**TD3 Module Sécurité Informatique**

**Exercice 7** : Soient deux partenaires A et B désireux d’ouvrir une session de communication, ils décident alors de choisir les valeurs non confidentielles du protocole DH : base g=3 et p=5. Si A choit comme valeur secrète a=4 et B choisit b=5 alors :

* + - 1. Déterminez la clé commune entre A et B
      2. Montrez que ce protocole est vulnérable à l’attaque de l’homme du milieu
      3. Proposez une méthode pour évite cette vulnérabilité.

**Exercice 8 :** Soient deux A et B deux partenaires voulant ouvrir une session de communication confidentielle utilisant la cryptographie symétrique, par exemple le chiffrement affine. Pour que A puisse communiquer, de manière sécurisée, la clé symétrique k = (a, b) à transmettre à B sur un canal non sécurisé, A décide avec B de choisir le crypto système RSA.

1. Si A choisit deux nombres premiers p=3 et q=11, quelles seraient sa clé publique pour pouvoir lui transmettre des messages codés, et sa clé privée pour décodés ces derniers.. De même pour B s’il choisit p=5 et q=7.
2. Comment A va transmettre la clé kp = (3,1)
3. Comment B saura que A est le véritable A et non un imposteur

**La solution sera chargée sur la plateforme Moodle en fin de round.**