**RELACION DE EJERCICIOS**

EJERCICIO 1:

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

1. **dividir el mensaje en dos sombras.**

Se divide en 110010 101100

1. **Realizar la misma actividad, pero para seis sombras.**

11 00 10 10 11 00

1. **Supongamos que una de las sombras no llega al destino. ¿Qué ocurre?**

No se puede descrifrar el mensaje, se necesitan todos para conocerlo.

EJERCICIO 2:

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

• k=3 • D=263

1. dividir el mensaje en 5 sombras, ocultando el valor original del dato (D).

q(x) = a0 + a1x + a2x2

a0=263

a1=421

a2=873

q(1)= 1.557 q(2)= blablabla

1. Recuperar el mensaje suponiendo que se han recibido sólo tres sombras de 5.

Quedaría un sistema de 3 ecuaciones con 3 sombras del que poder sacar a0, que es el mensaje original

1. En el caso extremo que se reciban 2 sombras cualesquiera, ¿cuáles serían los polinomios? ¿Qué problema existe?

Tendriamos dos ecuaciones de 3 incognitas por lo que no se podria resolver.

EJERCICIO 3

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

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

Podria funcionar como bit-commitment debido a que de primeras bob no puede conocer el contenido de b pero si Alice se lo comunica posteriormente porque le puede calcular el hash y compararlo.

EJERCICIO 4:

Considerando el protocolo de póker mental: a) generalizar el problema para 4 personas

A🡪B: Ekpub\_A(Mi)

B🡪A:Ekpub\_B(Ekpub\_A(Mj))) siendo j = 1…5

A:Dkpriv\_A(Ekpub\_A(Mk)) = Ekpub\_B(Mj)