```
15. i=0 Qo=1 X=1900.1 mod 2537=1900 power=1900 mod 2537=2386
       i=1  a_1=0  x=1900 power = 2386 mod 2537 = 2505
       j = 2  a2 = 1  X = 1900.2505 mod 2537 = 88  power = 2505 mod 2537 = 1024
       i=3 a3=1 X=88.1024 mod 2537=1317
                                                                      2537 /369000
                                                      14002 88
12675 8192
                                                      1317 8192
      return X = 1317 = 1900 mod 2537
     i=0 Qo=1 X=210.1 mod 2537=210 power=210 mod 2537=971
     1=1 a,=0 X=210 power=97 mod 2537=1614
     i= 2 a2=1 X=210.1614 mod 2537=1519 power=1614 mod 2537=2034
     1=3 Q3=1 X= 1519.2034 mod 2537 = 2117
                                                                 2537 14759500
 17. 将ATTACK轉為數字表示 00 19 19 00 02 10
      N=43·59=2537 將轉換後的數字4位為一組 3019646
                                                           2537 13089646
      因為 2525 < 2537 < 252525
                                                                      210
      第一組 0019 密文 C=(0019) mod 2537=>299(根據第4題)
                                                                      2100
     第二組 1900 密文 C = (1900) mod 2537=1317(根據第15題)
                                                                            6275025
     第三組 0210 密文 C=(02/0)3mod 2537=2117(根據第16題)
                                                                  2537 44100
                                                                     18730
     国此 ATTACK經RSA加密後為 2299 1317 2117
                                                                     17759
                                                                            17759
18.
                                                                   2537 1942841
     X \equiv 2 \pmod{3} Q_1 = 2 M_1 = 3
     X = 1 \pmod{4} Q_2 = 1 M_2 = 4 M = M_1 \cdot M_2 \cdot M_3 = 60
      X = 3 \pmod{5} a_3 = 3 m_3 = 5
    M_1 = \frac{M_1 \cdot M_2 \cdot M_3}{M_2} = 20 \quad M_2 = \frac{M_1 \cdot M_2 \cdot M_3}{M_2} = 15 \quad M_3 = \frac{M_1 \cdot M_2 \cdot M_3}{M_2} = 12
    inverse y, of M, modulo m, = 2 70 = 1 (mod3)
    inverse 82 of M2 modulo M2 = 3 45= 1. (mod4)
    inverse 23 of M3 modulo m3 = 3 36=1 (mod5)
                                                                2537 /2604996
    X= a, M, J, + a2 M2 J2 + a3 M3 J3 = 80+45+108 = 233 = 53 (mod 60)
                                                                     15222 2604996
```