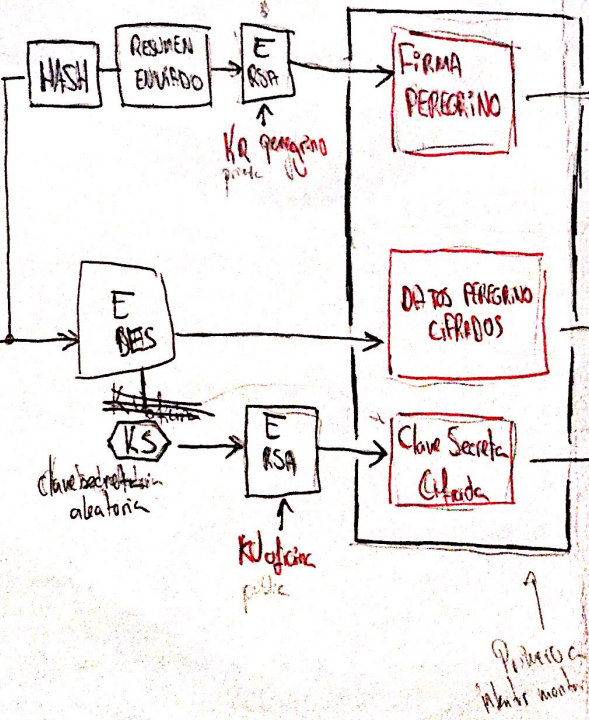


OJO REQUISITOS !!

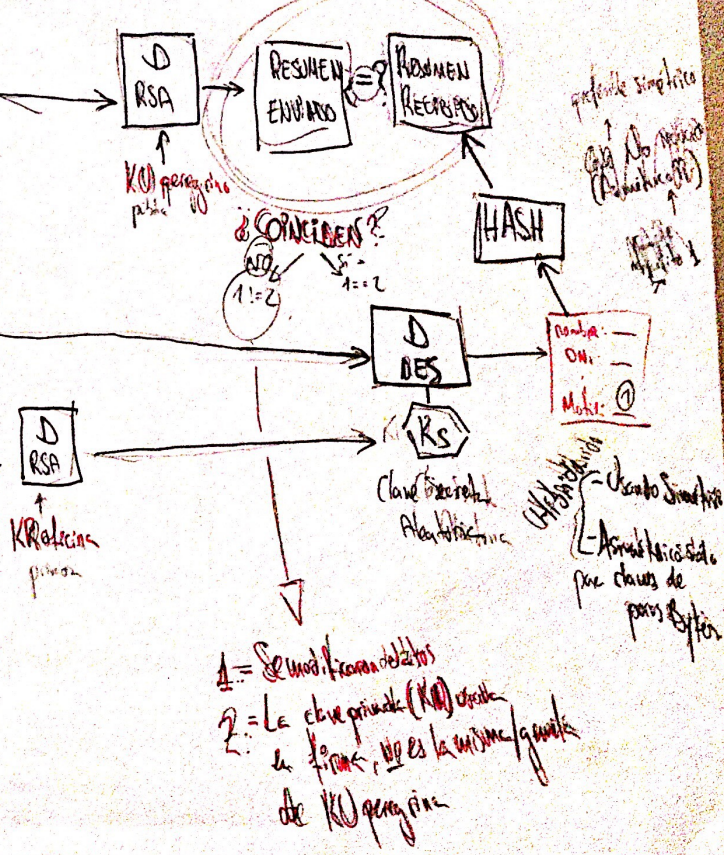
La clave aleatoria
tiene q seguir
la misma estructura

GENERAR COMPOSTELA

Datos Peregrino
Nombre: _____
DNI: _____
Materia: _____



DESEMPAQUETAR COMPOSTELA

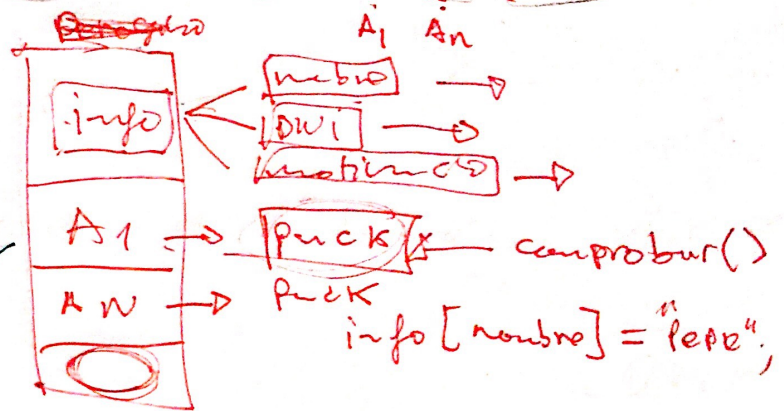
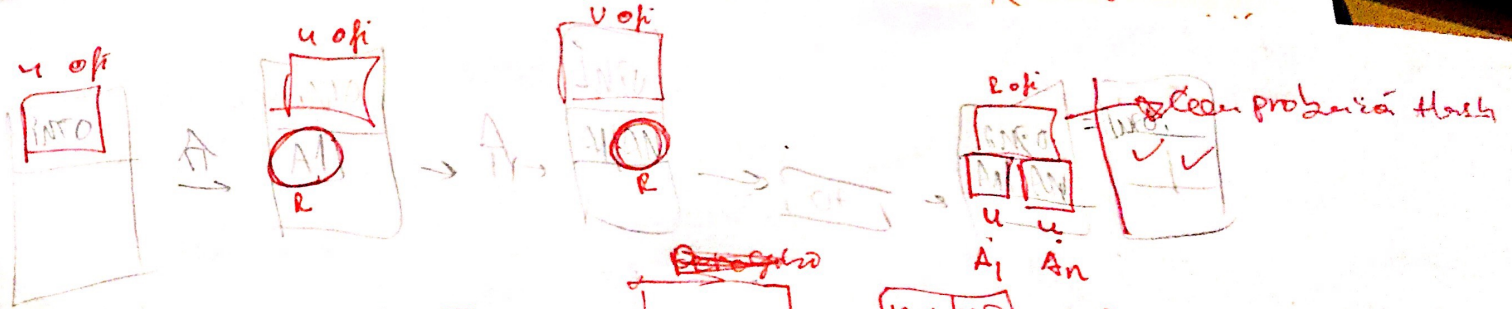


1 = Simetriza los datos
2 = La clave privada (KR) usada
en firma, no es la misma/guadada
de KR oficina

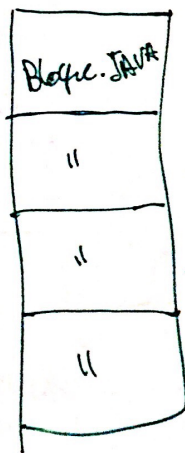
1 Computar Generar (long)
oficina
aleatorio 2
aleatorio 1
peregrino

Solo 1 vez...

HASH -> RS + RS



Compostelme



Paquete.JAVA

- "Peregrino" → Diccionario con los datos.
- "Albergue 1" → Paquete (SELLO).
- "Albergue 2" → Paquete (SELLO).
- "Albergue N" → Paquete (SELLO).