Módulo: ING1905 - Seguridad informática en la nube - (A49)

Actividad: Reto de aprendizaje 3. Crea tu propia criptografía

Nombre: Roberto Mora Balderas

Asesor: José Abdón Espínola González

Fecha: 30 de abril de 2023

Criptografía

A continuación, se expondrá la generación de un método criptográfico hipotético.

De acuerdo con lo visto en clase podríamos utilizar un método muy similar al “Diffie-Hellman”, esto debido a su practicidad y a su fácil implementación en internet.

Las características de este método hipotético serian:

- 1 sola clave final que se usara para cifrar y descifrar el mensaje, dicha clave no necesita intercambio entre los usuarios.
- La clave final vendrá de la combinación de 2 claves secretas, 1 clave individual y secreta para cada participante de la transmisión del mensaje (para el ejemplo los llamaremos participante A y participante B).
- Constaría de los siguientes pasos:
    1. Generación de número, de preferencia grande, estos números son compartidos entre participantes.
    2. Elección de clave secreta individual, numero de preferencia grande.
    3. Mediante matemáticas generar una relación entre la clave publica y los números seleccionados, de tal manera que:

$$Resultado = NumeroCompartidoMenor^{Clave\ Secreta} * k(NumeroCompartidoMayor)$$

Siendo k la relación matemática entre ambos números.

4. Ambos participantes realizan los pasos anteriores, y se comparten el resultado.
5. Finalmente, ambos realizan una última operación entre su clave secreta individual y el resultado que se compartieron en el paso anterior de la siguiente manera.

$$ClaveFinal = Resultado^{Clave\ Secreta} * k(NumeroCompartidoMayor)$$

- Esta clave final es la encargada de cifrar y descifrar el mensaje, la clave final será idéntica para ambos usuarios independientemente de su clave secreta, si se siguieron los pasos mencionados arriba y asumiendo que k es una relación que existe entre los números selectos.
- De acuerdo con la naturaleza del algoritmo y del tipo de cifrado las claves deben ser de al menos 256 bits para garantizar su seguridad, pudiendo aumentar en múltiplos de 4 bytes.

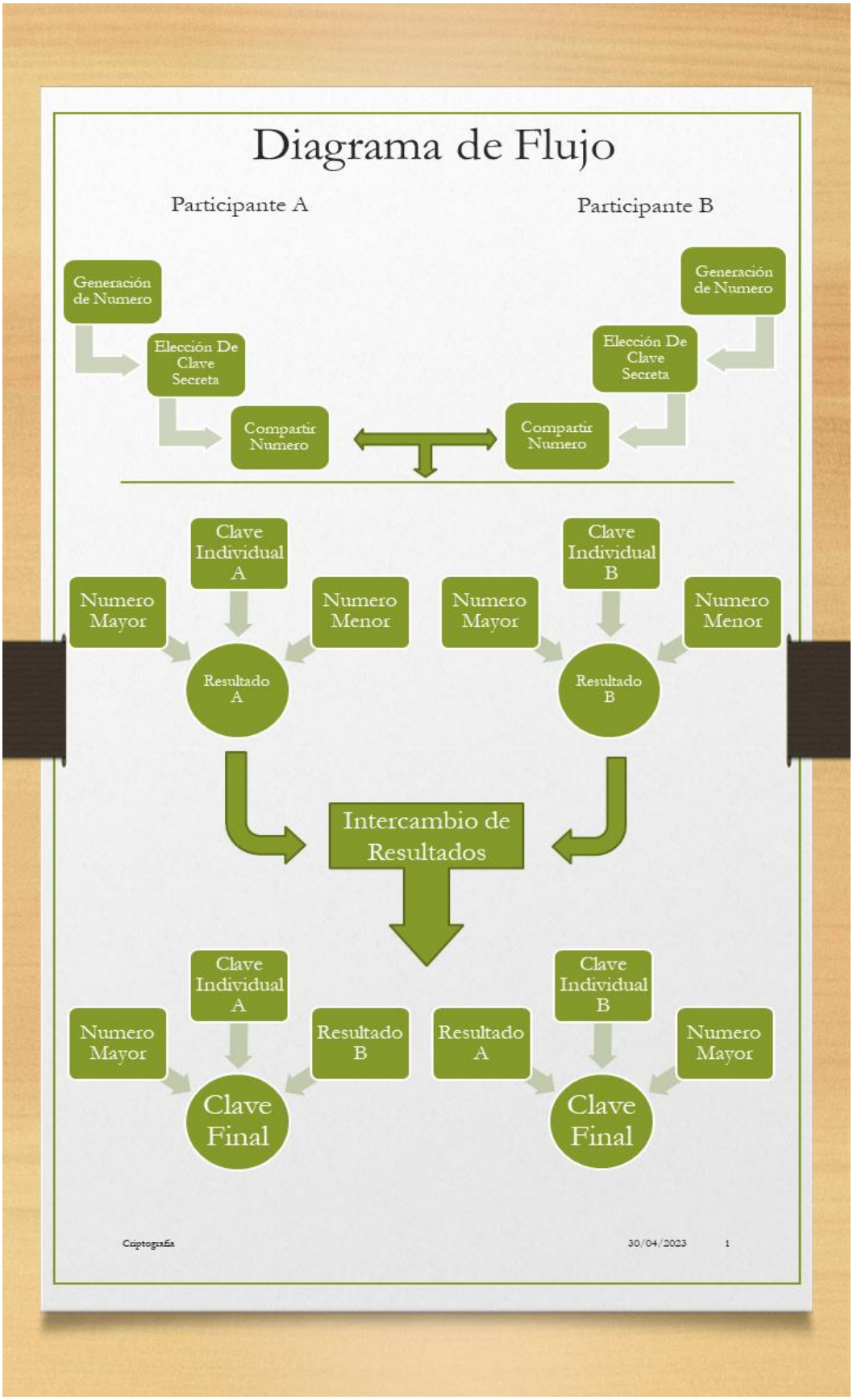
Diagrama de Flujo
Participante A
Participante B
Generación de Numero
Elección De Clave Secreta
Compartir Numero
Generación de Numero
Elección De Clave Secreta
Compartir Numero
Clave Individual A
Numero Mayor
Numero Menor
Resultado A
Clave Individual B
Numero Mayor
Numero Menor
Resultado B
Intercambio de Resultados
Clave Individual A
Numero Mayor
Resultado B
Clave Final
Clave Individual B
Resultado A
Numero Mayor
Clave Final
Criptografía
30/04/2023
1