Business Information Security

Assignment 2 worth 60% of overall course marks

Dr Alex Pudmenzky – 2024 S2

Assignment overview

This assignment must be completed individually by each student. This assignment requires a student to answer 6 questions (each with sub-parts) that focus on the course material covered across all weeks of the course. Assignment 2 is worth 60% of the overall course marks and will be marked as per the rubric in Table 1. A student's answer to each of the 6 questions (that is, each question and all its sub-parts) must not exceed 300 words (+10% tolerance per UQ policy). This word limit per question requires a student to soundly analyse/research each question and then structure a response in a concise, business informative fashion. There is no need to reference an answer unless referencing is specifically requested in the question. A student must construct each answer in her/his own words and in 'plain English' business language. Please note that each question in this assignment may well span work covered across all weeks (and not simply relate to one specific week).

This assignment assumes that a student is capable to assimilate information from not only this course, but also many other courses and reputable sources on the Internet as would be required in a business setting. Students are advised that the use of AI technologies to develop responses is strictly prohibited and may constitute student misconduct under the student code of conduct. Each assessment question evaluates students' abilities, skills and knowledge without the aid of AI.

Submission and formatting instructions

- Create and upload a single PDF document containing all answers to Turnitin on Blackboard.
- Use the file naming convention described in the submission link when it becomes available closer to the submission deadline (you may receive a deduction for incorrectly named files).
- Please ensure your student details (name & student number) are contained on each page of the submission in a suitably designed footer.
- Clearly label which question and if relevant sub-question you answer (e.g., Question 6a). You don't have to repeat the question.
- Answer in full sentences but you may want to use bullet points, numbering, or headers to help structuring your answer.
- Read each question carefully for additional formatting requirements specific to the question.

Table 1 - Marking rubric for Assignment 1.

Criteria	High distinction (10)	Distinction (8)	Credit (6)	Pass (5)	Marginal fail (4)	Fail (2)	Low fail (0)
Question 1 (10 marks)	You will receive the full mark assigned to the individual part-questions for the correct answer or zero for an incorrect or only partially correct answer for each part-question, i.e. no part-marks will be assigned for each part-question.						
Question 2 (10 marks)	a,b) Correct number shown and all steps leading to it correctly documented.	a,b) Each correctly documented step leading towards the answer will receive part marks. c,d) No part marks, i.e. only 0 or 1 mark.					a,b) No attempt or wrong number or no step documentation.
Question 3 (10 marks)	No part marks for sub-questions a,b,c,etc., i.e. only the mark indicated if the answer addresses the question correctly in its entirety or zero.						
Question 4 (10 marks)	Half-marks can be given to sub-questions a,b & f only. Sub-questions c,d & e can only receive 0 or 1 mark.						
Question 5 (10 marks)	For sub-question a, you earn 0.35 marks for each correct row out of a possible 17 rows. The total marks are then rounded up to the next integer. Sub-questions b & c can only receive integer marks.						
Question 6 (10 marks)	Each of the four sub-questions a,b,c & d can be awarded up to 2.5 marks, with the smallest increment being 0.5 marks, but only if a valid CVE has been specified.						No valid CVE specified.

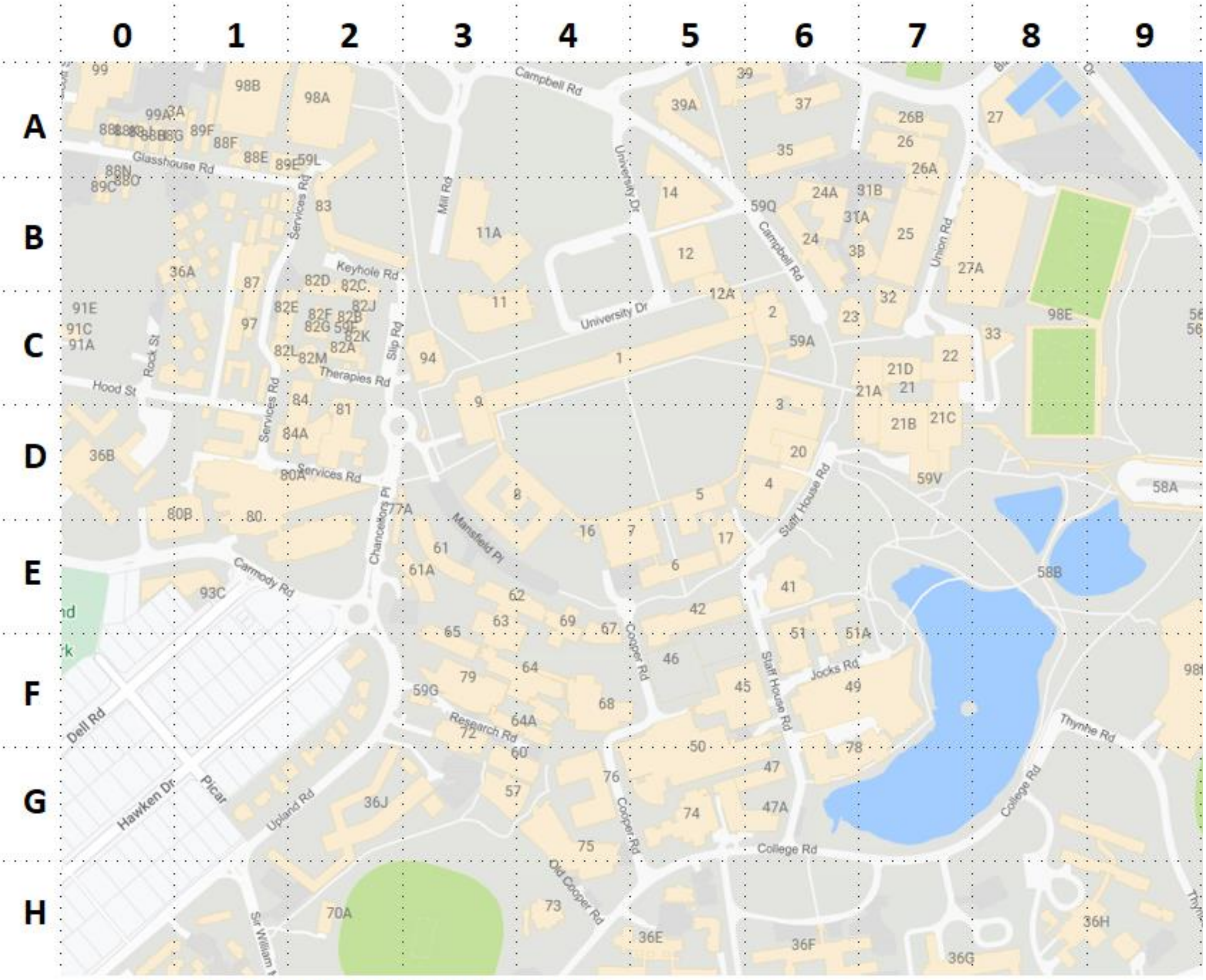
Question 1

a) You have found a treasure map at the Pizza Café (see Figure 1) containing an encrypted message that describes the coordinates of where a treasure is hidden on campus. Break the code using cryptanalysis and draw either a red **X** in the square where you think the treasure is or, alternatively, just note down the coordinates as In **[letter;number]** but that is less fun.

b) What is the name of the **cipher** used?

c) What is the **KEY**?

The encrypted message is:
Tsi qsmseuci zbv tq fzyke il fhp jlmtgiiyk zpwjpiyeqfa:
s9r51566bo6705j7bb6iv54nb9oiy449g795582l6529s0q22207b8981233pg58 ;
jpl(qauc_wqvlwzt_yyjcmj,10).



Tsi qsmseuci zbv tq fzyke il fhp jlmtgiiyk zpwjpiyeqfa:
s9r51566bo6705j7bb6iv54nb9oiy449g795582l6529s0q22207b8981233pg58 ; jpl(qauc_wqvlwzt_yyjcmj,10).

Figure 1 - Treasure Map with encrypted message.

(2%)

d) You have forgotten your login password but your friendly database administrator in your company has provided you with the hash of your password from the database which is:

694430bed946b0330e4d15e9bc3931123c122166da6d353bad32d4c09da3788c

What is your password?

e) What improvement suggestion do you have regarding database password storage in your company?

(2%)

f) Answer the following question:

```
57 68 61 74 20 69 73 20 69 74 20 63 61 6C 6C 65 64 20 77 68
65 6E 20 32 20 73 74 72 69 6E 67 73 20 68 61 76 65 20 74 68
65 20 73 61 6D 65 20 68 61 73 68 20 64 69 67 65 73 74 3F
```

(2%)

g) What is the image located here https://alexpudmenzky.com/BISM3205/number.gif displaying?

(1%)

h) Download the following zip file containing two images https://alexpudmenzky.com/BISM3205/shipPlane.zip. What do you notice when calculating the MD5 hash of each image (include the calculated MD5 hash in your answer)?

i) What does it tell you about MD5?

(2%)

j) Here is my encrypted message encrypted with my public key also supplied below. What does the message say?

```
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAucU+u7phfIspqebNE+LR0pZYb0Waa
NaX5WNTamO41MdSExiSuG7vTVIb+P4Vw0+BE+ElYFE7oYxyr+BPmsnNA986D3+RwrrELkfohL
UDkhETGzE7hwl4FHTgQ0o3RLDFsjjAqiqoQVQpItWAo4JYWi09C0MvfaclZLll3wL20FnZc867Tnd
Mhr11qw68HB9daW0BLkZk/loJy0FFjl1nU/ujBhVPkOvCCrZOLT0ZUXZnIST4kV5bVJ5kniIEOAmZ
VMo893gDAXTkrCJrPwYGheTSNwzbyXtbuSvPV/C+YBhBTV2sdTA0WTYckFE6FYxLzjt9OMehIy
MeXWFmT/TLKQIDAQAB
-----END PUBLIC KEY-----
```

BASE64 encrypted message using my public key above:

```
iE0E5eO/QYgiTuYiiHlTv60nxr1Q6gKV2LjVWca4Qbp4uw98qjpdxJV+trQO+ZRG2WZBGDQg/kR
MVShVy/AEaG4TGK9SZL1elbmLrVn0+AXCAwJaPovYhV7c62eg67XKO/Fk+ThQc/0PnullJgu7AL
OXr3aULuvIVGUm5u030fi2vwrjaCFfQl4QtxlfhFSP1/p0ftDsJPuj3NNx7ylIuAkTmcSc8fZ3/12xyz1
a72y+ASG3OTLwNACci/mZcr2gq7p/LkNFeHAYmUMh+ty5cijH9m+hgNWfw3TL0p2GMhLjNsD
MdjTonqBKZhFLsnCRj2z+ggBF88ay4L/XVlMjzA==
```

(1%)

Question 2

Your friend works at the Australian Security Intelligence Organisation (ASIO) and has found out you are completing a cyber security course at The University of Queensland. She wants to test your abilities and sends you an email reading "Follow the trail of hints given in the hidden message to arrive at a **single two-digit integer, greater than 0, in decimal notation**" followed by the text below.

lxxtw://epibtyhqirdoc.gsq/FMWQ3205/UVgshi.dmt

a) What is the two-digit integer number in decimal notation that is greater than 0?
b) Explain the steps you took to get to your result.

(8%)

c) How does the segmentation of IP addresses, which contain identifiers for both the computer and the network it belongs to, facilitate data routing across networks by identifying the specific location of the target computer? Provide an example of this segmentation by determining the host and network portion of the IP address 192.168.5.2, given a subnet mask of 255.255.128.0?

(1%)

d) You know that the following is either an encrypted message or a salted and hashed password, which one is it and why?

1mnsBzaua8EPXaZXuY29id45V0HaqRw1XLkSx5aVS5bEKi0Gco8V8VIqOY9P6Ekxo1UafNX9klsQMyMZU
EWdsVV5mVaRVEq74RJxxRb6FpnaCeSkqnNcTuA9bVk8sMN

(1%)

Question 3

a) In Kerberos, what are the main similarities between a client's request for a **Ticket-Granting Ticket (TGT)** and a **Service Ticket** from the KDC, and how do the credentials involved in each process differ?

(2%)

b) Both the **Ticket-Granting Ticket (TGT)** and the **Service Ticket** are encrypted in a way that prevents the client from reading them, but the client can still use them to access services. Why can't the client decrypt these tickets, and how do they still use them for authentication?

(2%)

c) In a Kerberos environment, if an attacker retrieves a user's **Ticket-Granting Ticket (TGT)** from a compromised workstation, can the attacker authenticate to services on the network? Why or why not?

(1%)

d) You work at your dream company, you go to have lunch and find a USB stick in the cafeteria, what do you do and why?

1. Plug the USB stick into your computer to check for any files.
2. Leave the USB stick where you found it.
3. Hand the USB stick to your IT department or security team.
4. Take the USB stick home to investigate it further.
5. Throw the USB stick in the trash to dispose of it.

(1%)

e) An Intrusion Detection System (IDS) raises alarms when it detects suspicious activity or policy violations, how does a false positive alarm differ from a false negative one? From a security perspective, which is least desirable?

(1%)

f) What would an attacker input into an authentication form asking for a username and a password, if they wanted to perform an SQL injection attack that would allow them to log in using the username *admin* without specifying the correct password?
Explain how each of the tokens they have to enter contributes to success using the full back-end SQL statement that is executed as an example. Which layer of the OSI model is this attack targeting?

(2%)

g) Can I access the "deep web" using a normal browser like Chrome or Firefox, or do I need the Tor browser? Why or why not, explain in a few sentences?

(1%)

Question 4

a) Secure/Multipurpose Internet Mail Extensions (S/MIME) provides a secure and reliable way to send and receive emails over the internet, protecting against eavesdropping, tampering, and impersonation.

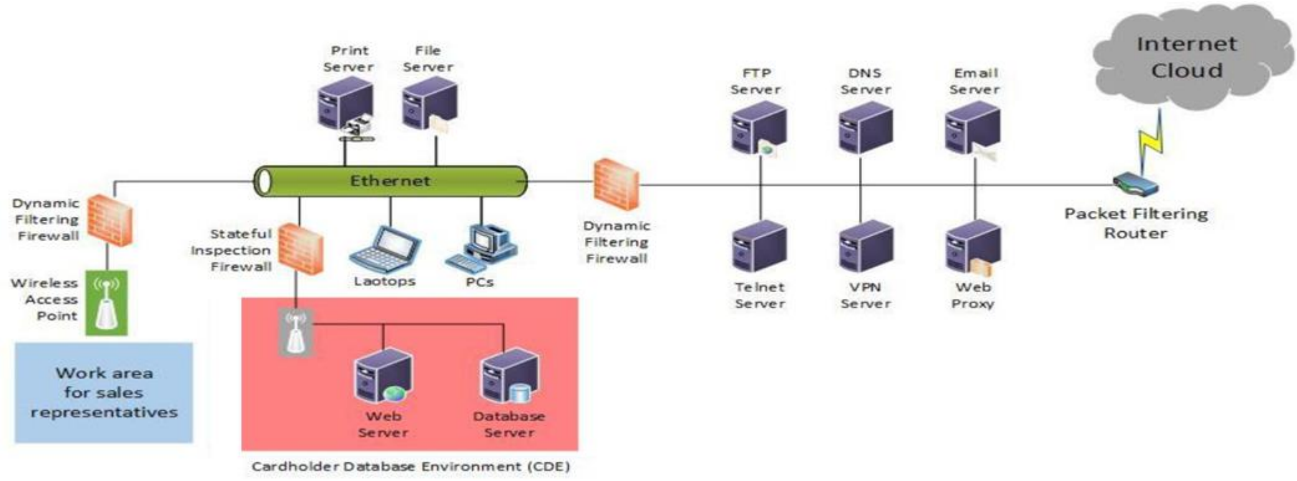
Here's a breakdown of the steps how S/MIME works to secure email communication:

1. Compose email text and attachments.
2. Create a symmetric session key and encrypt the email text and attachments with this key. This ensures that only the intended recipient(s) can read the email content.
3. Encrypt the session key with the recipient's public key and add this to the email using asymmetric encryption. This ensures that only the intended recipient(s) can decrypt the symmetric session key and read the email content.
4. Hash the total email (text, attachments, and encrypted session key). Encrypt the resulting digest with the sender's private key. Add this encrypted hash to the email package as a digital signature. Send the lot to the recipient.

What keys/certificates are needed A) at the sender's end, and B) at the receiver's end. Explain what each is used for.

(3%)

b) What major change would you make to the network design shown in this image to improve network security?



(2%)

c) Can Kerberos be used in web-based e-commerce solutions on the Internet? Explain your answer.

(1%)

d) Both S/MIME and TLS use a combination of public key and symmetric key encryption to ensure security. At which layer of the communication stack do these protocols operate?

(1%)

e) Quantum computers are not yet capable of breaking modern symmetric encryption algorithms like AES. Why are companies like Signal, Apple, Google, and Zoom already implementing quantum-resistant encryption algorithms today, even before quantum computers become a practical threat? Justify your answer.

(1%)

f) What are the primary objectives of conducting a security audit in an organization? In your answer, briefly explain how security auditing contributes to identifying vulnerabilities and improving overall security posture.

(2%)

Question 5

a) The diagram in shows a typical network configuration of an office connected to the Internet. Areas are labeled with numbers 1-4 and network devices are labeled with letters A-M. In the list below, assign the correct number and letter to each area and device. Numbers and letters must only appear once (insert any missing device name). It does not matter where a device is located in a work area. **(6%)**

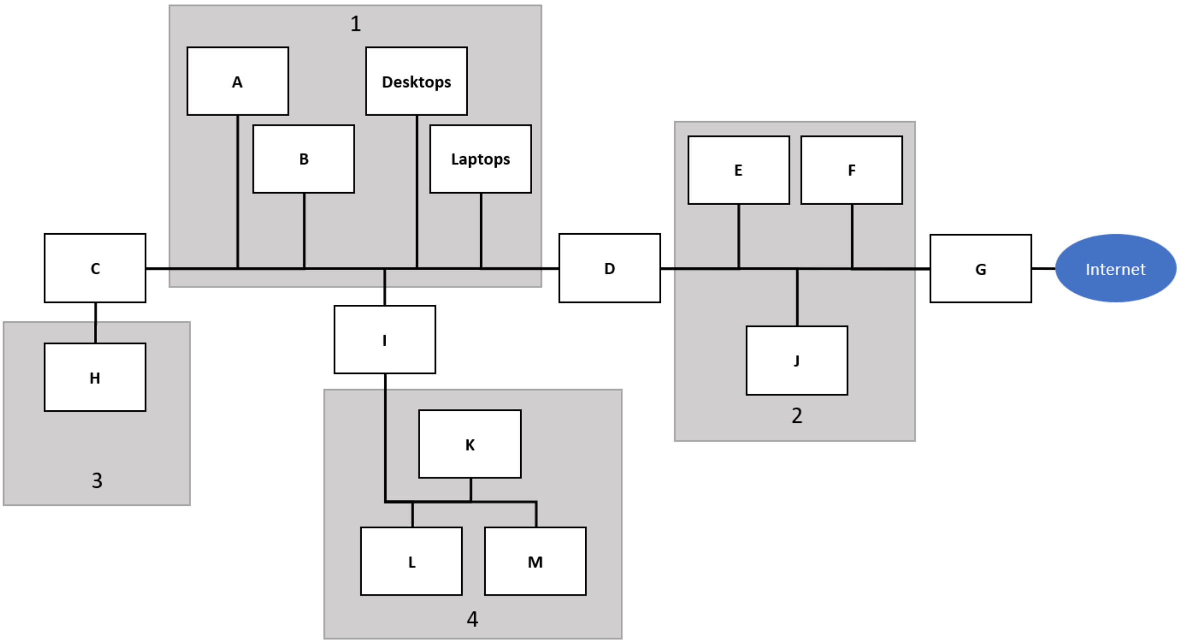


Figure 2 - Typical office network diagram.

Work areas:

Number (1-4)	Area name
	DMZ
	General Staff
	Cardholder Environment
	Sales Hot Desks

Devices:

Letter (A-M)	Device name
	File Server
	Stateful Inspection Firewall
	Wireless Access Point
	Email Server
	Web Proxy
	NIDS
	Database Server
	VPN Server
	Border Router
	Print Server
	Dynamic Filtering Firewall
	Web Server

b) Explain the similarity between creating a vanity onion address and finding the golden nonce in blockchain mining. In your answer, briefly describe what each process entails.

(2%)

c) In Bitcoin’s Proof of Work (PoW) mining process, what is the role of the "Golden Nonce", and how does it relate to the target difficulty?

(2%)

Question 6

Imagine you are a malicious hacker targeting a medium-sized business. Your goal is to compromise their computer system and gain unauthorized access.

a) Vulnerability: Using the NIST National Vulnerability Database (NVD), find a vulnerability in a system commonly used by businesses. State the ID (e.g. CVE-yyyy-xxxxx) and describe the vulnerability.
b) Exploitation: Describe how you would exploit this vulnerability to compromise the target system, including the initial access vector and explain how the vulnerability is used.
c) Impact: Outline the potential impact on the business.
d) Countermeasure: Propose a simple but effective countermeasure to defend against the attack.

(10%)