Cryptographie
TD8 – Diffie-Hellman
Nawfal MALKI, STI 4A TD2

1.
$A = g^a [p] = 3^6 [23] = 16$
$B = g^b [p] = 3^{15} [23] = 12$
$K = A^b [p] = 16^{15} [23] = 9$
$K = B^a [p] = 12^6 [23] = 9$

2.
$A = g^a [p]$
$K_b = A^b [p] = (g^a)^b [p] = g^{ab} [p]$
$K_a = B^a [p] = (g^b)^a [p] = g^{ba} [p]$
donc $K_a = K_b$

3.
Un attaquant C peut s'interposer entre Alice et Bob en utilisant la clé K1 pour interagir avec Alice et la clé K2 pour interagir avec Bob.

4.
Un algorithme d'authentification est nécessaire afin de vérifier l'identité des deux personnes avant de commencer à échanger des données.

5.
Le protocole Diffie-Hellman est utilisé dans le protocole SSL.