Introduction to Cryptography

Chapter 6: Secret sharing

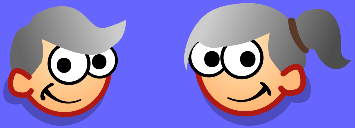
Manuel

Summer 2017

Outline

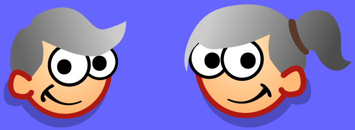
1. General setup
2. Shamir threshold scheme
3. Blakley's scheme

Intuition



Bob and Alice are now old, famous, and rich

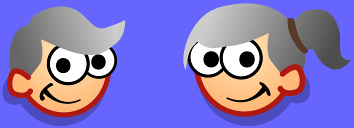
Intuition



Bob and Alice are now old, famous, and rich

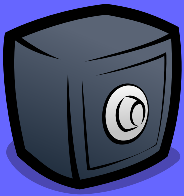
Their mean family wants to get all their money

Intuition



Bob and Alice are now old, famous, and rich

Their mean family wants to get all their money



- All their money is in a safe
- Only them know the secret combination
- They want to teach their family cooperation
- They split the combination such that they need to be at least three to reconstruct it

Simple secret splitting

Sharing a secret m between two people:

- Generate a random integer r
- Give r to a user and $m - r$ to the other

Simple secret splitting

Sharing a secret m between two people:

- Generate a random integer r
- Give r to a user and $m - r$ to the other

The idea easy extends to the general case of n people:

- Take $l > m$
- Generate $n - 1$ random integers, $r_1, \ldots, r_{n-1}$ between 1 and l
- Select $n - 1$ persons and give each an r_i, $1 \leq i < n$
- Give the remaining person $m - \sum_i^{n-1} r_i$

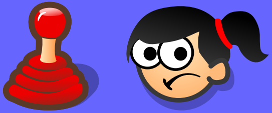
More refined setup

In the previous secret splitting strategy all the participants must be together in order to reconstruct the secret m. At times it might be desirable that only a subset of the people is able to reconstruct it.

More refined setup

In the previous secret splitting strategy all the participants must be together in order to reconstruct the secret m. At times it might be desirable that only a subset of the people is able to reconstruct it.

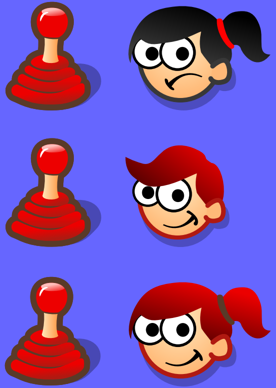
Example.



More refined setup

In the previous secret splitting strategy all the participants must be together in order to reconstruct the secret m. At times it might be desirable that only a subset of the people is able to reconstruct it.

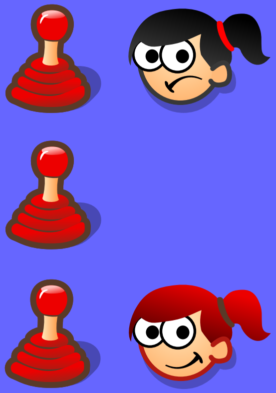
Example.



More refined setup

In the previous secret splitting strategy all the participants must be together in order to reconstruct the secret m. At times it might be desirable that only a subset of the people is able to reconstruct it.

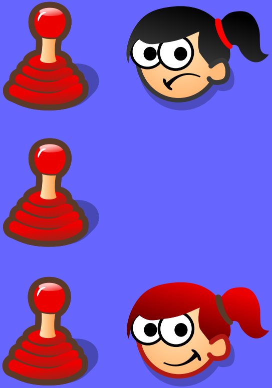
Example.



More refined setup

In the previous secret splitting strategy all the participants must be together in order to reconstruct the secret m. At times it might be desirable that only a subset of the people is able to reconstruct it.

Example.



Secret sharing

Definition

Let t and w be two integers such that $t \leq w$. A (t, w)-*threshold scheme* is a way to share a secret m among w people, such that any subset of at least t participants can reconstruct m, while no smaller subset is able to do it.

In practice, (t, w)-threshold schemes constitute a basic building block for many applications where information need to be shared among many users. For instance they can be used for broadcasting.

Outline

1. General setup
2. Shamir threshold scheme
3. Blakley's scheme

Basics on the scheme

Shamir threshold scheme was invented by Shamir in 1979

- Choose a prime p larger than the number of participants and the secret m
- Split m among w people such that t persons can reconstruct it
- Choose $t-1$ random integers, $r_1, \ldots, r_{t-1}$ mod p and define

$$S(X) = m + r_1 X + \cdots + r_{t-1} X^{t-1} \bmod p$$

- Give each participant a pair (x_i, y_i), with $y_i \equiv S(x_i) \bmod p$
- Keep $S(X)$ secret

If t people get together and share their pairs they can recover m

Recovering the secret

Lets see how t people can recover m

- Assume the t participants have the pairs $(x_1, y_1), \ldots, (x_t, y_t)$
- They can derive the following expression

$$\underbrace{\begin{pmatrix} 1 & x_1 & \cdots & x_1^{t-1} \\ 1 & x_2 & \cdots & x_2^{t-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & x_t & \cdots & x_t^{t-1} \end{pmatrix}}_{V} \begin{pmatrix} m \\ r_1 \\ \vdots \\ r_{t-1} \end{pmatrix} \equiv \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_t \end{pmatrix} \mod p \qquad (6.1)$$

- V is the Vandermonde matrix, which has determinant

$$\det V = \prod_{1 \leq j \leq k \leq t} (x_k - x_j)$$

- Eq. (6.1) has a unique solution when V is invertible
- From theorem 1.34, V is invertible if $\det V \not\equiv 0 \mod p$, i.e. for all k and j, $x_k \not\equiv x_j \mod p$

Example

We want to construct a (3,8)-threshold scheme to protect the secret message "secret", which corresponds to $m = 190503180520$.

We choose $p = 1234567890133$ to be larger than m and 8, and generate $r_1 = 482943028839$ and $r_2 = 1206749628665$. Then the polynomial of concern is

$$S(X) = 190503180520 + 482943028839X + 1206749628665X^2.$$

We now distribute the pairs (x_i, y_i), with $1 \leq i \leq 8$:

x_i	y_i	x_i	y_i
1	645627947891	5	675193897882
2	1045116192326	6	852136050573
3	154400023692	7	973441680328
4	442615222255	8	1039110787147

Example

If 2, 3, and 7 want to recover the message they construct

$$\begin{pmatrix} 1 & 2 & 4 \\ 1 & 3 & 9 \\ 1 & 7 & 49 \end{pmatrix} \begin{pmatrix} m \\ r_1 \\ r_2 \end{pmatrix} \equiv \begin{pmatrix} 1045116192326 \\ 154400023692 \\ 973441680328 \end{pmatrix} \bmod 1234567890133.$$

This yields

$$(m, r_1, r_2) = 190503180520, 482943028839, 1206749628665.$$

What if only two participants try to reconstruct the m?

Example

If 2, 3, and 7 want to recover the message they construct

$$\begin{pmatrix} 1 & 2 & 4 \\ 1 & 3 & 9 \\ 1 & 7 & 49 \end{pmatrix} \begin{pmatrix} m \\ r_1 \\ r_2 \end{pmatrix} \equiv \begin{pmatrix} 1045116192326 \\ 154400023692 \\ 973441680328 \end{pmatrix} \text{ mod } 1234567890133.$$

This yields

$$(m, r_1, r_2) = 190503180520, 482943028839, 1206749628665.$$

What if only two participants try to reconstruct the m?

A quadratic polynomial is defined by three points, and more generaly a polynomial of degree n is defined by $n+1$ points. Therefore if two participants share their information they will still miss a point and as such will not be able to reconstruct the polynomial at discover m. Note that there are inifinite number of possibilities for this last point.

More advanced sharing

Problem: in a company a secret is split into eight shares. The boss decides eight employees should be required to recover the secret. However he also requests that only four managers or only two board members should be able to recover the secret.

More advanced sharing

Problem: in a company a secret is split into eight shares. The boss decides eight employees should be required to recover the secret. However he also requests that only four managers or only two board members should be able to recover the secret.

Solution: give each regular employee one share, two to managers, and four to board members. The problem is solved, but note that now one board member together with one manager and two employees can recover the secret.

More advanced sharing

Problem: two companies share a bank vault. They want a setup where four employees from the first company and three from the second are required to be together in order to reconstruct the secret combination.

More advanced sharing

Problem: two companies share a bank vault. They want a setup where four employees from the first company and three from the second are required to be together in order to reconstruct the secret combination.

Solution: as each company needs more than 4 or 3 shares, each one could reconstruct the whole secret by itself. The idea is then to write the secret $s = s_1 + s_2$, and give s_1 as a shared secret for the first company while s_2 becomes a shared secret for the second company. Each of them can apply Shamir threshold scheme to recover its part of the secret. Finally they only need to meet to totally recover the secret combination.

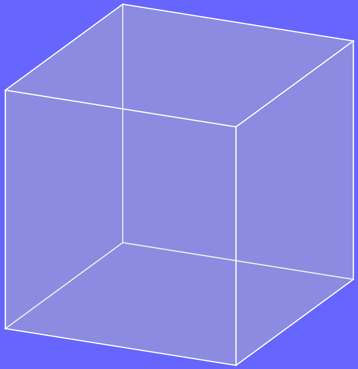
Outline

1. General setup

2. Shamir threshold scheme

3. Blakley's scheme

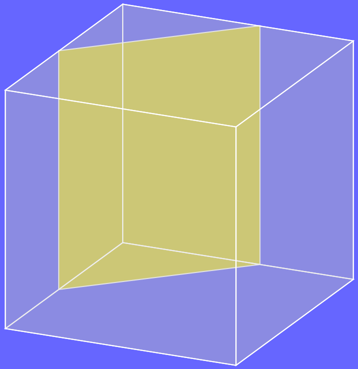
Basic idea



General rule:
In an n-dimensional space, n non-parallel hyperplane intersect at a specific point

Cryptographic view:
Give each user the equation of a hyperplane defined such that they all intersect at the secret m

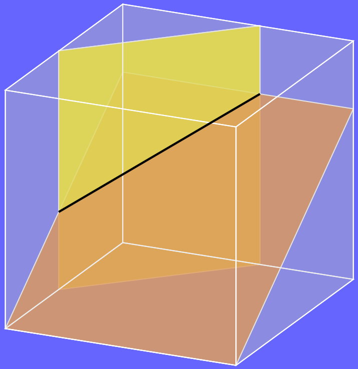
Basic idea



General rule:
In an n-dimensional space, n non-parallel hyperplane intersect at a specific point

Cryptographic view:
Give each user the equation of a hyperplane defined such that they all intersect at the secret m

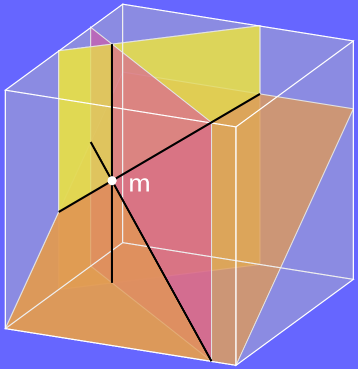
Basic idea



General rule:
In an n-dimensional space, n non-parallel hyperplane intersect at a specific point

Cryptographic view:
Give each user the equation of a hyperplane defined such that they all intersect at the secret m

Basic idea



General rule:
In an n-dimensional space, n non-parallel hyperplane intersect at a specific point

Cryptographic view:
Give each user the equation of a hyperplane defined such that they all intersect at the secret m

Practical setup

A 3-dimensional setup:

1. Choose a large prime p
2. Set x_s to the secret value
3. Select two random values y_s and z_s and define $m = (x_s, y_s, z_s)$
4. Consider the 3-dimensional space mod p
5. Give each participant i a plane passing by m:
    - Generate two random integers mod p, a_i and b_i
    - Define $c_i \equiv (z_s - a_i x_s - b_i y_s) \bmod p$
    - The equation of the plane is $z = a_i x + b_i y + c_i$

Recovering the secret

In a 3-dimensional setup three people can deduce the secret x_s:

- Each participant has a plane

$$a_i x + b_i y + c_i \equiv z \bmod p, \quad 1 \leq i \leq 3$$

- They construct the matrix equation

$$\underbrace{\begin{pmatrix} a_1 & b_1 & -1 \\ a_2 & b_2 & -1 \\ a_3 & b_3 & -1 \end{pmatrix}}_{M} \begin{pmatrix} x_s \\ y_s \\ z_s \end{pmatrix} \equiv \begin{pmatrix} -c_1 \\ -c_2 \\ -c_3 \end{pmatrix} \bmod p$$

- If $\det M$ is invertible mod p then the system of equations can be solved and x_s can be recovered

Example

Let $p = 73$, and suppose five people are given the following shares

$$\begin{cases} A: & z = 4x + 19y + 68 \\ B: & z = 52x + 27y + 10 \\ C: & z = 36x + 65y + 18 \\ D: & z = 57x4 - 12y + 16 \\ E: & z = 34x + 19y + 49 \end{cases}$$

A, B, and C decide to recover the secret:

$$\begin{pmatrix} 4 & 19 & -1 \\ 52 & 27 & -1 \\ 36 & 65 & -1 \end{pmatrix} \begin{pmatrix} x_s \\ y_s \\ z_s \end{pmatrix} \equiv \begin{pmatrix} -68 \\ -10 \\ -18 \end{pmatrix} \bmod 73$$

The solution yields $x_s = 42$, $y_s = 29$, and $z_s = 57$

Blakley vs. Shamir

Blakley's scheme

- Matrix M not always invertible
- Hard to select $a_i,\ b_i$, and c_i for M to be always invertible
- More general setup
- Much information carried by each participant $(a_i,\ b_i,\cdots)$

Shamir's threshold scheme

- Matrix V is invertible, as long as no two shares are congruent mod p
- Method can be view as a particular case of Blakley
- Little information carried by each participant (x_i, y_i)

Key points

- Explain what is secret sharing
- Describe Shamir's threshold scheme
- What is the key idea behind Blakley's scheme?
- Provide several examples where secret sharing is useful

Thank you!