Introduction to Cryptography

Homework 4

Submission date: 16.1.2004

1. This question is about the baby-step giant-step method for computing discrete logarithms.

   Work in the group Z^*_{107}, i.e., the group of numbers co-prime to 103, with multiplication modulo 107 as the group operation.

   a. One of the numbers 2 and 3 is a generator of Z^*_{107}. Find which number it is. Explain your answer. In particular, explain how you compute each value. (It is not ok to write that you used a calculator to compute a^e modulo 103, for $e>35$, as most calculators don't compute such values correctly.)

   b. Compute the discrete logarithm of the last two digits of your id number in Z^*_{107}, to the base of the generator you found in Step (a). Explain your calculation. (If the last two digits of your id are 00, 01, or if the discrete log is 5 or smaller, compute the discrete log of the next two digits in your id number.)

2. Consider a generic t-out-of-n secret sharing scheme. Let v denote the number of possible values that the secret might have, and let w denote the number of possible values that each share might have. (For example, for Shamir's scheme over a field Zp, we have $v=w=p$.)

   Show that w must be larger or equal to v for any secret sharing scheme. (It then follows that the number of bits needed to represent a share cannot be smaller than the number of bits needed to represent the secret itself.)

   Hint: use the fact that $t-1$ shares must provide no information about the secret. I.e., no matter what are the values of the $t-1$ shares, any value should be possible for the secret.