

ANNEXURE 2.2.2

K.S. INSTITUTE OF TECHNOLOGY

#14, Raghuvanahalli, Kanakapura main Road, Bengaluru – 560 109



Department of Computer Science & Engineering

QUALITY OF INTERNAL QUESTION PAPERS AND ASSIGNMENTS



K.S. INSTITUTE OF TECHNOLOGY, BANGALORE - 560109
SECOND INTERNAL TEST QUESTION PAPER 2023-24 ODD SEMESTER

USN									
-----	--	--	--	--	--	--	--	--	--

SET-A


Degree : BE
Branch : Computer Science and Engineering
Course Title : Cryptography
Duration : 90 Minutes

Semester: VII/A/B
Course Code: 18CS744
Date: 24-11-2023
Max Marks: 30


Note: Answer **ONE** full question from each part.

K-Levels: K1-Remebering, K2-Understanding, K3-Applying, K4-Analyzing, K5-Evaluating, K6-Creating

Q No.	Question	Marks	CO mapping	K-Level
PART-A				
1(a)	Construct elliptic curve encryption and decryption process using ECC Diffie –Hellman key exchange.	6	CO3	K3
(b)	Apply Elliptic curve arithmetic on the elliptic curve $E_{23}(1,1)$, $P=(3, 10)$ and $Q=(9,7)$. Find: i) $P+Q$ ii) $2P$	6	CO3	K3
(c)	Build Pseudo random number generator using RSA.	6	CO3	K3
OR				
2(a)	Make use of symmetric encryption and explain key distribution scenario.	6	CO3	K3
(b)	Apply Elliptic curve arithmetic on the elliptic curve $E_{11}(1, 6)$ for the curve defined by $y^2=x^3+1x+6$ with modulus of $p=11$. Determine all the points in $E_{11}(1,6)$.	6	CO3	K3
(c)	Make use of neat diagram and explain the following in distribution of public keys. i) Public Announcement ii) Public Key Authority.	6	CO3	K3
PART-B				
3(a)	Apply Elgamal cryptosystem algorithm for $q= 13$, its primitive root $\alpha=10$. A's private key is 5, B's private key is 6 and $M=17$. Perform encryption and decryption.	6	CO2	K3
(b)	Make use of neat daigram; explain the general format of X.509 certificate.	6	CO4	K3
OR				
4(a)	Apply Diffie –Hellman key exchange algorithm for $q= 71$, its primitive root $\alpha=7$. A's private key is 5, B's private key is 12. Find i) A's Public Key ii) B's Public Key iii) Shared Secret Key.	6	CO2	K3
(b)	Utilize an example and explain hierarchy of X.509.	6	CO4	K3


 Kavya M S
 Name and Signature of
 Course In charge


 Dr. REKHA B. VENKATAPUR
 Name and Signature of
 Module coordinator


 Principal
 Selected



K.S. INSTITUTE OF TECHNOLOGY, BANGALORE - 560109
SECOND INTERNAL TEST QUESTION PAPER 2023-24 ODD SEMESTER

USN

--	--	--	--	--	--	--	--	--	--

SET-B

Degree : BE
Branch : Computer Science and Engineering
Course Title : Cryptography
Duration : 90 Minutes

Semester: VII/A/B
Course Code:18CS744
Date: 24-11-2023
MaxMarks: 30

Note: Answer **ONE full** question from each part.

K-Levels: K1-Remembering, K2-Understanding, K3-Applying, K4-Analyzing, K5-Evaluating, K6-Creating

Q No.	Question	Marks	CO mapping	K-Level
PART-A				
1(a)	Identify the characteristics of elliptic curve over real numbers	6	CO3	K3
(b)	Apply Elliptic curve arithmetic on the elliptic curve $E_{13}(6, -9)$ for the curve defined by $y^2=x^3+6x-9$ with modulus of $P=11$. Determine all the points in $E_{13}(6, -9)$.	6	CO3	K3
(c)	Construct ECC Diffie –Hellman key exchange mechanism with neat diagram.	6	CO3	K3
OR				
2(a)	Illustrate the working of Micali-Schnorr pseudorandom bit generator using Elliptic Curve Cryptography.	6	CO3	K3
(b)	Apply Elliptic curve arithmetic on the elliptic curve $y^2=x^3-36x$ where $P=(-3,9)$ and $Q=(-2,8)$. Find: i) $P+Q$ ii) $2P$	6	CO3	K3
(c)	Make use of neat diagram and explain the following in distribution of public keys. i) Public available directory ii) Public Key certificates.	6	CO3	K3
PART-B				
3(a)	Apply Diffie –Hellman key exchange algorithm for prime no. $q=11$, its primitive root $\alpha=2$. A's private key is 9, B's private key is 3. Find i) A's Public Key ii) B's Public Key iii) Shared Secret Key.	6	CO2	K3
(b)	Make use of a neat diagram, explain the fields of X.509 Certificate along with its application.	6	CO4	K3
OR				
4(a)	Apply Elgamal cryptosystem algorithm for Prime No. $q=13$, its primitive root $\alpha=2$. A's private key is 3, B's private key is 7 and $M=4$. Perform encryption and decryption.	6	CO2	K3
(b)	Utilize an example and explain hierarchy of X.509.	6	CO4	K3

Pallavi R
 Name and Signature of
 Course In charge

Dr. Rekha B. Venkatapur
 Name and Signature of
 Module coordinator
 Dr. REKHA B. VENKATAPUR

[Signature]
 HOD CSE

[Signature]
 Principal



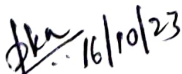
K S INSTITUTE OF TECHNOLOGY

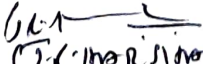
Bengaluru – 560109

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

CIE Question paper Scrutiny format

Course Name	User Interface Design
Course Code	18CS734
Course Incharge	Mrs. Pallavi K N
Academic year	2023-2024 [Odd]
Semester	7
CIE #	Internal Assessment-I
Set	A <input type="checkbox"/> B <input checked="" type="checkbox"/>
Scrutiny parameters	
Whether questions are according to assessment plan?	Yes <input checked="" type="checkbox"/> No <input type="checkbox"/> ; If No, Suggestions:
Whether questions prepared are within the covered syllabus?	Yes <input checked="" type="checkbox"/> No <input type="checkbox"/> ; If No, Suggestions:
Whether all questions are mapped to CO/PO properly?	Yes <input checked="" type="checkbox"/> No <input type="checkbox"/> ; If No, Suggestions:
Whether questions framed are according to Blooms level?	Yes <input checked="" type="checkbox"/> No <input type="checkbox"/> ; If No, Suggestions:
Whether marks distribution for each question are correct?	Yes <input checked="" type="checkbox"/> No <input type="checkbox"/> ; If No, Suggestions:
Whether questions paper follows the format displayed?	Yes <input checked="" type="checkbox"/> No <input type="checkbox"/> ; If No, Suggestions:
Difficulty level	Very High <input type="checkbox"/> High <input type="checkbox"/> Moderate <input checked="" type="checkbox"/> Low <input type="checkbox"/>
Percentage of Similarity questions in Set A & B	30%
Final decision	Accepted without corrections <input checked="" type="checkbox"/> Accepted with minor corrections <input type="checkbox"/> Not accepted <input type="checkbox"/>


Signature with date
of CIE Question paper setter


(S. K. R. Srinivasan)
Name and Signature with date
of CIE Question paper Scrutiniser





K S INSTITUTE OF TECHNOLOGY
Bangalore - 560109

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

CIE Question paper Scrutiny format

Course Name	CRYPTOGRAPHY
Course Code	18CS744
Course Incharge	Mrs. Pallavi R
Academic year	2023-2024
Semester	7th
CIE #	IA - 1
Set	A <input type="checkbox"/> B <input checked="" type="checkbox"/>
Scrutiny parameters	
Whether questions are according to assessment plan?	Yes <input checked="" type="checkbox"/> No <input type="checkbox"/> ; If No, Suggestions:
Whether questions prepared are within the covered syllabus?	Yes <input checked="" type="checkbox"/> No <input type="checkbox"/> ; If No, Suggestions:
Whether all questions are mapped to CO/PO properly?	Yes <input checked="" type="checkbox"/> No <input type="checkbox"/> ; If No, Suggestions:
Whether questions framed are according to Blooms level?	Yes <input checked="" type="checkbox"/> No <input type="checkbox"/> ; If No, Suggestions:
Whether marks distribution for each question are correct?	Yes <input checked="" type="checkbox"/> No <input type="checkbox"/> ; If No, Suggestions:
Whether questions paper follows the format displayed?	Yes <input checked="" type="checkbox"/> No <input type="checkbox"/> ; If No, Suggestions:
Difficulty level	Very High <input type="checkbox"/> High <input checked="" type="checkbox"/> Moderate <input type="checkbox"/> Low <input type="checkbox"/>
Percentage of Similarity questions in Set A & B	10%
Final decision	Accepted without corrections <input type="checkbox"/> Accepted with minor corrections <input type="checkbox"/> Not accepted <input type="checkbox"/>


Signature with date
of CIE question paper setter
16/10/23


Name and Signature with date
of CIE Question paper Scrutiniser
Dr. REKHA B. VENKATAPUR
16/10/23



K.S. Institute of Technology, Bangalore-560109.

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING ASSIGNMENT QUESTIONS-3

Academic Year	2022-23		
Batch	2020-24		
Year/Semester/section	III/V/A & B		
Subject Code-Title	18CS51- Management and Entrepreneurship for IT Industry		
Name of the Instructor	SUPREETHA GANESH	Dept	CSE

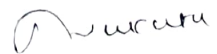
Assignment No: 3
Date of Issue:09-1-2023

Total marks:10
Date of Submission: 17-11-2023

Sl. No	Assignment Questions	K Level	CO	Marks
1.	What is ERP? Give the importance and need of ERP in the organization?	Apply (K4)	CO4	1
2.	Write a note on importance of management finance, accounting and Supply chain management in ERP software.	Apply (K4)	CO4	1
3.	Make use of project planning methodologies, briefly explain the steps involved in report writing.	Apply (K4)	CO4	1
4.	Research an ERP system or an ERP software application, and address the following: In your own words, define enterprise resource planning (ERP). Provide the name of the ERP system or the ERP software application you researched Briefly discuss the ERP system or the ERP software application and include how this resource can help an organization manage important aspects of its business. (Q & Solution – Cheggstudy)	Apply (K4)	CO4	1
5.	Write a note on i) Different types of patents. ii) MSME and its characteristics	Apply (K4)	CO5	1
6	Describe the steps involved in the setting up of Small Scale industries	Apply (K4)	CO5	1
7	Making use of concepts of IPR explain the following i)Patent ii) Trade secret iii) Trademark iv) industrial Design	Apply (K4)	CO5	1
8	What is term industrial policy? How do governments create comparative advantage in different sectors of the economy?	Apply (K4)	CO5	1
9	Describe the Case study of i)Microsoft ii)Air Decaan G.R Gopinath	Apply (K4)	CO5	1
10	Write a note on KIADB, KSSIDC ,DIC and NSIC ,TEKSOK	Apply (K4)	CO5	1


Signature of Course In charge


Signature of module coordinator


HOD

Head of the Department
Dept. of Computer Science,
K. S. Institute of Technology
Bangalore -560 109