Corrigé Type

Exo 01:

1. QF WJSHTSYWJ JXY UWJAZJ F QF HFKJYJWNF
2. On obtient le message chiffré : BX CHSYFSMCH HVM LCHEUH X BX YXPHMHCZX
3. Après le déchiffrement on obtient le message clair : ”cést juste”

Exo 02:

Dans ce schéma qui semble à première vue parfait, il y a unélément crucial qui n’a pasété prisén compte,ét ce dès le début : Bob (resp. Alice) n’a aucune certitude qu’il parle bien à Alice (resp. Bob).
Un attaquant, disons Charlie, peut alors se créer lui aussi une paire de clés publique / privée. Il intercepte la clé publique de Bobéténvoie la sienne à Alice, sans laisser transiter celle de Bob. De même il intercepte la clé publique d’Aliceéténvoie la sienne à Bob. Dans toute la suite des échanges, il peut d échiffrer les messages qu’il reçoit (puisque chiffrés avec sa clé publique), et les rechiffrer pour le bon destinataire, sans que ces deux là ne se rendent compte de rien. Cette attaque est appelée l’attaque de l’homme au milieu ou man in the middle en Anglais.

Pour l’éviter, il faut par exemple que les clés publiques soient certifiées par une tiers authorité, ou que Bob et Alice trouvent un autre moyen de vérifier leurs clés publiques (attest ées par un autre correspondant en lequel ils ont confiance au préalable, vérification occullaire derrière un écran étc).

Exo 03

1. (15^3) mod 187
2. P * Q = 187 et (P-1) * (Q-1) = 160 donc P = 187/Q. En remplace P par 187/Q dans la 2 équation on trouve Q = 17 et P = 11. **d*e mod 160 = 1** après le calcule on trouve d = 107.
3. P = 11 et Q = 17