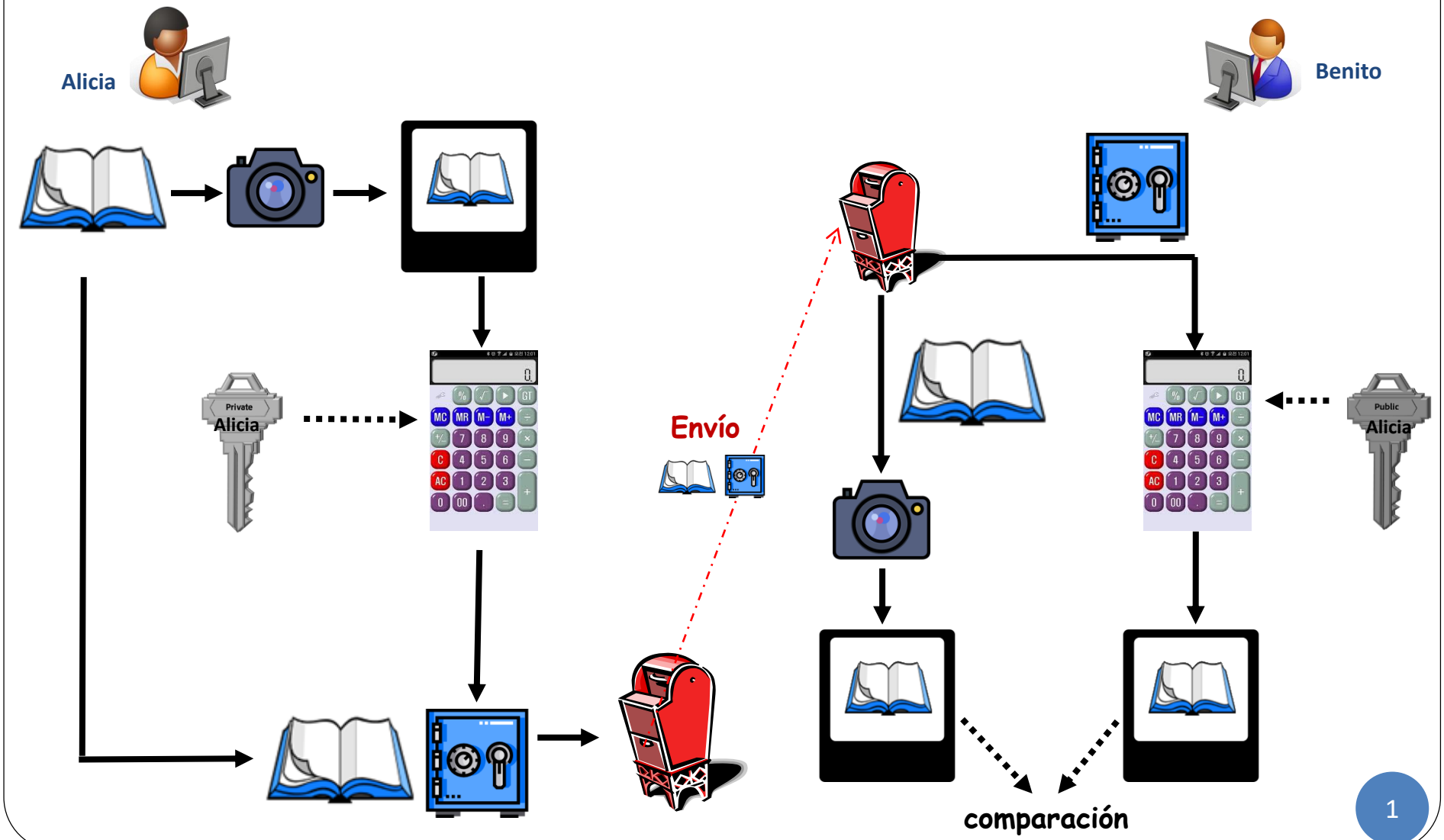
Abstracción del procedimiento de firma digital

- Libro = M, Fotografía = H(M)



Algoritmo	Salida (bits)	Tamaño del Mensaje – tamaño de bloque (bits)	Bloque interno (bits)	Longitud de la palabra (bits)	Operacio-nes	Colisiones
MD5	128	512	128	32	+, and, or, xor, rot	Si
SHA-1	160	512	160	32	+, and, or, xor, rot	Si
SHA-2 (224, 256)	224, 256	512	256	32	+, and, or, xor, shr, rot	No
SHA-2 (384,512, 512/224,512/ 256)	384, 512, 224, 256	1024	512	64	+, and, or, xor, shr, rot	No
SHA-3	224/256/ 384/512	1152/1088/832/ 576	1600 (5x5 array de palabras de 64 bits)	64	and, or, xor, rot	No