國立成功大學

115學年度碩士班招生考試試題

編　號：137

系　所：智慧資訊安全碩士學位學程

科　目：資訊安全

日　期：0203

節　次：第 1 節

注　意：1.不可使用計算機
2.請於答案卷(卡)作答，於試題上作答，不予計分。

1. **Terminology**
   Please provide the **Mandarin translation** and an **explanation** for the following technical terms, including core concepts and application scenarios. You may write the explanation in either Mandarin or English. **(20%)**

   (A) Side-Channel Attack

   (B) Homomorphic Encryption

   (C) Perfect Forward Secrecy

   (D) Principle of Least Privilege

   (E) Multi-Factor Authentication

2. Please explain why simply using SHA-256 is insecure when storing user passwords. **(10%)**
   Also, explain the concepts of Salt **(5%)** and Pepper **(5%)**.

3. In the Security Software Development Lifecycle (SSDLC), SAST (Static Application Security Testing) and DAST (Dynamic Application Security Testing) are two types of testing. Please define each one and compare them. **(20%)**

4. In the domain of Operational Technology (OT) security, implementing a one-way transmission mechanism (often referred to as a Data Diode) is a standard compliance requirement. A colleague has suggested that using "fiber optic bidirectional technology" (BiDi) is sufficient to achieve this requirement. Please evaluate this suggestion and explain your professional opinion. Specifically:

   (A) Please explain the technical concept of BiDi (Bidirectional) technology. **(5%)**

   (B) Does this approach meet the strict security requirements for one-way transmission? Why or why not? **(5%)**

   (C) How would you plan and implement a valid solution? **(10%)**

5. Please explain the concepts of Symmetric Encryption and Asymmetric Encryption, providing at least one algorithm example for each. **(14%)**
   Additionally, discuss the theoretical argument regarding why some academic perspectives consider Hash Functions to be distinct from "Encryption". **(6%)**