1 & 0 \\
 \hline
 0 & 1 & 0 & 0
 \end{array}
 \quad
 \begin{array}{r}
 0 & 1 & 0 & 0 \\
 + 1 & 1 & 1 & 0 \\
 \hline
 1 & 0 & 1 & 0
 \end{array}$$

Click to add notes

Slide 72 of 82 English (India)

Notes

+116

1D



1P

1P

1K

111803111 Atharva Kailas

Vinod

111803155 VIREN RAJES

111803161 Rohan Pravin

111803059 Sakshi Kaleka

Lecture-II-AES-IDEA

Round – 1

$$11 + 9 = 20 \text{ mod } 16 = 4 \text{ mod } 16$$

$S_1 = P_1 \cdot K_1 \quad S_2 = P_2 + K_2 \quad S_3 = P_3 + K_3 \quad S_4 = P_4 \cdot K_4$

$$\begin{array}{r}
 1 & 1 & 1 & 1 \\
 \times 1 & 0 & 1 & 0 \\
 \hline
 1 & 1 & 1 & 0
 \end{array}
 \quad
 \begin{array}{r}
 1 & 0 & 1 & 1 \\
 + 0 & 1 & 0 & 0 \\
 \hline
 1 & 0 & 1 & 0
 \end{array}
 \quad
 \begin{array}{r}
 1 & 1 & 0 & 1 \\
 + 1 & 0 & 1 & 0 \\
 \hline
 1 & 0 & 1 & 0
 \end{array}
 \quad
 \begin{array}{r}
 1 & 0 & 1 & 0 \\
 + 1 & 1 & 1 & 1 \\
 \hline
 1 & 1 & 1 & 0
 \end{array}$$

$S_5 = S_1 \text{ xor } S_3$

$$\begin{array}{r}
 1 & 1 & 1 & 0 \\
 1 & 0 & 1 & 0 \\
 \hline
 0 & 1 & 0 & 0
 \end{array}$$

$S_6 = S_2 \text{ xor } S_4$

$$\begin{array}{r}
 0 & 1 & 0 & 0 \\
 1 & 1 & 1 & 0 \\
 \hline
 1 & 0 & 1 & 0
 \end{array}$$

Click to add notes

Slide 72 of 82 English (United States)

Notes

+116

1D



1P

1P

1K

111803111 Atharva Kailas

Vinod

111803155 VIREN RAJES

111803161 Rohan Pravin

111803059 Sakshi Kaleka

Lecture-II-AES-IDEA

Slide 73 of 82

Equation 1: $S7 = S5 \cdot K5$

$$\begin{array}{r} 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ \hline 0 & 1 & 1 & 1 \end{array}$$

Equation 2: $S8 = S6 + S7$

$$\begin{array}{r} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ \hline 0 & 0 & 0 & 1 \end{array}$$

Equation 3: $S10 = S7 + S9$

$$\begin{array}{r} 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ \hline 1 & 1 & 0 & 0 \end{array}$$

Equation 4: $S9 = S8 \cdot K6$

$$\begin{array}{r} 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ \hline 0 & 1 & 0 & 1 \end{array}$$

Notes: Click to add notes

AutoSave Off | Home Insert Design Transitions Animations Slide Show Review View Recording Help

Vinod Pachghare VP

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

Clipboard Slides Slides

Font Paragraph Drawing Editing Voice Designer

Shapes Arrange Quick Styles Select Dictate Design Ideas

Find Replace

Clipboard

Slides

Key Generation

Round = 1

Generate the key for description

English (India)

+ 114

1D



1P

1P

1K

111803111 Atharva Kailas

Vinod

111803155 VIREN RAJES

111803161 Rohan Pravin

111803059 Sakshi Kaleka

Lecture-II-AES-IDEA

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

Vinod Pachghare VP

AutoSave Off

Clipboard Slides

Font Paragraph Drawing Editing Voice Designer

Shapes Arrange Quick Styles Find Replace Select Dictate Design Ideas

Find Replace Select Dictate Design Ideas

Click to add title

S11 = S9 xor S1 S12 = S9 xor S3 S13 = S10 xor S2 S14 = S10 xor S4

0 1 0 1	0 1 0 1	1 1 0 0	1 1 0 0
1 1 1 0	1 0 1 0	0 1 0 0	1 1 1 0
1 0 1 1	1 1 1 1	1 0 0 0	0 0 1 0

P1 = S11 P2 = S13 P3 = S12 P4 = S14

1 0 1 1	1 0 0 0	1 1 1 1	0 0 1 0
---------	---------	---------	---------

Click to add notes

Slide 74 of 82 English (India)

Notes

+114

1D



1P

1P

1K

111803111 Atharva Kailas

Vinod

111803155 VIREN RAJES

111803161 Rohan Pravin

111803059 Sakshi Kaleka

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

Search Vinod Pachghare VP

Clipboard Slides Slides Section

Font Paragraph Drawing Editing Voice Designer

Shapes Arrange Quick Styles Select Find Replace Dictate Design Ideas

71 Key Generation

72 Round = 1

73

74

75 Generate the key for decryption

76 Addition Mod 16

77 Summation of address for address module 16

Click to add notes

Slide 75 of 82 English (India)

Notes

+114

The screenshot shows a Microsoft PowerPoint presentation with the following details:

- Header:** AutoSave (on), File, Home, Insert, Design, Transitions, Animations, Slide Show, Review, View, Recording, Help.
- Search Bar:** Search, Vinod Pachghare VP.
- Clipboard:** Paste, New, Reuse, Slide, Slides, Section.
- Font, Paragraph, Drawing, Editing, Voice, Designer:** Standard ribbon tabs.
- Shapes Arrange, Quick Styles, Select, Find, Replace, Dictate, Design Ideas:** Advanced ribbon tabs.
- Slides:** The slide number is 75 of 82. The slide title is "Generate the key for decryption".
- Content:**
 - A bullet point: • Key:
 - The binary key value: 1010100111011110110010111000011
- Notes:** A note section is present at the bottom of the slide.
- Page Number:** +114 is visible in the bottom right corner.

1D



1P

1P

1K

111803111 Atharva Kailas

Vinod

111803155 VIREN RAJES

111803161 Rohan Pravin

111803059 Sakshi Kaleka

AutoSave (Off) Lecture-II-AES-IDEA

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

Vinod Pachghare VP

Clipboard Slides

Font Paragraph Drawing Editing Voice Designer

Font: 20pt A A' A'' A'''' Paragraph: 1 2 3 4 5 6 7 8 9 10 11 12pt

Numbered List Bulleted List Horizontal Line Vertical Line

71 Key Generation

72 Round =

73

74

75 Generate the key for description

76 Addition Mod 16

77 Summary of addition module 16

Addition Mod 16

- Suppose the number is n
- $n \text{ mod } 16 = (n + m) \text{ mod } 16 = 0$
- Where m is the addition modulo 16 of n.
- i.e. $16 - n = 0$
- Suppose $n = 1$ then $m = 16 - 1 = 15$
- $n = 2$ then $m = 16 - 2 = 14$

Click to add notes

Slide 76 of 82 English (India)

Notes 97%

1D



1P

1P

1K

111803111 Atharva Kailas

Vinod

111803155 VIREN RAJES

111803161 Rohan Pravin

111803059 Sakshi Kaleka

Lecture-II-AES-IDEA

Inverses of nibbles for addition modulo 16:

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

Click to add notes

Slide 77 of 82 English (India)

+114

1D



1P

1P

1K

111803111 Atharva Kailas

Vinod

111803155 VIREN RAJES

111803161 Rohan Pravin

111803059 Sakshi Kaleka

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

Search Vinod Pachghare

Clipboard Slides Slides New Reuse Slide Reset

Font Paragraph Drawing Editing Voice Designer

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

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

Drawing: Shapes Arrange Quick Styles Select Find Replace Dictate Design Ideas

Editing: Voice

Designer: Share Comments

Slide 76: Addition Mod 16

Slide 77: Inverse of addition modulo 16

Slide 78: Multiplication Mod 17

Slide 79: Inverse of addition for multiplication modulo 17

Slide 80: Key for encryption

Slide 81: Boxed text: $(K_1^5) \quad 1001 \quad 9 \quad 2 \quad 0010 \quad Z_1^1$
 $(K_2^5) \quad 0111 \quad 7 \quad 9 \quad 1001 \quad Z_2^1$
 $(K_3^5) \quad 0000 \quad 0 \quad 0 \quad 0000 \quad Z_3^1$
 $(K_4^5) \quad 1110 \quad 14 \quad 11 \quad 1011 \quad Z_4^1$
 $(K_5^4) \quad 1001 \quad 9 \quad 9 \quad 1001 \quad Z_5^1$
 $(K_6^4) \quad 1101 \quad 13 \quad 13 \quad 1101 \quad Z_6^1$

Slide 82: Click to add notes

Slide 81 of 82 English (India)

Notes

+ 114

1D



1P

1P

1K

111803111 Atharva Kailas

Vinod

111803155 VIREN RAJES

111803161 Rohan Pravin

111803059 Sakshi Kaleka

AutoSave

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

Clipboard Slides

Font Paragraph Drawing Editing Voice Designer

76 Addition Mod 16
77 Inverse of addition for addition mod 10
78 Multiplication Mod 17
79 Inverse of addition for multiplication
80 Key for encryption
81 Multiplication Mod 17
82 Inverse of multiplication for multiplication mod 17

Key for encryption

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

Click to add notes

Slide 80 of 82 English (India) 6.48 1x +CC 111+

1D



1P

1P

1K

111803111 Atharva Kailas

Vinod

111803155 VIREN RAJES

111803161 Rohan Pravin

111803059 Sakshi Kaleka

Click to add title

$(K_1^5) \quad 1001 \quad 9 \quad 2 \quad 0010 \quad Z_1^1$
(Multiplicative modulo 17)

$(K_2^5) \quad 0111 \quad 7 \quad 9 \quad 1001 \quad Z_2^1$
(Addition modulo 16)

$(K_3^5) \quad 0000 \quad 0 \quad 0 \quad 0000 \quad Z_3^1$
(Addition modulo 16)

$(K_4^5) \quad 1110 \quad 14 \quad 11 \quad 1011 \quad Z_4^1$
(Multiplicative modulo 17)

$(K_5^4) \quad 1001 \quad 9 \quad 9 \quad 1001 \quad Z_5^1$

$(K_6^4) \quad 1101 \quad 13 \quad 13 \quad 1101 \quad Z_6^1$

Click to add notes

Slide 81 of 82 English (India)

1D



1P

1P

1K

111803111 Atharva Kailas

Vinod

111803155 VIREN RAJES

111803161 Rohan Pravin

111803059 Sakshi Kaleka

AutoSave (Off) Lecture-II-AES-IDEA Search Vinod Pachghare VP

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

Clipboard Slides Layout Shapes Arrange Quick Styles Paste New Slide Reset Font Paragraph Drawing Editing Voice Designer

76 Addition Mod 16
Suppose the number is 10.
1. 10 mod 16 = 10
2. 10 + 10 mod 16 = 20 mod 16
3. 20 mod 16 = 4
4. 10 + 4 mod 16 = 14

77 Summation of addition mod 16
Multiplication Table for mod 16

78 Multiplication Mod 17
Suppose the number is 1.
1. 1 mod 17 = 1
2. 1 * 1 mod 17 = 1
3. 1 * 2 mod 17 = 2
4. 1 * 3 mod 17 = 3
5. 1 * 4 mod 17 = 4
6. 1 * 5 mod 17 = 5
7. 1 * 6 mod 17 = 6
8. 1 * 7 mod 17 = 7
9. 1 * 8 mod 17 = 8
10. 1 * 9 mod 17 = 9
11. 1 * 10 mod 17 = 10
12. 1 * 11 mod 17 = 11
13. 1 * 12 mod 17 = 12
14. 1 * 13 mod 17 = 13
15. 1 * 14 mod 17 = 14
16. 1 * 15 mod 17 = 15
17. 1 * 16 mod 17 = 16

79 Inverse of addition for multiplication
Multiplication Table for mod 17

80 Key for encryption
Key for decryption

81

82

(K_jⁱ) Integer Inverse in Integers Z_jⁱ Key for 1st Round

Click to add title

(K₁⁵) 1001 9 2 0010 Z₁¹
(Multiplicative modulo 17)

(K₂⁵) 0111 7 9 1001 Z₂¹
(Addition modulo 16)

(K₃⁵) 0000 0 0 0000 Z₃¹
(Addition modulo 16)

(K₄⁵) 1110 14 11 1011 Z₄¹
(Multiplicative modulo 17)

(K₅⁴) 1001 9 9 1001 Z₅¹

(K₆⁴) 1101 13 13 1101 Z₆¹

Click to add notes

Slide 81 of 82 English (India)

1D



1P

1P

1K

111803111 Atharva Kailas

Vinod

111803155 VIREN RAJES

111803161 Rohan Pravin

111803059 Sakshi Kaleka

Lecture-II-AES-IDEA

We can generate the keys as above for all 5 rounds

	Round -1	Round - 2	Round - 3	Round - 4	Round -5
Key -1	0010	0111	0101	1010	1100
Key - 2	1001	0100	0000	1101	0111
Key - 3	0000	1101	0010	1001	0011
Key - 4	1011	1100	1100	0101	1000
Key - 5	1001	1111	1101	0110	
Key - 6	1101	0110	1001	0101	

Click to add notes

Slide 82 of 82 English (India)

+114