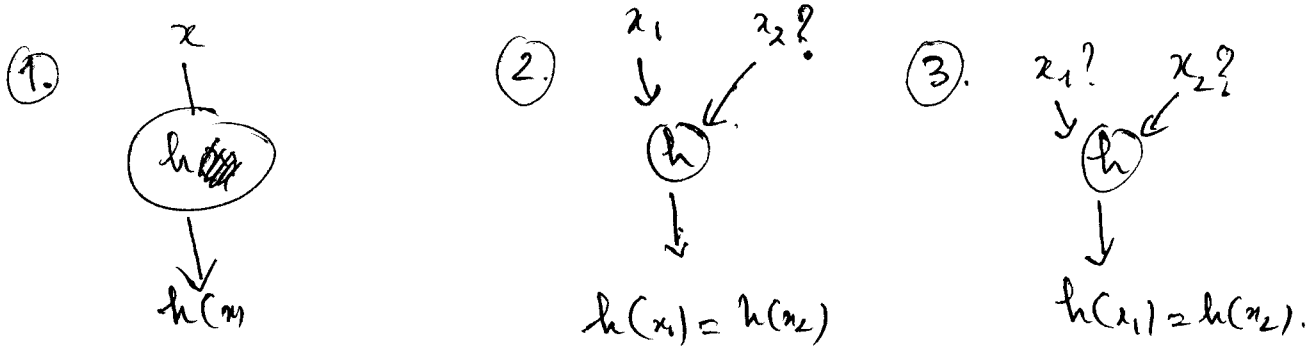
1. One-way : résistance à la pré-image.

2. Résistance à la seconde préimage.

3. Résistance aux collisions.



1. Etant donné $z = h(x)$. il est difficile de retrouver x.
En effet, dans le protocole suivant,
supposons que Bob crypte x le message, mais non pas la signature : Bob transmet $(e_k(\cdot) : DES, AES, \dots)$.

$$\left(e_k(x), sig_{k_{pub}}(z)\right).$$

supposons que Bob utilise RSA :

$$s = sig_{k_{pub}}(z) \equiv z^d \pmod n$$

Oscar peut calculer $s^e \equiv z \pmod n$

Si h n'est pas à sens unique, O. peut calculer $x = h^{-1}(z)$. $\Rightarrow$ h doit être one-way.