Cryptography

Problem set 4 - 17-18 IV 2013

Problem 1 Prove that if G, H are groups then $G \times H$ is a group.

Problem 2 Let $N = pq$ and let $[N, e_1], [N, e_2]$ be public keys of Alice and Bob respectively. Show that if Eve sends encrypted messages to Alice $c_1 = m^{e_1} \bmod N$ and Bob $c_2 = m^{e_2} \bmod N$ and you intercept them then you can recover m from c_1 and c_2. What is the success probability of your attack?.

Problem 3 Let $N = pq$ be a product of two distinct primes. Show that if $\phi(N)$ and N are known, then it is possible to compute p and q in polynomial time.

Problem 4 Let $N = pq$ be a product of two distinct primes. Show that if N and an integer d such that $3d = 1 \bmod \phi(N)$ are known, then it is possible to compute p and q in polynomial time.

Problem 5 Determine whether or not the following problem is hard. Let p be prime, and fix $x \in \mathcal{Z}^*_{p-1}$. Given p, x, and $y := [g^x \bmod p]$ (where g is a random value between 1 and $p-1$), find g; *i.e.*, compute $y^{1/x} \bmod p$. If you claim the problem is hard, show a reduction (to *i.e.*, discrete logarithm problem). If you claim the problem is easy, present an algorithm, justify its correctness, and analyze its complexity.

Problem 6 Prove formally that the hardness of the Computational Diffie-Helman (CDH) problem relative to $\mathcal{G}$ implies the hardness of the discrete logarithm problem relative to $\mathcal{G}$.