Exercise sheet 7, 16 January 2020

1. Use Shamir's secret sharing to share $s = 5$ over $\mathbb{F}_{103}$ in an 3 out of 5 fashion. Verify for two sets of 3 users that you can recover the secret.

2. In Shamir's secret sharing there is a lot of trust on the party S that shares the keys. A malicious S could give invalid shares to some people, so that any group of t people involving at least one of them would compute the wrong secret. To prevent this, all parties insist on S publishing some extra information.

   Let S publish g^s and g^{f_i} for $1 \leq i < t$, where g is the generator of some large DH group. Show how participant j can verify that his share $(j, f(j)$ is correct given the information provided by S.

3. Let the DH secret a be shared in a t out of n fashion. Show how to compute g^{ab} given g^b and the shares, without recomputing s, i.e. using the shares locally.

4. Let the RSA secret key d be shared in a t out of n fashion. Show how to do RSA decryption using shares locally, i.e. without recovering the secret s.
   Note, this one is much harder than for DH.