Home Assignment 1

Marcus Rodan, 9407087932

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

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

A-11 The acronyms ACS and ADS are both related to VbV (3D Secure). Explain them briefly.

A-15 When requesting a blind signature, why must Alice keep r secret?

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

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