Introduction to Cryptography

Solution of Homework 4

Question 1.

a. For every element g in the group it holds that $g^{106}=1$. If g is not a generator then there must be an exponent $e<106$ such that $g^{e}=1$. This exponent must divide 106 and therefore can be either 2 or 53. We should check whether $g^{2}=1$ or $g^{53}=1$. If both of these tests fail, g is a generator.

b. Use Shank's baby-step giant step algorithm. Let the last two digits of your id number be $0<=b<=99$. First compute the list $g,g^{2},\ldots,g^{11}$ (we therefore know the discrete log of the elements in this list.) Then compute the sequence of values $b,b\cdot g^{11}, b\cdot g^{2\cdot 11}, b\cdot g^{3\cdot 11},\ldots$ until you hit one of the elements in the list (this is guaranteed to happen for one the first 11 elements in this sequence). Suppose that we get that $b\cdot g^{i\cdot 11}=g^{j}$, where $1<=j<=11$. Then $b=j-i\cdot 11 \bmod 106$.

Question 2.

Consider any set of $t-1$ parties. These parties should have no information at all about the secret. In other words, each possible value for the secret should be equally likely.

Now, the value of the secret is fixed given the value of an additional share. The set of secrets that are computed as a function of the existing $t-1$ shares and the value of a new share must cover all the v possible value for the secret. Each value for the share results in a single value for the secret. Therefore there must be at least $w>=v$ possible values for the share.