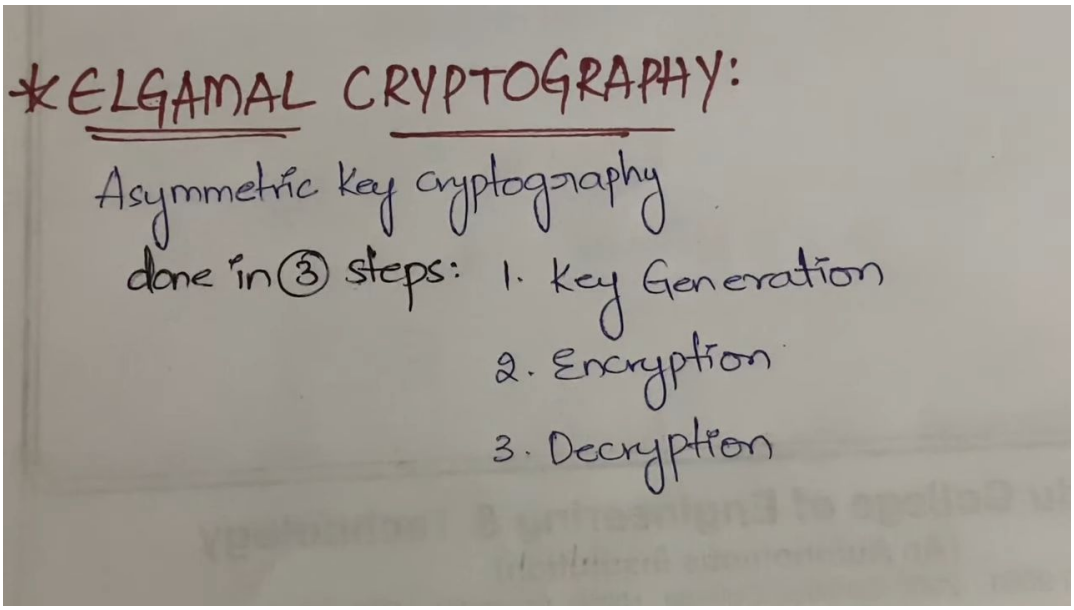
View, add and edit your notes in the app

#30 Elgamal Cryptography Algorithm - Asymmetric key cryptography |CNS

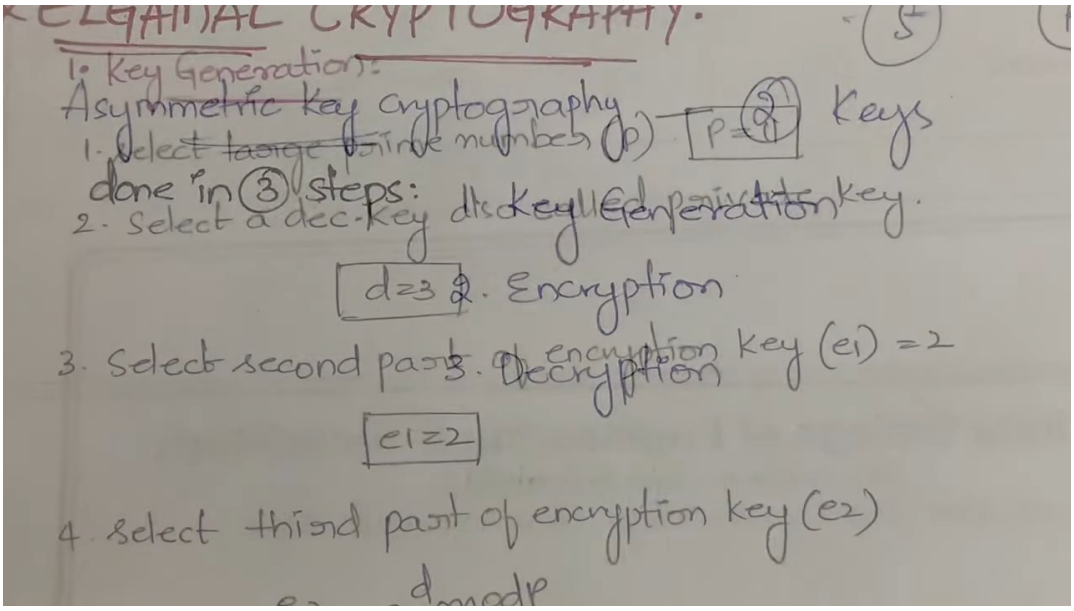
Generated on December 20, 2023

Summary

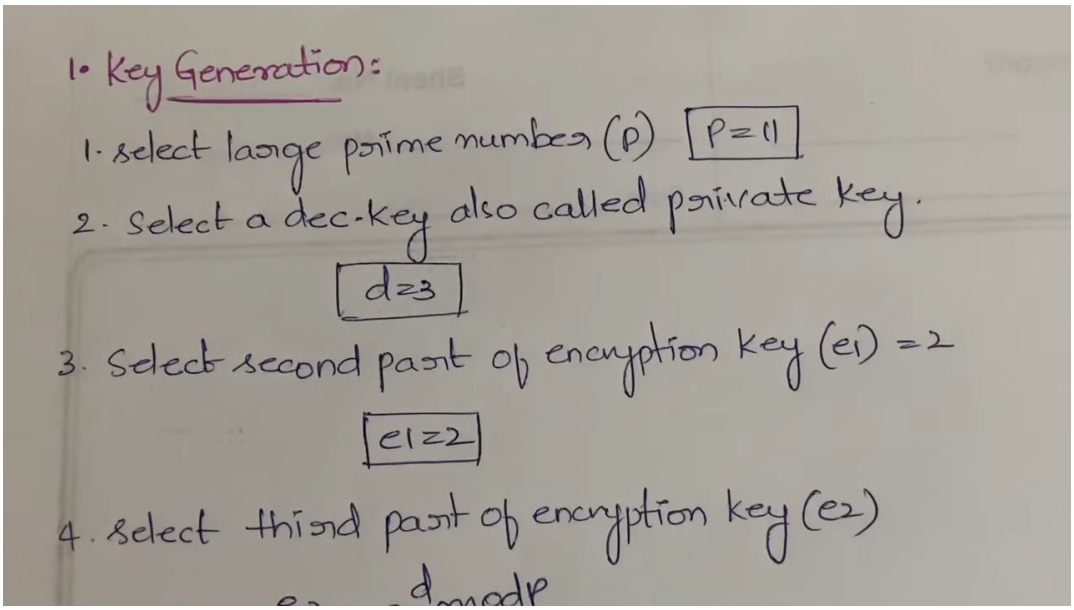
Notes	Screenshots	Bookmarks
0	14	0



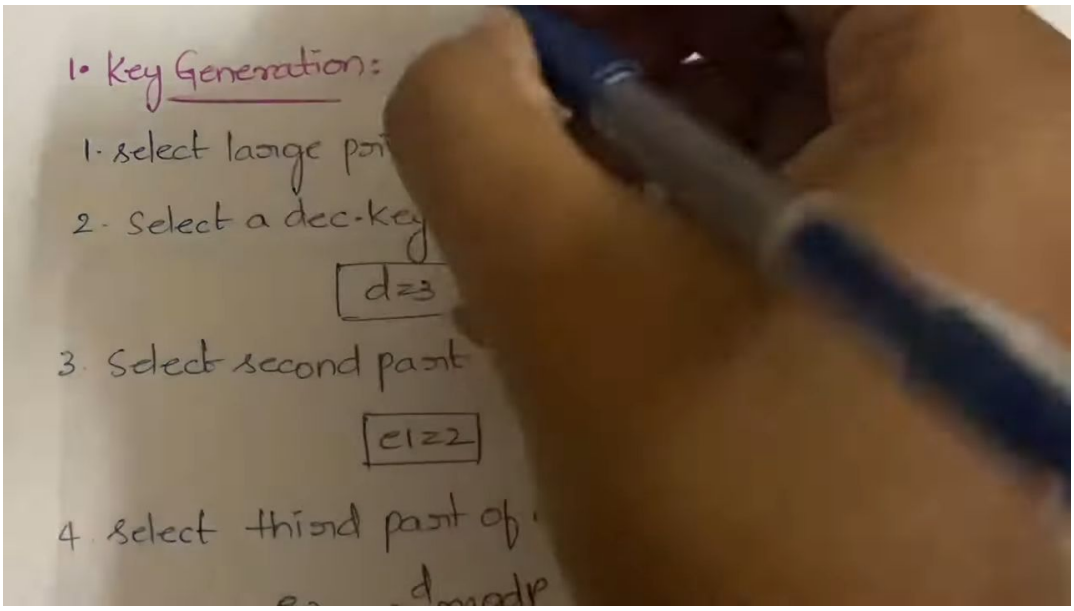
0:20


ELGAMAL CRYPTOGRAPHY.
1. Key Generation:
Asymmetric key cryptography
1. Select large prime numbers (p) P=11
done in 3 steps:
2. Select a dec-key
d=3
2. Encryption
3. Select second part
encryption key (e1) =2
e1=2
4. Select third part of encryption key (e2)
d mod p

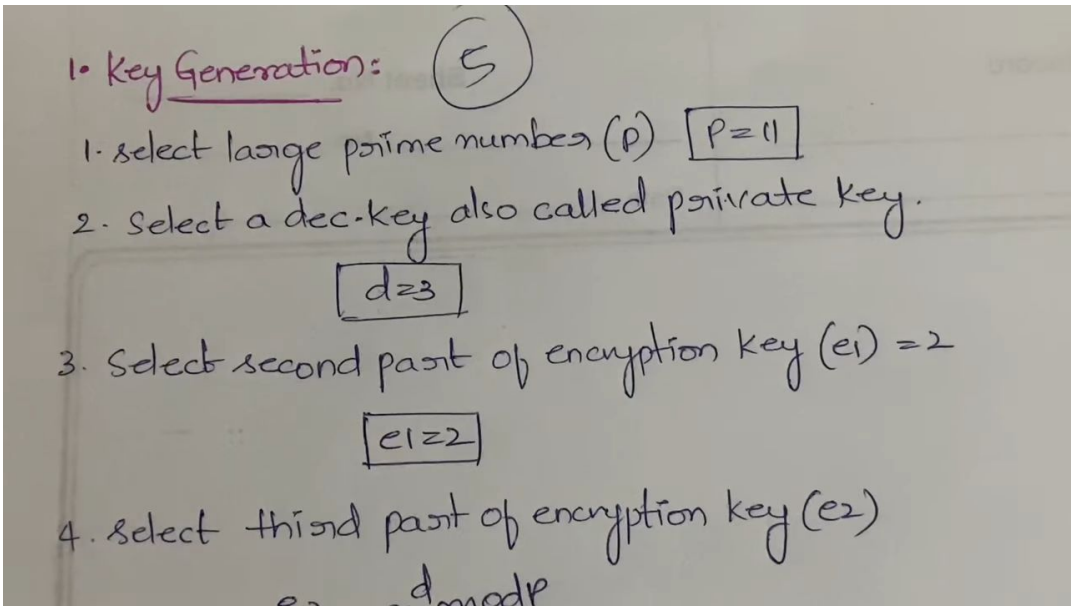
1:28


1. Key Generation:
1. select large prime numbers (p) P=11
2. Select a dec-key also called private key.
d=3
3. Select second part of encryption key (e1) =2
e1=2
4. Select third part of encryption key (e2)
d mod p

1:33


1. Key Generation:
1. select large pri
2. Select a dec-key
d=3
3. Select second part
e1=2
4. Select third part of

1:34


1. Key Generation:
5
1. select large prime number (p) p=11
2. Select a dec-key also called private key.
d=3
3. Select second part of encryption key (e1) =2
e1=2
4. Select third part of encryption key (e2)

1:37

1. select large prime number (p) $p=11$

2. Select a dec-key also called private key.

(d) $d=3$ ✓

3. Select second part of encryption key (e_1) = 2

$e_1=2$

4. Select third part of encryption key (e_2)

$$e_2 = e_1^d \bmod p$$

$$= (2)^3 \bmod 11 = 8 \bmod 11 = 8$$

▷ 2:14

(d) $d=3$ ✓

3. Select second part of encryption key (e_1) = 2

e_1 $e_1=2$ ✓

4. Select third part of encryption key (e_2)

e_2

$$e_2 = e_1^d \bmod p$$

$$= (2)^3 \bmod 11 = 8 \bmod 11 = 8$$

$e_2=8$

▷ 2:36

4. Select third part of encryption key (e_2)

Cal $\varepsilon_2 = e_1^{d} \bmod p$

$= (2)^3 \bmod 11 = 8 \bmod 11 = 8$

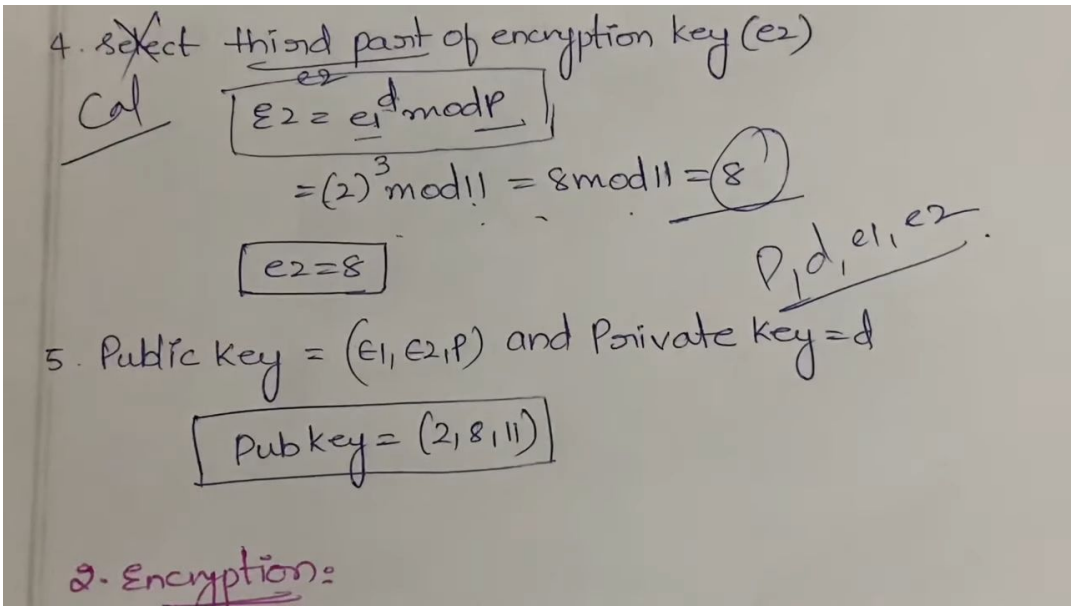
$e_2 = 8$

p, d, e_1, e_2.

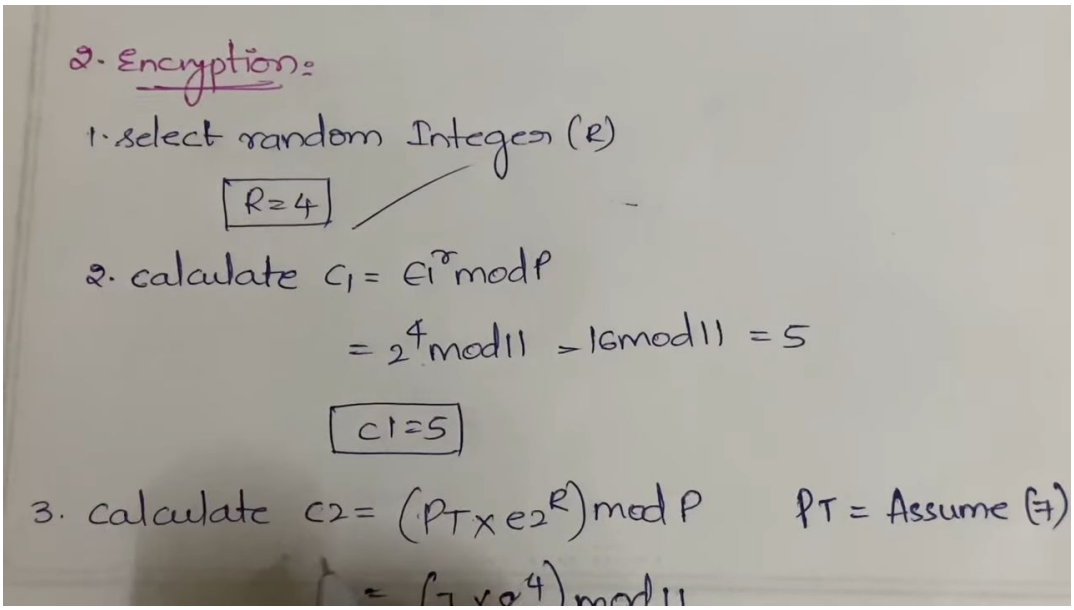
5. Public key = (e_1, e_2, p) and Private key = d

Pub key = $(2, 8, 11)$

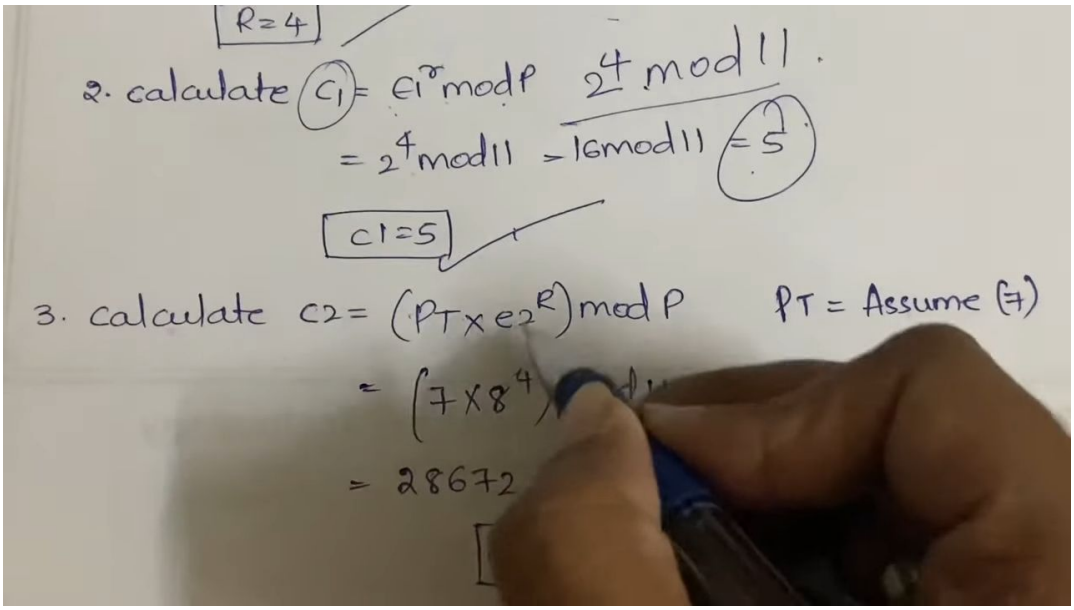
2. Encryption:



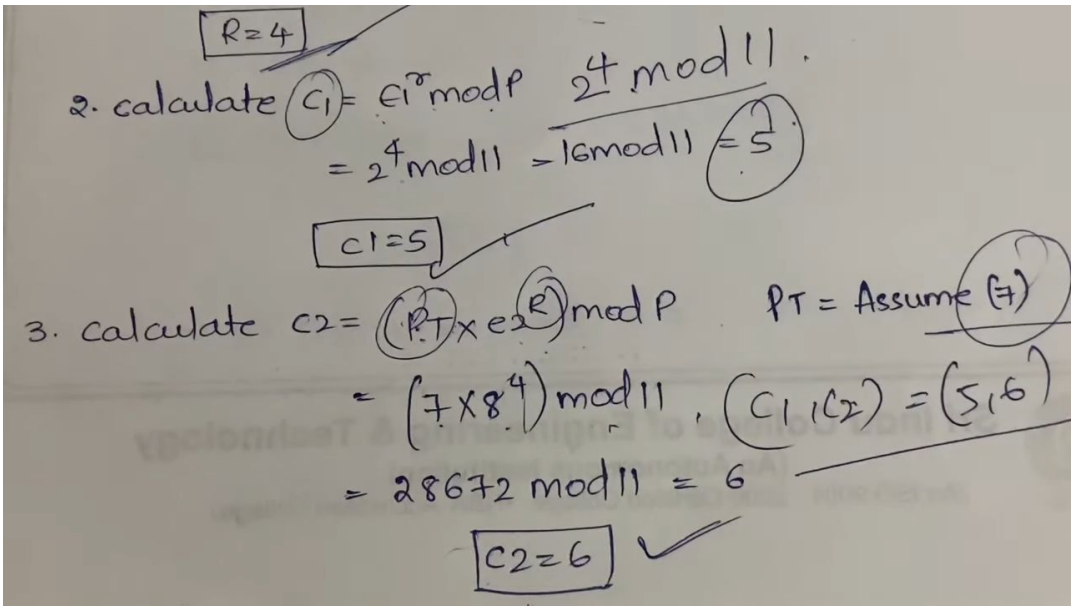
▷ 3:19



▷ 4:03


R=4
2. calculate C1 = ei^r mod p
= 2^4 mod 11
= 16 mod 11 = 5
C1=5
3. calculate C2 = (PT x e2^R) mod p
PT = Assume (7)
= (7 x 8^4)
= 28672

4:31


R=4
2. calculate C1 = ei^r mod p
= 2^4 mod 11
= 16 mod 11 = 5
C1=5
3. calculate C2 = (PT x e2^R) mod p
PT = Assume (7)
= (7 x 8^4) mod 11
(C1, C2) = (5, 6)
= 28672 mod 11 = 6
C2=6

5:16

$C_1, C_2 = (5, 6)$

3. Decryption:

1. $PT = \left[C_2 \times ((C_1)^D)^{-1}\right] \bmod P$

$= \left(6 \times ((5)^3)^{-1}\right) \bmod 11$

$= 6(5^3)^{-1} \bmod 11$

$= 6(125)^{-1} \bmod 11$

(6)

$= 125x \bmod 11 = 1$

5:24

3. Decryption:

1. $PT = \left[C_2 \times ((C_1)^D)^{-1}\right] \bmod P$

$= \left(6 \times ((5)^3)^{-1}\right) \bmod 11$

$= 6(5^3)^{-1} \bmod 11$

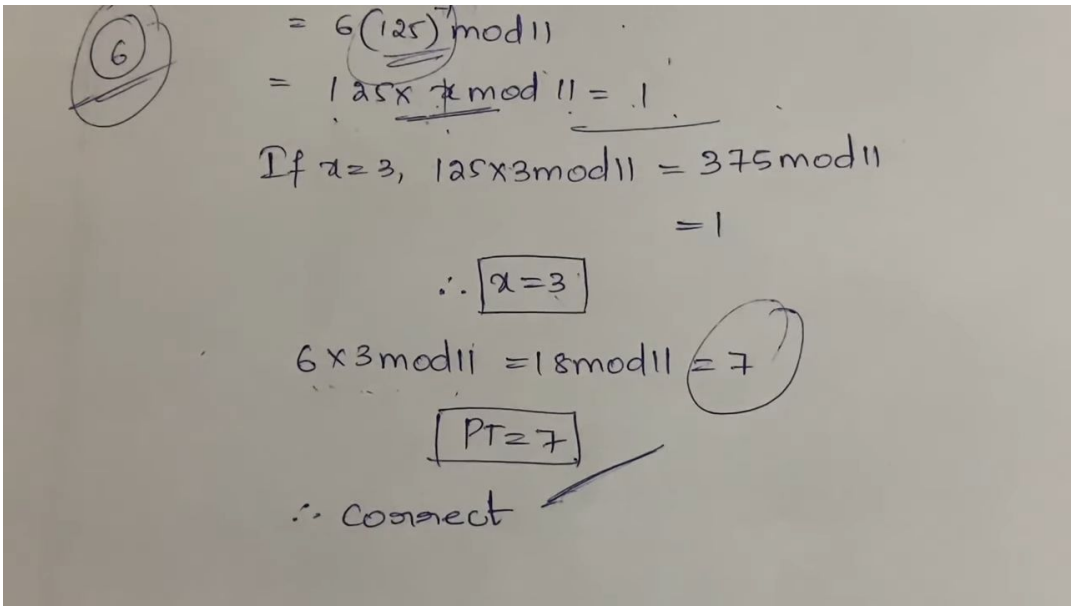
$= 6(125)^{-1} \bmod 11$

(6)

$= 125x \bmod 11 = 1$

If $x = 3$, $125 \times 3 \bmod 11 = 375 \bmod 11$

5:27


6
= 6(125)^x mod 11
= 125^x mod 11 = 1
If x=3, 125x3mod11 = 375mod11
=1
∴ x=3
6x3mod11 =18mod11 = 7
PT=7
∴ Correct

6:55