RMIT UNIVERSITY

School of Science

INTE1070/1071 Secure Electronic Commerce

Assignment 2

	Assessment Type: Individual assignment; no group work. Submit online via Canvas→Assignments→Assignment 2. Marks awarded for meeting requirements as closely as possible. Clarifications/updates may be made via announcements/relevant discussion forums.
	Due date: **Week 11, Friday the 9th Oct 2020 11:59pm** Deadlines will not be advanced, but they may be extended. Please check Canvas→Syllabus or via Canvas→Assignments→Assignment 2 for the most up to date information. As this is a major assignment in which you demonstrate your understanding, a university standard late penalty of 10% per each working day applies for up to 5 working days late, unless special consideration has been granted.
✓	**Weighting:** **50 marks (Contributes 50% of the total Grade)**

1. Overview

The objective of Assignment 2 is evaluating your knowledge on the topics covered in Lecture 5 to 10. Topics include Secure payment gateway, Secure Electronic Transaction (SET) Protocol, Secrets of Smart Card Security, Digital Cash, Cryptocurrency & Digital Ledger Technology in E-Commerce, Reliability of Large E-commerce systems, and Future Shopping and Ecommerce. Assignment 2 will focus on developing your knowledge behind secure payments and applying them in real e-commerce applications. In addition, this assignment will help to understand several promising technologies that can be used in e-commerce solutions and analyze their pros and cons. Moreover, this assignment will help you to learn how the reliability of an e-commerce system can be assured. Assignment 2 contains several problems related to the topics mentioned above. You are required to prepare the solutions with the description of the step-by-step processes as a single PDF or MS Word file and necessary codes.

Develop the solution of this assignment in an iterative fashion (as opposed to completing it in one sitting). You should be able to start preparing your answers immediately after the Lecture-5 (in Week-5). At the end of each week starting from Week-5 to Week-10, you should be able to solve at least one question.

If there are questions, you must ask via **the relevant Canvas discussion forums** in a general manner.

Submission instructions are detailed in Section 2.

2. Submission Instructions

Overall, you must follow the following special instructions:

- You must fulfil the requirements in the questions.
- For the questions that require implementation, you must implement the functionalities stated in the questions. Any change in a user interface is acceptable if the functionality is there.
- In your solution, you must show all of the steps with necessary code segments and screenshots for each question.
- Upload your solution as a single PDF or Word document in CANVAS. Also, upload codes as a single ZIP file in the CANVAS.
- Do not put the PDF withing the ZIP file.

3. Assessment Criteria

This assessment will determine your ability to:

- Follow requirements provided in this document and in the lessons.
- Independently solve a problem by using cryptography and cryptanalysis concepts taught over the first four weeks of the course.
- Meeting deadlines.

4. Learning Outcomes

This assessment is relevant to the following Learning Outcomes:

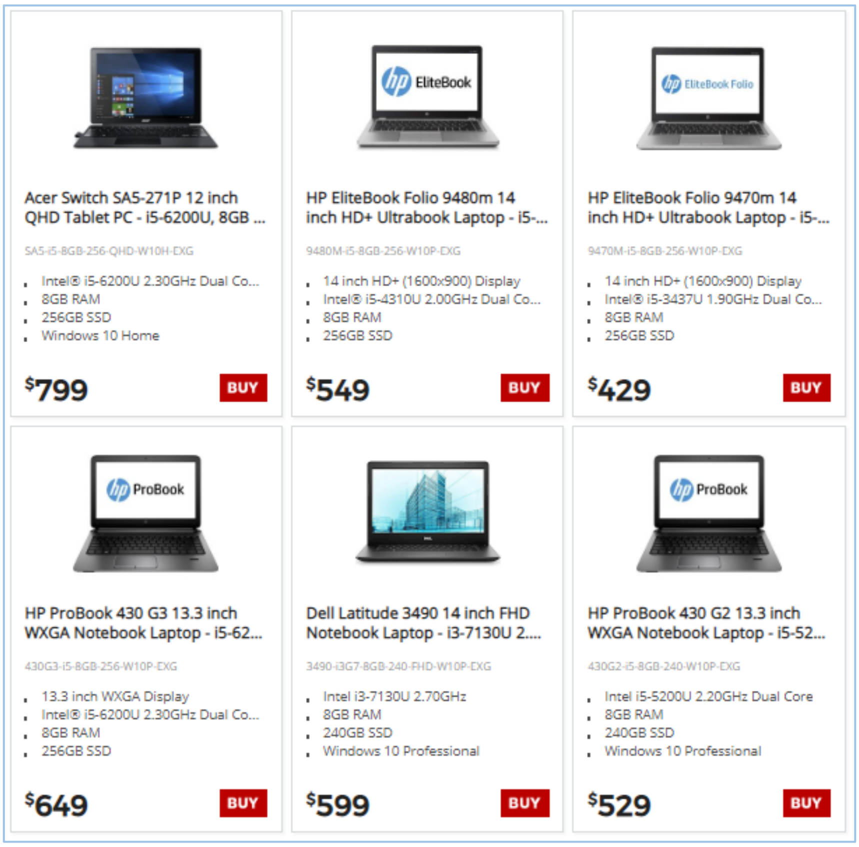
- CLO 1: Explain the range of threats to e-commerce security.
- CLO 2: Explain how cryptography can be, and is, used to achieve security.
- CLO 3: Describe the different standards in use for secure electronic commerce, such as certificates, MACs, etc.
- CLO 4: Describe and analyse standard security mechanisms.
- CLO 5: Analyse e-commerce systems currently in operation, such as electronic payment systems.
- CLO 6: Describe the different protocols in use for secure electronic commerce, such as SSL / TLS.

5. Assessment details

Please ensure that you have read **Section 1** to **3** of this document before going further. Assessment details (i.e. question Q1 to Q5) are provided in the **next page**.

Q1. Secure Payment Method Integration (Marks 16)

Assume that Alice has an E-Commerce Website where she sells different computer accessories. Initial HTML and PHP pages of Alice's E-Commerce Website are provided in the CANVAS. Please refer to the following **Figure-1.1** as an example of the **Product List** page of Alice's E-Commerce Website.



Acer Switch SA5-271P 12 inch QHD Tablet PC - i5-6200U, 8GB ...

SA5-i5-8GB-256-QHD-W10H-EXG

- Intel® i5-6200U 2.30GHz Dual Co...
- 8GB RAM
- 256GB SSD
- Windows 10 Home

$799 BUY

HP EliteBook Folio 9480m 14 inch HD+ Ultrabook Laptop - i5-...

9480M-i5-8GB-256-W10P-EXG

- 14 inch HD+ (1600x900) Display
- Intel® i5-4310U 2.00GHz Dual Co...
- 8GB RAM
- 256GB SSD

$549 BUY

HP EliteBook Folio 9470m 14 inch HD+ Ultrabook Laptop - i5-...

9470M-i5-8GB-256-W10P-EXG

- 14 inch HD+ (1600x900) Display
- Intel® i5-3437U 1.90GHz Dual Co...
- 8GB RAM
- 256GB SSD

$429 BUY

HP ProBook 430 G3 13.3 inch WXGA Notebook Laptop - i5-62...

430G3-i5-8GB-256-W10P-EXG

- 13.3 inch WXGA Display
- Intel® i5-6200U 2.30GHz Dual Co...
- 8GB RAM
- 256GB SSD

$649 BUY

Dell Latitude 3490 14 inch FHD Notebook Laptop - i3-7130U 2....

3490-i3G7-8GB-240-FHD-W10P-EXG

- Intel i3-7130U 2.70GHz
- 8GB RAM
- 240GB SSD
- Windows 10 Professional

$599 BUY

HP ProBook 430 G2 13.3 inch WXGA Notebook Laptop - i5-52...

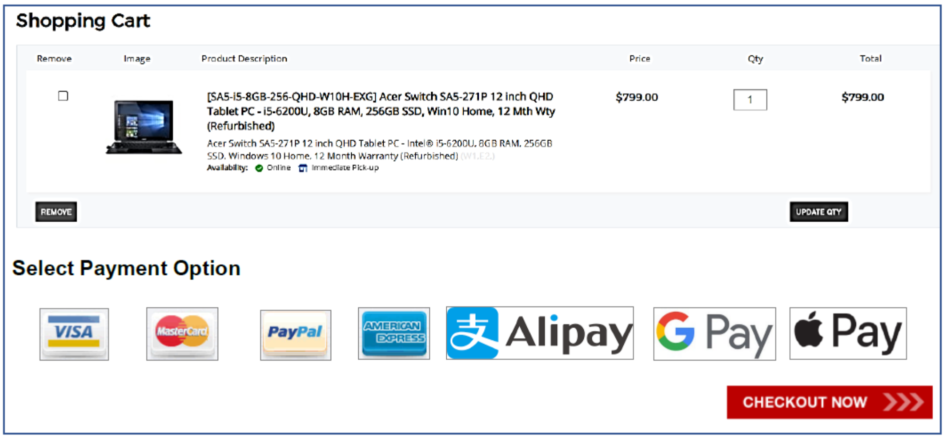
430G2-i5-8GB-240-W10P-EXG

- Intel i5-5200U 2.20GHz Dual Core
- 8GB RAM
- 240GB SSD
- Windows 10 Professional

$529 BUY

Figure-1.1: Product List Page of Alice's E-Commerce Website

When a customer clicks the "**BUY**" button of an item, the customer is forwarded to the following **Shopping Cart** page (**see Figure-1.2**) showing the selected items. Once the user clicks the "**CHECKOUT NOW**" button, it should go to the **Billing Information** page (**see Figure-1.3**).



Shopping Cart

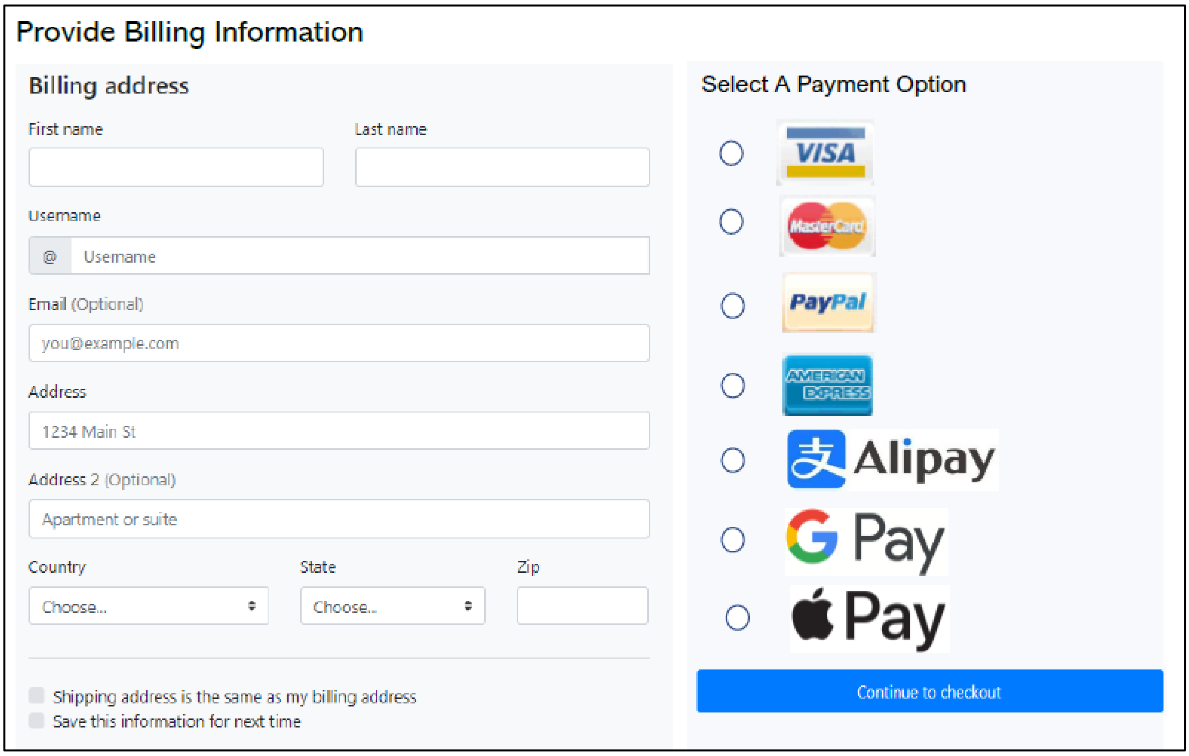
Remove	Image	Product Description	Price	Qty	Total
□		[SA5-i5-8GB-256-QHD-W10H-EXG] Acer Switch SA5-271P 12 inch QHD Tablet PC - i5-6200U, 8GB RAM, 256GB SSD, Win10 Home, 12 Mth Wty (Refurbished) Acer Switch SA5-271P 12 inch QHD Tablet PC - Intel® i5-6200U, 8GB RAM, 256GB SSD, Windows 10 Home, 12 Month Warranty (Refurbished) (W1.E2.) Availability: ✓ Online Immediate Pick-up	$799.00	1	$799.00

REMOVE UPDATE QTY

Select Payment Option

CHECKOUT NOW

Figure-1.2: Shopping Cart Page of Alice's E-Commerce Website



Provide Billing Information

Billing address

First name

Last name

Username

@ Username

Email (Optional)

you@example.com

Address

1234 Main St

Address 2 (Optional)

Apartment or suite

Country

Choose...

State

Choose...

Zip

□ Shipping address is the same as my billing address

□ Save this information for next time

Select A Payment Option

○ VISA

○ MasterCard

○ PayPal

○ AMERICAN EXPRESS

○ Alipay

○ G Pay

○ Pay

Continue to checkout

Figure-1.3: Shopping Cart Payment Page of Alice's E-Commerce Website

In order to increase sales of her E-Commerce Website, she wants to include different types of payment options such as PayPal, MasterCard, Visa, AmEx, Google Pay, Apple Pay, Alipay, etc. Please refer to the tutorials on integrating **PayPal** and **Google Pay** integrations as examples.

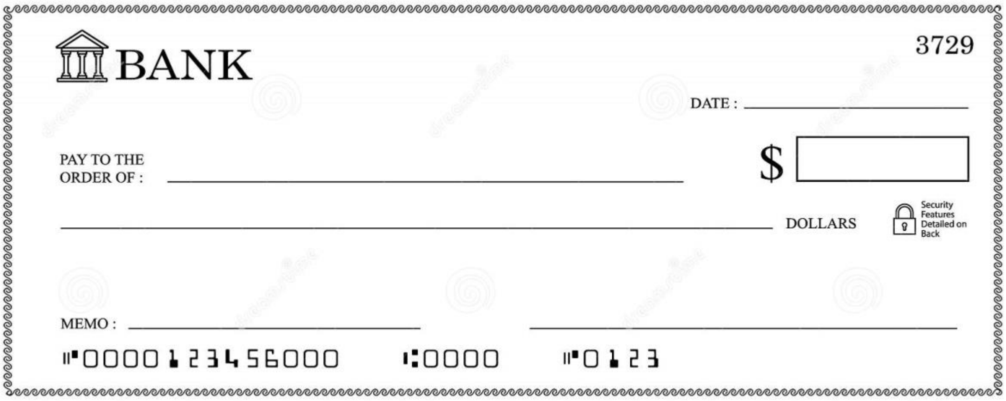
In this task, you need to integrate **at least four different payment options** as stated above in the given e-commerce application. To fulfil the requirements of this task you need to perform the followings:

(a) Upload the final files (e.g., HTML, PHP, and JavaScript files) as attachment in the CANVAS along with your assignment submission.

(b) In the assignment solution, provide step-by-step guidelines of integrating the selected four payment options with appropriate codes and screenshot of your output pages. Please note that you **do not** need to provide any video of the demonstration.

Q2. Multi-Signature (Marks: 6)

Imagine Alice, Bob, and Karen share a business. They have decided that whenever they purchase something for the business everyone must approve the transaction. They have made that known to their bank AusBank. The bank is aware that a check will have signatures of all for it to be valid. A typical blank check is shown below (see **Figure-2.1**).



BANK

3729

DATE : ____________________

PAY TO THE ORDER OF : ______________________________ $ ☐

______________________________ DOLLARS

Security Features Detailed on Back

MEMO : ____________________ ____________________

⑈0000123456000 ⑆0000 ⑈0123

Figure-2.1: A typical blank check

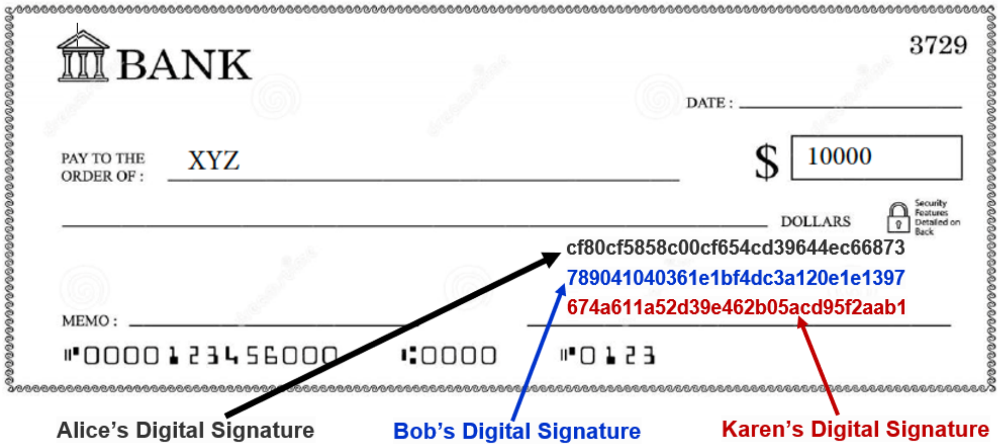

BANK
3729
DATE :
PAY TO THE ORDER OF :
XYZ
$
10000
DOLLARS
Security Features Detailed on Back
cf80cf5858c00cf654cd39644ec66873
789041040361e1bf4dc3a120e1e1397
674a611a52d39e462b05acd95f2aab1
MEMO :
⑈000123456000 ⑆0000 ⑈0123
Alice's Digital Signature
Bob's Digital Signature
Karen's Digital Signature

Figure-2.2: The bank check with payee name and amount containing digital signatures of payers: Alice, Bob, and Karen

(a) **Scenario-1:** Assume that Alice, Bob, and Karen want to issue a bank check of **$10,000** in favour of **XYZ** company. To make it clear, **XYZ** is the payee, the payable amount is **$10,000**, and Alice, Bob, and Karen are the payers of the check. The name of payee and the amount are printed on the check as shown in **Figure-2.2**. The check must be signed by each payer. Each payer has a public and private key pair that is generated using a Public-Key cryptosystem. Each payer will sign the message "**10000**" with their respective private key and generate a digital signature for the message. Bank knows the public keys of each payer. You are required to perform the following tasks:

i. For each payer, show detail computations of each step for generating digital signatures for the above message (M = 10000) using suitable key parameters (i.e., you are allowed to choose the required parameters by your own).

ii. Assume three digital signatures will be embedded somewhere on the blank space of the check as shown in **Figure-2.2**. Show how the bank will verify the signatures before deciding to accept/reject the digital check. Detail computations must be shown.

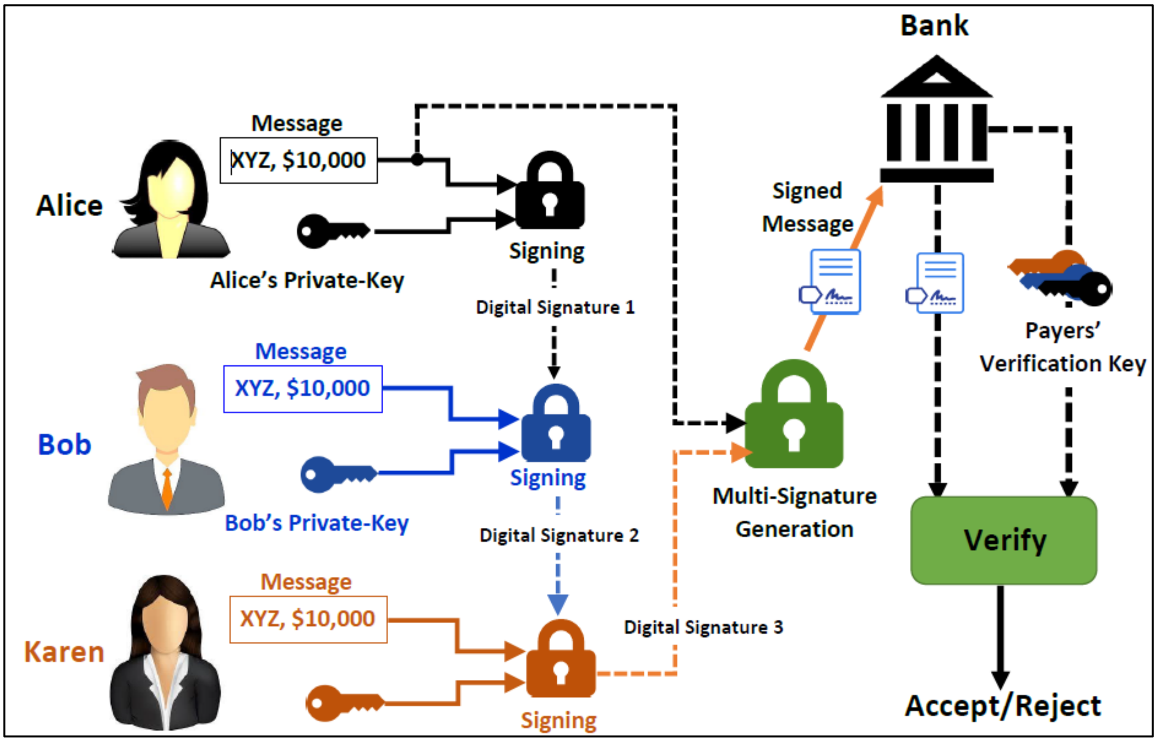


Figure-2.3: Signing and verification of payment message using Multi-Signature

(b) **Scenario-2:** With the situation mentioned in **Scenario-1** (see **Q2(a)**), Bank is worried that they have to verify three signatures separately every time a check comes from payers (i.e., Alice, Bob, and Charlie). In order to reduce computational burden, Bank wants to verify just one signature. Payers are also eager to combine three signatures into one. How can this be accomplished with multi-signature? An architecture of the multi-signature can be like the one as shown in **Figure-2.3**.

(c) You are required to **implement the multi-signature scenario** shown in **Figure-2.4** for the above message using suitable key parameters. You can use any programming language (e.g., PHP, JavaScript, etc.) for the implementation. Please note that the signature values shown in **Figure-2.4** are given just for illustration purpose. The multi-signature should be embedded somewhere on the blank space of the check as shown in **Figure-2.5**.

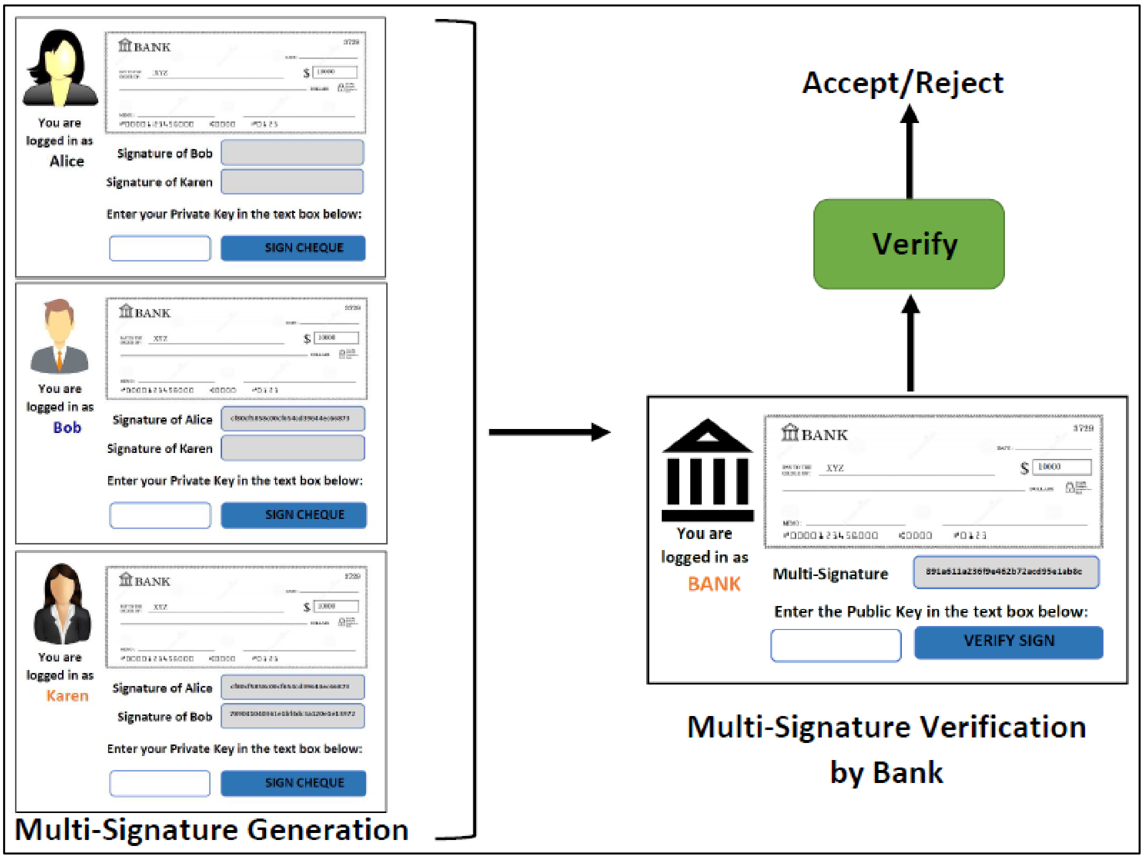

You are logged in as Alice
Signature of Bob
Signature of Karen
Enter your Private Key in the text box below:
SIGN CHEQUE
You are logged in as Bob
Signature of Alice
Signature of Karen
Enter your Private Key in the text box below:
SIGN CHEQUE
You are logged in as Karen
Signature of Alice
Signature of Bob
Enter your Private Key in the text box below:
SIGN CHEQUE
Multi-Signature Generation
Accept/Reject
Verify
You are logged in as BANK
Multi-Signature
Enter the Public Key in the text box below:
VERIFY SIGN
Multi-Signature Verification by Bank

Figure-2.4: Illustration of user interfaces signing and verification of payment message using Multi-Signature

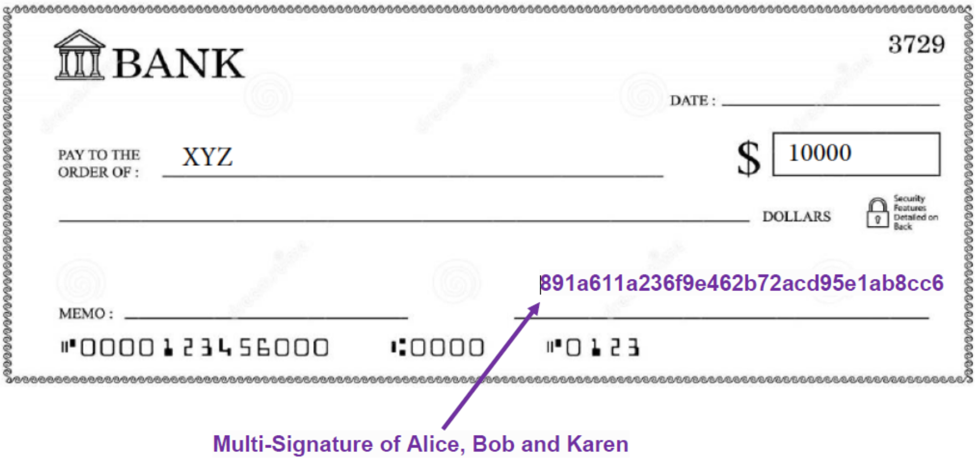

BANK
3729
DATE :
PAY TO THE ORDER OF :
XYZ
$ 10000
DOLLARS
Security Features Detailed on Back
891a611a236f9e462b72acd95e1ab8cc6
MEMO :
⑈0000123456000 ⑆0000 ⑈0123
Multi-Signature of Alice, Bob and Karen

Figure-2.5: The bank check with payee name and amount containing Multi-Signatures of payers: Alice, Bob, and Karen

Q3. Designing Reliable E-Commerce Systems (Marks 5)

An E-commerce company is setting up online business. They are expecting lots of clients to visit their website at the same time for purchasing items online. The company understands that the "n-tier architecture" is an industry-proven software architecture model. The architecture model is suitable to support enterprise level client-server applications by providing solutions to scalability, security, fault tolerance, reusability, and maintainability. It helps developers to create flexible and reusable applications.

Based on the above understanding, the company has decided to build a **3-tier** robust E-commerce site as shown in **Figure-3** to handle large number of e-transactions. The first tier, called *web-server cluster,* consists of a number of *web-servers* as application front-end. The second tier is known as *application-server cluster* and the third tier is named as *database-server cluster*. Similar to the first tier, both second and third tiers have a number of servers. Having multiple servers in every tier, offers higher reliability to the tier itself and to the overall multi-tier E-commerce system.

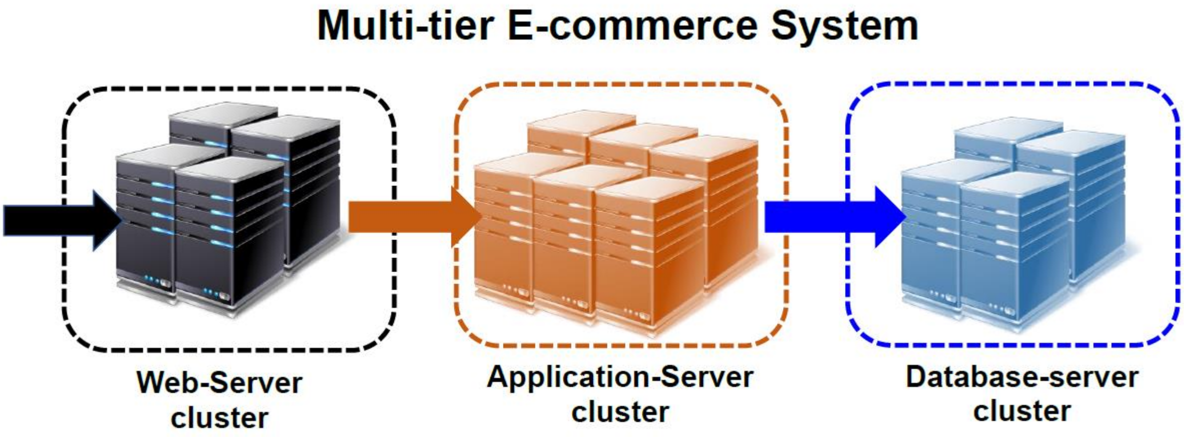


Figure-3: Three-tier E-Commerce System

However, company is running short of cash, and can only afford to buy old computers having only **80% (i.e., 0.8)** reliability. Despite this, the company is determined to build a web-server cluster with **99.999%** reliability, application-server cluster with **99.99%** reliability, and database-server cluster with **99.9%** reliability. Based on the requirement of the company, you need to determine the followings by showing detail computations:

a) How many servers would be required for different clusters?
b) What would be overall reliability of the **3-tier** E-commerce system?

Q4. Secure Identification in E-Commerce Application (Marks 6)

Assume a real-life like scenario where Alice goes to wonderland for shopping and having fun. Usually, she carries a debit card issued by XYZ bank and withdraws cash from ATM to purchase something. There are plenty of XYZ banks and ATM machines in wonderland. One day, while she was in a shopping mall, she realizes that her wallet is no longer in the pocket of her jacket. She has lost not only her ATM card but also all the ID cards. So, going to the bank and showing her ID card to prove her identity is not an option. The only thing she has is her mobile phone which can perform large mod calculation. She is embarrassed and disappointed.

She then remembers the advice given by the bank when she is in a difficult situation like this. The bank advised her to go to any branch office of XYZ and prove to them that she knows a secret without revealing the secret. They explained her the protocol. So, Alice goes to a branch office of XYZ and talks to branch officer Bob to prove that she knows a secret without revealing it.

How can the bank facilitate this with help of zero-knowledge-proof (ZKP) protocol? Assume bank is the trusted third party (TTP) deploying **Guillou-Quisquater (GQ) Identification or Schnorr Identification** method as the zero-knowledge-proof (ZKP) protocol, Alice is the prover and Bob is the verifier. Show all the steps in details and sequence diagram to illustrate how Alice convinces Bob. Also, show what the bank must prepare in advance to facilitate this.

Q5. Digital Cash (Marks 17)

In 1989 DAVID CHAUM started *DigiCash* to create an on-line digital currency as a secure and private payment method, as cash in the physical world. The *DigiCash* offered the following properties:

- *Inability of third parties to determine payee*: Without this a transaction can reveal an individual's whereabouts and lifestyle (e.g. payments made for movies, food, medicines, books etc.).
- *Ability of individuals to provide proof of payment*: Bank notes/coins suffer from problems like lack of proof of payment, black payments for bribes etc.

Everyone was excited about the prospect. Others started *Cybercash* and *Cybercoin*. Unfortunately, DigiCash soon died, and other digital currencies did not survive either.

Today, we have Cryptocurrencies, like *Bitcoin*, *LiteCoin*, *Ethereum* etc., which are a variant of old-style digital currencies. They are based on the Blockchain and a decentralized ledger where no single authority controls the actions.

Write **a report** with an in-depth analysis about the differences and similarities between the *digital currencies* and *cryptocurrencies* while emphasizing the followings (but not limited to):

- What are the prime reasons behind the failure of DigiCash and other digital currencies? Were there any technical or strategic flaws?
- Today, if you have to start the DigiCash and you have the support of venture firms, how would you do things differently from both technical and strategic perspectives to make it successful (e.g. mass adoption)?
- If you re-design DigiCash, what are the new features you would add to DigiCash? Why would you add those features? What benefits would that bring?
- Among the new Cryptocurrencies are there many similar to old style digital currencies? Identify a few of the new Cryptocurrencies and explain the similarities.
- Initially it seemed the new Cryptocurrencies would be adopted by many businesses. However, it did not quite go that way. What are the reasons? Why have they not been widely adopted?

As an alternative to the report writing, you can implement (with required user interfaces) a simple cryptocurrency-based payment system that can be used to buy and sell products in an E-Commerce Application. You can extend the Java-based crypto wallet example shown in Tutorial. You can implement the cryptocurrency-based payment system in any programming language.

6. Academic integrity and plagiarism (standard warning)

Academic integrity is about honest presentation of your academic work. It means acknowledging the work of others while developing your own insights, knowledge, and ideas. You should take extreme care that you have:

- Acknowledged words, data, diagrams, models, frameworks and/or ideas of others you have quoted (i.e. directly copied), summarized, paraphrased, discussed, or mentioned in your assessment through the appropriate referencing methods,
- Provided a reference list of the publication details so your reader can locate the source if necessary. This includes material taken from Internet sites.

If you do not acknowledge the sources of your material, you may be accused of plagiarism because you have passed off the work and ideas of another person without appropriate referencing, as if they were your own.

RMIT University treats plagiarism as a very serious offence constituting misconduct. Plagiarism covers a variety of inappropriate behaviors, including:

- Failure to properly document a source
- Copyright material from the internet or databases
- Collusion between students

For further information on our policies and procedures, please refer to the University website.

7. Assessment declaration

When you submit work electronically, you agree to the assessment declaration.

4. Rubric/assessment criteria for marking

All of the computations must be correct and only provided values must be used. Instructions must be followed.

<table>
<tr><th><b>Criteria</b>
The characteristic or outcome that is being judged.</th><th colspan="7"></th><th><b>Total</b></th></tr>
<tr><td><b>Question 1</b>
Secure Payment Method Integration</td><td>The integration of 4 different payment methods are shown step-by-step in the solution with necessary codes.
All of the payment methods are working correctly.
<b>16 Marks</b></td><td colspan="2">The integration of 3 different payment methods are shown step-by-step in the solution with necessary codes.
3 payment methods are working correctly.
<b>12 Marks</b></td><td colspan="2">The integration of 2 different payment methods are shown step-by-step in the solution with necessary codes.
2 payment methods are working correctly.
<b>8 Marks</b></td><td>The integration of 1 payment method is shown step-by-step in the solution with necessary codes.
1 payment method is working correctly.
.
<b>4 Marks</b></td><td>Not answered
<b>0 Marks</b></td><td><b>16 Marks</b></td></tr>
<tr><td><b>Question 2</b>
Multi-Signature</td><td colspan="2">Both Q2(a) and Q2(b) are answered correctly with detail computations.
<b>6 Marks</b></td><td colspan="2">Any 1 of the followings is satisfied:
1) Only 1 among Q2(a) and Q2(b) is answered correctly with detail computations.
<b>OR</b>
2) Both Q2(a) and Q2(b) are partially correct and detail computations are shown.
<b>OR</b>
3) Both Q2(a) and Q2(b) are correct, but detail computations are NOT shown.
<b>3 Marks</b></td><td colspan="2">Both Q2(a) and Q2(b) are attempted, but answers are not correct, and requirements are not fulfilled.
<b>1 Marks</b></td><td>Not answered
<b>0 Marks</b></td><td><b>6 Marks</b></td></tr>
</table>

Question 3 Designing Reliable E-Commerce Systems	Both Q3(a) and Q3(b) are answered correctly and explanations are excellent. **5 Marks**	Both Q3(a) and Q3(b) are answered correctly and explanations are satisfactory but not excellent. **4 Marks**	Any 1 of the followings is satisfied: 1) Only 1 among Q3(a) and Q3(b) is answered correctly and explanation is excellent. **OR** 2) Both Q3(a) and Q3(b) are partially correct and explanations are moderate. **OR** 3) Both Q3(a) and Q3(b) are answered correctly and explanations are not satisfactory. **2 Marks**	Both Q3(a) and Q3(b) are attempted. But, answered are not correct or explanations are not satisfactory. . **1 Marks**	Not answered **0 Marks**	**5 Marks**
Question 4 Secure Identification in E-Commerce Application	Answered correctly with detail step-by-step process. Explanations are excellent. Diagrams are provided for clear illustrations. **6 Marks**	Answer is partially correct, and detail step-by-step process is shown. Explanations are satisfactory. **4 Marks**	Answer is correct but detail step-by-step process is NOT shown. Explanations are not satisfactory. **2 Marks**	Answer is partially correct, and detail step-by-step process is shown. Explanations are not satisfactory. **1 Marks**	Not answered **0 Marks**	**6 Marks**

Question 5 Digital Cash	The report is extraordinary The report is prepared fulfilling all of the requirements **17 Marks**	The report is good but not up to the mark. The report is prepared fulfilling all of the requirements. However, could have been better. **14 Marks**	The report is average. The report is prepared fulfilling all of the requirements. However, the content is not enough to express the main theme of the given topic. **10 Marks**	The report is below average. The report is NOT prepared fulfilling all of the requirements. The key topics are not well connected. Presentation is poor. **7 Marks**	The report is poor. The report addresses only few of the requirements. The key topics are missing or not connected. Presentation is poor. **4 Marks**	The report is very poor. None of the requirements are addressed correctly. The key concept is missing. **2 Marks**	Not answered **0 Marks**	**17 Marks**