中央銀行所屬中央印製廠、中央造幣廠
110年新進人員聯合甄試
筆試試題

甄試類別：A15 資安管理員

筆試科目：專業科目 2

職位代碼：1

資通安全

<注意事項>

1. 作答前請先檢查答案卷編號與入場通知書之准考證編號、桌角號碼、甄試類別、測驗科目是否相符，如有不同應立即請監試人員處理，否則不予計分。
2. 請確認試題卷印製頁數是否缺漏，如有不足應立即請監試人員處理。
3. 作答方式：

(1)限以藍、黑色鋼筆或原子筆於答案卷上採橫式由左至右由上而下作答，並請從答案卷內第一頁開始書寫，違反者該科酌予扣分，不必抄題但須標示題號。

(2)答案書寫方式，應以西式橫書作答，作答時，切勿超出指定作答區，違反者不予計分。

(3)答案卷須保持清潔完整，請勿折疊、破壞或塗改入場通知書編號，亦不得書寫應考人姓名、入場通知書編號或與答案無關之任何文字或或符號，違者視其情節輕重，依應試規則予以扣分。

4. 本試題卷及答案卷務必繳回，未繳回者該科以零分計算。
5. 本項測驗不需使用電子計算器，請應考人勿攜入應考座位區，若應考人於測驗時將電子計算器放置於桌面或使用，經勸阻無效，仍執意使用者，除該科目成績以零分計外；該電子計算器將由監試人員保管至該節測驗結束後歸還。

專業科目 2：資通安全　(共 1 頁)
本科分數共 100 分

※請填入入場通知書編號:_____

題目一：【25 分】

請說明在資通安全上以下五項功能的意義：(一)私密性(Confidentiality)、(二)完整性(Integrity)、(三) 可用性(Availability) 、(四)來源辨識(Authentication)、(五)不可否認性 (Non-repudiation)。

題目二：【25 分】

請說明TLS、VPN、IPSec、SSH和DSA(或稱DSS)等五個與資訊安全相關技術或協定的功能。

題目三：【25 分】

電子憑證如工商憑證或自然人憑證等在資訊安全扮演很重要角色，請回答下列有關電子憑證問題：

(一)列舉三項運用某電子憑證前須檢查與該電子憑證相關資訊的程序。【9分】

(二)假設使用者甲已取得使用者乙之電子憑證並做完第(一)子題的檢查工作無誤，請設計程序供使用者甲可藉以鑑別對方確實是使用者乙；並說明可以鑑別對方原因。【16分】

題目四：【25 分】

請自下列密碼技術元件中選取部分(或全部)以設計出一適合機制(請用圖形區塊表示但須標示每一區塊所代表的之安全元件)，使網路上節點 A 欲傳送明文資料 M 給節點 B 時，此機制僅提供傳送資料完整性、資料來源鑑別性與發送者傳送資料不可否認性等三項功能，設計之機制須考量相同等級之安全下的效能，更不需其他額外功能以免影響傳輸效能。

請以下列參數說明你所設計的機制，又這些參數已安全地存在於適當的持有者

PR_A、PR_B：分別代表 A 和 B 之非對稱式密碼技術之私鑰

PU_A、PU_B：分別代表 A 和 B 之非對稱式密碼技術之公鑰

K：A 和 B 已共同擁有之對稱式密碼技術之密鑰

M：A 欲傳送給 B 之明文資料

C：A 傳送給 B 之封包資料

密碼技術元件：ECDSA、RSA、ECC、AES、3DES、DES、SHA2、MD5、Diffe-Hellman Key Exchange