Problem 1

Construction like 3.3

$M = \{0,1\}^\lambda$

$t = n$

n = total shares

Share(m):

$s_1 \leftarrow \{0,1\}^\lambda$

$s_2 \leftarrow \{0,1\}^\lambda$

$\vdots$

$s_{n-1} \leftarrow \{0,1\}^\lambda$

$s_n := s_1 \oplus s_2 \oplus \cdots \oplus s_{n-1} \oplus m$

return $(s_1, \ldots, s_n)$

reconstruct

return $(s_1 \oplus \cdots \oplus s_n)$

This is our n out of n sharing scheme.

We would prove this n out of n sharing scheme is secure but comparing it with a Random algorithm

S_{Real}

Query $(m \in \{0,1\}^\lambda)$:

$s_1 \in \{0,1\}^\lambda$ } Choose uniformly Random

$\vdots$

$s_{n-1} \in \{0,1\}^\lambda$

$K := s_1 \oplus \cdots \oplus s_{n-1}$

$s_n := K \oplus m$

return $(s_1, s_2, \ldots, s_n)$

$K \in \{0,1\}^\lambda$

$Pr[K] = \frac{1}{2^\lambda}$

$s_n \in \{0,1\}^\lambda$

$Pr[s_n] = \frac{1}{2^\lambda}$

S_{Random}

Query $(m \in \{0,1\}^\lambda)$:

$s_1 \leftarrow \{0,1\}^\lambda$

$\vdots$

$s_{n-1} \leftarrow \{0,1\}^\lambda$

$s_n \leftarrow \{0,1\}^\lambda$

return $(s_1, s_2, \ldots, s_n)$

$Pr[s_n] = \frac{1}{2^\lambda}$

In both case $\forall i \in \{1,n\}$ $Pr[s_i] = \frac{1}{2^\lambda}$

Thus $S_{Real} \equiv S_{Random}$.

CaS 538

3.8 Suppose there are 5 people on a committee: Alice (President), Bob, Charlie, David, Eve. Suggest how they can securely share a secret so that it can only be opened by:

- requirement
  i) Alice & any other person together can open the message
  ii) Any three people

Algorithm

⇒ We can use shamir's Secret Method here.

We will use $(6, 3)$ shamir secret where president Alice will get two secrets whereas all other people will get only one secret per person.

Threshold would be $t = 3$ secrets and total secrets are 6.

$$S_i = f_0 + f_1 i + f_2 i^2$$

Alice will get two of these.

S_1 and S_2

All others will get only one secret only.

Alice's share (message ↓)
$S_1 = f_0 + f_1 1 + f_2 1^2$
$S_2 = f_0 + f_1 2 + f_2 2^2$

Bob's share $S_3 = f_0 + f_1 3 + f_2 3^2$

Charlie's share $S_4 = f_0 + f_1 4 + f_2 4^2$

David's share $S_5 = f_0 + f_1 5 + f_2 5^2$

Eve's share $S_6 = f_0 + f_1 6 + f_2 6^2$

where f_0 = message $\in \{0, \ldots, P-1\}$

f_1, f_2 ← uniformly selected @ Random from $\{0, \ldots, P-1\}$

$S_1, S_2, \ldots S_6$ are all uniform Random Value

Reconstruct

To reconstruct you will need three secrets. So As Alice has two secrets, she can join with any one to open the message or any other three people with their Secret open the message
As we have three Unknowns, We need three equations to solve these linear Equations.

If these Systems of equation have a unique solution we can use linear Algebra to reconstruct the message.

$$\vec{S} \qquad A \qquad \vec{f}$$

$$\begin{bmatrix} s_1 \\ s_2 \\ s_3 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 2 & 4 \\ 1 & 3 & 9 \end{bmatrix} \begin{bmatrix} f_0 \\ f_1 \\ f_2 \end{bmatrix}$$

We Know

- We know A is invertible as this is Vandermonde Matrix.
- We also know this System of equation have a unique Sol^n as A is linearly Independent.

So,

$$A^{-1}\vec{S} = A^{-1}A\vec{f}$$

$$A^{-1}\vec{S} = I\vec{f}$$

$$A^{-1}\vec{S} = \vec{f}$$

So we get $\vec{f} = \begin{bmatrix} f_0 \\ f_1 \\ f_2 \end{bmatrix}$ f_0 is our message.

Alternatively, we can use Lagrange interpolation of Polynomial.

Problem 3

a) Describe Why a 6 out-of-9 threshold secret-Sharing Scheme does not suffice."

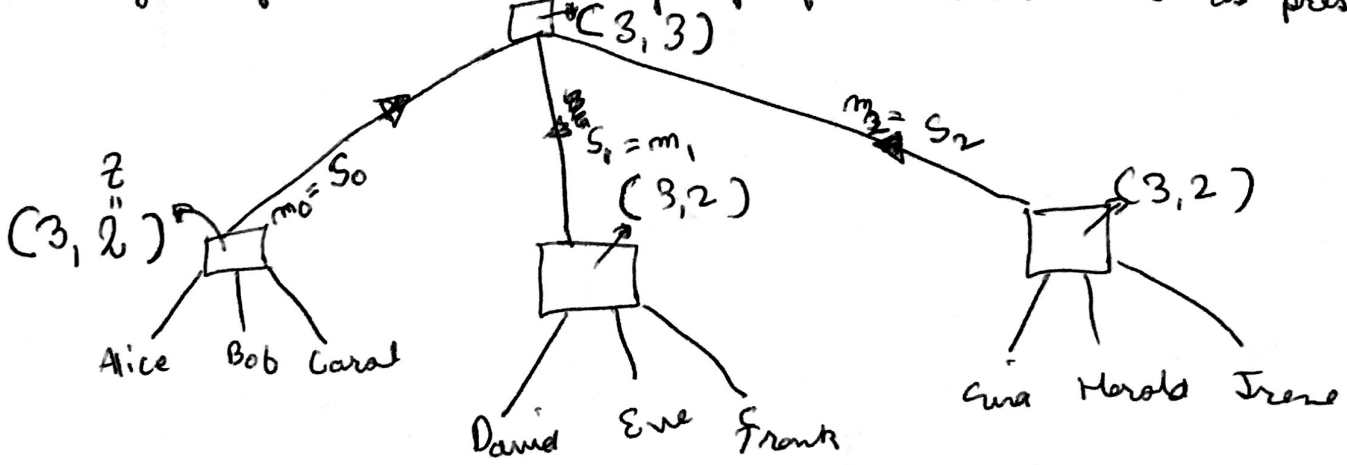
⇒ Counter Example.

If we select 6 people from two Subcommitte then one subcommitte would have no saying at all. The Constraint in the cryptosystem scheme says we need majority from all the group. The 6 people from Two group violets this constraint.

Hence,

6 out of 9 threshold secret-Sharing scheme does not suffice.

(6) Suggest how a dealer can share a secret, so that it can only be opened when a majority of each subcommittee is present.



Cahere (3, 2) is shamir Secret Sharing Scheme with 3 secrets and 2 threshold.

- We would have (3, 2) shamir Secret Sharing Scheme in all the Subcommitte. Now All groups will have three messages together which we can consider as S_0, S_1, S_2 for (3, 3) Scheme at the end.

After all the subcommittes have met their majority requirement we will combine messages from these three (3,2) scheme to create a final message in (3,3) scheme.

4a) if

$$x \equiv_{p-1} y \longrightarrow a^x \equiv_p a^y$$

$x = (p-1)K_x + r$

$y = (p-1)K_y + r$

$a^{p-1} \equiv_p 1$

$a^x \equiv_p a^{(p-1)Kx + r}$

$\equiv_p a^{(p-1)Kx} a^r$

$\equiv_p (a^{p-1})^{Kx} a^r$

$\equiv_p (1)\, a^r$

$\equiv_p a^r$

$a^y \equiv_p a^{(p-1)Ky + r}$

$\equiv_p (a^{p-1})^{Ky} a^r$

$\equiv_p 1\, a^r$

Hence,

$$\boxed{a^x \equiv a^y}$$

46) $g^x \equiv_p 1 \iff (p-1) \mid x$

If the forward proof:

$g^x \equiv_p 1$ Given, ⟶ Prove $(p-1) \mid x$

Suppose

$x \equiv_{p-1} r$

$x = (p-1)q + r$ where $0 \leq r < p-1$ ∴ Unique division theorem — (*)

Show $\boxed{r = 0}$,

$g^x = (p-1)q + r$

$g^x \equiv_p g^{(p-1)q + r}$

$\equiv_p 1 \; g^r$

$1 \equiv g^x \equiv g^r$

$g^r \equiv_p 1$ Hence r is either 0 or multiple of $(p-1)$

but we know $r < p-1$ from (*)

So $r = 0$

Hence

$x = (p-1)q + r$

$x = (p-1)q + 0$

$x = (p-1)q$ ⟺ Hence $\boxed{(p-1) \mid x}$

Now

$(p-1) \mid n \longrightarrow g^n \equiv_p 1$

$n = (p-1)q$

$g^n \equiv_p g^{(p-1)q}$

$\equiv_p \left(g^{(p-1)}\right)^q$

$\equiv_p (1)^q$

$\equiv_p 1$

$\boxed{g^n \equiv_p 1}$ //

(c) Show that if g is a generator, then the converse of part (a) also holds: if $g^x \equiv_p g^y$, then $x \equiv_{p-1} y$.

Given $g^x \equiv_p g^y$ ⟶ Prove $x \equiv_{p-1} y$

$g^{p-1} \equiv_p 1$ ∴ fermat's last theorem

$g^x \equiv_p g^y$

Divide both side by $\left(\frac{1}{g^y}\right)$ ∴ Inverse exist as this is mod p. Prime mod have inverses for all the elements.

$g^x g^{-y} \equiv_p g^y g^{-y}$

$g^{(x-y)} \equiv_p 1$

From (b) we know $p-1 \mid (x-y)$

So $p-1 \mid (x-y)$ is same as $\boxed{x \equiv_{p-1} y}$

(d)

$\langle g \rangle$

$a \equiv_p g^x$

Show

x is even $\longleftrightarrow$ a has a square root

First

x is even $\longrightarrow$ a has a square root

Given

$a \equiv_p g^x$

x is even so $x = 2n$

$a \equiv_p g^x \equiv_p g^{2n} \equiv_p (g^n)^2$

So Square root of $a = g^n$

Second

a has a square root $\longrightarrow$ x is even

Let root $s = g^y$ $\therefore$ s is a root of "a"

$(g^y)^2 \equiv_p a$ as it is a Square of some number

$\equiv_g x$

$g^{2y} \equiv_p g^x$

From 4C we know $2y \equiv_{p-1} x$

$p-1 \mid 2y - x$

$p-1$ is even

$2y$ is even

$(2y - x)$ has to be even as $(p-1)$ divides it

$(2y - x)$ is only even when x is even.

Thus x is even.

(e)

a) If a is a square $\longrightarrow a^{\frac{(p-1)}{2}} \equiv_p 1$

$(g^y)^2 \equiv_p a \equiv g^x$ — (*)

x is even from part d)

Let's analyze what $a^{\frac{p-1}{2}}$ is?

$a^{\frac{p-1}{2}} \equiv_p \left((g^y)^2\right)^{\frac{p-1}{2}}$ Replacing a for $(g^y)^2$ from (*)

- $\equiv_p \left((g^y)^x\right)^{\frac{p-1}{x}}$

$\equiv_p (g^y)^{p-1}$

$\equiv_p (g^{p-1})^y$

$\equiv_p (1)^y$

$\equiv_p 1$

e b) If a is non-square $\longrightarrow a^{\frac{p-1}{2}} \not\equiv_p 1$

Suppose,

$a^{\frac{p-1}{2}} \equiv_p 1$

We will solve this with <u>contradiction</u>

$a = g^x$

$x = 2n+1$

Please Turn Over

e''

$$1 \equiv a^{\frac{p-1}{2}} \quad \text{our assumption}$$

$$\equiv (g^{2n})^{\frac{p-1}{2}} \qquad a = g^n$$

$$\equiv (g^{2n+1})^{\frac{p-1}{2}}$$

$$\equiv_p (g^{2n} g)^{\frac{p-1}{2}}$$

$$\equiv_p (g^{2n \times \frac{p-1}{2}} \; g^{\frac{p-1}{2}})$$

$$\equiv_p ((g^{p-1})^n \; g^{\frac{p-1}{2}})$$

$$\equiv_p (1^n \; g^{\frac{p-1}{2}})$$

$1 \equiv_p g^{\frac{p-1}{2}} \implies$ Impossible

g being a primitive root. This is impossible. (generator) $\equiv_p 1^{(p-1)}$

Hence our assumption $a^{\frac{p-1}{2}} \equiv_p 1$ is false.

So we can say $a^{\frac{p-1}{2}} \not\equiv_p 1$

(f)

If $(g^x)^2 \equiv_p a \longrightarrow \left(g^{x+\frac{p-1}{2}}\right)^2 \equiv_p a$

let's evaluate $\left(g^{x+\frac{p-1}{2}}\right)^2 \bmod p$

$$\left(g^{x+\frac{p-1}{2}}\right)^2 \equiv_p \left(g^x\, g^{\frac{p-1}{2}}\right)^2 \equiv_p g^{2x}\left(g^{\frac{p-1}{2}}\right)^2$$

$$\equiv_p g^{2x}\, g^{p-1}$$

$$\equiv_p g^{2x}\, 1 \quad \therefore \text{fermat's last theorem}$$

$$\equiv_p \left(g^x\right)^2$$

$$\equiv_p a \qquad \text{as} \left(g^x\right)^2 \equiv_p a$$

- & Show $g^{\frac{p-1}{2}} \equiv_p 1$

$$\equiv \left(g^{p-1}\right)^2$$

$$\equiv 1^2$$

$$\equiv 1 \quad //$$

8) Show that if $p \equiv_4 3$, and a has a square root, then the value $a^{\frac{(p+1)}{4}} \bmod p$ is a square root of a.

To find if a value is square of a we can square the roots.

Hence

$$\left(a^{\frac{(p+1)}{4}}\right)^2 \equiv_p a^{\frac{p+1}{2}}$$

$$\equiv_p a^{\frac{p-1+2}{2}}$$

$$\equiv_p a^{\frac{p-1}{2}+\frac{2}{2}}$$

$$\equiv_p a^{\frac{p-1}{2}+1}$$

$$\equiv_p a^{\frac{p-1}{2}+1}$$

$$\equiv_p 1\ a^1$$

$$\equiv_p a$$

we see that a was really the squares of $\left(a^{\frac{p+1}{4}}\right)$