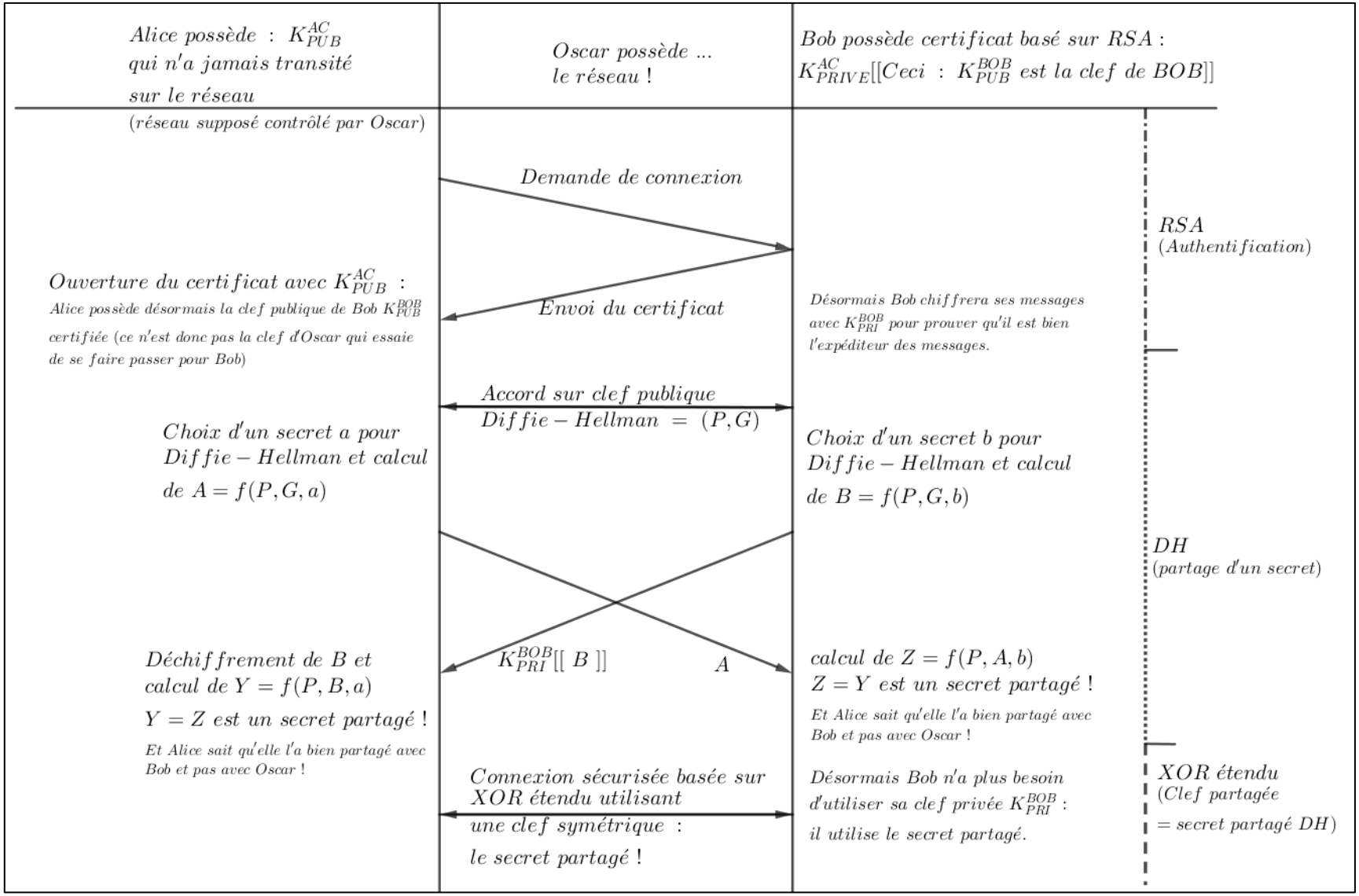

Remarques :

K[[message]] désigne le message qui a été chiffré par la clef K dans le cas de K^{AC} et K^{BOB}

Comprendre sur ce schéma que pour Diffie-Hellman, la clef publique est le couple (P, G) choisi parmi quelques couples connus de tous et disponibles sur internet (RFC 3526)

Pour Diffie-Hellman, les notations utilisées sont les mêmes que dans le cours pour P, G, a, A, b, B, Y et Z.

Il est important de connaître le reste du cours : ce schéma n'est qu'un résumé qui donne la trame de l'établissement d'une connexion sécurisée. Tout le reste du cours qui n'est pas indiqué là permet de savoir POURQUOI ce sont ces choix là qui ont été effectués et pas d'autres choix.