Name: Enrolment No:	UPES UNIVERSITY WITH A PURPOSE

UNIVERSITY OF PETROLEUM AND ENERGY STUDIES
Online End Semester Examination, December 2020

Course:	**Information Security Fundamentals**	**Semester:**	**V**
Program:	**B. Tech CSE+ Blockchain**	**Time**	**03 hrs.**
Course Code:	**CSBL3002**	**Max. Marks:**	**100**

SECTION A

1. **Each Question will carry 4 Marks**

S. No.	Question	CO
1	What do you know about Blockchain? What is the difference between Bitcoin blockchain and Ethereum blockchain?	CO1
2	Blockchain is a distributed database. How does it differ from traditional databases?	CO2
3	How does a block is recognized in the Blockchain approach? Is it possible in Blockchain to remove one or more block from the networks?	CO3
4	Name some popular platforms for developing blockchain applications.	CO5

5	Write and explain the output of following smart contract:
	
	pragma solidity ^0.8.3;
	
	contract Variables {
	string public text = "Hello";
	uint public num = 123;
	
	function doSomething() public {
	uint i = 456;
	
	uint timestamp = block.timestamp; // Current block timestamp
	address sender = msg.sender; // address of the caller
	}
	}
		CO4

SECTION B

1. **Each Question will carry 10 marks**
2. **Instruction: Write short/brief notes**

6	Discuss how (i) registering secure transactions, (ii) managing and securing digital relationships, (iii) eliminating intermediaries due to the high cost, and (iv) keeping track of previous actions can be benefitted from leveraging blockchain.	CO3, CO4
7	(a) Explain the significance of blind signature and how it is useful? (b) How will you handle the risk management when it comes to securing the transactions records? Can you explain what are off-chain transactions?	CO4
8	What are the key principles in Blockchain that are helpful in eliminating the security threats that needs to be followed in financial sector?	CO5
9	Write smart contract for digital identities using Solidity. **OR** a. What happens if the execution of a smart contract costs more than the specified gas? b. What does the gas usage in a transaction depend on and how is the transaction fee calculated?	CO1

SECTION C

1. **Each Question carries 20 Marks.**
2. **Instruction: Write long answer.**

10	(a) What is Double Spending? Is it possible to double spend in a Blockchain system? (b) What is Secret Sharing? Does it have any benefit in Blockchain technology?	CO2, CO3

11	a) What are function modifiers in Solidity? Mention the most widely used modifiers with an example. b) Write a smart contract using solidity for House Registry. **OR** Write output of following smart contracts written in solidity.	CO1, CO5, CO4

PROGRAM 1:

```
pragma solidity ^0.8.3;

contract IfElse {
    function foo(uint x) public pure returns (uint) {
        if (x < 10) {
            return 0;
        } else if (x < 20) {
            return 1;
        } else {
            return 2;
        }
    }

    function ternary(uint _x) public pure returns (uint) {
        return _x < 10 ? 1 : 2;
    }
}
```

PROGRAM 2:

```
pragma solidity ^0.8.3;

contract Payable {
    address payable public owner;
    constructor() payable {
        owner = payable(msg.sender);
    }
    function deposit() public payable {}
    function notPayable() public {}
    function withdraw() public {
         uint amount = address(this).balance;
        (bool success, ) = owner.call{value: amount}("");
        require(success, "Failed to send Ether");
    }
    function transfer(address payable _to, uint _amount) public {
        (bool success, ) = _to.call{value: _amount}("");
        require(success, "Failed to send Ether");
    }
}
```

PROGRAM 3:

```
pragma solidity ^0.8.3;
contract Function {
    function returnMany()
        public
        pure
        returns (
            uint,
            bool,
            uint
        )
    {
        return (1, true, 2);
    }
    function named()
        public
        pure
        returns (
            uint x,
            bool b,
            uint y
        )
    {
        return (1, true, 2);
    }
    function assigned()
        public
        pure
        returns (
            uint x,
            bool b,
            uint y
        )
    {
        x = 1;
        b = true;
        y = 2;
    }
    function destructingAssigments()
        public
        pure
        returns (
            uint,
            bool,
            uint,
            uint,
```

PROGRAM 4:

```
pragma solidity ^0.8.3;

contract Array {

    uint[] public arr;
    uint[] public arr2 = [1, 2, 3];

    uint[10] public myFixedSizeArr;

    function get(uint i) public view returns (uint) {
        return arr[i];
    }


    function getArr() public view returns (uint[] memory) {
        return arr;
    }

    function push(uint i) public {
        arr.push(i);
    }

    function pop() public {
        arr.pop();
    }

    function getLength() public view returns (uint) {
        return arr.length;
    }

    function remove(uint index) public {
        delete arr[index];
    }

    function examples() external {
        uint[] memory a = new uint[](5);
    }
}
```

```
        uint
    )
  {
    (uint i, bool b, uint j) = returnMany();
    (uint x, , uint y) = (4, 5, 6);

    return (i, b, j, x, y);
  }
  function arrayInput(uint[] memory _arr) public {}
  uint[] public arr;

  function arrayOutput() public view returns (uint[] memory) {
    return arr;
  }
}
```