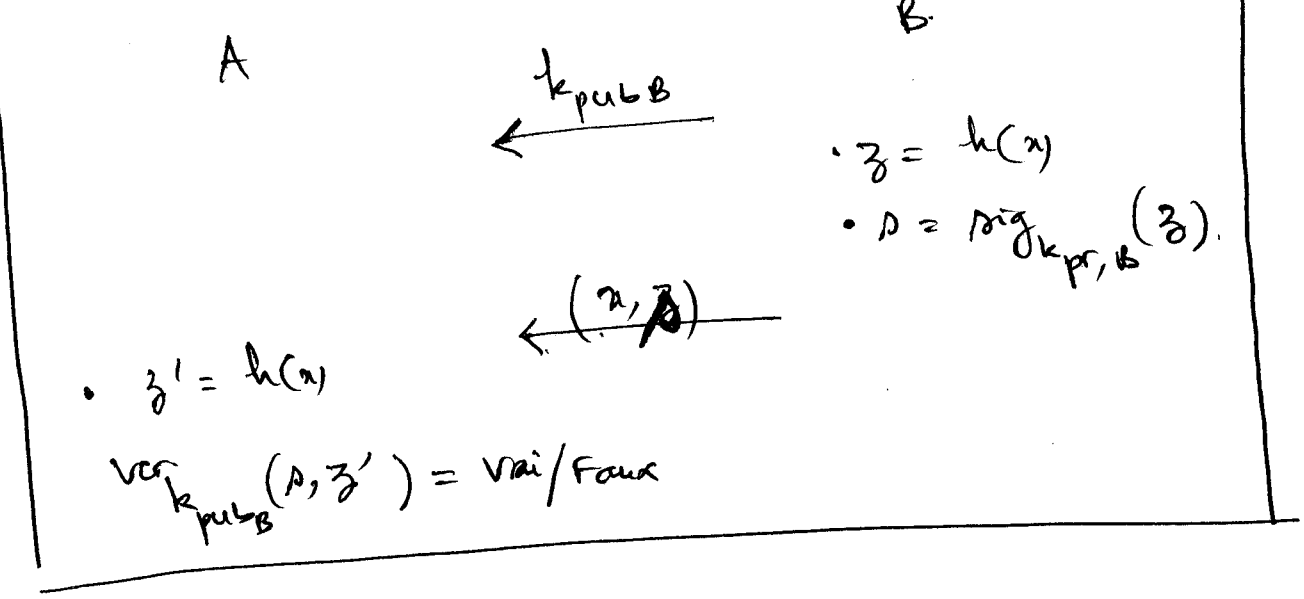
## §4.2. Fonctions de hachage.

Les fonctions de hachage sont des primitives pratiques pour signer de long messages. Elles permettent de calculer une empreinte du message de longueur fixe sans utiliser de clé. Ainsi la signature de x est plus courte que x.

**Protocole de base de signature avec fonction de hachage.**




**Propriétés de h**

- doit être rapidement calculable,
- de longueur fixe (128 – 512 bits)
- sensible aux modifications : toute modification de x résulte en valeur différente de $h(x)$

### §4.2.1. Sécurité et propriétés de h.