Math 4440 Michael Soltys Final Exam May 6, 2008

1.	
2.	
3.	
4.	
5.	
6.	
7.	
8.	
9.	
10.	
Tot.	
for grader's use	

Name _____ Student No. _____

No aids allowed. Answer all questions on test paper. Use backs of sheets for scratch work. ***Show all your work; there will be no credit for answers without a justification.***

Total marks: 100 — ten questions, each worth 10.
Total time: 2 and 1/2 hours.

1. Show that for all $a, b \in \mathbb{N}$, there exist *unique* $q, r \in \mathbb{N}$ such that $a = qb + r$ where $0 \leq r < b$.
2. Prove **Fermat's Little Theorem**: If p is prime, and $\gcd(a, p) = 1$, then $a^{p-1} = 1 \pmod{p}$.
3. Describe the ElGamal public key cryptosystem.
4. Show that $(a) \iff (b)$:
   (a) "We can efficiently break ElGamal"
   (b) "We can efficiently break Diffie-Hellman"
5. (a) Present the Rabin-Miller algorithm for primality testing.
   (b) Let $n > 1$ be any natural number; if $a^{(n-1)} \neq 1 \pmod{n}$, then a is called a *witness* of compositness of n. Show that if at least one witness exists in $\mathbb{Z}_n^*$, then at least half of the elements of $\mathbb{Z}_n$ are witnesses.
6. Present the RSA public-key cryptosystem. Then, suppose that the two primes p, q are chosen close together; show how one might then break RSA efficiently.
7. Describe the ECDLP (Elliptic Curve Discrete Log Problem) and explain briefly why it seems to be a computationally infeasible problem.
8. Let $M_1, M_2, \ldots, M_n, C$ be a subset sum problem where the weights $M_1, M_2, \ldots, M_n$ are super-increasing. Assume that a solution $x = x_1 x_2 \ldots x_n \in \{0,1\}^n$ exists (i.e., $C = \sum_{i=1}^{n} x_i M_i$); describe an efficient algorithm to compute it, and then show that the algorithm is correct.
9. Explain how to construct a cryptosystem based on a super-increasing subset sum problem.
10. Describe the "Lattice Cryptosystem" based on the Closest Vector Problem (CVP).

End of Exam