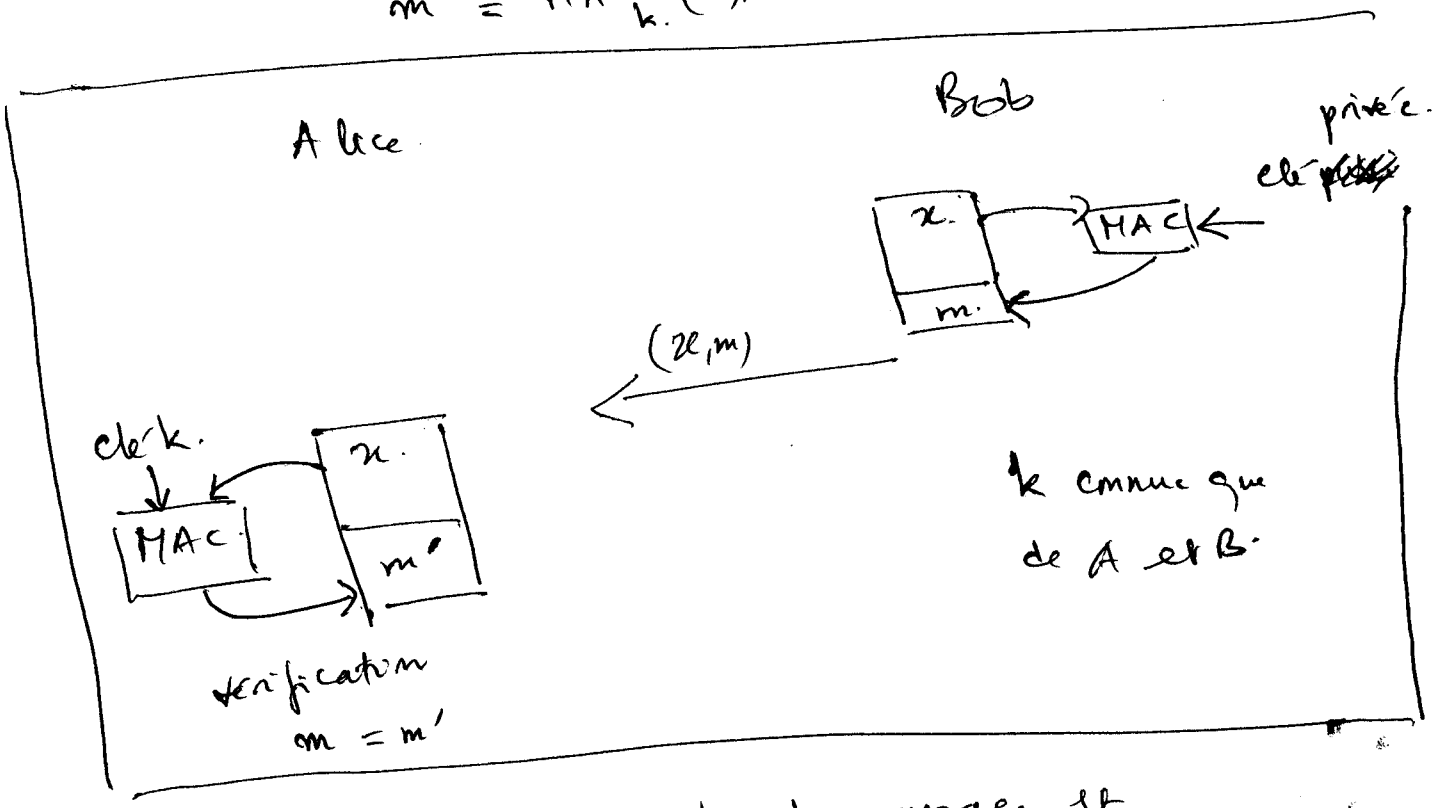
§ MAC : Message Authentification Codes.

§§ A) Propriétés et principes.

MAC ressemble à la signature numérique, en rajoutant un tag (empreinte) d'authentification au message x, mais il est basé pour le B-cryptage :

$$m = MAC_k(x).$$



⇒ • MAC assure l'intégrité des message et l'authenticité. En plus plus rapide que la cryptoclé publique. La non-répudiation n'est pas assurée.

• La construction est basée sur le B-cryptage et/ou hachage.

§§ B) Constructions de MAC.