Shared Secret Cryptography

Presentation by James Ragucci

Scenarios

- Pepsi executives want to have access to “secret formula” in case of emergency.
  - requirements
    - 6 directors or 3 vice presidents or 1 president
    - espionage resistant

Image: http://en.wikipedia.org/wiki/Pepsi

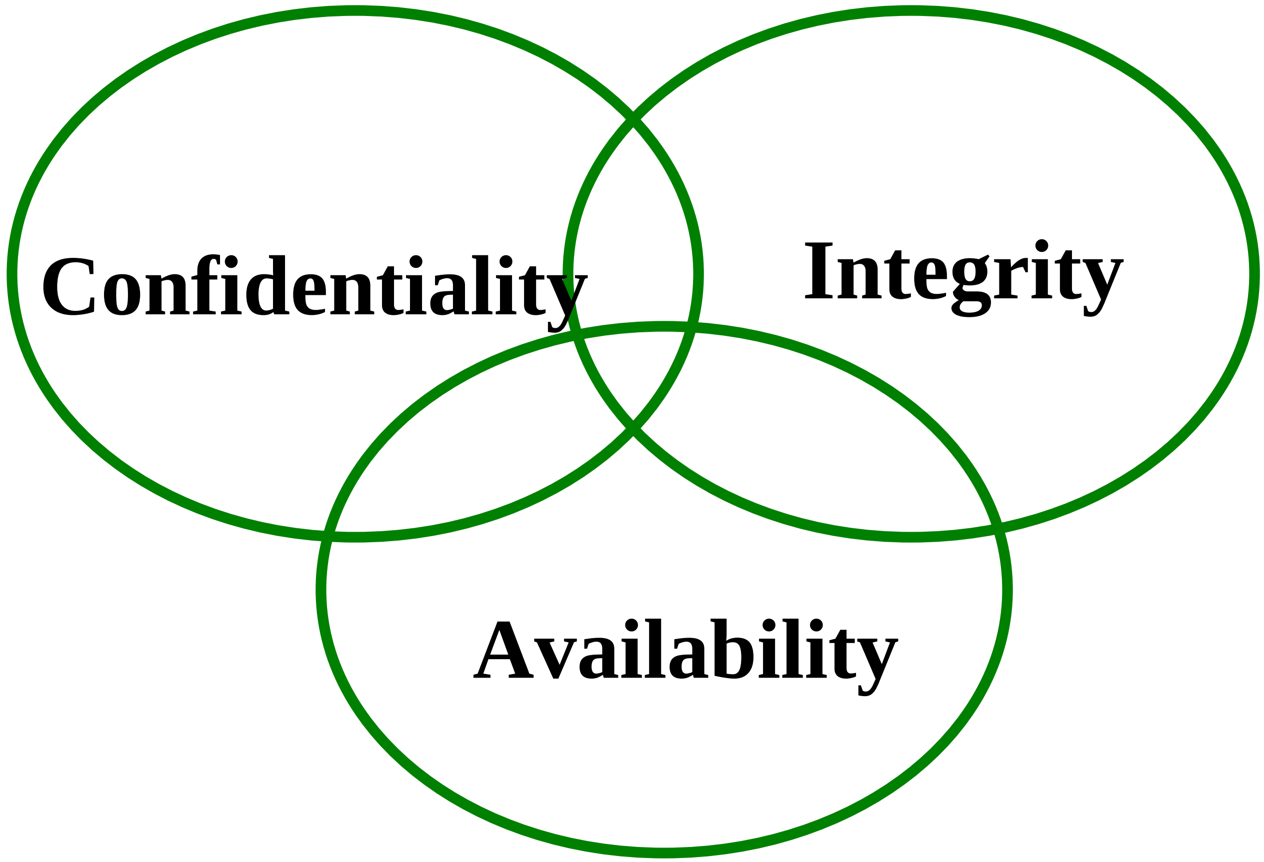
Another Scenario

- How to backup of your RSA private key.
  - second computer?
  - trust your friends with a copy of your private key?

Common Objective?

- Is it possible to store data amongst multiple semi-trusted people/nodes in a manner that doesn’t violate any of the three cornerstones of information security?

Assures C.I.A.



Solution: Shared Secret Cryptography

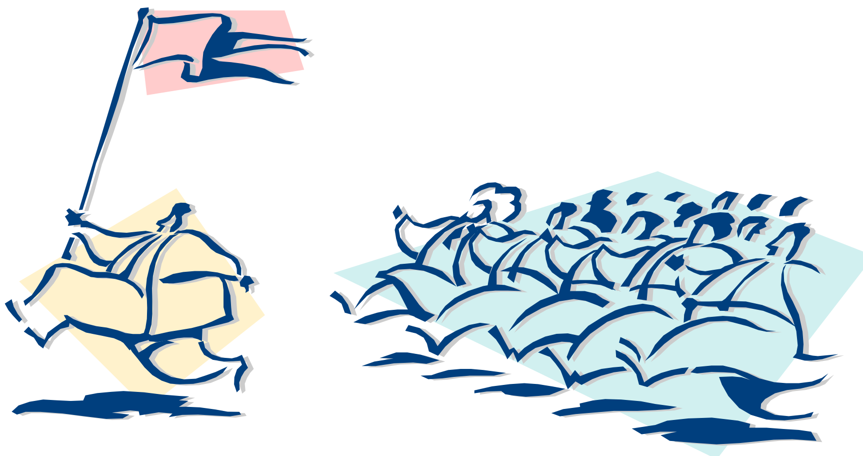
- Method of distributing a secret amongst multiple participants.
- Each participant holds a unique secret
- Secret reconstruction needs some of the pieces

Threshold Scheme Notation (n,t)

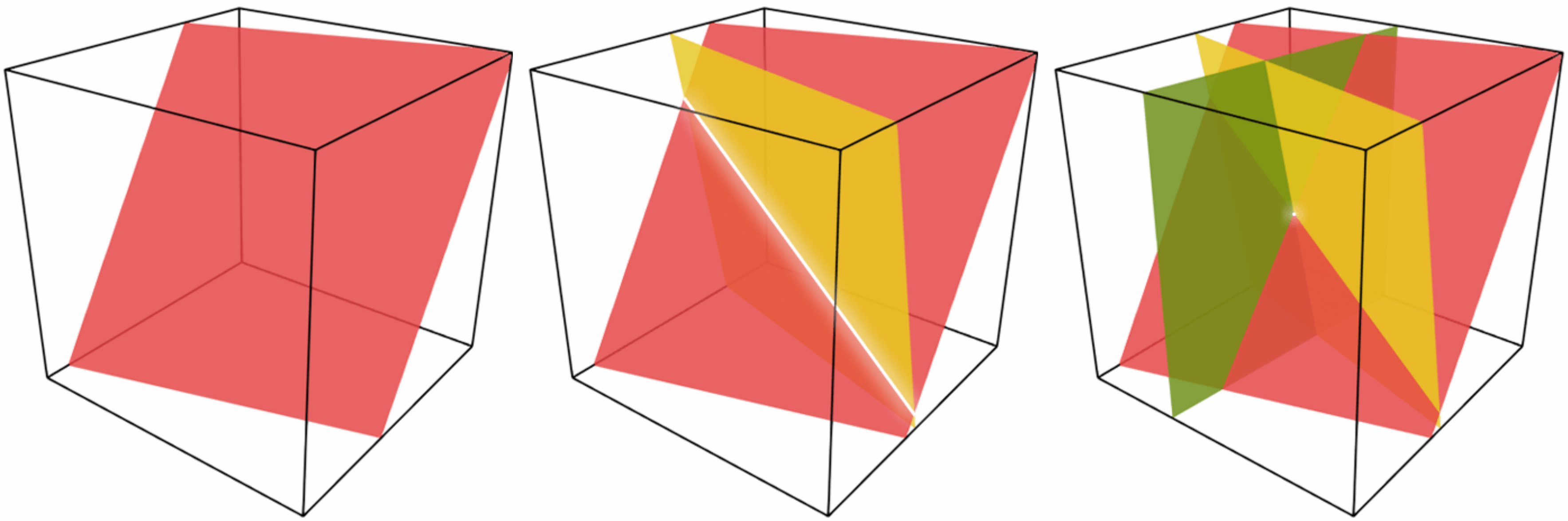
- Where n and t are positive integers.
- n is number of secrets generated
- t is amount of overall secrets needed to recover message
- t is less than or equal to n or else message is irretrievable

Why is this needed?

- **Protect data = encryption**
- **Protect key?**
- **Most secure scheme keep to keep a key**
  - **Computer**
  - **Human Brain**
  - **Safe**
- **Reliability/robustness:**
  - Key lost, can be reconstructed from the distributed parties



Secret Sharing Algorithms: Blakley's scheme



- Data located on intersection of hyperplanes
- Not too space efficient.
- Insider knows that the point lies in his plane (hence this scheme is not perfect)

Images from : http://en.wikipedia.org/wiki/Secret_sharing

Blakley's scheme: Described

- Pick a prime p.
- Create a point $Q(x_0, y_0, z_0)$ such that
  - Let x_0 be the secret.
  - Choose y_0, z_0 randomly mod p.
- Pick a,b, randomly mod p then set:

$$c \equiv z_0 - ax_0 - by_0 (mod P)$$

- Plane is $z=ax+by+c$

Blakley's scheme: Reassembly

- $a_i x + b_i y - z \equiv -c_i \pmod p$, $1 \leq i \leq 3$
- Yields matrix equation:

$$\begin{pmatrix} a_1 & b_1 & -1 \\ a_2 & b_2 & -1 \\ a_3 & b_3 & -1 \end{pmatrix} \begin{pmatrix} x_0 \\ y_0 \\ z_0 \end{pmatrix} \equiv \begin{pmatrix} -c_1 \\ -c_2 \\ -c_3 \end{pmatrix} \; mod\, p$$

- As long as determinant of matrix is nonzero mod p, matrix can be inverted and the secret found
- Row operations work as well

Blakley's Scheme Example

- Let p=73
- Suppose A-E are as follows:
  - A: z=4x+19y+68
  - B: z=52x+27y+10
  - C: z=36x+65y+18
  - D: z=57x+12y+16
  - E: z=34x+19y+49
- Convert A, B, C to:

$$\begin{pmatrix} 4 & 19 & -1 \\ 52 & 27 & -1 \\ 36 & 65 & -1 \end{pmatrix} \begin{pmatrix} x_0 \\ y_0 \\ z_0 \end{pmatrix} \equiv \begin{pmatrix} -68 \\ -10 \\ -18 \end{pmatrix} (mod\, 73)$$

$$\text{solution is } (x_0,\ y_0,\ z_0) = (42{,}29{,}57)$$

$$x_0 = 42$$

Blakley's Scheme Problems

- Not too space efficient.
- Insider knows that the point lies in his plane (hence this scheme is not perfect)

Secret Sharing Algorithms: Shamir's scheme

- Single variable polynomial of degree t-1 is uniquely identified by t different points
- Stores the secret as the Y-intercept of the polynomial
- Reconstructs the secrets using interpolation.
- Polynomial evaluated at 0 for secret generation.

Shamir's scheme - Continued

- With less than t shares the polynomial can’t be reconstructed.
- Think of the polynomial as an equation with t variables (the coefficients), we need at least t linearly independent equations in order to solve the equation.

Shamir's Scheme

- Dealer secretly choose elements

$$a_j \in \mathbb{Z}/p\mathbb{Z} \ , \ 1 \leq j \leq t-1$$

- Constructs polynomial:

Let $s \in \mathbb{Z}/p\mathbb{Z}$ be the secret.

$$a(X) = s + \sum_{j=1}^{t-1} a_j X^j$$

Degree $\leq$ t-1

- Dealer computes and distributes the shares $y_i = a(x_i)$, $1 \leq i \leq n$

Shamir Scheme in Action

$n = 5$, $t=3$, $p=17$, $s = 3$, $x_i=i$, $1 \le i \le 5$, $a_i=15$ & 14

$$a(X)=15X^2+14X+3$$

Shares are

$y_1=a(1)=15$ $y_4=a(4)=10$

$y_2=a(2)=6$ $y_5=a(5)=6$

$y_3=a(3)=10$

Secret Sharing Algorithms: Shamir's scheme

- Reconstruction Uses Lagrange Interpolation
  - use individual pieces to rebuild polynomial.
  - Once rebuilt calculate f(0)

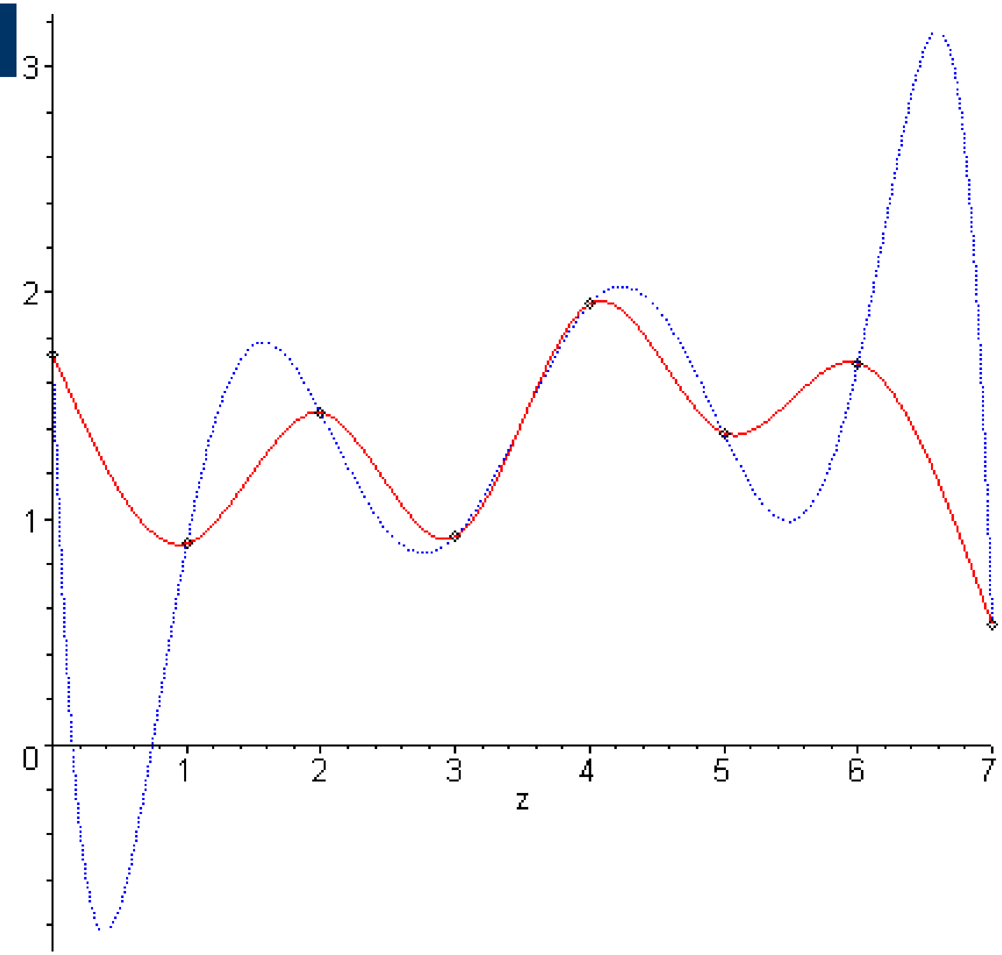


Image from:http://web.mat.bham.ac.uk/D.F.M.Hermans/msmxg6/ln/lnotes89.html

Reconstruction Formula

$$s = a(0) = \sum_{i=1}^{t} y_i \left(\prod_{j=1, j \neq i}^{t} \frac{x_j}{x_j - x_i} \right) mod\, p$$

$$a(0) = (15\frac{6}{2} + 6\frac{3}{-1} + 10\frac{2}{2}) mod\, 17 = 3$$

Properties of Shamir’s scheme [3]

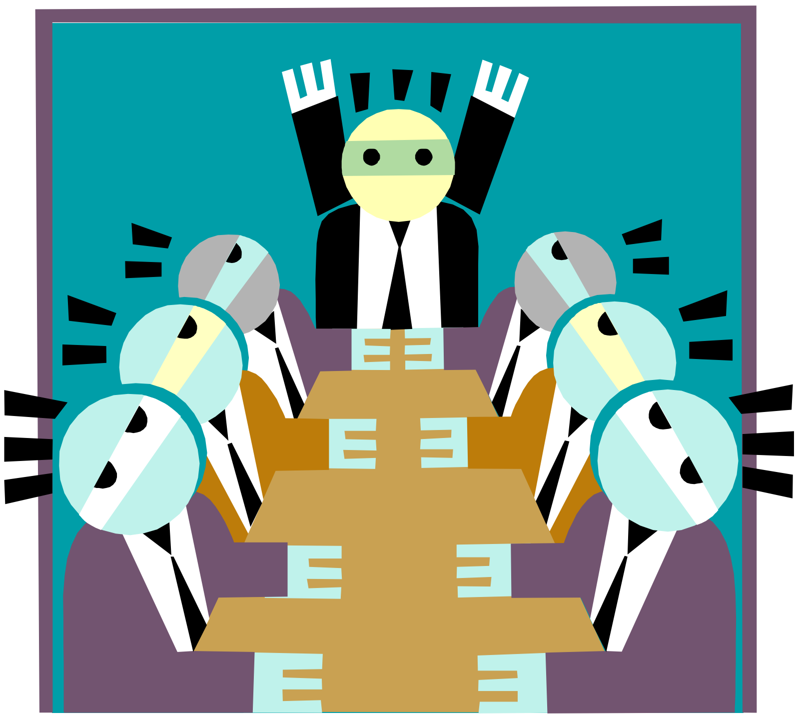
- 1. ***perfect:*** Given knowledge of any k − 1 or fewer shares, all values [0,p) of the shared secret remain equally probable

Lemma 15.2.4 *For any $s' \in \mathbb{Z}/p\mathbb{Z}$ there are exactly p^{t-m-l} polynomials $a'(X) \in \mathbb{Z}/p\mathbb{Z}[X]$ of degree $\leq t-1$ with $a'(0) = s'$ and $a'(x_i) = y_i$ $1 \leq i \leq m$.*
Let $s \in \mathbb{Z}/p\mathbb{Z}$ be the secret.

Properties of Shamir’s scheme [3] continued

- 2. ***ideal:*** The size of one share is the size of the secret
  - No extra information is provided beyond the size of the secret.

Properties of Shamir's scheme [3] continued



- 3. ***extendable:*** *for new users*. New shares (for new users) may be computed and distributed without affecting shares of existing users.
  - Application works for deletion as well.

Properties of Shamir’s scheme [3] continued

4. ***varying levels of control possible***: Providing a single user with multiple shares bestows more control upon that individual.

Properties of Shamir’s scheme [3] continued

5. ***no unproven assumptions*****:** Unlike many cryptographic schemes, its security does not rely on any unproven assumptions (e.g., about the difficulty of number-theoretic problems).

One Last Scenario

- Company A and B jointly share a bank vault.
- Want a system of opening vault so that
  - 4 A employees are present
  - 3 B employees are present
- How?

References

1. Shamir, A. How to share a secret, Communications of the ACM, v.22 n.11, p.612-613, Nov. 1979
2. Knuth, D. The Art of Computer Programming, Vol. 3: Seminumerical Algorithms. Addison-Wesley, Reading, Mass., 1997.
3. A. Menezes, P. vanOorschot, and S. Vanstone, "Handbook of Applied Cryptography," CRC Press, 1996.
4. G. Caronni and M. Robshaw, "An Introduction to Threshold Cryptography," in *CryptoBytes*. vol. 2.3, 1997, pp. 7-12.
5. Trappe, W. and C. Lawrence “Introduction to Cryptography: With Coding Theory.” Pearson, Washington 2nd ed., 2006