مولانا آزاد نیشنل اردو یونیورسٹی

سیمسٹر امتحانات **Semester Examination May 2026**

پروگرام: ایم ٹیک Programme: **M.Tech (Computer Science)**

سیمسٹر: Semester: II

مضمون مع کوڈ Title & Paper Code: **Blockchain Technology (MTCS251PET)**

جملہ Maximum Marks 70 وقت: Time: 3 Hrs گھنٹے

ہدایات:

یہ پرچہ تین حصوں پر مشتمل ہے: حصہ اول، حصہ دوم، حصہ سوم. ہر جواب کے لئے لفظوں کی تعداد شارۃً ہے. تمام حصوں سے سوالوں کا جواب دینا لازمی ہے.

1. حصہ اول میں 10 لازمی سوالات ہیں جو کہ مختصر جواب والے سوالات ہیں. ہر سوال کا جواب دینا لازمی ہے ہر سوال کے لئے 1 نمبر مختص ہے.

(Marks 10 =1 x 10)

2. حصہ دوم میں 8 سوالات ہیں، اس میں طالب علم کو کوئی پانچ سوالوں کے جواب دینے ہیں ہر سوال کا جواب تقریباً دو سو (200) لفظوں پر مشتمل ہے ہر سوال کے لئے 6 نمبرات مختص ہیں

(Marks 30 =6 x 5)

3. حصہ سوم میں پانچ سوالات ہیں. اس میں سے طالب علم کو کوئی تین سوالوں کے جواب دینے ہیں. ہر سوال کا جواب تقریباً پانچ سو (500) لفظوں پر مشتمل ہے. ہر سوال کے لئے 10 نمبرات مختص ہیں.

(Marks 30 = 10 x 3)

حصہ اول

حصہ اول میں 10 سوالات ہیں اور تمام سوالات لازمی ہیں۔ ہر سوال میں 1 نمبر ہوتا ہے۔ (10*1 = 10)

I Verifier زیرو نالج پروف (Zero-Knowledge Proof) میں تصدیق کنندہ۔

A) Knows the secret B) Does not learn anything beyond validity

C) Always trusts the prover D) Generates the proof

II یولر کا نظریہ (Euler's Theorem) کس نظریے کی توسیع ہے۔

A) Euclid's Algorithm B) RSA Algorithm

C) Chinese Remainder Theorem D) Fermat's Little Theorem

III جینیسس بلاک (Genesis Block) میں ہوتا ہے۔

A) Multiple previous hashes B) No previous hash
C) Two hashes D) Encrypted data only

IV بلاک میں نانس (Nonce) کا کیا کردار ہوتا ہے؟

A) Stores transactions B) Identifies users
C) Used in mining to find a valid hash D) Encrypts data

V ڈی پی او ایس (DPoS) میں لین دین (Transactions) کی توثیق (Validates) کون کرتا ہے؟

A) Elected delegates/validators B) Random users
C) All nodes D) Only miners

VI اگر مزید مائنرز (Miners) نیٹ ورک (Network) میں شامل ہو جائیں تو ڈفیکلٹی لیول (Difficulty Level) کیا ہوگا؟

A) Decrease B) Increase C) Remain constant D) Become zero

VII ایک ٹرانزیکشن (Transaction) 21,000 گیس (Gas) کو 50 گوئی (Gwei) پر استعمال کرتی ہے۔ فیس (Fee) ایتھریم (ETH) میں کتنی ہوگی؟

A) 0.0105 B) 0.000105 C) 0.105 D) 0.00105

VIII کل ٹوکنز (Total Tokens = 5,000) ہیں۔ ایک تجویز (Proposal) کے لیے 20 % کورم (Quorum) درکار ہے۔ کم از کم کتنے ووٹس (Votes) کی ضرورت ہوگی؟

A) 500 B) 800 C) 1,000 D) 1,200

IX 7 نوڈ (Node) کے کلسٹر (Cluster) میں لاگ انٹری (Log Entry) کو کمٹ (Commit) کرنے کے لیے کتنے نوڈز (Nodes) کا متفق ہونا ضروری ہے؟

A) 4 B) 5 C) 7 D) 8

X اگر بلاک سائز (Block Size = 1MB) ہو اور ہر ٹرانزیکشن (Transaction = 2 KB) ہو، تو ایک بلاک میں زیادہ سے زیادہ کتنی ٹرانزیکشنز (Transactions) ہو سکتی ہیں؟

A) 256 B) 512 C) 1024 D) 2048

حصہ دوم

2. زیرو نالج پروف (Zero-Knowledge Proof) کے تصور کی تفصیل سے وضاحت کریں۔ نیز (apart) اس کی خصوصیات (Properties) اور طریقہ کار (Working Mechanism) پر بھی بحث کریں۔

3. ہیشنگ (Hashing) کی اہم خصوصیات (Key Properties) کی وضاحت کریں۔ نیز ڈیجیٹل دستخط (Digital Signatures) اور بلاک چین ٹیکنالوجی (Blockchain Technology) میں SHA-256 کے کردار پر بھی بحث کریں۔

4. بلاک چین (Blockchain) میں فورک (Fork) کیا ہوتا ہے؟ اس کی اقسام (Types) کی وضاحت کریں۔

5. آرفن بلاک (Orphan Block)، اسٹیل بلاک (Stale Block) اور انکل بلاک (Uncle Block) پر تفصیل سے بحث کریں۔

6. بلاک چین (Blockchain) میں پروف آف ورک (Proof of Work) کے تصور کی وضاحت کریں۔ اس کے طریقہ کار (Working Mechanism)، اجزاء (Components)، فوائد (Advantages)، حدود (Limitations)، اور استعمالات (Applications) کو بیان کریں۔

7. ایتھیریم ورچوئل مشین (Ethereum Virtual Machine - EVM) کی ساخت (Architecture) اور طریقہ کار (Working) کی وضاحت کریں۔

8. بلاک چین (Blockchain) والیٹس (Wallets) کی مختلف اقسام (Types) پر بحث کریں اور ان کی خصوصیات (Features) کا تقابل (Compare) کریں۔

9. مختلف اقسام کے نوڈز (Nodes) — پیئر (Peer)، اینڈورسر (Endorser)، کمیٹر (Committer)، اور آرڈرنگ نوڈز (Ordering Nodes) کے کردار کی وضاحت کریں۔

حصہ سوم

10. دیا گیا: prime number p=23، generator g =5، private key x=6، اور پیغام message $m = 10$ random $k = 3$ کے ساتھ۔ Public key تلاش کریں، message کو Encrypt اور Decrypt کریں۔

11. مرکل ٹری (Merkle Tree) کے تصور کی تفصیل سے وضاحت کریں۔ اس کی ساخت (Structure)، طریقہ کار (Working)، فوائد (Advantages)، اور بلاک چین (Blockchain) میں استعمالات (Applications) کو مناسب مثال کے ساتھ بیان کریں۔

12. Byzantine Fault Tolerance - BFT کے تصور کی وضاحت کریں اور Distributed Systems میں Consensus حاصل کرنے میں اس کے کردار کا تجزیہ (discuss) کریں۔

13. ہائپر لیجر فیبرک (Hyperledger Fabric) میں مکمل ٹرانزیکشن لائف سائیکل (Transaction Lifecycle) کی وضاحت کریں۔

14. درج ذیل پر مختصر نوٹس (Short Notes) لکھیں:

Web3 (a)
(Decentralized Autonomous Organizations - DAO) (b)
(Cryptocurrency ICO) (c)