Exercise 3

Задание 1

$\varphi(k) = \varphi(36207) = \varphi(3^5)\,\varphi(149) = 3^5(1-\frac{1}{3})\cdot 148 = 23976$

$\varphi(c) = \varphi(2002) = \varphi(2)\,\varphi(11)\,\varphi(7)\,\varphi(13) = 1\cdot 10\cdot 6\cdot 12 = 720$

$\varphi(d) = \varphi(6) = \varphi(2)\,\varphi(3) = 1\cdot 2 = 2$

$\varphi(m) = \varphi(4) = 2^2(1-\frac{1}{2}) = 2$

$\varphi(x) = \varphi(265) = \varphi(5)\cdot\varphi(53) = 4\cdot 52 = 208$

Задание 2 $(6+5)^{36207^4} \bmod 265 \equiv C$

1) $K = 36207^4 \Rightarrow 11^K \bmod 265$

2) $\varphi(265) = 208$

3) $K = 208n + \text{в} = 36207^4$

4) $\text{в} \equiv 36207^4 \bmod 208 \equiv 81 \bmod 208$

$4 = \overset{2}{1}\,\overset{1}{0}\,\overset{0}{0}_2$

a_i	c	c^2	$c^2\cdot a$	$c^2 a \bmod k$
1	1	1	36207	15
0	15	225	225	17
0	17	289	289	81

5) $11^{208n+\text{в}} \bmod 265 \equiv 11^{208n}\cdot 11^{\text{в}} \bmod 265 \equiv$

$\equiv 11^{\text{в}} \bmod 265$

6) $11^{81} \bmod 265 \equiv C$

$81 = \overset{6}{1}\,\overset{5}{0}\,\overset{4}{1}\,\overset{3}{0}\,\overset{2}{0}\,\overset{1}{0}\,\overset{0}{1}_2$

(таблица будет представлена на след. странице)

a_i	c	c^2	$c^2 \cdot a$	$c^2 a \bmod k$
1	1	1	11	11
0	11	121	121	121
1	121	14641	161051	196
0	196	38416	38416	256
0	256	65536	65536	81
0	81	6561	6561	201
1	201	40401	444411	6

$C \equiv 6 \bmod 265$

Ответ $C \equiv 11^{36207^4} \bmod 265 \equiv 6 \bmod 265$

Задание 3 $C \equiv 265^{36207+6} \bmod 2002$

$m = 36213 = 1000110101110101_2$

a_i	c	c^2	$c^2 \cdot a$	$c^2 \cdot a \bmod k$
1	1	1	265	265
0	265	70225	70225	155
0	155	24025	24025	1
0	1	1	1	1
1	1	1	265	265
1	265	70225	18609625	1035
0	1035	1071225	1071225	155
1	155	24025	6366625	265
0	265	70225	70225	155
1	155	24025	6366625	265
1	265	70225	18609625	1035
1	1035	1071225	283874625	1035
0	1035	1071225	1071225	155
1	155	24025	6366625	265
0	265	70225	70225	155
1	155	24025	6366625	265

Ответ: $C \equiv 265 \bmod 2002$