This is the feedback for the COMP38411 Coursework

A. Feedback on question (a)

Other correct/valid points/answers will also be considered.

Security threats in the context are:

- Disclosure of sensitive information: Disclosure of a credit card number to an unauthorized person who may be able to use the credit card number to make purchases online.
- Repudiation of purchase by customer: A customer may falsely deny that she/he has purchased (or authorised the purchase of) a particular item.
- Unauthorised payment: A fraudulent merchant may double charge or receive payment without the authorisation of the customer.
- External attacks, such as impersonation of C (Customer), M (Merchant), and/or A (Acquirer).

B. Feedback on question (b)

- The protocol can prevent unauthorised disclosure of a customer's credit card number to a merchant when the customer makes a purchase from the merchant, as the number is encrypted with acquirer's public key and only the acquirer can decrypt it.
- The protocol cannot prevent false denial of a purchase, as the protocol does not contain any undeniable evidence (digital signature) of the purchase or payment authorization from the customer.
- The protocol cannot prevent unauthorised payment to the merchant because the protocol does not have any digital signature of the customer for the payment authorization. The merchant may replay the Payment sent by C (the third message in the protocol given).

C. Feedback on question (c)

Key security issues which should be considered in the design:

- A trusted third party, T, along with necessary security measures, are used to achieve fairness: T ensures that what is expected by C is identical to what C has been promised by M by verifying the respective copies of the Purchase-details, which has been agreed on by C and M and sent to T separately. Upon positive verification of the Purchase-details and payment authorization by A, T forwards the e-goods to C and payment confirmation to M.
- As the minimum, the Slip (containing credit card number) should be confidentiality protected.
- The Payment message sent by C should at least be authenticated.
- The Charge Request message sent by M should at least be authenticated.
- The Authorisation Request message should be signed for accountability/non-repudiation/dispute resolution, as this will lead to money transaction.

- The Authorisation Response message should be signed for accountability/non-repudiation/dispute resolution, as this serves as an evidence/receipt/confirmation of the purchase.
- These signatures should be timestamped and bound to the particular purchase made.
- All the signature verification keys should be certified by a trusted CA, valid and not on the CRL of the CA.
- It should be emphasized that the above mentioned security properties have direct impact on achieving fairness.

In addition,

- Assumptions used should be clearly stated and notation used should be clearly defined.
- Protocol message construction should be clear and the cryptographic primitives or building blocks used (particularly those from literature/research domain) should be clearly stated and reference cited and necessary proofs provided.
- The checks/verifications should be clearly described, and for each such verification, making clear for what property/purpose it is for.
- Design decisions should be properly justified.