考科編號：006

國立高雄海洋科技大學承辦臺灣港務股份有限公司104年度從業人員
助理管理師/助理工程師、助理事務員/助理技術員甄試

專業科目試題

筆試科目：網路與資訊安全

甄選類科：03 資訊

題號	題目
1	(1)DNSsec(DNS Security Extension)是用來防止那些網路攻擊？ (2)請簡單敘述它的工作原理。
	配分：20分，每小題各10分
2	(1)說明ARP協定的用途及運作方式。 (2)說明ARP poisoning 攻擊原理與過程。
	配分：20分，每小題各10分
3	在建立TCP連線前，欲連線之雙方必須先完成三向交握(Three-way Handshake) (1)請說明如何進行三向交握？ (2)TCP SYN Flood是用來進行DOS (Denial of Service)攻擊的一種手法，請問其攻擊原理與進行方式。
	配分：20分，每小題各10分
4	Diffie-Hellman金鑰交換協定(Key Exchange Protocol)能為通訊雙方建立一把共同的金鑰 (1)請說明Diffie-Hellman金鑰交換協定的運作過程。 (2)請說明其安全性。
	配分：20分，每小題各10分
5	令 E 為對稱式加密演算法，而 $E_k(m)$ 表示以 k 為加密金鑰(Key)運用 E 加密訊息 m 後所得之密文(Ciphertext)。D 為對應 E 之解密演算法，也就是對每個訊息 m，$D_k(E_k(m)) = m$ 均會成立。今假設網路上兩個個體 A 與 B 事先已秘密共同持有一把對稱式加密金鑰 k (1) 請利用 E 設計一個可重複執行之相互認證協定(Mutual Authentication Protocol)，使得 A 與 B 執行此協定後，可確認彼此均擁有 k，且任何第三者不能仿冒

題號	題目
5 （續）	A 或 B 成功地執行完成此協定。請注意：在執行過程中不可洩漏 k，也不能使用時間戳記(Timestamp)。 (2)也請分析所設計認證協定之安全性。
	配分：20 分，每小題各 10 分