Memoria Descriptiva.

Adrián Muñoz Lloret

Class Hash:

La función doHash obtiene una String cualquiera y la pasa a array de bytes. De esta forma puedo calcular el hash de cualquier cosa.
Como cifrado he usado el CBCPadding, para obtener un efecto avalancha, al que luego le calculo los últimos 16 bytes que serán el Hash.

Class MAC:

Es idéntica a la anterior, ya que una MAC es un hash cifrado (a grandes rasgos) y para crear el hash lo que hacemos es cifrarlo en AES.

Class Random:

Para esta he creado un double Semilla (en un principio lo hice con enteros pero no me valía para el método de MonteCarlo porque necesita números entre 0 y 1). Además creo una clase Hash para ir calculando los aleatorios.
Lo que voy haciendo es sumar todos los bytes del hash y calcular su resto módulo 1000 (de esta manera la probabilidad de que salgan los números extremos aumenta) y dividir el resultado entre 1000 para tener siempre un valor entre 0 y 1.

Como no conseguía que diera valores aleatorios, sino que repetía muchos, lo que hice fue crear un contador que se vaya sumando a la semilla e incrementandose.