MATH/CS 295: CRYPTOGRAPHY
HOMEWORK #6 ADDITIONAL PROBLEMS

Problem 2.A. In the Diffie-Hellman key exchange protocol, Alice and Bob choose a large prime p which they make public, but they break protocol to "add extra security" and when they choose a primitive root g for p, they keep it secret. Alice sends $x \equiv g^a \pmod{p}$ to Bob and Bob sends $y \equiv g^b \pmod{p}$ to Alice. Suppose Eve bribes Bob to tell her the values of b and y, but Eve cannot find out g. Show how Eve can determine g from the knowledge of p, y and b, under a reasonable hypothesis.