Løsningsforslag eksamen 2001.

Problem 1 2001: Here (a/b) denotes the Legendre or Jacobi symbol and the rules in section 5.4.2 is applied. $(107/23927) = (23927/107) = (68/107) = (2/107)^2(17/107) = (5/17) = (2/5) = -1$, and hence the congruence $x^2 \equiv 107 (\mathrm{mod}\, 23929)$ is not solvable.

Problem 2 2001: Applying $\log_a$ to these equations one gets the linear system of congruences:

$$\begin{aligned} 2x + 3y &\equiv 5 (\mathrm{mod}\, 190) \\ 11x + 31y &\equiv 14 (\mathrm{mod}\, 190) \end{aligned}$$

where $x = \log_a b$ and $y = \log_a C$. Solving gives $x = 17$ and $y = 117$.

Problem 3 2001: $2373 = 3 \cdot 791$ so a solution of the equation $x^{12} = 2 (\mathrm{mod}\, 2373)$ is by the Chinese remainder theorem the same as a solution of the system of the two congruences $x^{12} \equiv 2 (\mathrm{mod}\, 3)$ and $x^{12} \equiv 2 (\mathrm{mod}\, 791)$. However, the first of these congruences has no solution since 2 is not a square modulo 3. So no solutions.

Problem 4 2001: Let the public part of the key used in this signature scheme be (p, α, β) and a the secret part. If message m_1 and m_2 get the same signature (γ, δ), the verifier calculates $\beta^\gamma \gamma^\delta \equiv \alpha^{m_1} \equiv \alpha^{m_2}$. Therefore (γ, δ) is accepted as a signature for both m_1 and m_2 if and only if $m_1 = m_2$.

Problem 5 2001: Let $m = p \cdot q$ and calculate $\gcd(3 \cdot 2^n - 1, m)$ for $n = 1, 2, ..., 1000$, which will lead to a factorization of m and breaking of the system.

Problem 6 2001: a) The order of the primitive element x is $2^{248} - 1 = (2^{16})^{15} 2^8 - 1$. So $2^{248} \equiv (2^4)^2 \equiv -1^2 \equiv 1 (\mathrm{mod}\, 17)$ and hence 17 divides the order of x and hence x^{17} is not a primitive element.

b) $2^{248} \equiv (2^{22})^{11} 2^6 \equiv 18 (\mathrm{mod}\, 23)$, and hence since 23 is a prime number, $\gcd(2^{248} - 1, 23) = 1$. Therefore x^{23} is a primitive element in the field.