Air University
Final Examination: Spring 2025

Student ID 231269

Subjective
(To be solved on Answer Books only)

Subject: Cryptography
Class: F-23
Section(s): A, B
Course Code: CY 212 / CY 312.

Time Allowed: 3 Hrs
Max Marks: 100
FM's Name: Jameel Arif
FM's Signature:

INSTRUCTIONS

- Understanding the question is part of the exam.
- Use answer sheets for all responses.
- Diagrams must be neat and labeled.
- Calculators allowed.

Q1. **Marks (35) CLO: 3**

You are given the following two symmetric encryption algorithms: **AES** and **DES**.

a) Draw a **block diagram** of both algorithms (10 mark each).
b) Compare the **key sizes, number of rounds,** and **vulnerability to brute force attacks** (10 marks).
c) Identify 2 cryptographic weaknesses in DES that AES resolves. (7 marks)
d) Explain why AES is still vulnerable to **side-channel attacks** despite its mathematical strength. (8 marks)

Q2. **Marks (30) CLO: 2**

A hash function like SHA-1 outputs 160 bits :

a) Estimate how many unique messages must be hashed before the probability of a collision becomes ≥ 50%.
Hint: For an n-bit hash, collision ≈ $\sqrt{(2^n)}$

b) Based on your answer, explain why SHA-1 is now considered insecure for digital signatures.

c) Why is SHA-1 considered cryptographically broken despite being fast?

d) If you were to upgrade this system, which hash algorithm would you choose and why?

e) Describe the difference between hashing and encryption in 2 points.

f) Provide a real-life case where a SHA-1 collision caused a security threat.

Q3. **Marks (35) CLO- 5**

ECC and Key Management in Devices

Answer the following in bullet form (1–3 lines each) :

1. When does a device generate a **public/private key pair** – setup, install, or on-demand?
2. How long are keys used? Are they **session-based** or **persistent**?
3. Where is the **private key** stored in mobile devices?
4. Where does **Windows** store private keys? Mention **file path** or **service**.
5. Are keys **per-application** or shared system-wide? Give one example.
6. What is a **trusted store** and why is it important?
7. What are 2 major **risks** of letting an application generate its own **private CA**?