T-79.159 Cryptography and Data Security **Spring 2003**
Tutorial 8
Tue 1.4.2003 12–14 T3 or Wed 2.4.2003 18–20 T1

1. Use the Shamir's $(3, 5)$ threshold scheme to share the secret 4321.

2. Suppose that you know the shares $(2, 19535)$, $(4, 1583)$ and $(5, 44146)$ of a Shamir's $(3, 5)$-threshold scheme over the field $\mathbb{Z}_{2^{16}+1}$. Compute the shared secret.

3. Consider Shamir's (t, n)-threshold scheme over the finite field $\mathbb{F}$. Let $f(x) = a_0 + a_1 x + \cdots + a_{t-1}x^{t-1} \in \mathbb{F}[x]$ be the polynomial used for sharing, and let (x_i, y_i), $i = 1, \ldots, t$ be distinct shares (not necessarily corresponding to the first t parties), where $y_i = f(x_i)$ and $a_0 = s$ is the secret.

   (a) Show that coefficients of f corresponds to a solution $a_0, \ldots, a_{t-1}$ of the linear system

   $$\begin{pmatrix} 1 & x_1 & x_1^2 & \cdots & x_1^{t-1} \\ 1 & x_2 & x_2^2 & \cdots & x_2^{t-1} \\ \vdots & \vdots & & \vdots & \\ 1 & x_t & x_t^2 & \cdots & x_t^{t-1} \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{t-1} \end{pmatrix} = \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_t \end{pmatrix} .$$

   (b) Show that the system in 3a always has exactly 1 solution. Thus, t of the parties can always recover the secret.

   (c) Show that $t - 1$ parties cannot learn anything about the secret.

   (d) Show that there for each set of t players exists a public reconstruction vector r such that $s = r \begin{pmatrix} y_1 & y_2 & \cdots & y_t \end{pmatrix}^t$.

4. Although the secrecy of Shamir's (t, n)-threshold scheme is perfect, the correctness of the reconstructed secret is not guaranteed. Consider what happens if

   (a) The dealer gives incorrect shares to some of the players.

   (b) Some of the parties submit incorrect shares to the reconstruction phase.

   Can you think of any simple way to detect these cases, if all the other participants collaborate?