Home Assignment 1

Niklas Jnsson, 9208273772

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

A-4 What is the difference between a three-party scheme and a four-party scheme for credit card payments?

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

A-6 In SET, why is the Payment Information first symmetrically encrypted and not immediately encrypted with the Gateway's public key?

A-17 How can the cut–and–choose technique be used to make sure that identifying information is properly added into an untraceable coin?

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

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

A-28 Compare the PayWord protocol and the Peppercoin-like protocol in the lecture notes from the point of view of the customers, both in terms of what they pay, and in terms of what they need to compute to make a purchase.

A-29 What is meant by a probabilistic payment? How does the Electronic Lottery Tickets scheme differ from Peppercoin from the user's perspective? How do they differ from the Merchant's perspective?