INFORMATIQUE, SÉCURITÉ DES SI - ARCHITECTURE SI ET INFRASTRUCTURES

Cryptographie : comprendre et utiliser les moyens cryptographiques pour sécuriser un SI

Cette formation peut être organisée en intra entreprise.
De nombreuses fonctionnalités de sécurité reposent sur la cryptographie. Ce module introduit la cryptographie, les principales techniques de chiffrement, la cryptanalyse, les architectures de confiance, la sécurité des données et les chaînes de blocs. Il aborde les fondamentaux de la cryptographie et présente les applications pour sécuriser un SI.

PUBLIC ET PRÉ-REQUIS

informaticiens (niveau intermédiaire en sécurité) équivalent bac+2.
Prérequis : avoir suivi la formation risque : comprendre et analyser les risques des systèmes informatiques ou avoir les compétences associées à la formation (CYBERISK).

PROGRAMME

Comprendre la cryptanalyse

- histoire de la cryptographie ; rappels mathématiques ;
- cryptographie, stéganographie, cryptanalyse, cryptographie quantique (BB84) ;
- pratiquer la cryptanalyse sur un exemple simple.

Maîtriser les techniques de chiffrement

- chiffrements asymétriques et symétriques ;
- principaux algorithmes (RC4, DES, AES, Diffie-Helmann, RSA, courbes éliptiques ;
- chiffrement des données sur place, chiffrement de partitions (crypt, encrypt, scrypt, luks, GPG, SMIME, luks) ;
- chiffrement de flux de données (ssh, SSL, négociation TLS, HTTPS).

Utiliser la signature électronique

- fonctions de hachage (md5sum, SHA) ;
- mise en œuvre de la signature numérique (openssl), *best practice.*

Comprendre et déployer des architectures à clé publique

- certificats (norme X509v3), standard PKCS ;
- mise en œuvre d'une PKI.

Comprendre la mise en place d'écosystèmes de confiance

- protection des données ;
- b*est practices*.

OBJECTIFS & COMPÉTENCES

- Comprendre la cryptographie ;
- Savoir chiffrer, déchiffrer des données et des flux de données ;
- Utiliser la signature électronique ;
- Connaître les *best practices* et les principaux algorithmes ;
- Comprendre les certificats ; déployer une PKI ;
- Construire un écosystème de confiance et protéger les données ;
- Comprendre les chaînes de blocs et leurs applications.

Informations clés

Durée :
28 heures

Tarif :
Sur mesure

694 € par jour en inter / nous consulter pour un tarif sur mesure en intra

Contact

fc@utc.fr

LES + DE LA FORMATION

Entraînement sur des situations réelles ; pédagogie tournée vers la pratique ; formation partagée avec des étudiants ingénieurs.
Un temps réservé aux questions propres aux spécificités des activités de l'entreprise.

MÉTHODES PÉDAGOGIQUES

Modalités pédagogiques
Cours, exercices ; études de cas ; ateliers-projets et études de cas pour un SI d'entreprise.
Modalités d'évaluation
Évaluation formative effectuée à l'occasion de tests de connaissances ; travaux de mise en application ; étude.

POUR CANDIDATER

Inscription via formulaire (voir site web).