CORRIGÉ

Tle

Corrigé détaillé
6 exercices

Sécurisation des communications

> Ce qui est noté au contrôle, ce n'est pas le résultat seul : c'est le raisonnement posé, puis le calcul mené jusqu'au bout avec l'unité.

1 Vocabulaire

1. Symétrique : une seule clé partagée.
2. Asymétrique : paire clé publique / clé privée.

2 César

1. « QVL ».

3 XOR

1. 1010 XOR 0110 = 1100 ; 1100 XOR 0110 = 1010.

4 HTTPS

1. Il est beaucoup plus lent : on s'en sert seulement pour échanger une clé symétrique.

5 Certificat

1. À prouver que la clé publique appartient bien au site, grâce à la signature d'une autorité de confiance.

6 Signature

1. Il le signe avec sa clé privée ; chacun vérifie avec sa clé publique.

Corrige-toi toi-même. Compte tes points exercice par exercice : c'est ainsi qu'on voit où l'on perd, et ce n'est presque jamais là où on le croit.

Ce qui est évalué	Points	Ce qui fait perdre le point
Vocabulaire	2 pts	Définitions floues
Code juste et testé	2 pts	Cas limites oubliés
Justification	1 pt	Résultat non expliqué