Échange de clefs

26 ♦◇◇ Diffie-Hellman

Déterminer la clé commune d'Alice et Bob dans le cas où $p = 23$ et $g = 3$ et Alice choisit un nombre secret $x_a = 6$ et Bob choisit $x_b = 15$.

27 ♦♦◇ Attaque par le milieu de Diffie-Hellman

Décrire une attaque dans le protocole de Diffie-Hellman dans laquelle un attaquant *actif* (i.e. qui peut modifier les données pendant le protocole Diffie-Hellman) peut ensuite intercepter, déchiffrer et modifier toutes les communications qu'Alice ou Bob chiffrerait avec sa clé.

28 ♦◇◇ Fonctionnement clé privée vs clé publique

Expliquez les principes de fonctionnement de la cryptographie symétrique et de la cryptographie asymétrique, en mettant en évidence les différences entre ces deux catégories, leurs avantages et leurs inconvénients respectifs.

Vous pourrez illustrer votre réponse par un exemple de chaque catégorie, décrit aussi précisément que possible.

29 ♦◇◇ Clé privée vs clé publique

Dix-sept personnes veulent pouvoir s'échanger des messages deux à deux. Si elles choisissent un système à clé secrète, combien de clés faut-il en tout ? Même question pour un système à clé publique. Quels sont les avantages de chaque système ? Lequel conseillez-vous ?