```
P = Pmod N = C mod N
Prob 41
                                    P = C (mod N)
(2 = ((S = mod N) C) mod N
                              55-1 mod N = 1 => 55-1 = 1 (mod N)
Pa = Ca mod N
                              y (XN+1) = 455-1
p= P25-1 mod N
                              YXN+Y = yS5-1 => yS5-1 = y (mod N)
P = P25 (mod N)
PSS-1 = P2S-1 (mod N)
    = E[((SE mod N) C) mod N] mod N 3 S - (mod N)
PS = E[((S = mod N) C) mod N] mod N (mod N)
    ? ((SE mod N) C) mod N (mod N)
    = ((S=modN) CD) mod N (mod N)
    = {[(S = mod N) mod N][("mod N]] mod N (mod N)
    = ESP3 mod N (mod N)
```

PS = PS (mod N)