Examen de « Fondements de la sécurité informatique »
Master 2 – Informatique et droit
1e session

Aucun document autorisé – durée 1h30

Question 1 : Signature

Expliquer ce qu'est un algorithme de signature cryptographique. On précisera :

1) Les clefs nécessaires pour le faire fonctionner
2) Ce qu'il permet de faire à partir de quels éléments
3) Comment il est utilisé par deux tiers Alice et Bob
4) Le nom d'algorithmes de signature

Question 2 : Le protocole TLS

Expliquer comment fonctionne le protocole TLS. Veiller à citer proprement les algorithmes cryptographiques utilisés et leurs paramètres.

Question 3 : Social Engineering

Donner des idées sur comment l'on pourrait utiliser l'ingénierie sociale pour obtenir les notes d'un étudiant à l'université contre son gré. Que peut-on faire pour s'en prémunir ?

Question 4 : Chiffrement de bout en bout

Expliquer en quoi consiste le chiffrement de bout en bout. Expliquez en quoi c'est ou cela n'est pas une assurance de confidentialité des discussions entre les individus.