EE 465: Cryptocurrency and Blockchain Technologies (Autumn 2018)
Instructor: Saravanan Vijayakumaran
Indian Institute of Technology Bombay

Midsem Exam : 16 points — September 11, 2018

1. (a) (1 point) Write down the multiplication operation table over $\mathbb{F}_{11}$.
   (b) (2 points) Enumerate all the points of the elliptic curve $Y^2 = X^3 + 4X + 5$ over $\mathbb{F}_{11}$.
   (c) (2 points) For each point $P$ on the above elliptic curve, calculate the point $2P$.

2. (5 points) Answer the following questions in the context of the Bitcoin system.
   (a) Describe the steps involved in generating a Pay-to-Public-Key-Hash (P2PKH) address from a private key.
   (b) Alice wants to buy a book from Bob. He emails his Bitcoin P2PKH address to Alice. But a single character is missing from the address. Bob made a mistake while typing it. How can Alice find the **location and value** of the missing character in the address without contacting Bob?
   (c) The merchant Bob wants to create a *vanity P2PKH address* to share with this customers. He wants it to start with the characters `1bob....` How can he generate such an address?
   (d) Under what conditions is storing bitcoins in a P2PKH output safer than storing bitcoins in a pay-to-public-key output?
   (e) Suppose a merchant waits for six confirmations on a Bitcoin payment before transferring some goods to a customer. Describe how a 51% attacker can execute a double spend attack on such a merchant.

3. (2 points) The Merkle Patricia trie corresponding to the key-value pairs { 646f : ‘verb’, 646f67 : ‘puppy’, 646f6765 : ‘coin’, 686f727365 : ‘stallion’ } is given below. Suppose the last key-value pair (corresponding to the value ‘stallion’) is deleted from the trie. Write down the modified trie.

| | |
|---|---|
| rootHash | [ ⟨16⟩, hashA ] |
| hashA | [ ⟨⟩, ⟨⟩, ⟨⟩, ⟨⟩, hashB, ⟨⟩, ⟨⟩, ⟨⟩, hashC, ⟨⟩, ⟨⟩, ⟨⟩, ⟨⟩, ⟨⟩, ⟨⟩, ⟨⟩, ⟨⟩ ] |
| hashC | [ ⟨20 6f 72 73 65⟩, ’stallion’ ] |
| hashB | [ ⟨00 6f⟩, hashD ] |
| hashD | [ ⟨⟩, ⟨⟩, ⟨⟩, ⟨⟩, ⟨⟩, ⟨⟩, hashE, ⟨⟩, ⟨⟩, ⟨⟩, ⟨⟩, ⟨⟩, ⟨⟩, ⟨⟩, ⟨⟩, ⟨⟩, ’verb’ ] |
| hashE | [ ⟨17⟩, hashF ] |
| hashF | [ ⟨⟩, ⟨⟩, ⟨⟩, ⟨⟩, ⟨⟩, ⟨⟩, hashG, ⟨⟩, ⟨⟩, ⟨⟩, ⟨⟩, ⟨⟩, ⟨⟩, ⟨⟩, ⟨⟩, ⟨⟩, ’puppy’ ] |
| hashG | [ ⟨35⟩, ’coin’ ] |

4. (4 points) Answer the following questions in the context of the Ethereum system.
   (a) Decode the following using RLP decoding: `0xc6827a77c10401`.
   (b) How does the `nonce` field in the transaction data structure prevent replay attacks? Describe a replay attack which becomes possible if this field is omitted.
   (c) Explain why the `v` field in the transaction data structure is not mandatory and is included as a convenience to reduce computation. *Hint: Show how the public key can be identified from a message and signature* `(r,s)` *even when* `v` *is unknown.*
   (d) In Ethash mining, the `mixHash` field can be calculated from the partial header hash, `nonce`, and dataset (DAG). Explain the reasoning behind including the `mixHash` field in the header by describing a DoS attack (on nodes which validate blocks) which is possible if the `mixHash` field had been omitted.