IT430 IDEA SOLOUTION

Question no 1:
Assume you as a student is playing role of customer in E-cash payment system in which anonymity of the buyer is kept in view. You have purchased online Electronic Project essentials from online Supporting Company ABC that has also registered its account in the E- Cash bank.
You have to pay to merchant using the mentioned e-cash system following facts help you to calculate your coins minting and paying to customer anonymously.
For signatures you have to adopt the following mathematical expression:
Steps for Solving the Problem:
Serial #.re (Mod m)
"r" =((your ID 's least significant right most two digits) Mod 4)+2
_ Here "r" will vary according student to student based upon their VU ids and Mod here mean well
known "modulus" operator.
For example in case of your id is BC1304017001 pick the last two digits here these are 01 and take Modulus
operator with digit "4" "01" Mod 4=01 and apply the attained "r" in the minting and depositing stages of the
payment to Merchant all other factors are same for all students only the variation will be attained according to
factor "r" which will be calculated according to the above mentioned formula.
Public key of the bank consists of modulus 'm' and a no. 'e'. Here for simplicity of calculation you have to take
"m=7" and "e=3" it has been assumed all constraints of the system for taking values have been followed.
Serial # =00100.
And code sent back by bank using the following mathematical expression.
(**Serial #.re) d (mod m)**
_ Here "d=1/3" for all students for cause of simplicity. And you people have to mint coin having value
of "5$" in simple words multiply with "5" to all values "e" and "d" in all given above and below
mathematical expressions in assignment to calculate the correct value to mint five dollar coin . And
this is our own way to generate message digests to encrypt the values for security purposes.
And code again decoded by you using the following mathematical expression.
[(Serial #.re) d (mod m)]/r
_ Here you have done minting stage and after decoding stage you can sent that achieved values to
merchant to pay the merchant the five dollar coin value using the following concatenation expression
. Which he /she herself send to e-cash bank to get credited.
Coin = (Serial#) ([(Serial #.re) d (mod m)] /r)) ((Serial #.re) d (mod m))
Note: Here for coin generation you have just concatenated the expressions or values to get the coin value.
DISTRIBUTION OF MARKS ALONGWITH TABLE TO BE FILLED:
Observe all the above guidelines and rules as mentioned above to fill the following table to get graded your assignment.
Think with peace of mind and heart to go to the actual calculations. Think beyond the

boundaries to devise your own ways to decrypt and encrypt your messages to get the task done.
r = (23 Mod4) + 2
Answer:
r = (23) mod 4)+ 2
modulas operator 4 = 01
means mod 4 = 01
r = ((01) mod 4) + 2
m = 7 and e = 3
Serial # 00100
Message/Code sent by you to bank after your signatures
Serial # $r^e)^d$ (mod m) r = 1.365
Message/Code minted by bank and sent to you
(00100 ((23) mod e 4)$^{+2}$) (mod 7)
Message Code decoded by you
[(Serial # $r^e)^d$ (mode m)]/r
1.365 ((23)mod 4)$^{+2}$ = 1.365/5 = 0.273
Coin
coin =(Serial #)([Serial # $r^e)^d$(mod m)]r)
(Serial # r^e) ^{d}(mod m)) = (00100) (0.273) (1.365)
Why is there anonymity factor achieved by customer(One sentence answer)
Bank does not know the serial number because of blinding factor ‘r’
Why we have taken d=1/3 and e=3
For simplicity ‘e’ is given and ‘d’ always inverse of ‘e’

Electronic Cash (Ecash)
Electronic Money, E-Cash, is changing the way currency is perceived. While the change seems as revolutionary as the conversion from value-based mediums of exchange (e.g. gold, silver) to paper currency, it is actually only an evolution from current paper-based mediums. There are a number of benefits of E-Cash over greenbacks, but there are also new issues with which to contend. In addition to new issues, there are also new forms of old problems which E-Cash will not solve. In its current state electronic cash is a necessary innovation in the financial markets. However, it is highly doubtful that E-Cash will actually replace paper currency.

How it is used:

Ecash is used over the Internet, email, or personal computer to other workstations in the form of secured payments of "cash" that is virtually untraceable to the user. It is backed by real currency from real banks.
The way ecash works is similar to that of electronic fund transfers done between banks. The user first must have an ecash software program and an ecash bank account from which ecash can be withdrawn or deposited. The user withdraws the ecash from the account onto her computer and spends it in the Internet without being traced or having personal information available to other parties that are involved in the process. The recipients of the ecash send the money to their bank account as with depositing "real" cash.

Part No. 01
Message/Code sent by you to bank after your signatures
Serial # re)d (mod m) r = 1.365

Part No. 02
Message/Code minted by bank and sent to you
(00100 ((23) mod e 4)+2) (mod 7)

Part No. 03
Message Code decoded by you
[(Serial # re)d (mode m)]/r
1.365 ((23)mod 4)+2 = 1.365/5 = 0.273

Part No. 04
Coin
coin =(Serial #)([Serial # re)d(mod m)]r)
(Serial # re) d(mod m)) = (00100) (0.273) (1.365)

Part No. 05
Why is there anonymity factor achieved by customer(One sentence answer)

There anonymity factor achieved by customer because Bank does not know the serial number because of blinding factor 'r'

Part No. 06
Why we have taken d=1/3 and e=3
The reason of taking is this 'e' is given and 'd' always inverse of 'e

Serial #.re (Mod m)
"r" =((your ID 's least significant right most two digits) Mod 4)+2
_Here "r" will vary according student to student based upon their VU ids and Mod here mean well
known "modulus" operator.
For example in case of your id BC1304017001. You need to pick the last two digits here these are 01 and take

Modulus operator with digit “4”. “01” Mod 4=01 and apply the attained “r” in the minting and depositing stages of
the payment to Merchant all other factors are same for all students only the variation will be attained according to
factor “r” which will be calculated according to the above mentioned formula.
Public key of the bank consists of modulus ‘m’ and a no. ‘e’. Here for simplicity of calculation you have to take
“m=7” and “e=3” it has been assumed all constraints of the system for taking values have been followed.
Serial # =00100.
And code sent back by bank using the following mathematical expression.
(**Serial #.re) d (mod m)**
How IT WILL SOLVE BY USING VU ID