CODE
7401

TECHNOLOGIES DU NUMÉRIQUE ET SYSTÈME D'INFORMATION / SÉCURITÉ NUMÉRIQUE

POSSIBLE EN INTRA

PROTECTION DES DONNÉES : CRYPTOGRAPHIE POUR LA CYBERSÉCURITÉ

Face aux menaces et vulnérabilités des systèmes d'information, la protection des données est cruciale pour garantir confidentialité, intégrité et authentification. Cette formation vise à maîtriser la cryptographie et ses applications pratiques pour sécuriser les systèmes.

2345 € HT | **3 JOURS** (21 H.) | **VILLEURBANNE**
DU 23/06/2026 AU 25/06/2026

COMPÉTENCE PRINCIPALE VISÉE

Comprendre et appliquer les principes et mécanismes de la cryptographie pour assurer la sécurité des systèmes d'information.

LES + DE LA FORMATION

Mise en pratique avec OpenSSL, chiffrement et déchiffrement AES et RSA, calcul d'empreintes et signatures numériques, gestion et certification de clés PKI, exercices et études de cas guidés par un expert.

PUBLIC

- Responsables sécurité
- DSI : 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.

OBJECTIFS PÉDAGOGIQUES

- Mettre en œuvre des solutions cryptographiques (symétriques et asymétriques) pour garantir confidentialité, intégrité et authentification des données.
- Identifier les vulnérabilités et comprendre les méthodes de cryptanalyse et les attaques courantes.
- Gérer efficacement les clés et infrastructures PKI pour sécuriser les échanges et services numériques.

CONTENU

PARTIE 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

Cryptographie symétrique :

- Cryptographie symétrique Vs cryptographie asymétrique
- Cryptographie symétrique par flux (RC4, A5/1, etc.)
- Cryptographie symétrique par bloc (DES, AES, etc.)
- Étude détaillée de l'algorithme AES
- Avantages et limites de la cryptographie symétrique

Cryptographie asymétrique :

- Principe et Fondements de la cryptographie asymétrique
- Cryptographie basée sur le problème de factorisation : étude détaillée de l'algorithme RSA
- Cryptographie basée sur le logarithme discret : Cryptographie sur les courbes elliptiques
- Taille des clés, recommandations et justifications

Travaux pratiques :

- Mise en place de solutions de cryptographie AES et RSA: fonctionnement, chiffrement, déchiffrement et attaques.
- Prise en main de OpenSSL: chiffrement et déchiffrement

PARTIE 2 : HACHAGE ET SIGNATURE NUMERIQUE

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 fonction de hachage (focus sur l'attaque de collisions)
- Étude de quelques algorithmes MD5, SHA-1, SHA-256
- Applications : Stockage des mots de passe.

Scellements et signatures numériques :

- Scellement Vs Signature numérique
- Code d'Authentification de Message (HMAC, CBC-MAC, etc.)
- Signatures numériques : principe et fonctionnement
- Les algorithmes de signature numérique
- Applications : Intégrité et authentification dans les protocoles de communications
- Applications : Signature électronique des documents

Travaux pratiques :

- Calculs d'empreintes et de signatures avec OpenSSL
- Stockage des mots de passe : Mise en place de plusieurs solutions, comparaison et évaluation.

PARTIE 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

Travaux pratiques :

- Mise en place d'autorité de certification avec OpenSSL,
- création et signature de certificats, révocation, renouvellement, etc.

ÉQUIPE PÉDAGOGIQUE

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

MOYENS ET MÉTHODES PÉDAGOGIQUES

Cours - Travaux Pratiques - Exercices - Etude de cas et Echanges avec un expert du domaine Un support de cours sera remis à chacun des participants.

PROCHAINE SESSION

VILLEURBANNE : DU 23/06/2026 AU 25/06/2026

Frais pédagogiques individuels : 2 345 € H.T. (* Repas inclus)

L'ouverture de la session est conditionnée par un nombre minimum de participants. Nous consulter pour d'autres dates.

ÉVALUATION ET RÉSULTATS

Évaluation des acquis de la formation

Evaluation des acquis des apprenants par auto-examen. 90.5% des apprenants ont acquis la compétence principale visée. (sur 155 apprenants évalués sur cette thématique depuis 2020)

Évaluation de la satisfaction des participants en fin de formation (Niveau 1 KIRKPATRICK)

4.3 par les participants. (sur 192 participants ayant suivi une formation dans la thématique depuis 2020)

RENSEIGNEMENTS ET INSCRIPTION
Tel : +33 (0)4 72 43 83 93
Fax : +33 (0)4 72 44 34 24
mail : formation@insavalor.fr
Préinscription sur formation.insavalor.fr

Accueil des personnes en situation de handicap nécessitant un besoin spécifique d'accompagnement : nous contacter à l'inscription.

Actualisée le 14/10/2025