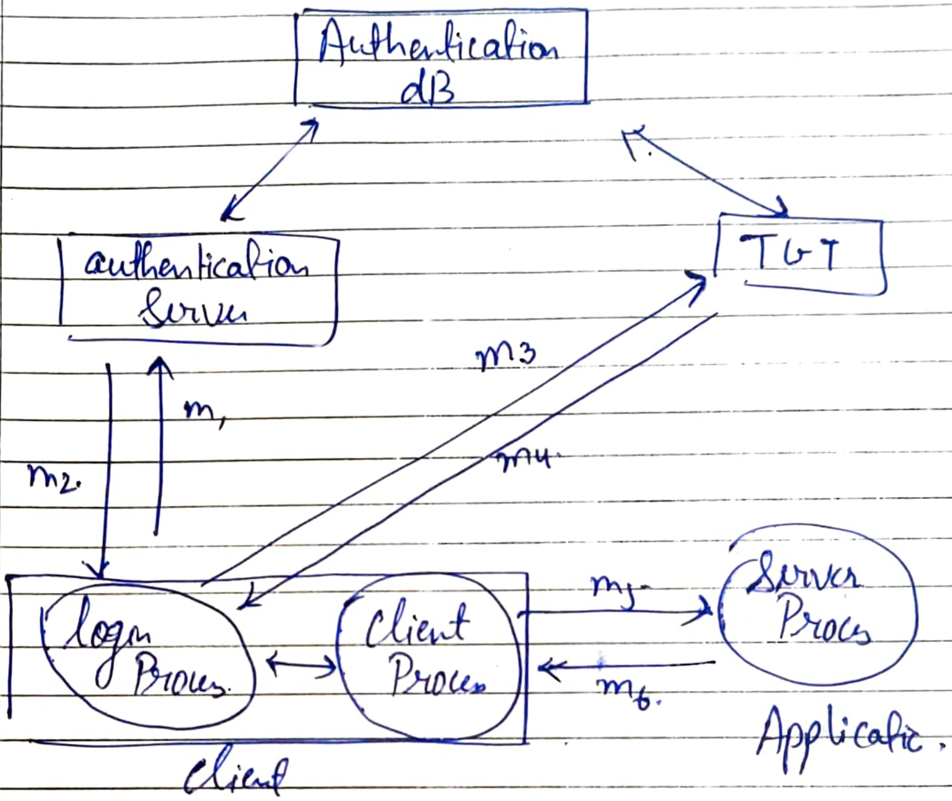
Name of the Subject: E-COMMERCE & E-SEC. Subject Code: IT-718

Seat No: IT076 Student ID: 18ITUBN116 Branch/Sem: IT-VII

Q2 (a).



$m_1 = (ID_c, N_1)$

$m_2 = C_2 = E((N_1, K_1, C_1), K_c)$

$C_1 = E_g((ID_c, ID_g, T_{s_1}, T_{e_1}, K_1), K_g)$

$m_3 = (ID_S, N_2, C_1, C_3)$

$C_3 = E((ID_c, T_1), K_1)$

$m_4 = C_5 = E((N_2, K_2, C_4), K_1)$

$C_4 = E((ID_c, ID_S, T_{s_2}, T_{e_2}, K_2), K_S)$

$m_5 = (C_4, C_6)$

$C_6 = E((ID_c, T_2), K_2)$

$m_6 : C_1 = E(T_3, K_2), T_3 = T_{2+1}$

ID_g = ~~Tgs~~ Ticket Granting Server Identifie.

ID_c = Client Identifier.

ID_s = Application Server Identifie.

N_i = Nounce

K_c = Client Secret key.

K_s = App. Server Secret key.

K_g = Ticket granting Server Secret key.

K_1 = Ticket Granting Ticket Session key.

K_2 = Service Granting Ticket Session Key.

T_{si} = Starting Time of Validity of Ticket.

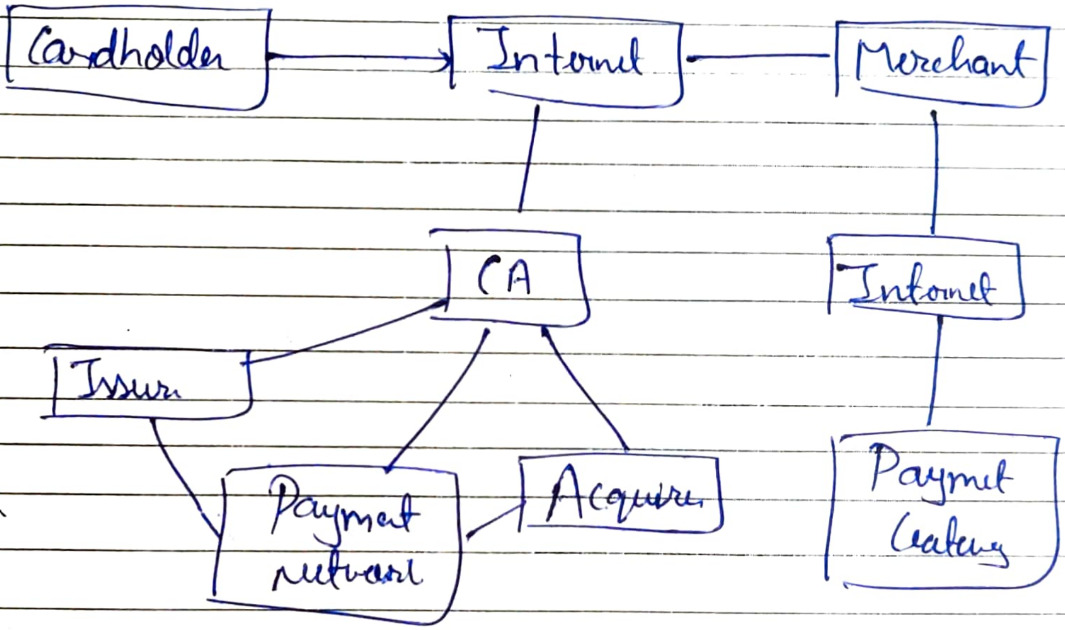
T_{ei} = Ending Time of validity of Ticket

T_i = Time Stampt.

Q2 (b).

Secure Electronic Transaction (SET)

- Open Encryption & Security Specification to protect Internet Credit Card.



- Cardholder:- Purches interact with merchant from personal Computers over Internet.

- Merchant:- A Person that has good Services to sell to cardholder.

- Issuer:- A financial Instituation, such as a bank that provide the cardholder with payment card.

Name of the Subject: ECES Subject Code: IT-718

Seat No: IT076 Student ID: 18ITUBN116 Branch/Sem: IT-VII

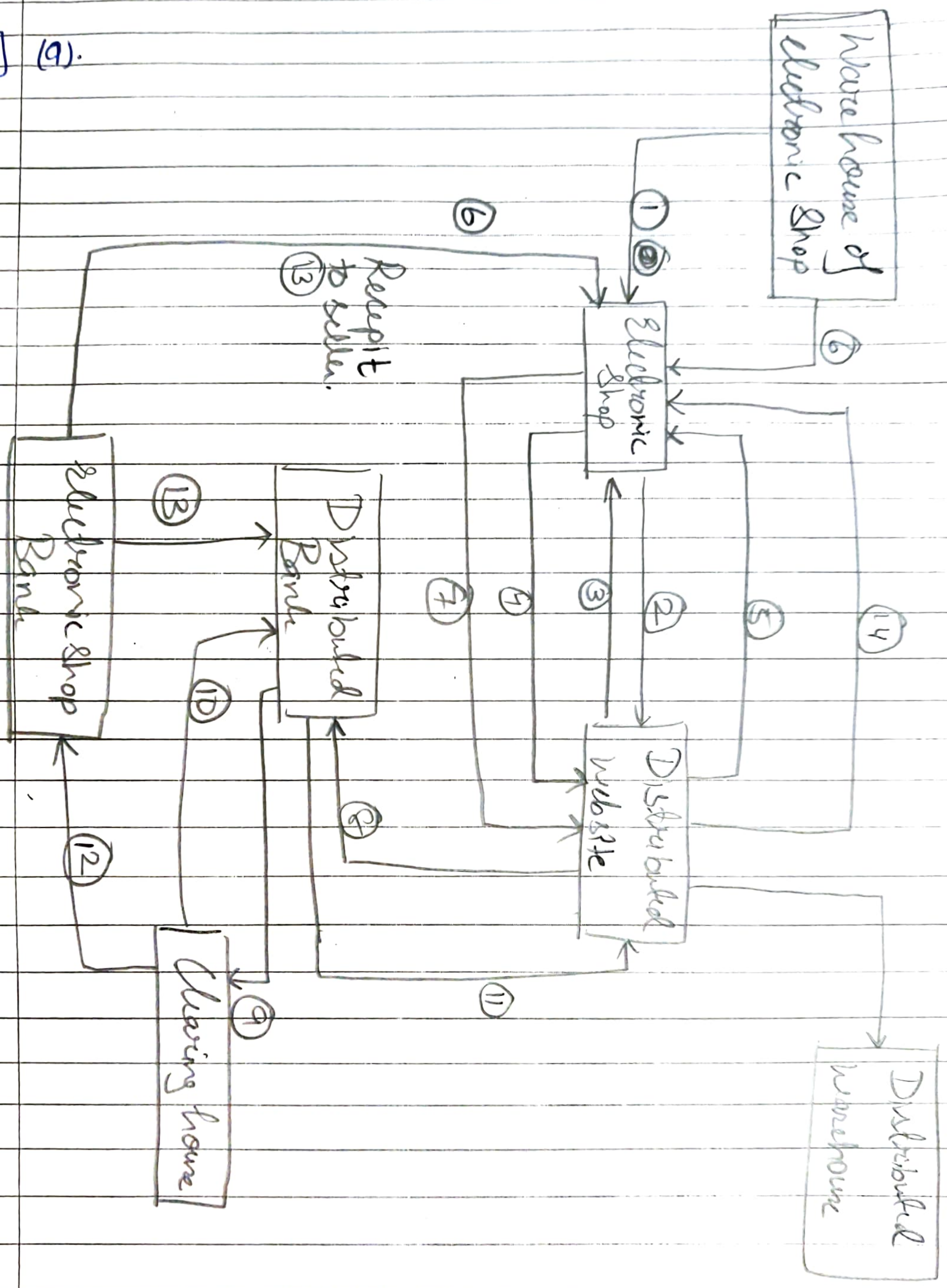
— Acquirer:- A financial Institution that ~~et~~ establishes an account with merchant & processes payment card

— Payment Gateway:- A operator by the acquirer or a designed 3rd party that processes payment mess.

— CA:- An entity that is trusted to issue X.509 V3 public key Certificate for Cardholder, merchants & payment gateway.

Section – II Date: 11/10/2021 Signature of Student:

Q3 (a).


Warehouse of electronic Shop
Electronic Shop
Electronic Shop Bank
Distributed Bank
Distributed website
Clearing house
Distributed Warehouse
Receipt to seller.
1
2
3
4
5
6
7
8
9
10
11
12
13
14

PTO

Name of the Subject: ECES Subject Code: IT-718

Seat No: IT076 Student ID: 18ITUBN116 Branch/Sem: IT-VII

Point Description

(1) — Stock goes below level.

(2) — Enquire Availbity

(3) — Display Various electronic Item

(4) — Places order

(5) — Ack. order & Send bill

(6) — Item Received.

(7) — Send Cheque

(8) — Cheque Sent after ~~verf~~ verification of Seller's public key Certificate

(9) — Send Cheque for Clearance

(10) — Ok's Clearance — (11)

~~(11)~~ (12) — Debit advice to Electronic Shop's bank.

(13) — Credit to distributor's bank A/c

(14) — Remainder if bill not paid within 15 days.

Name of the Subject: ECFS Subject Code: IT-718

Seat No: IT076 Student ID: 18ITUBN116 Branch/Sem: IT-VII

Q3 (b).

A SA is a logical Connection involving 2 devices that transfer data with the help of IPsec protocol.

- SA offers data protection for unidirectional traffic.
- An IPsec Tunnel feature 2 Undirectional SA, which offers a secure, full duplex for data.
- Parameters are:- Destination Address
  SPI
  Key
  Crypto Algorithm & Format.
  Key Lifttime.
  Authentication Algo.

Section – II Date: 11/10/2021 Signature of Student: