**Norwegian University**
**of Science and Technology**
**Department of Mathematical Sciences**

Faglig kontakt under eksamen:
Kristian Gjøsteen, tlf. 73 59 35 20

lørdag 15. desember 2001
Kl. 9-14

Sensur: uke 2

Hjelpemidler: A

**Problem 1**
Number $m = 23929$ is prime. Determine without exhaustive search if the equation $x^2 \equiv 107 \mod m$ is solvable or not. Explain your reasoning.

**Problem 2**
Let $p = 191$ and $a$ be a primitive element of $\mathbb{Z}_p^*$. For $b, c \in \mathbb{Z}_p^*$ it was found that $a^7 b^8 c^{10} = a^2 b^{10} c^{13}$ and $a^{12} b^{23} c^{40} = a^{26} b^{12} c^9$. Find $\log_a b$, $\log_a c$. Write down your steps.

**Problem 3**
Find the number of solutions for $x^{12} \equiv 2 \mod 2373$. Explain your reasoning.

**Problem 4**
Describe ElGamal signature scheme. Explain why a change in the message would be detected and why Bob could not produce another message with Alice's signature (it is not possible to copy the signature).

**Problem 5**
For his RSA data Jim chooses a random $p < 2^{1000}$ and $q$ of the form $q = 3 \cdot 2^n - 1$, $500 < n < 1000$. Devise an attack on Jim's cryptosystem. Explain the steps of the attack and evaluate the number of operations needed to succeed.

**Problem 6**
Given a primitive polynomial $f(x)$ over $\mathbb{F}_2$ of degree 248.

a) Is $g(x) = x^{17}$ primitive? Why?

b) Is $h(x) = x^{23}$ primitive? Why?