Home Assignment 1

Filip hfelt, 9405313173

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

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

A-8 How does the SET protocol provide non-repudiation?

A-9 In 3D Secure, describe briefly what happens after the Merchant/MPI receives the PARes from the issuer.

A-13 What is the difference between *authorization* and *authentication* in VbV (3D Secure)?

A-16 In the DigiCash scheme, explain how Alice could trick the bank into signing something completely different than a coin, e.g., the message "The Bank should give 1000 SEK to Alice". How could such user misbehaviour be avoided?

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-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-27 In the PayWord protocol, give the Bank's algorithm for verifying how much money should be taken from the user's account.