C.Sc. 619 -2080 ✡

Tribhuvan University
Institute of Science and Technology
2080
✡

Master Level /II Year/ IIIrd Semester/ Science
Computer Science and Information Technology (C.Sc. 619)
(Advanced Crytography)

Full Marks: 45
Pass Marks: 22.5
Time: 2 hours.

Candidates are required to give their answers in their own words as for as practicable.
The figures in the margin indicate full marks.

Group A

Attempt any TWO questions. **(2×10=20)**

1. Explain the working mechanism of Feistel Structure. Is AES based on Feistel structure? Why and why not? List out the operation performed in each round of AES. (5+3+2)
2. Explain the digital signature generation process using ELGamal crypto system. Choose any Elliptical curve and show the addition process of two points in that Elliptical curve. (6+4)
3. List the properties of cryptographic hash function. What are session and interchange keys? Explain, how Kerberos system provides third party authentication. (3+2+5)

Group B

Attempt ALL questions. **(5×5=25)**

4. What do you mean by CIA triad? List out the possible thread on each of the component.
5. Z_6 is not a field but Z_7, why? Explain your answer with the properties of a field.
6. What is discrete logarithm problem? What can be the value of discrete logarithm of 4 under modulo 13 with the base 3.
7. Explain the Markle-Damgard construction model of Hash value generation.
8. Explain the Fiat-Shamir Protocol of secret sharing with example.

C.Sc.621-2080 ✡

Tribhuvan University

Institute of Science and Technology

2080

✡

Master Level /II Year/ IIIrd Semester/ Science

Computer Science and Information Technology (C.Sc. 621)

(Fuzzy Systems)

Full Marks: 45

Pass Marks: 22.5

Time: 2 hours.

Candidates are required to give their answers in their own words as for as practicable.

The figures in the margin indicate full marks.

Group A

Attempt any TWO questions. **[2×10=20]**

1. Construct two fuzzy sets A and B using R and L-functions respectively over the domain of discourse 10 to 50 with an interval of 5. [10]
   Now compute
   a. $B_{0.8}^{+}$
   b. $A \cap B$
   c. Compute support and Core of A and B
   d. Height of $(\bar{A})$

2. State extension principle. Why extension principle is important in fuzzy systems? Consider a Multiple Input Single Output(MISO) system where a fuzzy numbers N1 and N2 are defined by the set N1={0.1/20, 0.53/30, 0.8/40, 1/50, 0.7/60} and N2={ 0.3/40, 0.4/50, 0.5/60, 1/70, 0.8/80, 0.33/90}. Suppose we have a fuzzy arithmetic operation N= N1+N2. Now construct the fuzzy set for N with its elements and membership values using Max-Min extension principle. [2+2+6]

3. Create fuzzy rule based systems containing the fuzzy rules that are applicable to zero order Sugeno and first order Sugeno models. Show how inference is done in those models. [10]

Group B

Attempt ALL questions. **[5×5=25]**

4. Construct any two fuzzy relations R and S, and show whether $R \circ S = S \circ R$ for Max-Min composition. [5]

5. How crossover and mutation operations are done in genetic algorithm? [5]

6. What are adaptive controllers? Describe the components of adaptive controller. [2+3]

7. Describe how defuzzification of fuzzy sets is done? [5]

8. Define membership function in fuzzy set. Given fuzzy sets A={1/a, 0/b, 1/c}, B={0/a,1/b, 1/c} and C={0.5/a, 0.5/b, 0.5/c}. Represent the sets using Kosko Cube. [1+4]

C.Sc.618-2080 ✡

Tribhuvan University

Institute of Science and Technology

2080

✡

Master Level /II Year/ III Semester/ Science
Computer Science and Information Technology (C.Sc. 618)
(Principle of Programming Language)

Full Marks: 45
Pass Marks: 22.5
Time: 2 hours.

Candidates are required to give their answers in their own words as for as practicable.
The figures in the margin indicate full marks.

Group A

Attempt any TWO questions. **(2×10=20)**

1. What is language translation? Explain different stages in the process of translation of a program from its original syntax into executable form in detail. (2 + 8)

2. Explain abstract data type, encapsulation, and information hiding in brief. What is type equivalence? (6 + 4)

3. What is sequence control? Explain sequencing with arithmetic expressions in detail. (2 + 8)

Group B

Attempt ALL questions. **(5×5=25)**

4. What are different reasons of studying programming languages? Explain. (5)

5. What are different factors that lead to differences among implementation of the same language on virtual computers? What do you mean by hierarchies of virtual machines? (2 + 3)

6. Explain type conversion and coercion with example. (5)

7. Compare class with object. Explain polymorphism in brief. (2 + 3)

8. Define exception. Explain exception handler in brief. (1 + 4)

C.Sc.624-2080 ✡

Tribhuvan University

Institute of Science and Technology

2080

✡

Master Level /II Year/ IIIrd Semester/ Science

Computer Science and Information Technology (C.Sc. 624)

(Remote Sensing and GIS)

Full Marks: 45

Pass Marks: 22.5

Time: 2 hours.

Candidates are required to give their answers in their own words as for as practicable.

The figures in the margin indicate full marks.

Group A

Attempt any TWO questions. **(2×10=20)**

1. Describe IFOV, Swaths and Nadir with illustrations. Compare with digital image classification with visual image interpretation in terms of input of operator/photo interpreter in terms of output.

2. Describe methods of data capture in GIS. Explain the different methods of image overlay operations with illustrations.

3. Differentiate between active and passive sensor? How radar system works? Explain.

Group B

Attempt ALL questions. **(5×5=25)**

4. What is remote sensing? How it differ from GPS?

5. What are the advantages of aerial photographs? How do you calculate scale of vertical photograph?

6. What do you mean by georeference image? How it is obtained?

7. Differentiate between supervised and unsupervised classification.

8. What is the relationship between image visualization and image interpretation?