T-79.159 Cryptography and Data Security **Spring 2004**
Tutorial 9
Thursday 1.4.2004 14.15, room T3.
Markku-Juhani O. Saarinen <mjos@tcs.hut.fi>

1. In a secret sharing scheme such as Shamir's polynomial system, how big should the field (i.e. modulus) be for good security ? What about threshold cryptosystems such as threshold ElGamal ?

2. Consider a group of 3 persons, Alice, Bob, and Carol. Each person encrypts all of his/her data with his/her personal key which has been somehow jointly generated. Try to come up with a very simple scheme that would allow any pair of two persons to jointly recover the key (and data) of the third person, should he/she get hit by a bus.

Hit by bus	Pair that can recover the key
Alice	Bob and Carol
Bob	Alice and Carol
Carol	Alice and Bob

3. Consider Shamir's threshold secret sharing scheme based on a 3-degree polynomial over $GF(10007)$. Five shares are:

$$\begin{aligned} f(1) &\equiv 1770 \pmod{10007} \\ f(2) &\equiv 9366 \pmod{10007} \\ f(3) &\equiv 9724 \pmod{10007} \\ f(4) &\equiv 1204 \pmod{10007} \\ f(5) &\equiv 2180 \pmod{10007} \end{aligned}$$

   How many shares are required to construct the polynomial – do you need them all ? If not, does it matter which ones you use ?

   What is the secret $f(0)$? Please give the polynomial as well.