111 年特種考試地方政府公務人員考試試題

等　別：三等考試
類　科：資訊處理
科　目：資訊管理與資通安全

甲、申論題部分：

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：

㈠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）

㈡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）

【解題關鍵】
1.《考題難易》：★★
2.《破題關鍵》：資安身分驗證應用題，只要了解生物辨識技術即可作答。

【擬答】

㈠**生物辨識技術**（biometrics）是指用數理統計方法對生物進行分析，現在多指對生物體（一般特指人）本身的生物特徵來區分生物體個體的電腦技術。

種類	原理	優點	缺點	安全性	方便性
指紋辨識	利用手指紋路圖像特徵辨識身分	1.指紋具有獨特性 2.資料庫建立較早，也較完整	1.指紋容易被有心人取得 2.屬接觸式辨識，有衛生考量 3.指紋容易因磨損或水分影響辨識結果	良	優
虹膜辨識	透過紅外線攝影機，根據眼球微血管分布變化來辨識	1.虹膜特徵紋理結構複雜且不易被複製或取得。 2.辨識精確度極高	1.掃瞄範圍鎖定眼睛，辨識速度較慢 2.紅外線掃瞄可能傷害眼睛 3.需有獨特的辨識裝置，成本較高	優	良
指靜脈辨識	利用近紅外線取得手指中靜脈圖像特徵辨識身分	1.指靜脈具有獨特性且幾乎無法被偽造 2.不限單一手指辨識	1.需有獨特的辨識裝置，建置成本較高 2.屬接觸式辨識，有衛生考量	優	良
聲紋辨識	利用人聲帶和聲道生理結構不	1.每個人說話習慣所呈現聲波	1.當辨識背景過於嘈雜，容易	普	優

全國最大公教職網站 https://www.public.com.tw

	同，分析說話者特性來辨識	幅度不同，具有獨特性	影響辨識結果 2.使用者可能因身體狀況而變聲影響辨識		
人臉辨識	利用人臉五官輪廓的角度、距離來建立 3D 結構模型辨識身分	1.屬於非接觸式辨識，使用者不會有衛生考量 2.辨識過程簡單、直覺、快速 3.不需受辨識者額外動作配合，可直接擷取影像	1.辨識過程易受場域光線、攝影角度影響 2.建檔數過多時，不適合進行 1:N 比對	普	優

㈡手機的認證大部分是利用人臉辨識生物辨識技術，利用人臉五官輪廓的角度、距離來建立 3D 結構模型辨識身分，

1.優點

⑴屬於非接觸式辨識，使用者不會有衛生考量

⑵辨識過程簡單、直覺、快速

⑶不需受辨識者額外動作配合，可直接擷取影像

2.缺點

⑴辨識過程易受場域光線、攝影角度影響

⑵建檔數過多時，不適合進行 1:N 比對

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：

㈠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）

㈡給定一個 8 位元的資料，10010010，它的 ECC 碼為何？（10 分）

㈢若收到 111100110110，接收端如何更正錯誤？（5 分）

【解題關鍵】

1.《考題難易》：★★★★

2.《破題關鍵》：網路技術應用題，了解漢明錯誤更正碼計算方式即可作答，但需要耐心慢慢運算，才不會算錯。

【擬答】

㈠漢明碼的內容可以分成兩個部分：

1.以傳輸資料中 2 的冪次位元部分（第 1,2,4,8…個位元）當同位位元(Parity Bit) p_i，分別由第 k 個位元中符合（2^i AND k）≠0 的所有位元中計算 1 的個數，結果則視採用奇同位檢查或偶同位檢查而定；若採用奇同位檢查則結果若為奇數個 1 則取 0，偶數個 1 則取 1；反之若採偶同位檢查，則結果若為奇數個 1 則取 1，偶數個 1 則取 0。

2. 其他部分（3,5,6,7…）則當成資料位元（data bits）

	1	2	3	4	5	6	7	8	9	10	11	12
資料位元			d_1		d_2	d_3	d_4		d_5	d_6	d_7	d_8
同位位元	p_1	p_2		p_4				p_8				

㈡例如若欲傳送的資料為 10010010，並採用偶同位檢查

	1	2	3	4	5	6	7	8	9	10	11	12
資料位元			d_1		d_2	d_3	d_4		d_5	d_6	d_7	d_8
同位位元	p_1	p_2		p_4				p_8				
原始資料			1		0	0	1		0	0	1	0
傳送資料	1	1	1	1	0	0	1	1	0	0	1	0

$p1 = d1 \oplus d2 \oplus d4 \oplus d5 \oplus d7 = 1$

$p2 = d1 \oplus d3 \oplus d4 \oplus d6 \oplus d7 = 1$

$p3 = d2 \oplus d3 \oplus d4 \oplus d8 = 1$

$p4 = d5 \oplus d6 \oplus d7 \oplus d8 = 1$

所以真正傳送 ECC 是 111100110010

㈢漢明碼的檢查

對各組核對位元作檢查，若 e_i 為核對位元 p_i 與其相關資料位元的同位檢查結果，則（$e_{m-1}e_{m-2}...e_0$）$_2$ 即為錯誤的位元位置，只要更正此一位元即可。例如採用偶同位檢查後接收到的資訊是 111100110110，則

$e_0 = p1 \oplus d1 \oplus d2 \oplus d4 \oplus d5 \oplus d7 = 1 \oplus 1 \oplus 0 \oplus 1 \oplus 0 \oplus 1 = 0$

$e_1 = p2 \oplus d1 \oplus d3 \oplus d4 \oplus d6 \oplus d7 = 1 \oplus 1 \oplus 0 \oplus 1 \oplus 1 \oplus 1 = 1$

$e_2 = p3 \oplus d2 \oplus d3 \oplus d4 \oplus d8 = 1 \oplus 0 \oplus 0 \oplus 1 \oplus 0 = 0$

$e_3 = p4 \oplus d5 \oplus d6 \oplus d7 \oplus d8 = 1 \oplus 0 \oplus 1 \oplus 1 \oplus 0 = 1$

因此錯誤發生在 1010=10 個位元，只要將第 10 個位元直接更正為 0，收到的資料應該是 10010010

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）

【解題關鍵】
1.《考題難易》：★★★★
2.《破題關鍵》：人工智慧應用題，掌握 Softmax 與 SVM 兩種方法的分類效果即可作答。

【擬答】

因為風險值=(資訊資產價值×威脅等級×弱點等級)，因此風險值計算需要考量下列因素：

㈠ Softmax 函式，或稱歸一化指數函式，是邏輯函式的一種推廣。它能將一個含任意實數的 K 維向量{z}「壓縮」到另一個 K 維實向量σ{z} 中，使得每一個元素的範圍都在(0,1)之間，並且所有元素的和為 1(也可視為一個 (k-1)維的 hyperplane 或 subspace)。因此若用 MNIST 資料集進行手寫數字分類深度學習，所構建的深度學習網路最後一層為 10 路 softmax 層，它將返回一個由 10 個機率值（總和為 1）組成的陣列。每個機率值表示當前數位圖像屬於 10 個數字類別中某一個的機率。

㈡支援向量機 SVM 就是在特徵空間中找到一條最佳的分類超平面，能夠讓正、負樣本距離該超平面的間隔（margin）最大化。通常來說，SVM 的優化策略是樣本到分類超平面的距離最大化。也就是說儘量讓正負樣本距離分類超平面有足夠寬的間隔，這是基於距離的衡量優化方式。Softmax 線性分類器的損失函數計算相對概率，又稱交叉熵損失「Cross Entropy Loss」。線性 SVM 分類器和 Softmax 線性分類器的主要區別在於損失函數不同。SVM 使用 hinge loss，更關注分類正確樣本和錯誤樣本之間的距離「Δ＝1」，只要距離大於 Δ，就不在乎到底距離相差多少，忽略細節。而 Softmax 中每個類別的得分函數都會影響其損失函數的大小。例如類別個數 C＝3，兩個樣本的得分函數分別爲[10, -10, -10]，[10, 9, 9]，真實標籤爲第 0 類。對於 SVM 來說，這兩個 Li 都爲 0；但對於 Softmax 來說，這兩個 Li 分別爲 0.00 和 0.55，差別很大。因此實際應用時用支援向量機(Support Vector Machine, SVM)技術做分類會得到較佳的分類結果。

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)

【解題關鍵】
1.《考題難易》：★★★
2.《破題關鍵》：量子電腦運用概念題，掌握量子電腦特性與量子密碼觀念即可作答。

【擬答】

㈠**量子電腦（Quantum computer）**是一種使用量子邏輯進行通用計算的裝置。不同於傳統電腦，量子計算用來儲存數據的物件是量子位元，它用量子演算法來操作數據。若該問題已經有提出速算的量子演算法，只是困於傳統電腦無法執行，那量子電腦確實能達到未有的高速；若是沒有發明演算法的問題，則量子電腦表現與傳統無異甚至更差。量子電腦具有下列特性：

1. 疊加性 (Superposition)
假設每一個量子位元都可能會有兩種狀態，不是順時針旋轉就是逆時針旋轉，若我們把一個粒子放到一個暗箱裡，然後用一個微弱的脈衝打進去，此時箱子內的粒子可能是順時針，也可能是逆時針，若不打開箱子看，我們無法得知這個粒子旋轉的方向。這種所有狀態都可能出現的情況就稱為疊加性。

2. 測量性 (Measurement)
在箱子打開之前，量子是以疊加的狀態存在，也就是順時針旋轉或逆時針旋轉都有可能。一旦箱子被打開後，答案就公佈了，量子的疊加性也隨之消失。

3. 可逆性 (Reversing)
在量子運算中，所有運算在未經測量前都是可逆的。

4. 不可複製性 (No-cloning)
無法對處於疊加狀態中的量子進行複製。

5. 糾纏性 (Entanglement)
無法分解成任意兩個量子態的乘積。

㈡量子電腦對傳統密碼學的威脅

由於量子電腦可以對同一個問題的不同狀態進行同步的處理，所以量子電腦可以更有效率地來執行這個猜謎遊戲。若讓 14 個量子就進入疊加狀態，可同時代表 2^14 種可能發生的狀態，然後把這些處於疊加狀態的粒子放入量子電腦中執行。由於量子電腦可以同時嘗試所有可能的答案，一個單位時間後，量子電腦就會告訴我們正確的謎底為何，而傳統電腦可能需要非常長的時間才能完成所有可能答案的搜查。此時需要利用量子密碼學（Quantum cryptography）。量子密碼學泛指利用量子力學的特性來加密的科學。量子密碼學最著名的例子是量子密鑰分發，而量子密鑰分發提供了通訊兩方安全傳遞密鑰的方法，且該方法的安全性可被資訊理論所證明。目前所使用的公開金鑰加密與數位簽章（如 ECC 和 RSA）在具規模的量子電腦出現後，都會在短時間內被破解。量子密碼學的優勢在於，除了古典密碼學上的數學難題之外，再加上某些量子力學的特性，可達成古典密碼學無法企及的效果。例如，以量子態加密的資訊無法被複製。又例如，任何試圖嘗試讀取量子態的行動，都會改變數子態本身。這使得任何竊聽量子態的行動會被發現。