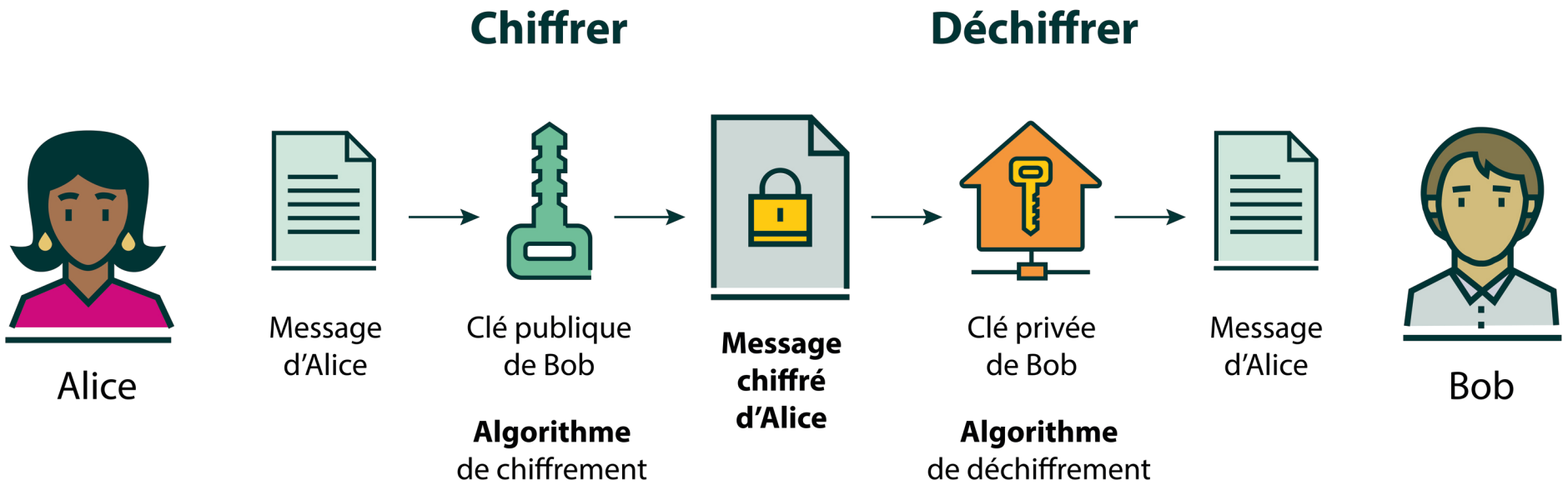
Cryptographie asymétrique



Alice et Bob ont tous deux leur paire de clés. Alice a récupéré la clé publique de Bob en mains propres ou par Internet. Dans ce dernier cas, par sécurité, Alice a comparé, par téléphone ou messagerie, l'empreinte de la clé publique de Bob pour être sûre qu'il n'y a pas eu falsification durant le « transport ». Bob déchiffre le message d'Alice avec sa clé privée.

La cryptographie asymétrique, inventée dans les années 1970, résoud le problème ancestral de l'échange sécurisé d'un « procédé » ou d'une clé secrète de chiffrement-déchiffrement dit symétrique.
Une signature cryptographique est insérée dans le message chiffré pour attester, dans le cas présent, qu'Alice est bien l'auteure du message.

XENATON