

等 別：三等考試
類 科：資訊處理
科 目：資訊管理與資通安全
考試時間：2 小時

座號：_____

※注意：(一)禁止使用電子計算器。

(二)不必抄題，作答時請將試題題號及答案依照順序寫在試卷上，於本試題上作答者，不予計分。

(三)本科目除專門名詞或數理公式外，應使用本國文字作答。

一、密碼可以用來做身分認證，但是缺點是密碼太長容易忘記！比較新的認證方式是運用生物辨識技術：

(一)何謂生物辨識技術？列舉至少五種生物辨識技術，並依安全性（Security）和方便性（Convenience）等級（假設分 3 級：優、良、普）做論述。（20 分）

(二)目前手機的認證大部分是利用何種生物辨識技術？它有何優缺點？（5 分）

二、電腦系統或網路設備在做資料傳輸時，為了減少資料重送次數，一般會利用錯誤更正碼技術做資料傳輸：

(一)所謂漢明錯誤更正碼（Error Correction Code, ECC）是把 8 個位元 $d_1 d_2 d_3 d_4 d_5 d_6 d_7 d_8$ 的資料加入 4 個同位位元（Parity Bit） $p_1 p_2 p_4 p_8$ （假設偶同位），使其成為 $p_1 p_2 d_1 p_4 d_2 d_3 d_4 p_8 d_5 d_6 d_7 d_8$ 的 ECC 碼。詳細說明每個同位位元檢驗的位置。（10 分）

(二)給定一個 8 位元的資料，10010010，它的 ECC 碼為何？（10 分）

(三)若收到 111100110110，接收端如何更正錯誤？（5 分）

三、深度學習（Deep Learning）是目前相當熱門的技術，它的應用非常廣泛，諸如病毒碼檢測、聊天機器人、汽車防碰撞、醫學腫瘤影像辨識等。說明深度學習訓練時以分類為例子，為何其最後一級採用的是歸一化指數函數（Softmax）做分類，但實際應用時卻用支援向量機（Support Vector Machine, SVM）技術做分類？（25 分）

四、2022 年諾貝爾物理學獎由法國學者阿斯佩（Alain Aspect）、美國學者克勞澤（John F. Clauser）以及奧地利學者塞林格（Anton Zeilinger）共同獲得，表揚他們發現量子糾纏（Quantum Entanglement）並打下了量子電腦、量子密鑰系統的基礎，確立了可違反貝爾不等式，和開創性的量子通訊科學。何謂量子電腦？它對目前資安的密碼學有何影響？（25 分）