RÉPUBLIQUE FRANÇAISE
Liberté Égalité Fraternité

ENSI CAEN | executive education

Cryptographie

Durée
14h (2 jours)

Lieu
ENSICAEN

Prochaine session :
29 janvier 2025

Effectif minimum
4 personnes

Tarif
1500 €
net de taxe par personne, accueil et déjeuner inclus

La cryptographie est une science récente qui est aujourd'hui omniprésente dans notre société. Souvent mal connue, elle est utilisée pour protéger nos communications et nos informations, englobant à la fois les communications sur internet, les cartes de paiement, carte Vitale, etc.

Objectifs de la formation

- Acquérir une culture autour de cette science
- Comprendre son fonctionnement, ses enjeux actuels et futurs
- Maitriser les différents modèles

Public

Toute personne souhaitant accroître ses connaissances dans le domaine

Prérequis

Pas de prérequis nécessaire

Modalités pédagogiques

La formation alterne présentations et manipulations

Contenu de la formation

L’histoire de la cryptographie et notions importantes (confidentialité, intégrité)

Chiffrement symétrique

- Chiffrement par blocs et mode opératoire
- Générateur pseudo-aléatoire et chiffrement à flots
- Fonction de hachage et code d’authentification de messages

Problème d’échange de clé et chiffrement asymétrique

- Principe de la cryptographie asymétrique et protocole d’échange de clés (Diffie-Hellman)
- Chiffrement asymétrique (RSA, El-Gamal)

Signature électronique

- Signature RSA
- Standard DSA

Authentification

- Principe de challenge/réponse
- Exemples rapides Schnorr – Guillou-quisquater

Cas pratique – introduction au tiers de confiance et certificats

- Délégation de confiance
- PKI
- Certificats

Perspectives

- Conséquences de l’ordinateur quantique (Shor, Groover, nouveau challenge)

- Chiffrement homomorphe

Attestation de formation

Une attestation de formation est transmise aux apprenants à l’issue de la formation professionnelle. Elle certifie le suivi de la formation et l’acquisition des compétences.

Évaluation des acquis

Les acquis des apprenants seront évalués au travers d’exercices réalisés tout au long de la formation.

Satisfaction des apprenants

Au terme de la formation, les apprenants renseigneront un formulaire de satisfaction.

Financements

Le plan de développement des compétences