

---

# SECRET SHARING SCHEMES

---

**CIS 400/628 — Spring 2005**  
**Introduction to Cryptography**

**This is based on Chapter 10 of Trappe and Washington**

# SECRET SPLITTING

## Problem

- ▶ I want to send Alice & Bob a message  $m \in \mathbb{Z}_n$
- ▶ **But** I want to be sure that the only way Alice & Bob can read  $m$  is if they both agree to unlock the message.

## Solution: Split the message

Pick  $r \stackrel{\text{ran}}{\in} \mathbb{Z}_n$ .

Send Alice  $r$ .

Send Bob  $(m - r) \bmod n$ .

- ▶ **Why does this work?**
- ▶ **How can we generalize this to  $k$  people?**

# SECRET SPLITTING, CONTINUED

## Problem

- ▶ We want to split a secret  $m \in \mathbb{Z}_n$  among  $w$  people  $\ni$
- ▶ If any  $t \leq w$  of them agree to open the secret, they can,
- ▶ **But**, if only  $t' < t$  of them agree, they cannot.

## THE SHAMIR THRESHOLD SCHEME

### Basic Idea

$t$  points determine a  $t - 1$  degree polynomial  $p$   
and  $p(0) = m$ .

# SHAMIR'S SCHEME, CONTINUED

## Setup

Pick a prime  $p$  larger than any possible message.

## Encoding the message

Choose  $s_1, \dots, s_{t-1} \stackrel{\text{ran}}{\in} \mathbb{Z}_p$

Set  $s(x) \stackrel{\text{def}}{=} m + s_1x + s_2x^2 + \dots + s_{t-1}x^{t-1} \pmod{p}$

## Distributing the secret

For  $i = 1, 2, \dots, w - 1, w$

Send person number  $i$  the pair  $(x_i, y_i)$  where

$x_i \stackrel{\text{ran}}{\in} \mathbb{Z}_p$  (but make sure  $i \neq j \implies x_i \neq x_j$ )

$y_i \stackrel{\text{def}}{=} s(x_i)$

# UNLOCKING THE SECRET, VERSION 1

$t$  folks get together

Their shared info is  $(x_1, y_1), \dots, (x_t, y_t)$ .

How do you reconstruct the polynomial?

We know

$$y_k = m + s_1 x_k^1 + s_2 x_k^2 + \dots + s_{t-1} x_k^{t-1} \pmod{p},$$

for  $k = 1, \dots, t$ .

So we solve the following for  $m, s_1, \dots, s_{t-1}$

$$\begin{pmatrix} 1 & x_1 & \dots & x_1^{t-1} \\ 1 & x_2 & \dots & x_2^{t-1} \\ \vdots & \vdots & & \vdots \\ 1 & x_t & \dots & x_t^{t-1} \end{pmatrix} \begin{pmatrix} m \\ s_1 \\ \vdots \\ s_{t-1} \end{pmatrix} = \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_t \end{pmatrix}.$$

The above is the **Vandermonde matrix**,  $V$ .

**FACT:**  $\det V = \prod_{1 \leq j < k \leq t} (x_k - x_j)$ .

This is  $= 0 \pmod{p}$  **iff**  $x_k = x_j$  for some  $k \neq j$ .

## UNLOCKING THE SECRET, VERSION 2

Shared info  $(x_1, y_1), \dots, (x_t, y_t)$ .

Let

$$X_k \stackrel{\text{def}}{=} \{1, \dots, t\} - \{k\}$$
$$\ell_k(x) \stackrel{\text{def}}{=} \prod_{i \in X_k} \left( \frac{x - x_i}{x_k - x_i} \right) \pmod{p}$$

Note  $\ell_k(x_k) = 1$  and, when  $j \neq k$ ,  $\ell_k(x_j) = 0$ .

### The Lagrange Interpolation Polynomial

$$p(x) = \sum_{k=1}^t y_k \ell_k(x) \quad \leftarrow \text{degree } t - 1$$

Note  $p(x_i) = y_i$  for  $i = 1, \dots, t$  (Why?)

$$\therefore s(x) = p(x) \text{ and } M = \sum_{k=1}^t y_k \prod_{i \in X_k} \left( \frac{-x_i}{x_k - x_i} \right) \pmod{p}.$$

# BLAKLEY'S SECRET SHARING SCHEME

## Basic Ideas for $(w, 3)$

- ▶ Go 3D.
- ▶ Give each person a plane  $\ni$  any three planes share only a single pt. =  $M$

## Setup

- ▶  $p$ , a prime
- ▶  $x_0 \in \mathbb{Z}_p$ , a secret
- ▶  $y_0, z_0 \stackrel{\text{ran}}{\in} \mathbb{Z}_p$
- ▶  $Q = (x_0, y_0, z_0)$ , a point

## For each person

- ▶ Choose  $a, b \stackrel{\text{ran}}{\in} \mathbb{Z}_p$
- ▶ Compute  $c \equiv z_0 - a \cdot x_0 - b \cdot y_0 \pmod{p}$   
 $z = a \cdot x + b \cdot y + c$  is a plane.

What is the picture?

For  $(w, t)$  with  $t > 3$ , go  $t$ D.