SAE S1-02

- Bob veut communiquer des informations secrètes à Alice
- Alice crée une clé publique qui servira au chiffrement du message par Bob et une clé privée qui lui servira au déchiffrement du message.
- Alice choisit initialement deux nombres premiers p et q et calcule le produit de ces deux nombres : n=pq. La clé publique est composée finalement de deux nombres (n,e) où e est un nombre premier choisi pour être premier avec (p-1)(q-1).
- La sécurité du cryptage repose notamment sur la difficulté de factoriser un nombre n en produits de nombres premiers lorsque ceux-ci sont suffisamment grands.
- La clé privée est constituée du nombre entier d compris entre 1 et (p-1)(q-1) et inverse de e modulo (p-1)(q-1).

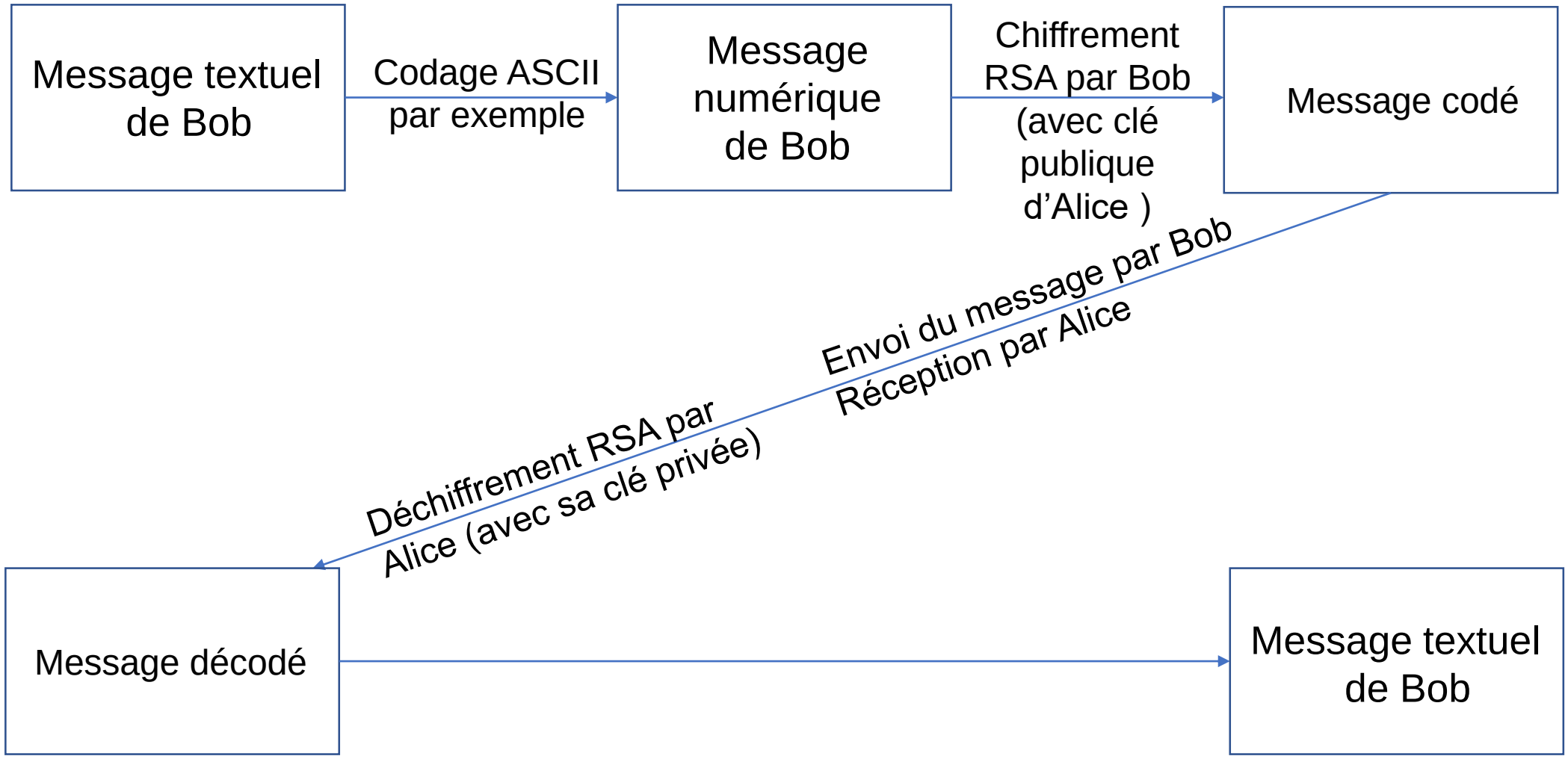
- Soit M le message présenté comme un nombre naturel inférieur ou égal à n.
- Le message chiffré sera présenté comme l'entier naturel C tel que :

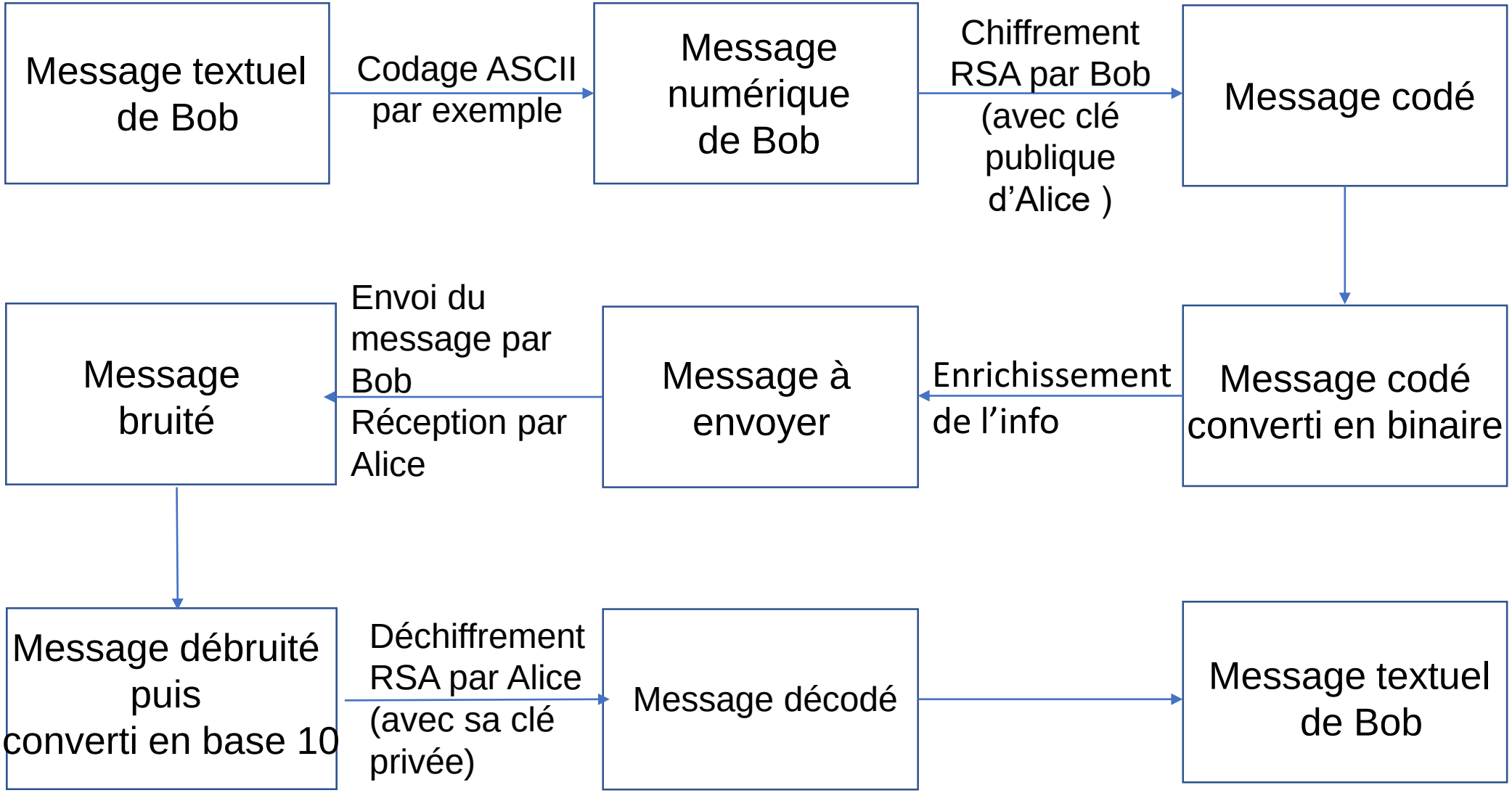
$$M^e \equiv C[n]$$

- Pour déchiffrer C on utilise d car on peut montrer que :

$$M \equiv C^d[n]$$

- La rapidité de chiffrement et déchiffrement du message repose donc en bonne partie sur notre capacité à réaliser des calculs modulaires d'exponentiation rapidement


Message textuel de Bob
Codage ASCII par exemple
Message numérique de Bob
Chiffrement RSA par Bob (avec clé publique d'Alice)
Message codé
Envoi du message par Bob
Réception par Alice
Déchiffrement RSA par Alice (avec sa clé privée)
Message décodé
Message textuel de Bob


Message textuel de Bob
Codage ASCII par exemple
Message numérique de Bob
Chiffrement RSA par Bob (avec clé publique d'Alice)
Message codé
Message codé converti en binaire
Enrichissement de l'info
Message à envoyer
Envoi du message par Bob
Réception par Alice
Message bruité
Message débruité puis converti en base 10
Déchiffrement RSA par Alice (avec sa clé privée)
Message décodé
Message textuel de Bob