NSI · TERMINALE / EXERCICES CORRIGÉS

Sécuriser les communications

Astrolab Cours · astrolabcours.fr

Ex. 1 Chiffre de César ●○○ Application

Chiffrer le mot NSI avec le chiffre de César de clé 3, puis déchiffrer QXLW.

Indice

Décaler de 3 vers l'avant pour chiffrer, vers l'arrière pour déchiffrer.

Chiffrer

N → Q, S → V, I → L : QVL.

Déchiffrer

NSI devient QVL, et QXLW se déchiffre en NUIT.

Ex. 2 Le XOR ●●○ Méthode

Message 1011, clé 0110. Calculer le message chiffré avec XOR, puis montrer qu'un deuxième XOR avec la clé redonne le message.

Indice

XOR : 1 si les deux bits sont différents.

Chiffrer

1011 XOR 0110 = 1101.

Déchiffrer

1101 XOR 0110 = 1011.

La conclusion

On retrouve 1011 : la même clé chiffre et déchiffre, c'est un chiffrement symétrique.

© Astrolab Cours · astrolabcours.fr/nsi/terminale/securiser-les-communications/ · Tous droits réservés : usage personnel uniquement, republication et usage commercial interdits

Ex. 3 La mauvaise clé ●●○ Piège

Alice veut envoyer un message secret à Bob. Elle le chiffre avec sa propre clé publique. Bob peut-il le lire ?

Indice

Quelle clé déchiffre ce qu'a chiffré la clé publique d'Alice ?

L'erreur

Seule la clé privée d'Alice peut déchiffrer ce message : Bob ne l'a pas.

La correction

Alice doit chiffrer avec la clé publique de Bob : seul Bob, avec sa clé privée, pourra lire.

Ex. 4 Pourquoi HTTPS mélange les deux ●●● Type bac

Expliquer pourquoi HTTPS n'utilise pas seulement le chiffrement asymétrique, ni seulement le symétrique.

Indice

Penser à la vitesse et à l'échange de clé.

Seulement symétrique

Il faudrait transmettre la clé secrète au serveur sans protection : un espion la capterait.

Seulement asymétrique

Il est beaucoup plus lent : chiffrer toute une page ou une vidéo serait trop coûteux.

La solution

L'asymétrique sert uniquement à échanger une clé symétrique ; tout le reste est chiffré en symétrique, rapide.

© Astrolab Cours · astrolabcours.fr/nsi/terminale/securiser-les-communications/ · Tous droits réservés : usage personnel uniquement, republication et usage commercial interdits