10 1000 0100

110054809 易頡

4.b) $i=0$ $a_0=0$ $X=1$ power $= 11^2 \bmod 645 = 121$

$i=1$ $a_1=0$ $X=1$ power $= 121^2 \bmod 645 = 451$

$i=2$ $a_2=1$ $X=1 \cdot 451 \bmod 645 = 451$ power $= 451^2 \bmod 645 = 226$

$i=3$ $a_3=0$ $X=451$ power $= 226^2 \bmod 645 = 121$

$i=4$ $a_4=0$ $X=451$ power $= 121^2 \bmod 645 = 451$

$i=5$ $a_5=0$ $X=451$ power $= 451^2 \bmod 645 = 226$

$i=6$ $a_6=0$ $X=451$ power $= 226^2 \bmod 645 = 121$

$i=7$ $a_7=1$ $X=451 \cdot 121 \bmod 645 = 391$ power $= 121^2 \bmod 645 = 451$

$i=8$ $a_8=0$ $X=391$ power $= 451^2 \bmod 645 = 226$

$i=9$ $a_9=1$ $X=391 \cdot 226 \bmod 645 = 1$

5 c)

$11^2 \bmod 645 = (11^1 \bmod 645)^2 \bmod 645 = 11^2 \bmod 645 = 121$

$11^4 \bmod 645 = (121 \bmod 645)^2 \bmod 645 = 121^2 \bmod 645 = 451$

$11^8 \bmod 645 = (451 \bmod 645)^2 \bmod 645 = 451^2 \bmod 645 = 226$

$11^{16} \bmod 645 = (226 \bmod 645)^2 \bmod 645 = 226^2 \bmod 645 = 121$

$11^{32} \bmod 645 = (121 \bmod 645)^2 \bmod 645 = 121^2 \bmod 645 = 451$

$11^{64} \bmod 645 = (451 \bmod 645)^2 \bmod 645 = 451^2 \bmod 645 = 226$

$11^{128} \bmod 645 = (226 \bmod 645)^2 \bmod 645 = 226^2 \bmod 645 = 121$

$11^{256} \bmod 645 = (121 \bmod 645)^2 \bmod 645 = 121^2 \bmod 645 = 451$

$11^{512} \bmod 645 = (451 \bmod 645)^2 \bmod 645 = 451^2 \bmod 645 = 226$

6. d) $11^{644} \bmod 645 = (11^{512} \bmod 645) \cdot (11^{128} \bmod 645) \cdot (11^4 \bmod 645)$

$= [(226 \cdot 121) \bmod 645] \cdot (11^4 \bmod 645)$

$= (27346 \bmod 645) \cdot (11^4 \bmod 645)$

$= (256 \cdot 451) \bmod 645$

$= 115456 \bmod 645$

$= 1$

121 × 121: 121, 242, 121, 14641

645) 14641 = 22: 1290, 1741, 1290, 451

451 × 451: 451, 2255, 1804, 203401

645) 203401 = 315: 1935, 990, 645, 3451, 3225, 226

645) 51076 = 79: 4515, 5926, 5805, 121

226 × 226: 1356, 452, 452, 51076

451 × 121: 451, 902, 451, 54571

645) 54571 = 84: 5160, 2971, 2580, 391

391 × 226: 2346, 782, 782, 88366

645) 88366 = 137: 645, 2386, 1935, 4516, 4515, 1

226 × 121: 226, 452, 226, 27346

645) 27346 = 42: 2580, 1546, 1290, 256

256 × 451: 256, 1280, 1024, 115456

645) 115456 = 179: 645, 5095, 4515, 5806, 5805, 1