姓名: 謝崇志 學號: 111061610

1. **Discuss the advantages and disadvantages of public-key and symmetric-key cryptosystems. (10 points)**

Ans:

公鑰(非對稱式加密)和對稱式加密系統是用來保護數據的兩種不同類型的加密算法。兩者都有其優缺點，而選擇哪一種取決於具體的用例。

公鑰加密系統:

也稱為非對稱加密，使用兩個不同的鑰匙：公鑰和私鑰。公鑰用於加密數據，而私鑰用於解密數據。公鑰加密的主要優點之一是它不需要安全通道來交換密鑰。公鑰可以自由分發，任何人都可以使用它來加密數據。只有擁有私鑰的人才能解密數據，因此即使公鑰被攔截，數據仍然安全。公鑰加密的另一個優點是它可以用於數字簽名，可以用於驗證數據的真實性和完整性。非對稱加密通常用於大量用戶需要同時加密和解密消息或數據的系統中，尤其是在運算速度和計算資源充足的情況下。 該系統的一個常用案例就是加密電子郵件，其中公鑰可以用於加密消息，私鑰可以用於解密。

然而，公鑰加密也有一些缺點。其中一個是它通常比對稱加密更慢和計算密集。這使得它不太適合加密大量數據。另一個缺點是它更容易受到某些攻擊的影響，例如中間人攻擊，攻擊者攔截公鑰並用自己的公鑰替換。

對稱加密系統:

使用相同的鑰匙進行加密和解密，這使它比公鑰加密更快和更有效，通常用於加密大量數據。對稱加密的主要優點之一是其速度和效率。它比公鑰加密更快和更有效，通常用於加密大量數據。另一個優點是它較少受到某些攻擊的影響，例如中間人攻擊。然而，對稱加密也有一些缺點。其中之一是它需要安全通道來交換密鑰。如果攻擊者攔截密鑰，他們可以輕易地解密數據。

討論密鑰長度方面:

對稱和非對稱加密之間的另一個功能差異與密鑰的長度有關，密鑰的長度以比特為單位，並且與每個加密算法提供的安全級別直接相關。在對稱加密中，密鑰是隨機選擇的，其長度通常設置為 128 或 256 位，具體長度取決於所需的安全級別。 然而，在非對稱加密中，公鑰和私鑰之間在數學上相關聯，這意味著兩者之間存在算術聯繫。 攻擊者可能利用該模式破解密文，因此非對稱密鑰需要更長的密鑰長度，才能提供相同級別的安全性。 密鑰長度的差異是如此明顯，以至於 128 位的對稱密鑰和 2,048 位非對稱密鑰才能提供大致相同的安全級別。

2. **Describe the polynomial-time reduction $A \leq_{ploy} B$. (10 points)**

Ans:

在計算機科學中，多項式時間歸約（Polynomial-time reduction），是一種將一個計算問題 A 轉化為另一個計算問題 B 的方式，轉化時間是多項式時間。這種

方法的想法是，如果存在一種算法可以在多項式時間內解決問題 B，那麼也可以使用相同算法作為子程序在多項式時間內解決問題 A。
正式地說，$A \leq_{poly} B$ 表示存在一個多項式時間可計算的函數 f，對於問題 A 的每個實例 x，都存在一個問題 B 的實例 $y = f(x)$，當且僅當 y 的答案為“是”時，x 的答案才為“是”。
要解決問題 A，可以使用歸約函數 f 將輸入轉換為問題 B 的實例，使用多項式時間算法解決問題 B，然後使用 y 的答案來獲得 x 的答案。問題 A 的算法的時間複雜度是歸約函數 f 的時間複雜度和問題 B 算法的時間複雜度之和。
多項式時間歸約是計算複雜度理論中的一個重要概念，它使我們可以比較不同問題的計算難度，並基於它們的最壞情況時間複雜度將它們分類到複雜度類中。
縮減類型:
三種最常見的多項式時間縮減類型，從限制最多到最少，分別是
Many-one reductions、Truth-table reductions 和 Turing reductions。其中最常用的是 Many-one reductions，最一般的歸約是 Turing reductions，最嚴格的是 Many-one reductions，Truth-table reductions 佔據了兩者之間的空間。

3. **What is the Kerckhoff's principle in cryptanalysis? (10 points)**

Ans:

Kerckhoff's principle 是密碼學中的一個基本概念，一個加密系統應該是安全的，即使除了密鑰以外的系統所有信息都是公開的。換句話說，加密系統的安全性不應依賴於算法本身的保密性，而應依賴於密鑰的保密性。當一個訊息被加密演算法處理後，即使入侵者已經或得到完全存取加密訊息的權限，並且知道使用了什麼演算法，該訊息仍然應該保持安全。這是因為，即使系統的設計和細節一開始沒有被公開，它們仍然可能被未經授權的人發現，因此應該天然具有安全性。
這一原則以荷蘭語言學家和密碼學家 Auguste Kerckhoff 的名字命名，他在 19 世紀末首次提出了這一原則。他認為，密碼系統的安全性應該僅取決於密鑰，而不是算法或其實現的保密性。這一原則已成為現代密碼學中廣泛接受的標準，因為它促進了透明度，鼓勵密碼學家專注於開發強大和安全的加密算法，即使其設計和實現對潛在攻擊者是公開的也能承受攻擊。

4. **We use DES in cipher feedback mode (CFB) to encrypt a plaintext m = m1m2 . . . m100 into a ciphertext c1c2 . . . c100, where each mi is 16-bit long. The ciphertext is sent to Bob. If c16 and c26 are missing and c9 and c89 are received as c09 and c089 wrongly, what mi 's can B compute correctly from the received ciphertext? (10 points)**

Ans:

根據老師的講義:

1. A transmission error in c_i affects correctness of m_i and the next [n/s] plantext blocks.
2. Self-synchronized after[n/s] if and entire block is lost.

在密碼反饋（CFB）模式下，DES 加密一個與明文相同長度的密文塊，並將其用於加密下一個明文塊。在這種情況下，每個明文塊長度為 16 位，需要加密 100 個塊。

因為DES ，所以 $n = 64$，$s = 16$，因此$[n/s] = 4$

如果 c16 和 c26 缺失，我們無法接收到 m16~m20 和 m26~m30。

如果 c09 和 c089 ，我們無法正確接收到 m9~m13 和 m89~m93。

所以我們正確接收到 m1~m8、m13~m15、m21~m25、m31~m88、m94~m100

所以總共可以接收到正確的 80 個明文。

5. Assume that a plaintext bit M is given with $Pr[M = b] = pb$, where b ∈ {0, 1}. Assume that random key K of the one-time pad encryption is chosen by $Pr[K = 0] = 0.42$ and $Pr[K = 1] = 0.58$. Consider the one-time pad encryption $C = M \oplus K$.

(a) Assume that an adversary A1 guesses M randomly without even examining the ciphertext C. Show that the success probability of A1 is exactly 0.5. (10 points)

Ans:

如果對手 A_1 在不檢查密文 C 的情況下隨機猜測明文位元 M，則 A_1正確的機率恰好為 0.5。因為明文位元 M 有等機率為 0 或 1，而 A_1 在沒有額外的信息可以幫助他做出明智的猜測，因此 A_1 有 0.5 的機遇猜對，所以 A_1 的成功機率為 0.5。

$$Pr[A_1\ succeed]$$
$$= Pr[\ A_1 = M' \cap M = M']$$
$$= Pr[\ A_1 = \ 0 \cap M = 0] + Pr[\ A_1 = \ 1 \cap M = 1]$$
$$= \frac{1}{2}\ p_0 + \frac{1}{2}\ p_1$$
$$= \frac{1}{2}\ (p_0 + p_1)$$
$$= \frac{1}{2}$$

(b) Suggest a good strategy A2 of guessing M if p0 and p1 are known. (15 points)

ANS:

如果對手A_2知道機率p_0 and p_1，則A_2可以使用以下策略猜測明文位元 M:

計算鑰匙位元 K=0, K=1 的機率，給定觀察到的密文 C，

使用 Bayes' theorem:

$$\Pr[K=0 \mid C] = \Pr[C \mid K=0] \frac{\Pr[K=0]}{\Pr[C]}$$

$$\Pr[K=1 \mid C] = \Pr[C \mid K=1] \frac{\Pr[K=1]}{\Pr[C]}$$

這裡，$\Pr[C \mid K]$是給定鑰匙 K 時密文 C 的機率，等於$\Pr[C \mid K]$= $\Pr[M \oplus K = C] = \Pr[M = K \oplus C] = p_0$ (如果 C $\oplus$ K = 0)和p_1 (如果 C $\oplus$ K = 1)。機率$\Pr[C]$是密文 C 的 marginal probability。可以計算如下:

$$\Pr[C] = \Pr[C \mid K=0]\Pr[K=0] + \Pr[C \mid K=1]\Pr[K=1]$$

一旦A_2計算出機率$\Pr[K=0 \mid C]$和$\Pr[K=1 \mid C]$，A_2可以按照以下方法猜測明文位元 M:

$$Pr[M=0|C=0] = \frac{0.58\,p_0}{0.58\,p_0 + 0.42\,p_1}$$

$$Pr[M=1|C=0] = \frac{0.42\,p_1}{0.58\,p_0 + 0.42\,p_1}$$

$$Pr[M=0|C=1] = \frac{0.42\,p_0}{0.42\,p_0 + 0.58\,p_1}$$

$$Pr[M=1|C=1] = \frac{0.58\,p_1}{0.42\,p_0 + 0.58\,p_1}$$

如果$\Pr[K=0 \mid C] > \Pr[K=1 \mid C]$，則猜測 M=0。
如果$\Pr[K=0 \mid C] < \Pr[K=1 \mid C]$，則猜測 M=1。
如果$\Pr[K=0 \mid C] = \Pr[K=1 \mid C]$，則隨機猜測。
這個策略基於一個觀察:鑰匙位元 K 被認為是等機率為 0 和 1，因此 M 與觀察到的密文位元 C $\oplus$ K 相等的機率與給定觀察到的密文 C 時 K=0 或 K=1 的機率成比例。通過 Bayes' theorem 計算這些機率，A_2可以對明文位元 M 做出明智的猜測。

6. Use the Chinese Remainder Theorem to compute 0 ≤ x < 1785 for x mod 7 = 1, x mod 15 = 3, and x mod 17 = 12. (15 points)

Ans:

Given:

$$x \bmod 7 = 1$$
$$x \bmod 15 = 3$$
$$x \bmod 17 = 12$$

Compute the inverse:

$$(15 * 17)^{-1} \bmod 7 = 5$$
$$(7 * 17)^{-1} \bmod 15 = 14$$
$$(7 * 15)^{-1} \bmod 17 = 6$$

Compute:

$$x = r_1 N_1 (N^{-1} \bmod n_1) + \cdots + r_m N_m (N^{-1} \bmod n_m)$$

因此

$$x \equiv 1 * (15 * 17) * 5 + 3 * (7 * 17) * 14 + 12 * (7 * 15) * 6$$
$$\equiv 1275 + 4998 + 7560 \ (mod\ 1785)$$
$$\equiv 1338 (mod\ 1785)$$

7. In the SubBytes of AES, $f(x) = x^{-1} \bmod X^8 + X^4 + X^3 + X + 1$..
Compute f(01100011). (20 points)

Ans:

Compute gcd(a, b):

$$X^8 + X^4 + X^3 + X + 1 = (X^2 + X + 1)(X^6 + X^5 + X + 1) + (X^5 + X^4 + X)$$
$$(X^6 + X^5 + X + 1) = X(X^5 + X^4 + X) + (X^2 + X + 1)$$
$$(X^5 + X^4 + X) = (X^3 + X + 1)(X^2 + X + 1) + (X + 1)$$
$$(X^2 + X + 1) = X(X + 1) + 1$$

Compute reversely:

$$1 = (X^2 + X + 1) - X(X + 1)$$
$$= (X^2 + X + 1) - X((X^5 + X^4 + X) - (X^3 + X + 1)(X^2 + X + 1))$$
$$= (X^6 + X^5 + X + 1) - X(X^5 + X^4 + X) - X[(X^5 + X^4 + X) - (X^3 + X + 1)(X^2 + X + 1)]$$
$$= (X^6 + X^5 + X + 1) - X(X^5 + X^4 + X) - X(X^5 + X^4 + X) + X(X^3 + X + 1)(X^2 + X + 1)$$
$$= (X^6 + X^5 + X + 1) - X(X^5 + X^4 + X) - X(X^5 + X^4 + X) + X(X^3 + X + 1)[(X^6 + X^5 + X + 1) - X(X^5 + X^4 + X)]$$
$$= (X^4 + X^2 + X + 1)(X^6 + X^5 + X + 1) - X(X^3 + X + 1)X((X^8 + X^4 + X^3 + X + 1) - (X^2 + X + 1)(X^6 + X^5 + X + 1))$$
$$= (X^7 + X^6 + X^4 + X + 1)(X^6 + X^5 + X + 1) + (X^5 + X^3 + X^2)(X^8 + X^4 + X^3 + X + 1)$$

因此

$$(X\text{^}6 + X\text{^}5 + X + 1)^{-1} = X^7 + X^6 + X^4 + X + 1$$

所以

$$f(01100011) = 11010011$$