AJEENKYA
D Y PATIL UNIVERSITY

End Term Examinations (April/May 2019)

School: School of Engineering **Program: BCA-CTIS**

Course: Applied Cryptography **Course Code: CSC246**

Semester: IV **Max Marks: 30** **Duration (mins): 60**

Note- 1.Figures to the right indicates full marks.

2. Attempt any three questions.

Q1)

a) List and Explain any 10 cryptographic attacks (5)
b) What is cryptographic hash function? (5)

Q2)

a) Find primitive root q of p , where p=13. (2)

b) Write algorithm for deffie Hellman key exchange algorithm ? Find Kab using Deffie Hellman key exchange algorithm where p= 23, q= 5

a=5, b=15. (8)

Q3)

a) Encrypt message “humpty dumpty sat on a wall” where key used is “ball” using columnar transposition & permutation cipher. (2)
b) Encrypt “mumbai” where key is “volley ball” using play fair cipher. (2)
c) Explain Digital Signature with diagram. (6)

Q4)

a) Explain Kerberos with the help of diagram. (5)
b) Encrypt M=8 and Decrypt the same P=23 and q=11 using RSA Algorithm. (5)

Q5)

a) Encrypt and decrypt “welcome to ADYPU” where key is “ Hello World” using Play fair cipher. (2)

b) Solve the following for Sdes Algorithm for single round where the plain text is 01101101 and key is 1100011110 P10 is [3 5 2 7 4 10 1 9 8 6] and P8 is [6 3 7 4 8 5 10 9] IP [2 6 3 1 4 85 7] E/P [4 1 2 3 2 3 4 1] P4[2 4 3 1] IP-1[2 6 3 1 4 8 5 7]

S0

	C0	C1	C2	C3
R0	1	0	3	2
R1	3	2	1	0
R2	0	2	1	3
R3	3	1	3	2

S1

	C0	C1	C2	C3
R0	0	1	2	3
R1	2	0	1	3
R2	3	0	1	0
R3	2	1	0	3

(8)

*******ALL THE BEST*******