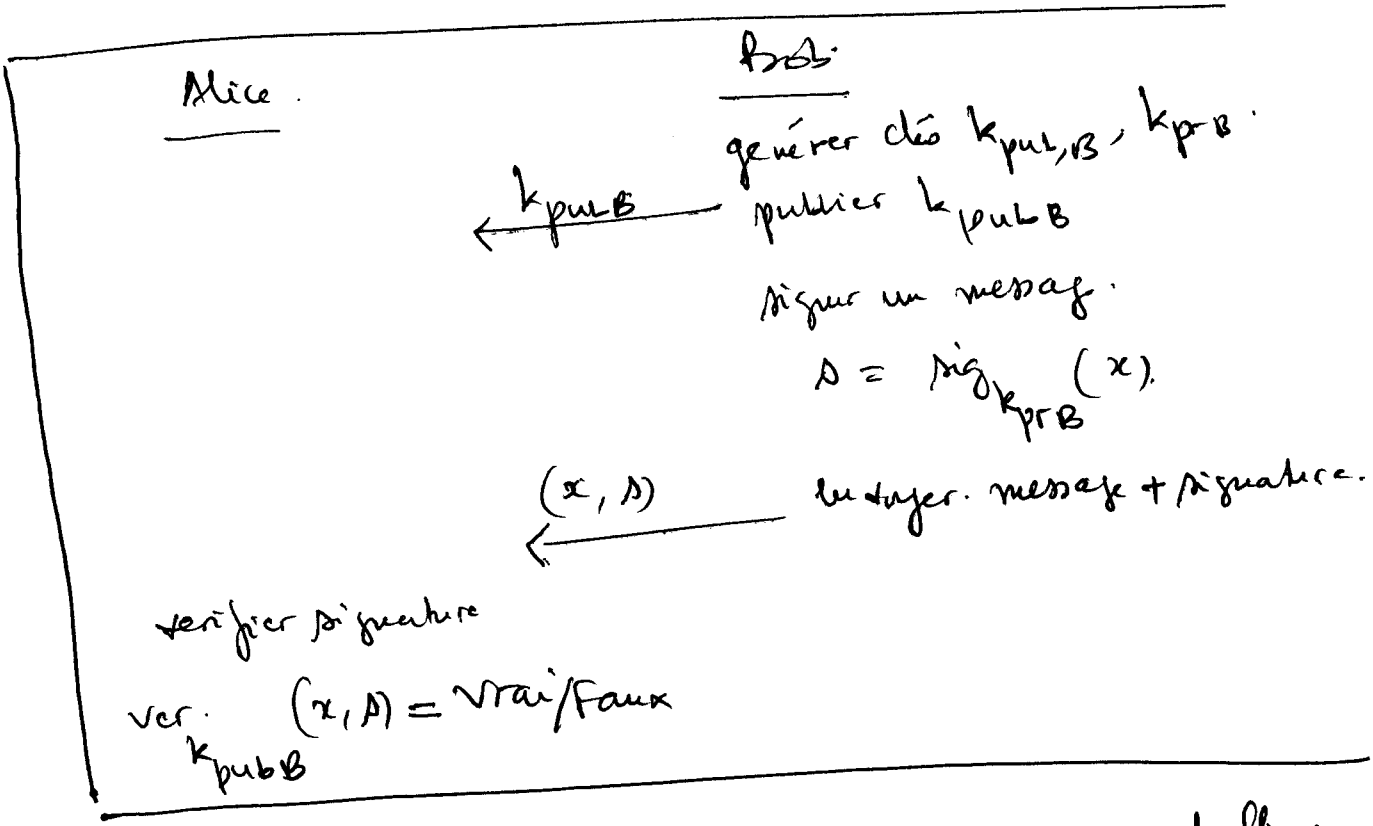
→ Bob envoie sa clé publique k_{pubB} à Alice ;

forme un message x ; le signe par un algorithme de signature sig et calcul $s = sig(x, k_{prB})$ en utilisant sa clé privé k_{prB}. Bob envoie la paire (x, s) à Alice qui la vérifie par un algorithme de vérification utilisant k_{pubB}. Noter que s est un nombre qui dépend du message x.

D'où le protocole :



→ Service de sécurité atteints avec nos connaissances actuelles :

1. Confidentialité : (par crypto symétrique, moins par Asym).
2. Intégrité. } signatures numériques et MAC.
3. Authentification }
4. Non-Répudiation. Signature.