PROTECTION DES DONNÉES : CRYPTOGRAPHIE POUR LA CYBERSÉCURITÉ

NUMERIQUE RESPONSABLE

opéré par INSA VALOR

Maîtriser des fondements mathématiques et de la mise en œuvre des solutions de cryptographie permettant d'offrir les services de sécurité (confidentialité, intégrité, authentification, non-répudiation, etc.)

Villeurbanne
100 % présentiel

3 jours
21 heures

23 - 25 juin 2026
INTRA possible

2 345 € H.T. / pers.
INTER entreprise

Approfondissement des techniques cryptographiques

Application pratique et utilisation d'outils spécialisés

Formation continue / financement OPCO possible

OBJECTIFS PÉDAGOGIQUES

- Maîtriser la mise en œuvre des mécanismes pour offrir les services de confidentialité, d'intégrité et d'authentification.
- Connaître les principaux algorithmes de chiffrement à clé secrète et à clé publique.
- Appréhender la cryptanalyse et les attaques connues.
- Maitriser la vision globale des enjeux liés à la protection des données.

PUBLIC CIBLE

DSI, Responsables sécurité, Développeurs, Chefs de projets, Ingénieurs techniques. Toute personne impliquée dans les systèmes d'information ou souhaitant acquérir des connaissances en cryptographie pour garantir les différents services de sécurité.

PRÉREQUIS

Des connaissances générales en mathématiques et en algorithmique sont souhaitables afin de tirer pleinement profit de la formation.

FORMATEURS

Enseignant/chercheur INSA Lyon du département Telecoms / Laboratoire CITI. Spécialiste en sécurité, réseaux, IoT et évaluation de performances.

MÉTHODES PÉDAGOGIQUES

- Cours, Travaux Pratiques, exercices, étude de cas et échanges avec un expert du domaine.
- Un support de cours sera remis à chacun des participants.

CONTENU

1) Cryptographie

Introduction : terminologie et vocabulaire, historique et acteurs à connaître, services de sécurité fournis par la cryptographie, menaces et vulnérabilités, concepts mathématiques de base.

2) Hachage et signature numérique

- Fonctions de hachage : concept et cas d'utilisation, propriétés mathématiques et fondement algorithmique, hachage simple (Unkeyed) et sécurisé (Keyed), sécurité et longueur du hachage, attaques contre les fonctions de hachage (focus sur l'attaque de collisions), étude de quelques algorithmes MD5, SHA-1, SHA-256, applications : Stockage des mots de passe.

3) CLES et PKI

- Gestion de clés cryptographiques et plateforme à clés publiques (PKI) : principe de distribution/pré-distribution/échange de clés symétriques/asymétriques, gestion de clés symétriques et problèmes associés, gestion de clés asymétriques et problèmes associés, attaque de l'homme du milieu/algorithme Diffie-Hellman, certification des clés publiques, norme X.509, modèles d'infrastructures de gestion de clés publiques, étude détaillée du modèle à base d'autorités de certification, exemple d'application (étude du protocole TLS), étude d'autres modèles (DANE, PGP, modèles à base de blockchain).

ÉVALUATION ET RÉSULTATS

- Évaluation des acquis des apprenants réalisée en lors de la formation par des exercices, des travaux pratiques et un questionnaire ouvert contextualisé.
- 90.5% des apprenants ont acquis la compétence principale visée.
- Résultat obtenu pour 155 participants évalués ayant suivi une formation dans la thématique sur les 5 dernières années.
- Évaluation du ressenti des participants en fin de formation (Niveau 1 KIRKPATRICK)
- Le niveau de satisfaction globale est évalué à 4.3/5 par les participants.
- Évaluations réalisées auprès des 192 participants ayant suivi une formation dans la thématique sur les 5 dernières années.

ACCESSIBILITÉ

Cette formation est handi-accessible.
Contactez-nous !