Løsningsforslag eksamen 2002.

Problem 1 2002: $\phi(n) = 30\cdot 40 = 1200$ and $1 = 6\cdot 1200 - 313\cdot 23$ so the decryption function is $d_k(y) = y^{887} (\bmod\, n)$.

Problem 2 2002: $(\alpha^2+1)^{-1} = \alpha$ and the decryption function is given by $d(z) = \alpha z + \alpha^2$

Problem 3 2002: $x \equiv 2^{37686} (\bmod\, 155)$ is by the Chinese remainder theorem the same as a solution of the system of the two congruences $x \equiv 2^{37686} (\bmod\, 5)$ and $x \equiv 2^{37686} (\bmod\, 31)$, and $x \equiv 3^{1456} (\bmod\, 65)$ is equivalent to the solution of the two congruences $x \equiv 3^{1456} (\bmod\, 5)$ and $x \equiv 3^{1456} (\bmod\, 13)$. $x \equiv 2^{4\cdot 9421+2} (\bmod\, 5)$ which gives that $x \equiv 4 (\bmod\, 5)$. $x \equiv 3^{4\cdot 364} (\bmod\, 5)$ gives that $x \equiv 1 (\bmod\, 5)$. Hence the system of congruences is not solvable.

Problem 4 2002: Applying $\log_c$ to these two congruences one obtain The linear system of congruences:

$$3x + 10y + 3 \equiv 50 + 2x + 13y + 8 (\bmod\, 100)$$
$$2x + 7y + 10 \equiv 4x + 12y + 11 (\bmod\, 100)$$

which gives that $x = \log_c a = 52$ and $y = \log_c b = 99$.

Problem 5 2002: Here (a/b) denotes the Legendre or Jacobi symbol and the rules in section 5.4.2 can be applied. $(22/p) = (2/p)(11/p) = 1(11/p) = -(p/11) = -(10/11) = -(2/11)(5/11) = (5/11) = (11/5) = (1/5) = 1$, so the quadratic congruence is solvable.

Problem 6 2002: $e_K(x, k_1) = (\alpha^{k_1}, x\beta^{k_1}) = (7, 30)$ and $e_K(x, k_2) = (\alpha^{k_2}, x\beta^{k_2} = (49, 139)$ Now $49 = 7^2$, hence $k_2 = 2k_1$. Therefore with $k = k_1$ one gets $\beta^k = (x\beta^{2k})/(x\beta^k) = 139 \cdot 30^{-1} (\bmod\, 10007)$ and $x = 30 \cdot (\beta^k)^{-1} = 30 \cdot 30 \cdot 139^{-1} = 4758$

Problem 7 2002: $f(x) = (x^7+1)(x^{127}+1)$. The order of the group is $2^{1463}-1$ and $2^{1463} - 1 = 2^{6\cdot 243+5} - 1 \equiv 32 - 1 \equiv 3 (\bmod\, 7)$ hence $x^7 + 1$ has only one root, namely 1. $2^{1463} = 2^{126\cdot 11+77} \equiv 2^{7\cdot 11} \equiv 1 (\bmod\, 127)$, Hence 127 divides the order of the group, and there are 127 solutions in the field to the equation $x^{127} + 1 = 0$. From this we can say that there are 127 solution to the given equation in the given field when the zeros are not counted with multiplicity, and 128 if they are counted with multiplicity.

Problem 8 2002: $p = 1619$, so $p - 1 = 1618$. Now $\gcd(1618, 3) = 1$, hence the function $f : \mathbb{Z}_p \to \mathbb{Z}_p$ given by $f(x) = (x+1)^3$ is a composition of the two bijections g given by $g(x) = x + 1$ and h given by $h(x) = x^3$. This gives that the curve will contain exactly $2 \cdot (p-1)/2 + 1 = 1619$ points.