RELACIÓN DE EJERCICIOS (TEMA 3)

EJERCICIO 1:

Considerando el protocolo de división de secretos y M= 110010101100:

a) Dividir el mensaje en dos sombras.
b) Realizar la misma actividad, pero para seis sombras.
c) Supongamos que una de las sombras no llega al destino. ¿Qué ocurre?

EJERCICIO 2:

Considerando el protocolo de compartición de secretos y las siguientes condiciones:

- k=3
- D=263

a) Dividir el mensaje en 5 sombras, ocultando el valor original del dato (D).
b) Recuperar el mensaje suponiendo que se han recibido sólo tres sombras de 5.
c) En el caso extremo que se reciban 2 sombras cualesquiera, cuáles serían los polinomios. ¿Qué problema existe?

EJERCICIO 3:

Considerando el protocolo de bit-commitment y el uso de las funciones hash:

a) ¿Qué ocurre si Alice envía a Bob H(R1,b),R1?

EJERCICIO 4:

Considerando el protocolo de póker mental:

a) Generalizar el problema para 4 personas: