Quiz 3

1. Which of the following(s) about bitcoin scripts is true: AC
   a. The language is Turing-incomplete
   b. The language supports loop
   c. The language supports jump
   d. Bitcoin memory can be randomly accessed by scripts.

2. Validating a Bitcoin transaction tx is commonly set up between tx as the redeeming transaction and its input as the funding transaction. Then, transaction validation is operated by running the unlocking script in the redeeming transaction against the locking script in the funding transaction. Here, the locking transaction is called____ and the unlocking script, also called_____ scriptPubKey and scriptSig

3. Analyze the security of the following script, and identity vulnerabilities, if any: Integer Overflow

```
mapping (address => uint256) public balanceOf;
function transfer(address _to, uint256 _value) {
   require(balanceOf[msg.sender] >= _value);
   balanceOf[msg.sender] -= _value;
   balanceOf[_to] += _value;
}
```

4. [True/False] In a reentrancy attack, the attacker can drain *all* cryptocurrencies/tokens held in the victim smart contract, despite of the specific account controlled by the attacker.

5. Ethereum Improvement Proposal 150 or EIP150 states that the cost for EXTCODESIZE should be increased from 20 gas to 700 gas. What is this EIP intend to do?:
   a. Prevent reentrancy attack
   b. Prevent denial of Service (DoS) attack
   c. Prevent Buffer overflow attack
   d. Prevent selfish mining

6. The life cycle of a smart contract involves the following operations in order:
   a. compile, execute, deploy
   b. deploy, compile, execute
   c. compile, deploy, execute
   d. execute, compile, deploy

7. [True/False] Ethereum has two types of accounts: externally account owned account and contract account.
8. [True/False] Storing a value in solidity's memory is more expensive than doing that in its external storage.
9. About blockchain states, which of the followings is/are incorrect? A,E
   a. Ethereum stores Ether balance in per-transaction UTXO.

b. Ethereum stores Ether in per-account balances.
c. Ethereum state includes not only Ether balances but also smart-contract storage.
d. Ethereum smart-contract storage is randomly accessible.
e. Ethereum smart-contract storage is a stack.

10. Which of the following about Ethereum transaction/message is incorrect? C

a. An Ethereum transaction can be interpreted as an Ether transfer function.
b. An Ethereum transaction can be interpreted as an invocation to smart contract function.
c. An Ethereum transaction can be interpreted as an internal invocation (invocation by another smart contract).
d. An Ethereum message also transfers Ether to the receiver account.
e. An Ethereum message can specify an EOA to be a receiver account.

11. Which of the following about reentrancy attack is incorrect? B, C

a. In a reentrancy attack, it is the victim smart contract that is reentered.
b. In a reentrancy attack, it is the attacking smart contract that is reentered.
c. In a successful reentrancy attack, the internal state of smart contract being reentered is updated since the first entrance.
d. In a successful reentrancy attack, the internal state of smart contract being reentered is not updated since the first entrance.

12. Which of the following is/are techniques to prevent reentrancy attacks? A, C, F

a. Synchronize the concurrent accesses to a victim smart contract
b. Synchronize the concurrent accesses to an attacker smart contract
c. Use send() in the victim smart contract
d. Use send() in the attacker smart contract
e. Make sure the victim's internal state change is before interacting external smart contracts.
f. Make sure the attacker's internal state change is before interacting external smart contracts.