Table Content

Question 1

Jan 2025

Question 1

a) Symmetric encryption typically involves two main processes for transforming plaintext to ciphertext, which are Substitution and Transposition. Describe each type of process and provide **ONE (1)** example of ciphertext, using the following sentence as plaintext:

HAPPY GRADUATION DAY! (6 marks)

Chp 2

b) The Feistel cipher is a symmetric structure commonly used in the construction of block ciphers. Describe **THREE (3)** approaches to enhance the security of a Feistel cipher. (9 marks)

Chp 2

c) The Advanced Encryption Standard (AES) does not utilise the Feistel structure, which typically divides the input data into two halves and processes them in a series of rounds. Briefly explain the **FOUR (4)** stages involved in the AES encryption process. (8 marks)

Chp 2

d) Compare and contrast the Brute Force Attack and the Dictionary Attack as strategies used by cryptanalysts to discover the plaintext or key. (2 marks)

[Total: 25 marks]

Chp 2

Oct 2024

Question 1

a) Provide a diagram of symmetric block encryption of Data Encryption Standard with labels. (18 marks)

Chp 2

b) Provide **FIVE (5)** common components in symmetric encryption and asymmetric encryption. (5 marks)

Chp 2

c) What are the two main operations in the Feistel network structure? (2 marks)

[Total: 25 marks]

Chp 2

May 2024

Question 1

a) Based on *Figure 1*, answer the **Question 1 a) (i), (ii) and (iii).**

Issued By	
Common Name (CN)	DigiCert Global G2 TLS RSA SHA256 2020 CA1
Organisation (O)	DigiCert Inc
Organisational Unit (OU)	<Not Part of Certificate>

Figure 1: Snippet of a HTTPS (Hypertext Transfer Protocol Secure) certificate

(i) Identify the cryptographic function that uses Message Authentication Code (MAC) when establishing a secure communication. (1 mark)

Chp 3

(ii) Explain the usage of the selected cryptographic function in maintaining security in a HTTPS connection. (6 marks)

Chp

(iii) Besides HTTPS, describe **TWO (2)** areas that the selected cryptographic function can be applied to. (4 marks)

b) Differentiate the approaches in using brute force and dictionary attacks in a symmetric encryption cryptanalysis. (6 marks)

Chp 2

c) Describe the difference between Feistal Cipher and AES (Advanced Encryption Standard) algorithm in terms of the structure, round functions, key schedule and data processing. (8 marks)

[Total: 25 marks]

Chp 2

Question 2

Jan 2025

Question 2

a) Public-key cryptography is a cryptographic system that uses pairs of keys. Briefly explain **THREE (3)** requirements that must be fulfilled for public-key encryption to function properly. (6 marks)

Chp 3

b) Alice and Bob are implementing the Diffie Hellman key exchange protocol to establish a shared secret key over an untrusted network securely. They have agreed upon the prime number $\mathbf{q = 7}$ and the primitive root $\boldsymbol{\alpha = 3}$. Alice's private key is $\mathbf{XA = 2}$ and Bob's private key is $\mathbf{XB = 3}$.

(i) Find the public key **(YA)** for Alice and the public key **(YB)** for Bob, and include the working steps for both calculations. (6 marks)

Chp 3

(ii) Compute the common shared secret key for both Alice **(KA)** and Bob **(KB)**, showing all the steps involved in the calculation for each of them. (4 marks)

Chp 3

c) RSA (Rivest-Shamir-Adleman) is a widely used public key cryptosystem that enables secure data transmission and digital signatures. Interpret the step-by-step process of RSA key generation by including the mathematical calculations or formulas involved at each step. (9 marks)

[Total: 25 marks]

Chp 3

Oct 2024

Question 2

Ben and Ann use Diffie Hellman (DH) Key Exchange to communicate through an untrusted network. Both agree on parameter 'Alpha' and 'q' as values of three and seven respectively. Ben generated a random number of two while Ann generated a random number of four.

a) What is the value of the public key of Ben? Describe the steps of your calculation. (4 marks)

Chp 3

b) What is the value of the public key of Ann? Describe the steps of your calculation. (4 marks)

Chp 3

c) Calculate Ben's final secret key value. Show the steps of your calculation. (4 marks)

Chp 3

d) Calculate Ann's final secret key value. Show the steps of your calculation. (4 marks)

Chp 3

e) Provide **FOUR (4)** requirements based on the above parameters for DH to work. (4 marks)

Chp 3

f) Give **ONE (1)** reason that DH allows keys between Ann and Ben to be securely exchanged. (5 marks)

[Total: 25 marks]

Chp 3

May 2024

Question 2

a) Provide a scenario of HTTP cookie replay attack targets an organisation's network infrastructure. Map the impacts of attacks on the **THREE (3)** security requirements: confidentiality, integrity, and availability. (6 marks)

Not found

b) Using a diagram, interpret the function of Kerberos in ensuring smooth access for a university student transitioning between several network resources without the necessity for multiple authentication attempts. Identify the important components and explain the authentication flow within the Kerberos protocol to enable single sign-on functionality within a university network setting. (10 marks)

Chp 4

c) Using Alice and Bob as example, describe the steps they adopt Diffie-Hellman to exchange keys securely over the untrusted network. You can present the answer in a diagram. (9 marks)

[Total: 25 marks]

Chp 3

Question 3

Jan 2025

Question 3

a) Consider an Automated Teller Machine (ATM) that provides convenience for users who may not have access to smartphones or the Internet to withdraw cash or perform banking transactions. Briefly explain **THREE (3)** security concepts and provide **ONE (1)** example of the requirements associated with the ATM system. (9 marks)

b)

June 5, 2024 – Article

The Real Danger of Cybersecurity to Malaysia's Enterprise Landscape
Attributed to Datuk Tan Seng Kit, Group Managing Director, Strateq Group

Cybersecurity threats in Malaysia are on the rise, and businesses must take steps to safeguard against these threats in order to protect their valuable data and assets. As a veteran of the enterprise solutions industry – having spent more than two decades looking at how technology can improve the operational efficiency of companies, I am keenly aware of the perks and the dangers of the global increasing shift towards digital.

One of the most significant cybersecurity threats in Malaysia is a type of attack that overwhelms a website or network with traffic, making it unavailable to legitimate users. This type of attack is often carried out by botnets, which are networks of compromised devices controlled by hackers.

Source:https://strateqgroup.com/home/index.php/2024/06/05/the-real-danger-of-cybersecurity-to-malaysias-enterprise-landscape/

(i) Based on the excerpt from the article above, identify whether the type of cybersecurity attack being discussed is passive or active. Provide an explanation in your answer. (5 marks)

Chp 1

(ii) A successful attack leads to a serious compromise of security. Briefly explain **THREE (3)** categories of active attacks that are difficult to prevent due to the wide variety of potential physical, software, and network vulnerabilities. (9 marks)

Chp 1

c) Identify **ONE (1)** class of intruders whose objective is to gain access to the system or increase the range of privileges. (2 marks)

[Total: 25 marks]

Chp 8

Oct 2024

Question 3

a) Describe **THREE (3)** aspects of public-key encryption are protecting. (8 marks)

Chp

b) Discuss **TWO (2)** aspects of public-key encryption in order to for it to work. (6 marks)

c) What are the **THREE (3)** problems Kerberos solves? (9 marks)

Chp 4

d) "Private keys must be registered with X.509 Certification Authority for Secure/Multipurpose Internet Mail Extension that uses Public-Key Certificates."
Is the above statement true or false? (2 marks)

[Total: 25 marks]

Chp 5

May 2024

Question 3

a) Demonstrate the process by which a client and server establish a secure session using Transport Layer Security (TLS). Provide the steps involved, including the handshake process together with symmetric and asymmetric key exchange mechanisms. (8 marks)

Chp 6

b) Explain the roles of AH (Authentication Header) and ESP (Encapsulating Security Payload) in IP Security (IPsec). (6 marks)

Chp 7

c) Security Association (SA) aims to achieve authentication and confidentiality for IP packets. Describe the **THREE (3)** parameters in a SA between two gateways. (6 marks)

Chp 7

d) Identify the **FIVE (5)** key services in Pretty Good Privacy (PGP). (5 marks)

[Total: 25 marks]

Chp 5, tut 5

Question 4

Jan 2025

Question 4

a) As an IT Manager assigned to educate your organisation about cybersecurity, many employees mistakenly categorise all cybersecurity attacks as viruses. Provide **THREE (3)** different types of viruses to help raise their awareness. (9 marks)

Chp 10

b) The ideal solution to the threat of viruses is prevention. Identify **TWO (2)** elements used by Generic Decryption (GD) as advanced antivirus techniques to detect even the most complex viruses. (4 marks)

Chp 10

c) Tera Tech Sdn. Bhd. intends to implement an Intrusion Detection System (IDS) following a cybersecurity attack incident. Classify **TWO (2)** different approaches used by IDS to help your client choose the most suitable solution to strengthen their security posture. (6 marks)

Chp 6

d) A company wishes to use IP Security (IPSec) to secure its communication over the Internet and ensure the protection of its sensitive data. As a consultant, provide **THREE (3)** applications of IPSec that can enhance the company's network security and help them make informed decisions about implementing this technology. (6 marks)

[Total: 25 marks]

Oct 2024

Question 4

a) Secure Shell provides a protocol for secure network communications that is relatively simple and inexpensive to implement. With the aid of a diagram, describe Secure Shell Transport Layer Protocol packet formation. (18 marks)

b) Based on Open System Interconnection (OSI), what are the **TWO (2)** layers in the OSI model that Stateful Inspection Firewall protects? (2 marks)

c) Describe virus in **FOUR (4)** phases. (5 marks)

[Total: 25 marks]

Chp 10

May 2024

Question 4

a) Based on *Figure 4*, propose and allocate **THREE(3)** security technologies to enhance network security. Justify your choice of placement according to each function.

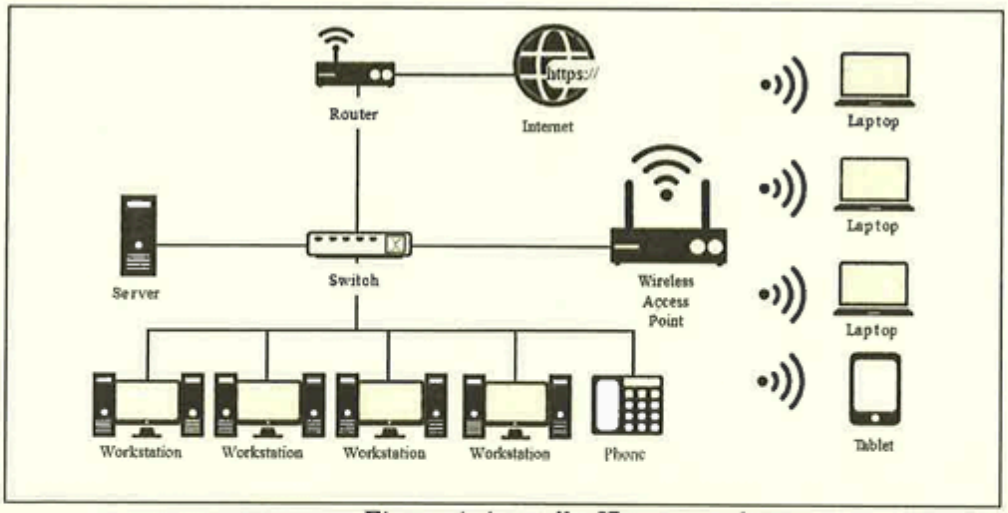

Figure 4: A small office network

(12 marks)

b) Logic bomb attacks share similarities with viruses in their execution process. Relate the **FOUR (4)** phases that constitute the execution of a logic bomb attack. (8 marks)

c) Given the RSA encryption formula of $C = M^e \pmod n$, where C is the ciphertext and M is the plaintext, provide the decryption formula and indicate the public (KU) and private key (KR). Make necessary assumptions. (5 marks)

[Total: 25 marks]

Focus

- Chapter 1
    - Key Security Concepts
    - Security Attacks
- Chapter 2
    - Advanced Encryption Standard
    - Feistel Cipher
    - Symmetric & Asymmetric Encryption
    - Cryptanalysis
- Chapter 3
    - RSA Encryption Algorithm (No calculation)
    - Approaches to Message Authentication
- Chapter 4
    - Kerberos Server
- Chapter 5
    - PGP Operation
- Chapter 6
    - SSL Record Protocol
- Chapter 7
    - Application of IPSEC
- Chapter 8
    - Intruder
- Chapter 9
    - Firewalls Characteristics
- Chapter 11
    - Risk Management