Quiz

Your Name: _____

For this quiz, you should **work alone**. You may use your course notes, but no other resources. Answer all the questions as well as you can. Good answers will be clear, consise, and correct.

Notations

Key pair: KU_x is the p**U**blic key, KR_x is the p**R**ivate key
Alice's keys: KU_A (Alice's public key), KR_A (Alice's private key)
Bob's keys: KU_B (Bob's public key), KR_B (Bob's private key)

Encryption: $E_K(m)$ is the encryption of message m using key K. (This notation is used for both symmetric and asymmetric encryption, the key determines the intended encryption.)

Hashing: H is a cryptographic hash function.

Concatenation: $A||B$ is the concatenation of the two bitstrings.

1. Colleen Cryptofferson is designing a new cryptocurrency based on a consensus-based public ledger, and considering several possible ways to report a transaction where Alice sends coin X to Bob. (You may assume X is a string that is used to validly identify Alice as the owner of the coin.)

For each scheme, indicate if it is reasonable, or write a short explanation why it is terrible.

a. $E_{KU_A}(X \text{ to } KU_B)$

b. $E_{KR_A}(X \text{ to } KU_B)$

c. $E_{KU_A}(X \text{ to } KR_B)$

d. $E_{KR_A}(X \text{ to } KR_B)$

2. Darcy Discerning suggests that Colleen Cryptofferson should use

$$E_{KR_A}(H(X \text{ to } KU_B))||X \text{ to } KU_B$$

instead. Is this a good idea? (If not, explain what it is not a good way to report a transaction; if so, explain what it is better than any of the options in question 1.)

3. To implement her cryptosystem, Colleen Cryptofferson needs a blockchain design. Emily Elephant suggests making the block header:

Label	**Bytes**	**Description**
`block_number`	16	Number of this block
`merkle_root`	32	Hash of Merkle tree of all transactions
`nonce`	16	Nonce found to generate this block

A block is (`block header` || `transactions`). A block is valid if all of the following are true (but no other validity checks are required):

a. $H(blockheader)$ (interpreted using the Base58 encoding as used in bitcoin addresses) starts with 'Emily'.
b. The `block_number` in the block is the previous block's `block_number` + 1 (and the genesis block uses `block_number` = 0).
c. The `merkle_root` in the block header is the hash of the root of a Merkle tree constructed from the `transactions`.

Give at least two major problems with Emily's design.

Problem 1:

Problem 2:

4. What are some technically misleading or incorrect statements in the Morgan Spurlock bitcoin explanation video?

