Home Assignment 1

Emma Asklund, 9507215581

Complete the eight A-assignments below and solve them individually.

A-3 Give two common ways to prove/make probable that the person making a card-not-present transaction is in physical possession of the card. Compare the two alternatives in terms of security.

A-7 Is SSL required in SET? Motivate your answer.

A-14 The multiplicative property of RSA provides for blind signatures. What is meant by "the multiplicative property of RSA"?

A-18 When Alice buys something from Bob using the untraceable E-cash scheme, why is it impossible for Bob to learn the identity of Alice?

A-19 In the untraceable E-cash protocol in the lecture notes, the serial number of a coin is a signature from the bank, i.e., produced using the bank's private key. Why (in a technical sense) can the bank not map this serial number to Alice?

A-20 How is Alice's identity revealed if she double spends a coin in the untraceable E-cash scheme?

A-33 In Bitcoin, one transaction can list several outputs. The hash of the transaction must be well-defined, so the outputs must be ordered. Give another reason why these must be ordered.

A-34 How is the difficulty in Bitcoin block hashing adapted so that it (almost) always takes about 10 minutes for the system to produce a new block, regardless of the computational power that enters the system?