



Mesurer les enjeux théoriques, techniques et stratégiques liés à la protection de l'information numérique
Connaître le cadre juridique relatif à l'utilisation du chiffrement en France et dans le monde.

PROGRAMME

Présentation

- La présentation des modèles d'attaque et définition des niveaux de sécurité d'un protocole de chiffrement.

Chiffrement

- Connaître et comprendre les notions de chiffrement par blocs et de chiffrement..

Fonction de hachage

- Maîtriser les concepts de générateur de nombres pseudo-aléatoires (PRNG) et de fonction de hachage.

Algorithmes de chiffrement

- Connaître les principaux algorithmes de chiffrement..

Certificats et monnaies virtuelles

- Administrer les certifications des clés publiques, révocation, renouvellement et archivage des clés.
- Le fonctionnement des monnaies virtuelles.



5

JOURS

35

HEURES

OBJECTIFS

Comprendre la cryptographie et le fonctionnement de la monnaie virtuelle

PUBLIC | PRÉREQUIS

PUBLIC

Administrateur des systèmes et réseaux, responsable cybersécurité,

PRÉREQUIS

Connaissance de la structure matérielle et architecturale d'un ordinateur

INFOS PRATIQUES

HORAIRES DE LA FORMATION

de 9 h 00 à 12 h 30 et de 13 h 30 à 17 h 00

MÉTHODOLOGIE

PÉDAGOGIQUE

Théorie | Cas pratiques | Synthèse

MODALITÉS D'ÉVALUATION

Évaluation qualitative des acquis tout au long de la formation et appréciation des résultats

DATES ET LIEUX

Aucune session ouverte