FORMATION COURTE

INFORMATIQUE, SÉCURITÉ, SI

CRYPTOGRAPHIE : COMPRENDRE ET UTILISER LES MOYENS CRYPTOGRAPHIQUES POUR SÉCURISER UN SI

inter/intra entreprise

Dates : consulter le calendrier
Durée : 4 jours ; 28 heures
Lieu : Compiègne
Tarif : consulter le dépliant « Tarifs »
Prérequis : avoir suivi la formation Risque : comprendre et analyser les risques des systèmes informatiques, ou avoir les compétences associées à la formation (CYBERISK)
Référence produit : CYBERCRYPT

LES POINTS FORTS

▶ 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'organisation.

POUR ALLER PLUS LOIN

Formations : Protection : prévenir et assurer la protection des systèmes informatiques (CYBERPROT) ; Architectures résilientes : concevoir une infrastructure informatique résiliente (CYBERRES) ; Défense : défendre un système informatique (CYBERDEF)

EN SAVOIR +
www.utc.fr → Formation continue et VAE

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.

Objectifs

- 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.

Public

Informaticiens (niveau intermédiaire en sécurité) équivalent bac+2.

Modalités pédagogiques

Cours ; exercices ; ateliers-projets et études de cas pour un SI d'entreprise.

Modalités d'évaluation

Évaluation effectuée à l'occasion des tests de connaissances ; travaux de mise en application ; étude.

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 elliptiques) ;
- Chiffrement des données sur place, chiffrement de partitions (crypt, encrypt, scrypt,

luks, GPG, SMIME) ;
• 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 practices*.

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 ;
• *Best practices*.

Intervenants

Nos intervenants sont issus des secteurs économiques publics, privés, académiques et professionnels. Ils comptent généralement plus de 10 ans d'expérience professionnelle dans leur domaine d'expertise.