Home Assignment 1

Fredrik Magnusson, 9502163596

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

A-2 Describe an attack that the *CVV1* code on a credit card prevents. Why is it not effective against skimming?

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-5 How does the Merchant verify the dual signature in SET?

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-22 Briefly explain the differences between session-level aggregation, aggregation by intermediation and universal aggregation.

A-30 Compare the anonymity given by the untraceable E-cash scheme and Bitcoin.

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.