106年公務人員高等考試一級暨二級考試試題　代號：21930　全一頁

等　　別：高考二級
類　　科：資訊處理
科　　目：資訊管理與資通安全研究
考試時間：2 小時　座號：_____

※注意：㈠禁止使用電子計算器。
㈡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。
㈢本科目除專門名詞或數理公式外，應使用本國文字作答。

一、近年來資安事件頻傳，為強化各機關對資安事件應變能力，需明確訂定資安事件應變作業程序，其中應變作業應含事前安全防護、事中緊急應變及事後復原作業，請列舉五項有關事中緊急應變作業的具體措施。（25 分）

二、為使執行資安事件調查時，能有效保全及運用數位證據，確保數位證據的同一性，請說明人員於執行數位證據識別、蒐集、擷取、封緘及運送，五個作業程序的內容為何？（25 分）

三、請說明如何利用公開金鑰密碼系統來達到下列四種資訊安全控制需求：機密性（Confidentiality）、身分鑑別（Authentication）、完整性（Integrity）與不可否認性（Non-repudiation）。（25 分）

四、區塊鏈被視為是金融科技（Fintech）與物聯網（IoT）等產業不可或缺的應用趨勢，請說明區塊鏈技術中如何利用單向雜湊函數（One-way Hash Function）等技術來達到不可竄改及去中心化等特性？（25 分）