Secret Sharing Schemes

- Databases
- Money vaults in banks
- Weapons of mass destruction (WMD)

Access Protocol

- President
- CEO
- Any two VPs (*n* is the total number of VPs)
- Any VP and a Manager
- Any 3 Managers (*m* is the total number of Managers)

Let a Secret Access Key (SAK) consist of three parts: {*a;b;c*}

*Example*1: secret key *K*=314159265={3001002;1005006;4009005}

The Algorithm

1. Consider a quadratic equation $Y=aX^2+bX+c$
2. Consider points *P*(0); *P*(1); *P*(2); *P*(3);…; *P*(*s*), where

   s=*m*+*n*: *P(k)*=(*X(k)*,*Y(k)*);
3. For every *k* (*X(k)*, *Y(k)*) satisfies the quadratic eqn;
4. Assign {*P*(1); *P*(2); *P*(3)} to the President;
5. Assign {*P*(1); *P*(2); *P*(3)} to the CEO;

6. Assign $\{P(0); P(k)\}$ to k-th VP
7. Assign $\{P(n+i)\}$ to i-th Manager
8. Consider a combination of three points $\{P(j); P(q); P(t)\}$ $\{j; q; t$ are distinct integers between 0 and $s\}$;
9. Solve the system of <u>*linear*</u> equations where p, h, d are unknowns:

$$X(j)^2p+X(j)h+d=Y(j)$$

$$X(q)^2p+X(q)h+d=Y(q)$$

$$X(t)^2p+X(t)h+d=Y(t)$$

10. If $p=a; h=b; d=c$, then access is granted

Example2: n=3; *m*=4.

- Let *a*=1; *b*=2; *c*=5.
- Consider a function $Y=f(X)=X^2+2X+5$
- Let $X(0)=0$; and for $i=1,2,3,\ldots$ $X(2i-1)=i$; $X(2i)=-i$;

  i = 1; x(2*1-1)=i=1; x(2*1)=-1;

  i = 2; x(2*2-1)=x(3)=2; x(2*2)=x(4)=-2

k	0	1	2	3	4	5	6	7
X(k)	0	1	-1	2	-2	3	-3	4
Y(k)	5	8	4	13	5	20	8	29

- Let the combination of points be {$P(0)$; $P(2)$ and $P(4)$}
- Solve the system of linear equations:

$$d=5; \quad p-h+d=4; \quad 4p-2h+d=5$$

Solution: $d=5$; $p=1$; $h=2$

Consider combination of the 3rd VP and 4th manager

Example:

3rd VP = {P(0); P(3)} = {(0,5);(2,13)}

4th manager = {P(3+4)} = {P(7)} = {(4,29)}

{(0,5);(2,13); (4,29)}

$[0^2]p+[0]h+d=5$

$[2^2]p+[2]h+d=13$

$[4^2]p+[4]h+d=29$

$d=5$

$4p+2h+5=13$

$16p+4h+5=29$