First Internal Assessment Test ** Database Management System ***CSCL 502**
Full Marks: 20 ******Allotted Time: 60 Mins *****Date: September 19, 2023

1. Answer all Questions

a. Define Logical data independence.

b. Is Data inconsistency related to Data redundancy? Justify your answer.

c. Differentiate between Set Difference and Intersection RA operators through an example.

d. Define the concept of Key Constraint and Participation Constraint through examples.

e. What is a foreign Key Constraint? Why are such constraints important?

(C01, 1+1+2+2+2=8)

2. A company Database needs to store information about Employees (identified by SSN, Salary and Phone as attributes), Departments (identified by Dno, Dname and Budget as attributes) and Children of Employees (with name and age as attributes). Employees work in Departments; each Department is managed by an Employee; a child must be identified by name when the parent (Who is an Employee; assume that only one parent works for the company) is known. We are not interested in information about a child once the parent leaves company.

Draw an ER diagram capturing the above said information and also present the equivalent relational schema. (C01, 4+2 =6)

3. Consider the following relational Schema: Suppliers (Sid, Sname, Address), Parts (Pid, Pname, Color), Catalog (Sid, Pid, Cost). Write the RA expression for the following queries.

- Find the supplier names who supply all red parts.
- Find the pids of parts supplied by at least two different suppliers.
- Find the suppliers name who supply some red part and some green part.

[C03, 2+2+2 =6]

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING, UNIVERSITY OF CALCUTTA

CLASS TEST FOR M. SC. SEMESTER-II, 2023

Full Marks: 30 Time: 1 hour

2x5=10

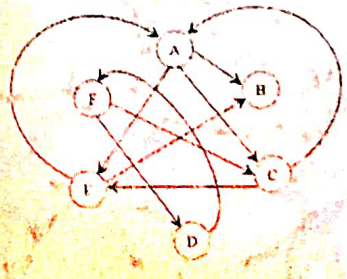
1. Answer any five of the following:

   a) In a distributed system, what is the significance of finding two or more events as concurrent?
   b) Define the global state of a system.
   c) Define name transparency and explain its significance in a distributed system.
   d) Compare syntactic versus semantic distribution transparency.
   e) Explain how the forward and backward intersection of cuts are related to consistent state recording.
   f) Why, in a distributed system, periodic synchronization of clocks in the participating sites is not considered good?

4x5=20

2. Answer each of the following:

   a) How clocks in nodes are synchronized for Lamport's logical clock model in a distributed system?
   b) "It is required to record the state of the channel through which the first marker is delivered to any node as empty for the sake of consistent state record" - do you agree with this comment in the context of the Chandy-Lamport's state recording algorithm? Justify your opinion within 150 words.
   c) Is it possible to follow a Master clock in a Master node as the system's clock for an entire distributed system? Justify your opinion within 150 words.
   b) What would be the impact for finding initiator nodes if the network has more than one node with in-degree zero? Justify your opinion within 150 words.
   e) Identify the node set that can be reached from node A in the figure attached, in a maximum of 2-hops. Also identify the node(s) for the attached figure that can act as possible initiator node(s) for diffusion computation algorithms. Also, for each of the possible initiator nodes(s), identify the order in which the nodes will be traversed till all nodes in the network are reached.



M.Sc. 2nd Semester Midsem Examination

Subject:Automata and Compiler Design Paper Code: CSMC 202

(Full Marks – 20, Time: 1hr)

1. Answer any *four*: 2×4=8

a) If there are n no. of inputs, how many outputs are generated by *Mealy* and *Moore* machines separately? Justify your answer.

b) Why do you need a *DFA* to be minimized?

c) Find a grammar in *Chomsky Normal Form* equivalent to $S \rightarrow aAbB, A \rightarrow aA \mid a, B \rightarrow bB \mid b$.

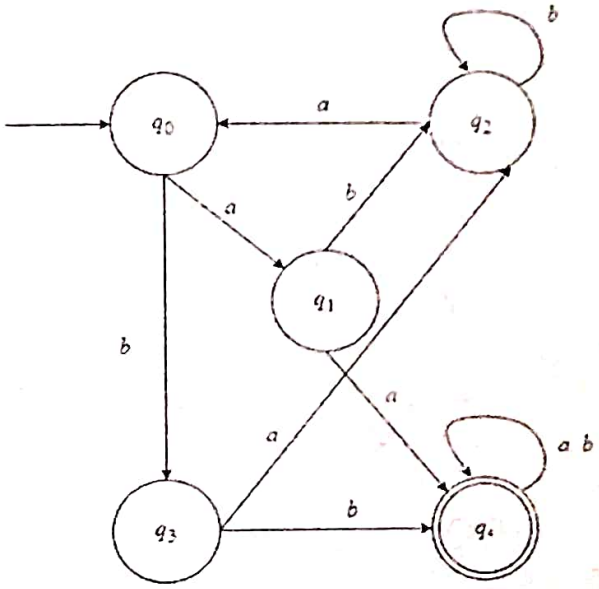
d) Derive the strings concretely generated by the *regular* expression $r = (1+01)^*(0+\lambda)$.

e) When is a production said to be *useless*? Explain with example.

2. Answer any *three*: 4×3=12

a) Construct a *Turing Machine* that accepts the language of 010 over $\Sigma = \{0, 1\}$.

b) Minimize the following *DFA*:



c) Construct a *Moore Machine* equivalent to the *Mealy Machine M* defined as follows:

Present State	Next State			
	G=0		G=1	
	State	Output	State	Output
→q_1	q_1	1	q_2	0
q_2	q_4	1	q_4	1
q_3	q_2	1	q_3	1
q_4	q_3	0	q_1	1

d) Construct a grammar in *Greibach Normal Form* equivalent to the grammar $S \rightarrow AA \mid a$, $A \rightarrow SS \mid b$.

Mid term Examination M.Sc. (Second Semester) Cryptography & Network Security Full Marks: 30

Answer all Questions

a. Encrypt the message "meet me at hill" using the Hill cipher with the key .

9	5
4	7

Show your calculations and the result. Show the calculations for the corresponding decryption of the ciphertext to recover the original plaintext.

b. "Hill cipher succumbs to a known plaintext attack if sufficient plaintext–ciphertext pairs are provided." --- Comment with necessary Justification.

c. Comment on the performance of Public Key Cryptography and Secret Key Cryptography for protecting spoofing attack.

d. Find the Multiplicative inverse of 23 in Z_{100}.

e. The encryption Key in a transposition cipher is [3,2,6,1,5,4]. Find the decryption key.

f. Consider a cipher. The cipher is affine, but the keys depend on the position of the character in the PT. If the PT character to be encrypted is in position i, the keys are defined as

The multiplicative key is the (i mod 12) th element in Z_{26}^*

The additive key is the (i mod 26)th element in Z_{26}

Encrypt the message "Exam is fun" using this cipher.

g. Illustrate the meet in the middle attack through an example.

h. Consider a desktop publishing system used to produce documents for various organizations.

- Give an example of a type of publication for which confidentiality of the stored data is the most important requirement.
- Give an example of a type of publication in which data integrity is the most important requirement.
- Give an example in which system availability is the most important requirement.

a b c d e f g h

[6+2+2+5+1+5+6+3 = 30]

Second Mid term Examination M.Sc. (Second Semester) Cryptography & Network Security Full Marks: 30

Answer any six questions (6 x 5 =30)

a. "Strength of an encryption algorithm depends on the Sub-key generation algorithm also"—Discuss in context of DES algorithm.

b. Prove that $< Z_6 *, X >$ is an abelian group. Is AES a Feistel Cipher? Comment with justification.

c. Use Extended Euclidean algorithm to find the inverse of $(x^4 + x^3 + 1)$ in $GF(2^5)$ using the modulus $(x^5 + x^2 + 1)$.

d. In context of RSA, explian the role of trapdoor one way function.

e. Define Knapsack cryptosystem. Write an algorithm to find Inverse of Knapsacksum.

f. Compare the strength among the versions of DES with necessary clarification.

g. Find the orders of all elements in the group $<Z_7, +>$. Why is the Galois field so important in cryptography?

h. Define a state in AES. Compare the substitution in DES and AES. Why do we have one S-box in AES, but several in DES?

2023

COMPUTER SCIENCE

Paper : CSMC-201

(Advanced Database Management System)

Full Marks : 70

The figures in the margin indicate full marks.

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

Answer ***question nos.*** **1, 2** and ***any four*** questions from the rest.

1. Answer ***any five*** questions : 2×5

(a) Distinguish between shared lock and exclusive lock.

(b) Consider the universal relation R = {A, B, C, D, E, F, G, H, I, J} and the set of functional dependencies are AB → C, A → DE, B → F, F → GH, D → IJ. Find out the primary key for the above relation.

(c) What is the CAP theorem in distributed database?

(d) State the motivation for using checkpoint in transaction.

(e) Define serializable schedule.

(f) State two disadvantages of log-based recovery system.

(g) What is allocation transparency in distributed database management system? Write one importance of it.

2. Answer ***any five*** questions : 4×5

(a) Explain the different kinds of anomalies present in database management system with examples.

(b) Differentiate between cascade schedule and recoverable schedule.

(c) Suppose a book file contains 20000 records stored in 4000 blocks. For nonlinear search, assume the level is 4. Find out cost of following select operations for any two searching techniques:

(i) σ (ID = 002 (CATALOG))

(ii) σ (year > 1995 (CATALOG))

where year and ID are attributes and CATALOG is relation.

(d) Explain shadow paging with the help of a suitable diagram.

(e) Write following query for local transparency and location transparency level :

Select SNAME from SUPPLIER where SNUM = "S003".

where relation is :

SUPPLIER (SNUM, SNAME, CITY).

(f) Explain document database with the help of a suitable example.

(g) How do you prevent deadlock using wait-die and wound-wait deadlock prevention technique?

3. (a) What is extendible hashing?

(b) Insert following data using extendible hashing technique :

16, 4, 6, 22, 24, 10, 31, 7, 9, 20, 26

(c) Calculate time complexity of above specified technique. 2+6+2

4. (a) What is conflict serializability?

(b) Consider each of the following locking protocols and justify whether conflict serializability holds or not for these :

(i) Always hold an exclusive lock before writing, hold exclusive lock until end-of-transaction. No shared locks are ever obtained.

(ii) In addition to (i), obtain shared lock for reading. Shared lock can be released at any time.

(iii) With (ii), two-phase locking.

(iv) As in (ii), in addition all the locks held until end-of-transaction. 2+8

5. (a) What is a precedence graph?

(b) Explain the rules to make precedence graph. Prepare precedence graph for following schedule. S : R1(Y), R1(Z), R5(V), R5(U), W5(U), R2(Y), W2(Y), W3(Z), R4(Y), W4(Y), R4(Z), W4(Z), R1(V), W1(V).

(c) Check whether the schedule is conflict serializable or not by using the precedence graph. 2+4+4

6. (a) Explain ARIES recovery protocol with an example.

(b) How is it better from Validation based scheme? 7+3

7. (a) What is heuristic query optimization?

(b) Optimize the following query using heuristic query optimization technique :

Select *Lname* from EMPLOYEE, PROJECT, WORKS_ON where *Pname* = *"Aquaries"* and *PROJECT. PNo.* = *WORKS_ON. PNo.* and *EMPLOYEE. SSN* = *WORKS_ON. SSN* and *Bdate*> *'1957-12-31'*,

where relations are as follows :

EMPLOYEE (Fname, Lname, SSN, Bdate, Add, Gender, Salary)

PROJECT (Pname, PNo., Plocation, Dnum)

WORKS_ON (SSN, Pno., Hours) 2+8

8. (a) Explain reconstruction, disjointness and completeness property during fragmentation.

(b) Explain horizontal fragmentation and vertical fragmentation with suitable examples. 5+5

2023

COMPUTER SCIENCE

Paper : CSMC-202

(Advanced Operating Systems)

Full Marks : 70

The figures in the margin indicate full marks.

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

Answer ***question nos.*** **1, 2** and ***any four*** questions from the rest.

1. Answer ***any five*** questions : 2×5

(a) Define correctness of control algorithms for a distributed system.

(b) What is binding by types in the context of process migration?

(c) What are the two call semantics used in SUN RPC?

(d) Which of the following is the smallest time stamp according to Vector clock model?

[2,5,1,3], [1,3,0,2], [1,5,2,31], [1,3,0,1]

(i) [2,5,1,3] (ii) [1,3,0,2] (iii) [1,5,2,3] (iv) [1,3,0,1].

(e) How do you differentiate between semantic transparency and syntactic transparency?

(f) Why token-based algorithms are said to be inherently safe?

(g) What is the disadvantage if cache are maintained in the client nodes to improve efficiency?

2. Comment on the correctness of the statements below and justify your opinion (***any five***) : 4×5

(a) In diffusion computation model, a process that diffuses a query never knows whether the communication will be an engaging or non-engaging query for the recipient.

(b) A state recording is consistent if and only if every message that has been recorded as sent is also recorded as received in the destination.

(c) An horizontal straight line 'Cut' parallel to the timeline reflects global state recording.

(d) Symmetric algorithms have high message complexity, and is subject to a single point of failure.

(e) Given, the timestamps for two events A and B are T(A) and T(B), respectively, using the Lamport's logical clock, T(A) < T(B) implies that event A occurred before event B.

(f) In the context of the Chandy-Lamport's state-recording algorithm,– a node within degree 0 in a directed graph topology cannot act as the 'Initiator Node' for Chandy-Lamport's state-recording algorithm.

(g) Building a common address space for an entire distributed system accessible to any client node, may be implemented by mounting the file systems of different nodes, important for individual client, in the respective client rites.

3. (a) State at least two different motivations behind process migration.

(b) Describe the sender-initiated process migration approach.

(c) What is stability? What is done to improve the stability of the system for sender-initiated process migration?

(d) Define pre-emptive and non pre-emptive process migrations. 2+4+2+2

4. (a) What is the role of IDL (interface definition language) in RPC?

(b) "Call by Reference is best suitable for RPC." — Comment on correctness of the statement and justify your opinion.

(c) What is an Orphan Call in RPC?

(d) How a client process is bound with the expertor of a remote procedure in case of SUN RPC? 1+4+2+3

5. (a) What are the drawbacks of the centralized deadlock detection algorithm?

(b) Describe Mitchell-Merritt algorithm for deadlock detection in a distributed environment. Illustrate the same with an example. 3+7

6. (a) What is inverted tree topology?

(b) Describe Raymond's algorithm to ensure mutual exclusion of processes run from multiple nodes in a distributed system.

(c) What would be the worst-case complexity for the above algorithm for a system with N processes running in that many nodes in the system?

(d) Compare performances of symmetric algorithms vis-à-vis token-based algorithms for mutual exclusion. 1+5+1+3

7. (a) What are forward and backward intersections?

(b) The following events occur in a system of four processes :

process p1	**process p2**	**process p3**	**process p4**
event e1;	*event e4;*	*event e6;*	*event e9;*
send message to p2;	*receive message from p3;*	*send message to p2;*	*event e10;*
event e2;	*receive message from p1;*	*event e7;*	
event e3;	*event e5;*	*receive message from p2;*	
	send message to p3;	*event e8;*	

(i) Draw an event trace diagram for the system.

(ii) List the event precedence in the system for every pair of events between which such precedence exists.

(iii) List the concurrent pair of events. 2+(4+2+2)

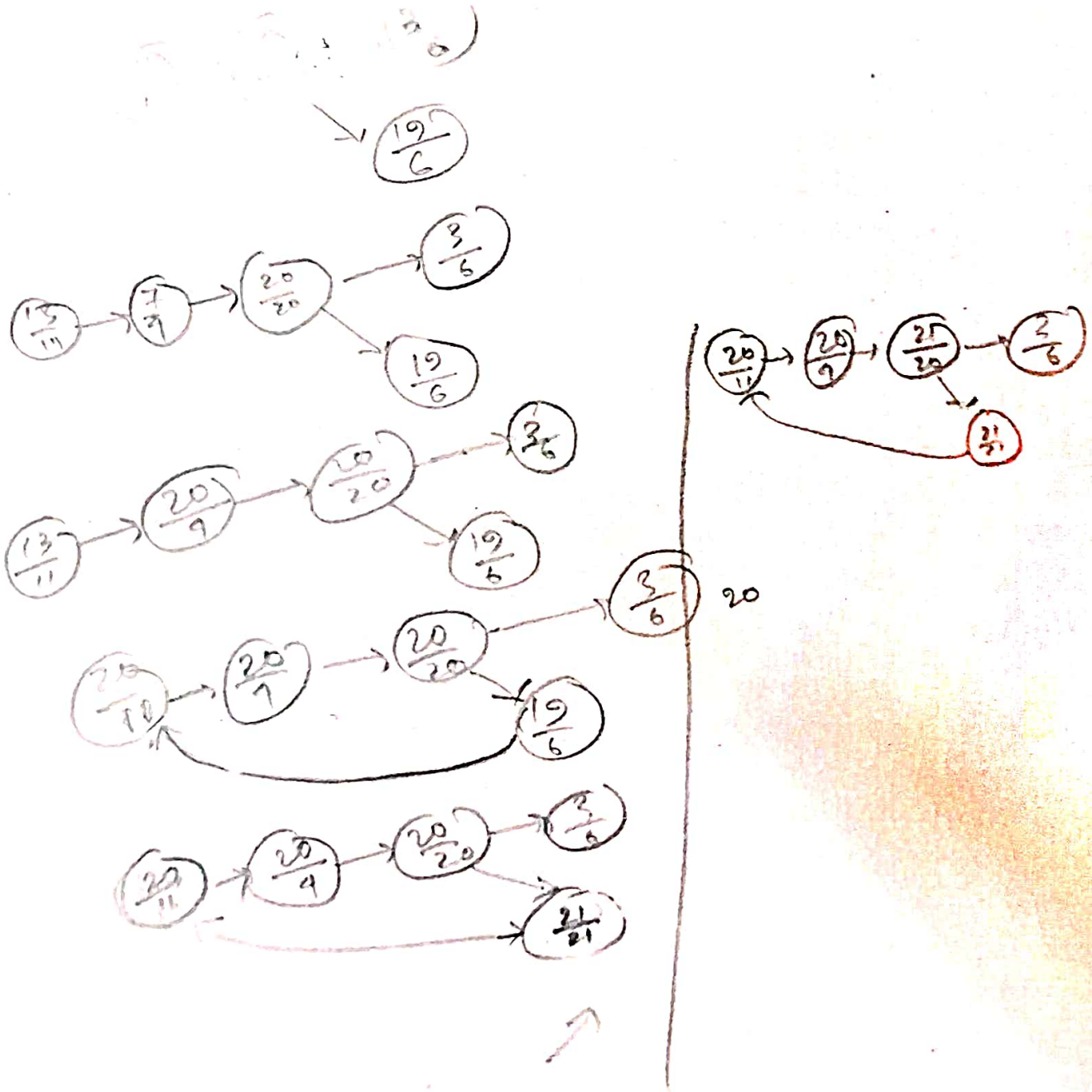
8. (a) How do you define a vector clock for a distributed environment with N nodes?

   (b) Explain how the problem of concurrent event detection in Lamport's clocking can be solved by vector clocking.

   (c) Explain how the use of stubs helps in making an RPC mechanism transparent.

   (d) Why resource migration is often considered as the most critical challenge for migrating a process?

1+3+3+3



2023

COMPUTER SCIENCE

Paper : CSMC-203

(Automata and Compiler Design)

Full Marks : 70

The figures in the margin indicate full marks.

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

Answer ***Question nos.*** **1, 2** and ***any four*** from the rest.

1. Answer ***any five*** questions : 2×5

   (a) How will you eliminate useless symbols from context-free grammars? Give an example.

   (b) Differentiate between tokens, patterns, and lexemes.

   (c) How many different DFAs can be constructed with '*n*' number of states and '*m*' number of input symbols? Assume that the initial state is fixed.

   (d) Write down the conditions to be satisfied for a CFG to be in CNF.

   (e) Point out the differences between Moore and Mealy machines with examples.

   (f) What is the concept of pass in compiler? How can you reduce the number of passes?

   (g) Write a grammar which generates strings of 0*s* and 1s with an unequal number of 0s and 1s.

2. Answer ***any five*** questions : 4×5

   (a) Write down a CFG which will generate $a^n cb^n$ for n >= 0.

   (b) What are the differences between parse tree and syntax tree? Explain with an example.

   (c) Write down the three-address code for : p > q AND r < s OR u > r.

   (d) What are the functions of error handling? Remove left recursion from the following grammar :

   $A \rightarrow ABd \mid Aa \mid a$

   $B \rightarrow Be \mid b.$

   (e) Construct the DFA that accepts the regular expression : (0+1)*(00+11) (0+1)*.

   (f) Write quadruples, triples, and indirect triples for the expression :

   – (a*b) + (c+d) – (a+b+c+d).

   (g) What are the implications of CNF and GNF of grammar?

3. (a) Construct a Turing machine for the language $\{a^n b^n c^n\}$.

   (b) Show that a string can be derived from this machine. Write down the intermediate steps. 6+4

4. (a) Write the algorithm for shift-reduce parsing.

   (b) Consider the following grammar :

   $S \rightarrow aABe$

   $A \rightarrow Abc \mid b$

   $B \rightarrow d.$

   Using shift-reduce parser algorithm, parse the input string abbcde.

   (c) Explain, in detail, the different conflicts that arise in bottom-up parsing. 4+3+3

5. A syntax directed translation scheme that takes strings of a's, b's, and c's as input and produces as output the number of substrings in the input string that correspond to the pattern a(a|b)*c+(a|b)*b. For example, the translation of the input string 'abbcabcababc' is '3'.

   (a) Write a CFG that generates all strings of a's, b's, and c's.

   (b) Write the semantic attributes for the grammar symbols.

   (c) For each production of the grammar, present a set of rules for evaluation of the semantic attributes. 10

6. (a) "There are some CFG for which shift-reduce parsing cannot be used." — Comment.

   (b) Consider the following grammar :

   rexp → rexp | rexp

   rexp → rexp rexp

   | rexp *

   | (rexp)

   | letter

   where, |, *, (,), and letter are terminals.

   (i) What type of language will be derived by the grammar?

   (ii) Show whether the grammar is unambiguous or not. If it is ambiguous, convert it into an unambiguous one. 4+(3+3)

7. Convert the regular expression abb (a|b)* to DFA using the direct method and minimize it. 10

8. (a) When a flow graph is said to be reducible?

   (b) Consider the following statements :

   G := C*(A+B) + (A+B)

   C := A+B

   A := (C+D) + (E-F)

   (i) Draw the DAG for the above statements.

   (ii) What is the optimal ordering of DAG to make the code optimized? Explain with the above code. 2+8

2023

COMPUTER SCIENCE

Paper : CSMC-204

(Cryptography and Network Security)

Full Marks : 70

The figures in the margin indicate full marks.

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

Answer ***Question nos.*** **1, 2** and ***any four*** from the rest.

1. Answer ***any five*** questions : 2×5

   (a) State the role of Trap door one way function in Cryptography.

   (b) Test the primality of the integer 19 using square root test.

   (c) Is it possible to perform an encryption algorithm in parallel on multiple blocks of Plaintext?

   (d) What is Euler's Totient function? Compute the value of Φ (32).

   (e) Is AES a Feistel cipher? Justify your answer.

   (f) A club has only 100 members. How many secret keys are needed for the given cases?

      (i) If everyone trusts the President of the club, i.e., messages are transferred between members through President.

      (ii) If President decides that two members should communicate, then the President creates a temporary key to be used between the two. The temporary key is encrypted and sent to both members.

   (g) Give an example of Cryptanalysis attack. How is it different from Brute force attack?

2. Answer ***any five*** questions : 4×5

   (a) In the elliptic curve E(l, 2) over G(l 1) field, state the equation of the curve and find all the points on the curve.

   (b) Discuss the importance behind choosing the algebraic structure $< Z\Phi(n)^*, x >$.

   (c) Show that the group $< Z_7, X >$ is a cyclic group.

   (d) Compare between the principal ideas followed by the entity authentication schemes : Password based, Challenge Response, and Zero Knowledge Proof.

   (e) Why do you think the mixing transformation (MixColumn) is not needed in DES, but is essential in AES?

(f) "Sub-key generation process also affects the strength of an encryption technique." — Comment with justification in the context of DES algorithm.

(g) Determine the multiplicative inverse of $X^3 + X + 1$ in GF (2^4) with irreducible polynomial $X^4 + X + 1$.

3. (a) Illustrate the working principle of Hill Cipher considering Plaintext = "We live in an insecure world" and Key is equal to K = [03 02]
[05 07].

(b) Describe the trust model used by PHP protocol through an example. 6+4

4. (a) Describe the Elgamal Cryptosystem.

(b) Show that the complexity of the encryption algorithm is computationally easy.

(c) Show that finding out the PT from CT by an intruder becomes computationally infeasible whereas for an authorised person it is computationally easy. 5+3+2

5. (a) State the conditions that a hash function should satisfy.

(b) Prove that the difficulty of the Pre-image attack in message integrity is proportional to 2^n, where n is the number of bits.

(c) Describe the Needham-Schroeder algorithm for both way authentications. 3+3+4

6. (a) Describe the Clogging attack in context of Key Exchange protocol. How can it be prevented?

(b) Define the term "authentication" and "Integrity".

(c) How the HMAC algorithm differs from MD5? (3+2)+2+3

7. (a) Why are the probabilistic algorithms preferable over deterministic algorithm for finding prime number?

(b) Describe Miller-Rabin test for generating strong pseudo-prime.

(c) How the CFB mode is used for generating stream cipher? 2+5+3

8. (a) Describe the RSA based Digital Signature scheme.

(b) Is it possible to offer the service 'non-repudiation' through Digital Signature? Justify your answer. 5+5