期末題庫練習

注意:期末考試不能使用計算機

1. Prove or disprove that that 2 is a primitive root of 13. Why do we need to select a primitive root to serve as α in the Diffie-Hellman algorithm mentioned above?
   (2是否為13的質根?說明是或不是的原因) (在DH演算法中，為何選用質根來作運算?)

2. What is the Security of Diffie-Hellman algorithm?

   (DH 演算法的安全性原因為何?)

3. Alice and Bob use the Diffie-Hellman key exchange technique with a common prime q = 23 and a primitive root α= 5.
   (a) If Bob has a public key Y_B = 10, what is Bob's private key X_B?
   (b) If Alice has a public key Y_A = 8, what is the shared key K with B?
   (Alice跟Bob兩人作DH金鑰交換，使用的質數是23，質根是5. (a)如果Bob的公鑰是10, 那Bob的私鑰為何? (b)如果Alice的公鑰是8, 那兩人協調的金鑰為何?)

4. What is the the DOS/Clogging attack in Diffie-Hellman?

   (DH 演算法可能遭遇 DOS/Clogging 攻擊, 試說明之)

5. Please describe the ECDHE.

   (試說明如何用 ECC 來做 DH 金鑰交換)

6. Man-in-the-Middle attack could happen in the Diffie-Hellman key exchange protocol. Let the system parameters q = 11 and α= 7. Suppose the private keys of Alice (sender), Bob (receiver), and Darth (attacker) are 3, 9, and 6, respectively. What is the shared key between Alice and Darth? (5%) What is the shared key between Darth and Bob? (5%)

   (DH 金鑰交換可能會遭遇中間人攻擊。令系統參數 q = 11 and α= 7. 假設 Alice(傳送者), Bob(接收者), Darth(攻擊者)三人的私鑰分別是 3, 9, 6. 請問 Alice 跟 Darth 之間協調的金鑰為何? Darth 跟 Bob 之間協調的金鑰為何?)

7. What is the purposes of ARP? DNS?

   (ARP 的用途何在?DNS 的用途何在?

8. What is the SYN Flooding? Smurf attack?

   (說明何謂 SYN Flooding? Smurf attack?)

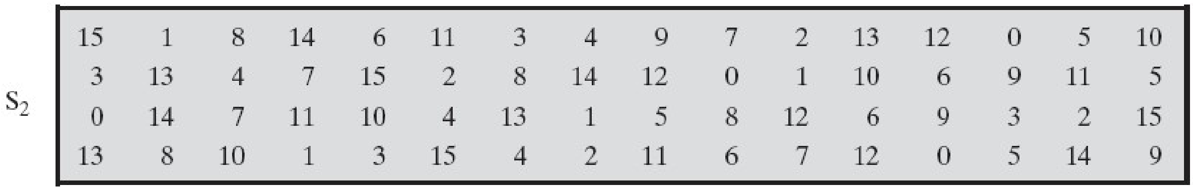
9. Explain the main functions of MAC address, IP address, and Port number in data transmission through internet.

   (網路通訊需要 MAC address, IP address,及 Port number,試分別說明其用途)

10. Explain the basic difference between HTTP and HTTPS.

    (試說明 HTTP 與 HTTPS 的差異)

11. Given S2 below, what is the output regarding input as 011000.
    (給定 S2 如下, 請問當 S2 輸入是 011000 時，輸出為何?)



S_2	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9

12. What are the differences between block ciphers and stream ciphers?

    (區塊加密與串流加密的差異?)

13. Please show how to perform the 3-DES with two keys? How to perform the 3-DES with three keys? (20%) (如何用兩把金鑰執行 3-DES? 如何用三把金鑰執行 3-DES?)

14. What is the avalanche effect (雪崩效應) in DES?
(DES 中提到的雪崩效應，是甚麼意思?)

15. Compare the concepts of cryptography (密碼學) and steganography(資訊隱藏). What are their differences?(密碼學與資訊隱藏主要的差別為何?)

16. What are the advantages and disadvantages of LSB (Least Significant Bit) algorithms used in steganography?

(資訊隱藏演算法中常用的 LSB 方法有何優缺點?)

17. What is the NFT (Non-fungible token)?
(NFT 是甚麼?)