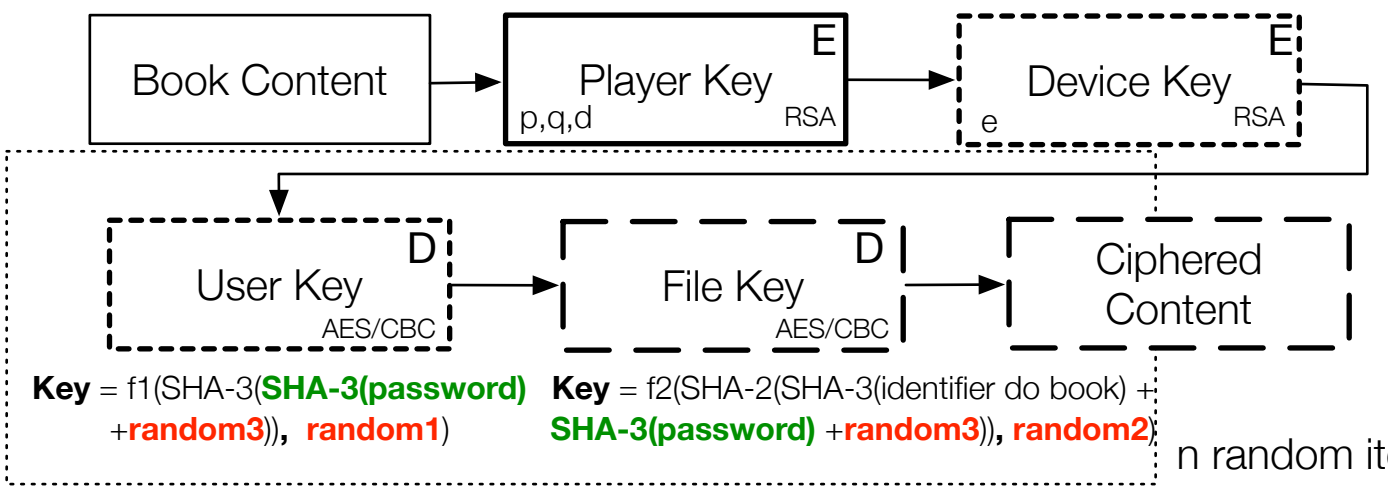

Know: random 3 **Needs:** random2 and random1

Note: The server and the player knows: SHA-3(password)

f1(bit[] array_secret, bit[] valor_aleatorio):
-> p = array_secret + valor_aleatorio
-> p = p << 1
-> p = p mod valor_aleatorio

f2(bit[] array_secret, bit[] valor_aleatorio):
-> p = array_secret mod valor_aleatorio
-> p = p + 3
-> p = p >> 1