Løsningsforslag eksamen 2004.

Problem 1 2004: $(x^5+x^3+x^2+1)^{-1} = x^6+x^2$ and the decryption function will be $d(t) = (x^6+x^2)\cdot t + x^6+x^5+x^4+x^3+x^2+x$

Problem 2 2004: $x \equiv 2^{356} \equiv 2^{70\cdot 5+6} \equiv 64 (\bmod 71)$ $2x \equiv 3^{318483} \equiv 3^{30\cdot 10616+3} \equiv 3^3 \equiv 27 (\bmod 31)$, which gives $x \equiv 29 (\bmod 31)$, and one finds that $x = 277$.

Problem 3 2004: Take the square of the first equation one obtains $4a^6b^4 \equiv g^4$. Divide this by the second equation one obtains $a^4b^{-1} \equiv g^{-2}$. Take the last equation and divide by the product of the first two equations, gives the equation $a^3b \equiv g^{-5}$. Multiply the two equation obtained and obtain $a^7 \equiv g^{-7}$. If $\gcd(p-1,7) = 1$, then $\log_g a = -1$ and $\log_g b = -2$, otherwise one just have the congruences $7\log_g a \equiv -7 (\bmod p-1)$ and $7log_g b \equiv -14 (\bmod p-1)$

Problem 4 2004: $27 = 3^3$ and $81 = 3^4$, $(\alpha^{k_1})^4 = (\alpha^{k_2})^3$ so $4\cdot k_1 = 3\cdot k_2$. $56^4 = m^4\beta^{4k_1}$ and $19^3 = m^3\beta^{3k_2}$ dividing the first equation by the second one one get that $m = 56^4 \cdot 19^{-3}$ everything calculated modulo 3001, which becomes 2490.

Problem 5 2004: The straight line has equation $y = 9x$, so one find the third point on that line and the curve by factoring $x^3 - 10x^2 + 9x = x(x-1)(x-9)$, which gives the point $(9,10)$. Hence, $C = (9,61)$

Problem 6 2004: $n = 3001\cdot 7001$ and hence $\phi n = 3000\cdot 7000 = 21000000$ We can solve $x \equiv 433^{-1} (\bmod 3000)$ and $x \equiv 433^{-1} (\bmod 7000)$ which is the same as solving the system $x \equiv 433^{-1}$ modulo each of the numbers 3, 7, 8 and 125. This gives $x \equiv 1 (\bmod 3)$, $x \equiv 6 (\bmod 7)$, $x \equiv 1 (\bmod 8)$ and $x \equiv 97 (\bmod 125)$. This together gives $x = 97$.

Problem 7 2004: The function $f(x) = x^3$ from $\mathbb{Z}_n^*$ to $\mathbb{Z}_n^*$ has a kernel isomorphic to $\mathbb{Z}_3$ and hence the image has size $\phi(n)/3$ and are isomorphic to $\mathbb{Z}_7 \times \mathbb{Z}_8 \times \mathbb{Z}_{125} \times \mathbb{Z}_8 \times Z_{125}$. Hence the probability $p_0 = 2/3$, $p_1 = 0$, $p_2 = 0$ $p_3 = 1/3$ while all the other probabilities are 0.

Problem 8 2004: One has that that the order of an element is either 2, q or $2q$. To check that the order is not 2 is fast, $a \neq \pm 1$. And a has order q if and only if a is a quadratic residue modulo p, which can be checked with the laws of quadratic residues. Here (a/b) denotes the Legendre or Jacobi symbol and the rules in section 5.4.2 are applied. $(213/10007) = (10007/213) = (209/213) = (213/209) = (4/209) = 1$ so 213 has order q. $(87/10007) = -(10007/87) = -(2/87) = -1$ so 87 has order $2q$.