Home Assignment 1
EITN41

Rasmus Olofzon, 9104192472

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

Blah blah blah.

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

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

A-23 *In PayWord, a unit could be, e.g., one cent (or one öre), so even though the payments are "micro", the hash chains could be pretty long. Could this pose a storage problem to Alice, who has to generate the entire chain when (before) she makes her first purchase from a merchant?*

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

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?*

A-31 *How much is the transaction fee for a Bitcoin transaction and how is it determined?*

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?*