1. Assume that a plaintext bit M is given with Pr[M = b] = p_b, where b ∈ 0, 1. Assume that random key K of the one-time pad encryption is chosen by Pr[K = 0] = 0.6 and Pr[K = 1] = 0.4. Consider the one-time pad encryption C = M ⊕ K

(a) Assume that an adversary A_1 guesses M randomly without even examining the ciphertext C. Show that the success probability of A_1 is exactly 0.5. (20 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 strategyA_2 of guessing M if p_0 and p_1 are known. (20 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 ⊕ K = 0)和p_1 (如果 C ⊕ 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:

$$Pr[\,M = 0|C = 0] = \frac{0.6\,p_0}{0.6\,p_0 + 0.4\;p_1}$$

$$Pr[\,M = 1|C = 0] = \frac{0.4\,p_1}{0.6\,p_0 + 0.4\;p_1}$$

$$Pr[\,M = 0|C = 1] = \frac{0.4\,p_0}{0.4\,p_0 + 0.6\;p_1}$$

$$Pr[\,M = 1|C = 1] = \frac{0.6\,p_1}{0.4\,p_0 + 0.6\;p_1}$$

如果$\Pr[\,K = 0\,|\,C\,] > \Pr[\,K = 1\,|\,C\,]$，則猜測 M=0。
如果$\Pr[\,K = 0\,|\,C\,] < \Pr[\,K = 1\,|\,C\,]$，則猜測 M=1。
如果$\Pr[\,K = 0\,|\,C\,] = \Pr[\,K = 1\,|\,C\,]$，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 ⊕ 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。

2. The Euclidean algorithm computes gcd(a, b).
   (a) Give the algorithm and show that its computation time is polynomial in the total length m of a and b, where m = len(a) + len(b). (10 points)

Ans:
假設 $len(a) < len(b)$，那麼第一次迭代會將 b 除以 a，得到的商 q 和餘數 r 會滿足以下等式:

$$b = aq + r$$

由於 $r < a$，我們可以得到以下不等式:

$$len(r) \leq len(a) - 1$$

然後我們可以用 a 代替 b，r 代替 a，並重複進行相同的運算，在第二次迭代中，我們得到:

$$a = rq_1 + r_1$$

由於 $r_1 < r$，所以

$$len(r_1) \leq len(r) - 1 \leq len(a) - 2$$

重複進行這些步驟，每次將長度至少減少 1，最後我們得到一個餘數 0 的方程式:

$$r_{i-1} = r_i\,q_{i+1}$$

這代表 a 和 b 的最大公因數為r_i，因此在最壞的情況下，算法需要執行 len(b)次迭代，每次迭代需要 O(n)的時間進行一個除法和幾個常數時間操作。因此算法的總運行時間為$O(len(a)len(b))$，根據$m = len(a) +$

$len(b)$，我們可以將$len(a)$和$len(b)$都限制在 m 以內，因此算法的時間複雜度可以簡化為

$$\big(len(a)+len(b)\big)*O\big((len(a)-len(b)+1)*len(b)+len(a)+len(b)\big)$$
$$=O(m^3+m^2)$$
$$=O(m^3)$$

```
 Euclidean(a, b):
{
        While(b != 0)
        {
                a = a mod b;
                swap(a, b);
        }
        return a;
}
```

(b) Solve the equation r × 128 + s × 54 = 2. (10 points)

Ans:

$$128 = 2*54+20$$
$$54=2*20+14$$
$$20=1*14+6$$
$$14=2*6+2$$
$$6=3*2+0$$

因此 $gcd(128,54) = 2$，所以可以計算出:

$$2=14-2*6$$
$$=14-2*(20-14)$$
$$=14-2*\big(20-(54-2*20)\big)$$
$$=14-2*\Big(20-\big(54-2*(128-2*54)\big)\Big)$$
$$=14-2*\big(20-(54-2*128+4*54)\big)$$
$$=\big(54-2*(128-2*54)\big)-2*\big((128-2*54)-54+2*128-4*54\big)$$
$$=54-2*128+4*54-2*128+4*54+2*54-4*128+8*54$$
$$=-8*128+19*54$$
$$=r*128+s*54$$
$$r=-8，s=19$$

3. In the SubBytes of AES, $f(x) = x^{-1} \bmod X^8+X^4+X^3+X+1$. Compute $f(11101001)$. (20 points)

Ans:

Compute gcd(a, b):

$$X^8 + X^4 + X^3 + X + 1 = (X+1)(X^7 + X^6 + X^5 + X^3 + 1) + X^5$$
$$(X^7 + X^6 + X^5 + X^3 + 1) = (X^2 + X + 1)X^5 + (X^3 + 1)$$
$$X^5 = X^2(X^3 + 1) + X^2$$
$$(X^3 + 1) = X\,(X^2) + 1$$

Compute (x, y) reversely:

$$\begin{aligned}1 &= (X^3 + 1) - X\,(X^2) \\ &= (X^3 + 1) - X(X^5 - X^2(X^3 + 1)) \\ &= (X^3 + 1) - X(X^5 - X^2(X^7 + X^6 + X^5 + X^3 + 1) - (X^2 + X + 1)X^5) \\ &= (X^3 + 1) - X(X^5 - X^2(X^7 + X^6 + X^5 + X^3 + 1) - (X^2 + X + 1)((X^8 + X^4 \\ &\quad + X^3 + X + 1) - (X+1)(X^7 + X^6 + X^5 + X^3 + 1))\end{aligned}$$

整理完後，$X^6 + X^3 + X^2 + X$ 是 $X^7 + X^6 + X^5 + X^3 + 1$ 的 inverse

所以

$$f(11101001) = 01001110$$

4. Use the Chinese Remainder Theorem to compute $0 \le x < 352$ for x mod 3 = 1, x mod 11 = 3, and x mod 16 = 13. (20 points)

Ans:

Compute the inverse:

$$(11 * 16)^{-1}\, mod\; 3 = 2$$
$$(3 * 16)^{-1}\, mod\; 11 = 3$$
$$(3 * 11)^{-1}\, mod\; 16 = 1$$

Compute:

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

因此

$$\begin{aligned}x &\equiv 1 * (11 * 16) * 2 + 3 * (3 * 16) * 3 + 13 * (3 * 11) * 1 \\ &\equiv 352 + 432 + 429\ (mod\ 528) \\ &\equiv 157(\ mod\ 528)\end{aligned}$$