Assignment for Nov. 12th.

1. Suppose we have 98 people in a room. For each person \( x \), let \( f(x) \) be the last four digits of \( x \)'s Social Security Number. Calculate the probability that \( f(x) = f(y) \) for some pair \( x \neq y \) in the room? (Hint: It's less that forty percent.)

2. Given the same room full of 98 people, let \( g(x) = 2^{f(x)} \pmod{191} \) with \( f(x) \) as defined in problem 1. What is the probability that \( g(x) = g(y) \) for \( x \neq y \) in the room? Explain your answer.

3. Suppose Bob's Elgamal public code is \( p = 3948771024761 \), his primitive root is \( \alpha = 138331186077 \) and key \( \beta = \alpha^a = 1724172158218 \) (where \( a \) is secret). He wants to send the message 298398711 to Alice – and sign it.

   He supposedly sends \((m, r, s) = (298398711, 2560116850843, 342851724060)\) where \( r = \alpha^k \) (and \( k \) is another secret exponent) and \( s = (m - ar)/k \pmod{p - 1} \). Determine whether the message indeed came from Bob. (Yes or no.)

4. Suppose that Eve has somehow found that Bob's secret \( k \) (used above) was equal to 1231357701. Show that she can now determine his other secret exponent \( a \). What is it?

   Of what use will that information be to Eve in the current situation?