

Exercise 3

$$K = 36203$$

$$c = 2003$$

$$d = 12$$

$$m = 1$$

$$n = 24$$

$$\textcircled{1} \quad \varphi(36203) = \varphi(41) \cdot \varphi(883) = 40 \cdot 882 = 35280$$

$$\varphi(2003) = 2002$$

$$\varphi(12) = \varphi(3) \cdot \varphi(4) = 2 \cdot 4 \left(1 - \frac{1}{2}\right) = 4$$

$$\varphi(1) = 1$$

$$\varphi(24) = 3^3 \left(1 - \frac{1}{3}\right) = 24 - \frac{24}{3} = 18$$

$$\textcircled{2} \quad (12+5)^{36203} \pmod{24}$$

$$17^{36203} \pmod{24}$$

$$17^{36203} \pmod{24}$$

$$\varphi(24) = 18$$

$$\begin{array}{r} 36203 \mid 18 \\ 36 \\ \hline 20 \end{array} \quad \begin{array}{l} 2011 \Rightarrow 11111011011 \end{array}$$

$$\begin{array}{r} 18 \\ \hline 23 \\ 18 \\ \hline 5 \end{array}$$

$17^{2011} \text{ mod } 18$

$a \quad b \quad b^2 \quad b^3 \cdot a \quad b^3 \cdot a(m)$

1	1	1	17	17
1	17	289	4913	17
1	17	289	4913	17
1	17	289	4913	17
1	17	289	4913	17
0	17	289	289	1
1	1	1	17	17
1	17	289	4913	17
0	17	289	289	1
1	1	1	17	17
1	17	289	4913	<u>17</u> = 10001

$17^{18} \text{ mod } 28$

$a \quad b \quad b^2 \quad b^3 \cdot a \quad b^3 \cdot a(m)$

1	1	1	17	17
0	17	289	289	17
0	19	361	361	10
0	10	100	100	19
1	19	361	6137	<u>8</u>

Problem: 8

(3)

$27^{12+36203} \text{ mod } 2003$

$27^{36215} \text{ mod } 2003$

$\phi(2003) = 2002$

$18 = 10010_2$

$$\begin{array}{r} 36215 / 2002 \\ \underline{2002} \\ 16193 \\ \underline{6016} \\ 10177 \end{array}$$

28¹⁸ mod 2002

a b b² b³ a b⁴(m)

1	1	1	27	207
0	27	729	729	729
0	729	531441	531441	977
1	977	829921	2240867	1483
0	1483	2199289	2199289	1093 = 1000/1000/012

28¹⁰⁹³ mod 2003

a b b² b³ a b⁴(m)

1	1	1	27	27
0	27	729	729	729
0	729	531441	531441	646
0	646	417316	417316	692
1	692	488864	12929328	1966
0	1966	3865156	3865156	1369
0	1369	1874161	1874161	1356
0	1356	1838736	1838736	1985
1	1985	3940225	106386085	836
0	836	541696	541696	886
1	886	784996	21194892	1149

Omben: 1149