EL ÁRBOL HASH DE MERKLE
(MERKLE TREE)

¿QUÉ ES?
El árbol hash de Merkle es una **estructura de datos**. Fue propuesta en 1979 para asegurarse que los datos que se intercambian por la red no han sido alterados. Bitcoin usa versiones avanzadas de esta estructura de datos para sus transacciones.

¿CÓMO FUNCIONA?
Explicaré el funcionamiento con un ejemplo muy simple. Supongamos que vamos a transmitir la información "Juan Mena mata hoy". Se aplica una función de hash a cada palabra. Supongamos que la función hash consiste en sumar los valores ASCII de cada letra. Nota que esta es una mala función hash porque palabras con las mismas letras, como "mona" y "mano", tienen el mismo valor hash, pero sirve para ilustrar la idea. Como resultado, las palabras se transforman en:

- h("Juan")= 74+117+97+110=398
- h("Mena")=77+101+110+97=385
- h("mata")=109+97+116+97=419
- h("hoy")=104+111+121=336

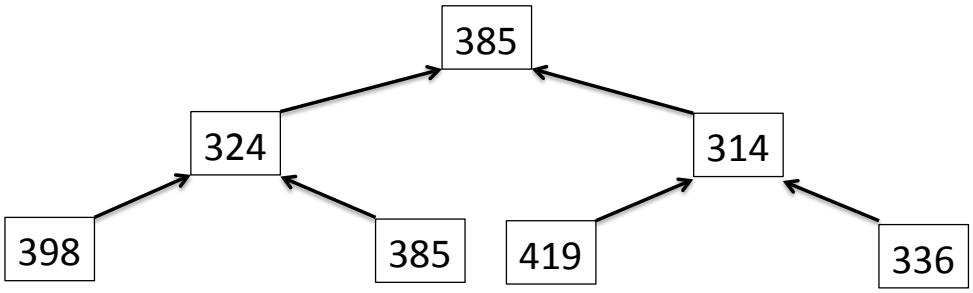
A continuación, se concatenan los pares de valores resultantes y se les vuelve a aplicar la función hash:

- h("398385")=51+57+56+51+56+53=324
- h("419336")=52+49+57+51+51+54=314

Finalmente, estos pares se concatenan y se les vuelve a aplicar la función hash:

- h("324314")=51+50+52+51+49+52=305

Estos valores se suelen visualizar de la siguiente manera:



A esta manera de visualizar una estructura de datos se la conoce como árbol. Sí, ya sé, no parece árbol (curiosidades de la ciencia de la computación). Imagínate un árbol invertido. Si te lo imaginas así, el primer nodo de arriba es la raíz y los últimos de abajo son las hojas (lo tengo claro, a este árbol le falta el tronco).
Para verificar que la información original no ha sido alterada, se manda la raíz del árbol hash de Merkle junto con la información. Si la raíz que recibes no es igual a la raíz que tu

calculas con la información recibida, entonces hubo un problema en la transmisión de los datos. También se puede mandar el árbol completo para revisar dónde ocurrió la alteración. En un árbol hash de Merkle real las hojas (que pueden ser bastante más que 4) suelen ser el hash de grandes bloques de datos o archivos completos.

¿Y AHORA QUÉ?

Ahora que ya saben de qué se trata el árbol hash de Merkle, vuestra misión es implementar un juego de salón cuya dinámica tenga como elemento central dicho árbol. El juego debe cumplir con las siguientes reglas:

1) Debe mezclar **azar y estrategia**. Es decir, una parte de las jugadas depende del azar (por ejemplo, se lanza un dado o se recoge una carta de un mazo) y otra parte requiere que de un poco de habilidad (conocimiento de cómo opera el árbol hash de Merkle). El Bingo es un juego de puro azar. Por más que juegues toda tu vida, no te haces mejor jugando Bingo porque nada depende de tu habilidad. El ajedrez por otra parte es pura estrategia. El Carioca en cambio, mezcla azar (las cartas que recibes son producto del azar) y estrategia (tu decides cómo jugar las cartas que te tocan).
2) Debe tener una breve historia donde se establezcan el **objetivo** del juego y las **reglas**. Alguien o algo en la historia de tu juego debe lograr un objetivo. El objetivo suele ser simple (debes cruzar una puerta, tomar una copa, salvar a un pueblo de la destrucción, etc), pero hay obstáculos que impiden conseguirlo tan fácilmente.
3) El objetivo y las reglas del juego deben caber en **una página**.

¿CÓMO NOS ORGANIZAMOS?

- **10.15-10.25:** Cada integrante del grupo, de manera individual, inventa un primer borrador de juego que luego presentará al grupo en no más de 1 minuto.
- **10.25-10.40:** Cada integrante presenta su idea (máx 1 minuto) y luego el equipo genera el juego grupal (decidiendo qué elementos de qué propuestas se incorporarán en el juego final)
- **10.40-11.10:** Se construye el juego, se prueba, se refina y se le pone nombre.
- **11.10-11.30: BREAK**
- **11.30-12.00:** Dos miembros del equipo se quedan en el puesto para presentar el juego. Los otros dos miembros visitan otros juegos (al menos dos). y hacen un ranking de sus favoritos.
- **12.00-12.05:** Los visitantes elaboran su ranking (aún secreto) de juegos favoritos.
- **12.05-12.35:** Se intercambian los roles (los visitantes ahora presentan el juego y los presentadores se transforman en visitantes).
- **12.35-12.40:** Los visitantes elaboran su ranking (aún secreto) de juegos favoritos.
- **12.40-12.45**: Se nombran los juegos favoritos

¿Y LA EVALUACIÓN?

Es muy simple: Si te veo participar activamente, tienes un 7. Si te veo imitando al perezoso de Zootopia, tienes un 1.