資訊安全

40647027S 陳冠潁

1. 針對(E_1, D_1)，我們可以構造兩組 cipher，$(c_1, c_1), (c_3, c_4)$，送去給挑戰者解密，假如挑戰者選擇第一組，則
$\mathrm{D}\big(\mathrm{k}, (c_1, c_1)\big) = \mathrm{D}(\mathrm{k}, c_1) \because D(k, c_1) = D(k, c_1)$，可以檢查回傳的訊息是否是$\mathrm{D}(c_1)$，來知道挑戰者選第一組解密。
反之選擇第二組會可能解密失敗被 reject，因此可以成功攻破 CCA-secure，所以$\big(E_{1,} D_1\big)$不為 AE-secure。

   但(E_2, D_2)，加密出來會是一組兩個相同的 c，如: (c, c)，解密也需要兩個 c 相同才能解開，則不能使用上述的攻擊方法成功破解 CCA-secure，因此此加解密方式仍然為 AE-secure。

2.

(1)

$$\mathrm{L}\big(c^\lambda \bmod n^2\big) * \mu \bmod \mathrm{n} = \frac{\mathrm{L}\big(c^\lambda \bmod n^2\big)}{\mathrm{L}(g^\lambda \bmod n^2)} \bmod \mathrm{n}$$

By Carmichael's theorem. $c^\lambda = (g^m r^n)^\lambda = g^{m\lambda} * r^{m\lambda} = g^{m\lambda}$

Make use of the relationship $((1+n)^x) \equiv 1 + \mathrm{nx} \pmod{n^2}$

$$g^{m\lambda} = ((1+n)^\alpha \beta^n)^{\lambda m} = (1+n)^{\alpha\lambda m} \beta^{n\lambda m} \equiv (1 + \alpha\lambda mn) \bmod n^2$$

代回原式:

$$\frac{\mathrm{L}\big(c^\lambda \bmod n^2\big)}{\mathrm{L}(g^\lambda \bmod n^2)} \bmod \mathrm{n} = \frac{L(1+\alpha\lambda mn)}{L(1+\alpha\lambda m)} \bmod n = \frac{\alpha\lambda mn}{\alpha\lambda n} \bmod n = m$$

(2)

Assume that $\mathrm{c} = E_k(m, r)$, multiply it by a random encryption of 0, i.e. compute $c{r_1}^n \bmod n^2 = E_k(m, rr_1 \bmod n)$.

3. (1) The cardinality of the subgroup generated by g divides the cardinality of Z∗N = ϕ(N) = p*q. By definition, it holds that gcd(r, p*q) = 1, because r is chosen from Z_{pq}^*. Then the order of h is equal to the order of g, implying that g = h. If r would be chosen from Z_{pq}, then $g^m h^r$ would be indistinguishable from a uniformly chosen element of g.

   (2) c = $g^m h^r = g^m (g^k)^r = g^m g^{kr}$又已知 c, g, m，因此如果能在有效率的時間內找出 kr 則能破解此系統，但求解 kr 為 descrite logarithm problem 並不存在有效率的求解算法，因此此問題為 computationally impossible。

4.

$$c' = (c * 2^e)\ mod\ n = (2^e * m^e)\ mod\ n = ((2m)^e)\ mod\ n$$

因為 2m 有可能大於 n，所以解密完變成(2m) mod n，且我們能知道最低位為 1 或 0，且 n 必為奇數，則如過 LSB 是 0，代表(2m) mod n 是偶數<n，可以知道 m<n/2，反之 m>n/2，以此類推可以用二分搜尋的方式將 m 的範圍持續縮小，直到上下界相等，則能得到 m。

明文為: It was the best of times, it was the worst of times, it was the age of wisdom, it was the age of foolishness.

程式碼在: attack.py

5. 寫在另一份 PDF: LAB.HW3.pdf